Test Results Summary for Catalyst 9800 Series Wireless Controller and EWC 17.1 for Japan (Release Version 17.1.20200103)

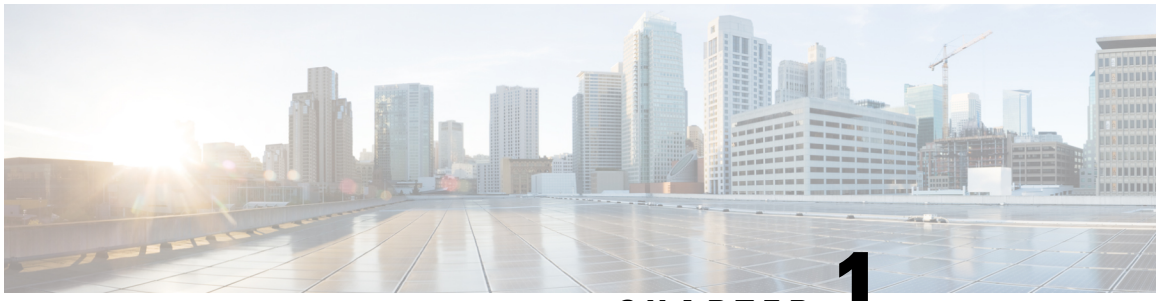
First Published: 2020-01-23

Last Modified: 2020-03-11

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

© Cisco Systems, Inc. All rights reserved.

CONTENTS



CHAPTER 1

Overview

Catalyst 9800 and EWC test

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

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

- New features in Catalyst 9800 and EWC 17.1
- High priority scenarios and basic regression features
- Inputs from Cisco SEs/ TAC

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

The following products are covered in the test execution:

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

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

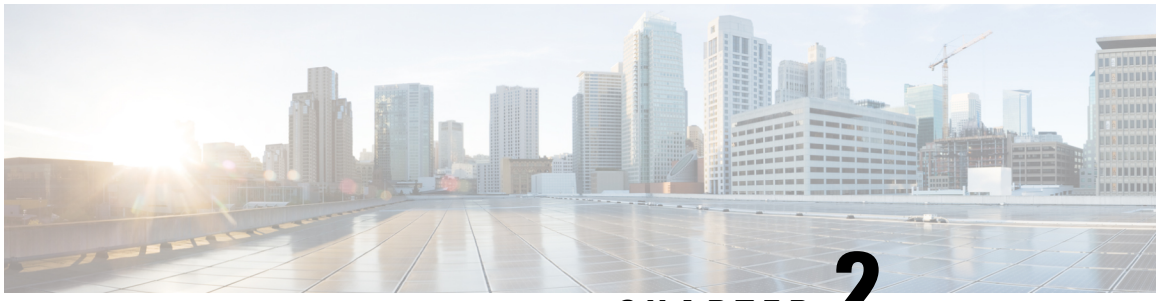
Acronyms

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

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

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

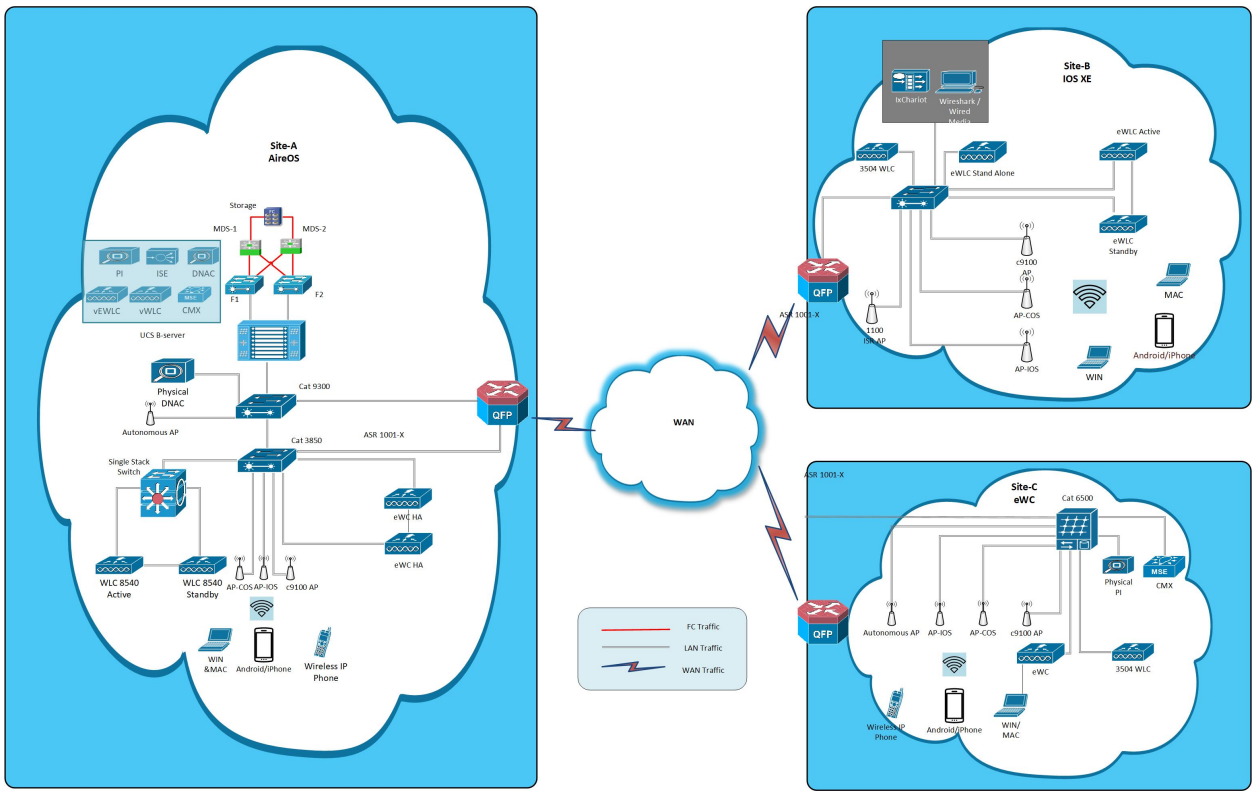
Acronym	Description
WPA	Wi-Fi Protected Access
WSM	Wireless Security Module



CHAPTER 2

Test Topology and Environment Matrix

Test Topology



Component Matrix

Category	Component	Version
Controller	Cisco Catalyst 9800 Series Wireless Controller	17.1
	Cisco Catalyst 9800-CL	17.1
	Cisco Catalyst 9800-L Wireless Controller	17.1
	Cisco Embedded Wireless Controller on Catalyst Access Points	17.1
	Wireless LAN Controller 8540	8.10.105.0
	Wireless LAN controller 5520	8.10.105.0
	Wireless LAN controller 3504	8.10.105.0
	Virtual Controller	8.10.105.0
	CME 1562/1850/1830	8.10.105.0
	CME 4800/3800/2800	8.10.105.0
Applications	Prime Infrastructure (Virtual Appliance, UCS based)	3.8.0.0.284
	ISE(VM)	2.7
	CMX(Physical (3375), VM)	10.6
	DNAC	1.3.1
	MSE(Physical (3365), VM)	8.0.150.0
	APIC-EM Controller appliance	1.6
	Cisco Jabber for Windows, iPhone	12.6.0
	Cisco Air Provisioning App	1.4
	Cisco Wireless App	1.0.228

Category	Component	Version
Access Point	Cisco AP 9115	17.1
	Cisco AP 9120	17.1
	Cisco AP 9130	17.1
	Cisco 1100 ISR	17.1
	Cisco AP 4800	15.3
	Cisco AP 3800	15.3
	Cisco AP 2800	15.3
	Cisco AP 3700	15.3
	Cisco AP 2700	15.3
	Cisco AP 1700	15.3
	Cisco AP 1850	15.3
	Cisco AP 1830	15.3
	Cisco AP 1815	15.3
	Cisco AP 1810	15.3
	Cisco AP 1570	15.3
	Cisco AP 1562	15.3
	Cisco AP 1542	15.3
	Cisco AP 1532	15.3
	Cisco AP 702I	15.3
Switch	Cisco Cat 9300	17.1
	Cisco Cat 9200L	17.1
	Cisco Cat 9800	17.1
	Cisco 3750V2 switch	15.0(2)SE2
	Cisco Cat 6509-E	15.1(1)SY1
Chipset	5300, 6300 AGN	15.40.41.5058
	7265 AC	20.120.0
	Airport Extreme	7.7.9

Category	Component	Version
Client	Operating System(JOS)	Windows 8 & 8.1 Enterprise
		Windows XP Professional
		Windows 10
	Apple Mac Book Pro, Apple Mac Book Air (JP Locale)	Mac OS 10.15
	iPad Pro	iOS 13.3.1
	iPhone 6, 6S ,7 & 11 (JP Locale)	iOS 13.3.1
	Samsung Galaxy S7,S10, Nexus 6P, Sony Xperia XZ	Android 10.0
	Wireless IP Phone 8821	11.0.4-14
	End points	Windows 7 Enterprise
		Apple Mac 10.15
		Windows 8 & 8.1
		iPhone 6,6S ,7 & 11
		Windows 10
		Samsung Galaxy S4, S7,S10, Nexus 6P, Sony Xperia
	Cisco AnyConnect VPN Client	4.8.175
Module	Hyper location Module	NA
Active Directory	AD	Windows 2008R2 Enterprise
Call Control	Cisco Unified Communications Manager	12.5.0.99832-3/12.5.0.99832-3-1(JP)
Browsers	IE	11.0.11
	Mozilla Firefox	72
	Safari	13
	Chrome	79

What's New ?

EWC

- EWC HA
- PSK + Multi-auth Support
- EoGRE Support for ME
- iPSK Peer-2-Peer Blocking
- BSS Coloring on AX APs

- Scheduled Config Download
- Cisco Catalyst 9800 Series Wireless Controller WebUI enhancements - Phase 2
- DNAC Support for EWC
- CMX Parity for Cisco Catalyst 9800 Series Wireless Controller ME
- Browser Rendering Coverage
- EWC Crashes(DHCP/Troubleshootings)
- EWC Day0 Elimination

Cisco Catalyst 9800 Series Wireless Controller

- ISSU
- DNA Assurance
- Cisco Catalyst 9800 Series Wireless Controller Crashes(DHCP/Troubleshootings)
- PSK + Multi-auth Support
- mDNS Support for Wired Guest Ac
- NAT Support for Mobility Tunnel
- iPSK P2P blocking
- Open DNS
- RSSI and SNR in ASSOC request
- WGB
- Intelligent Capture
- DNAc support for Cisco Catalyst 9800 Series Wireless Controller
- Support of Trap notification via SNMP3
- mDNS AP support
- Mesh and Flex+Bridge Support on all Indoor Wave 2 AP's
- Inter Release Controller Mobility
- Browser Rendering Coverage

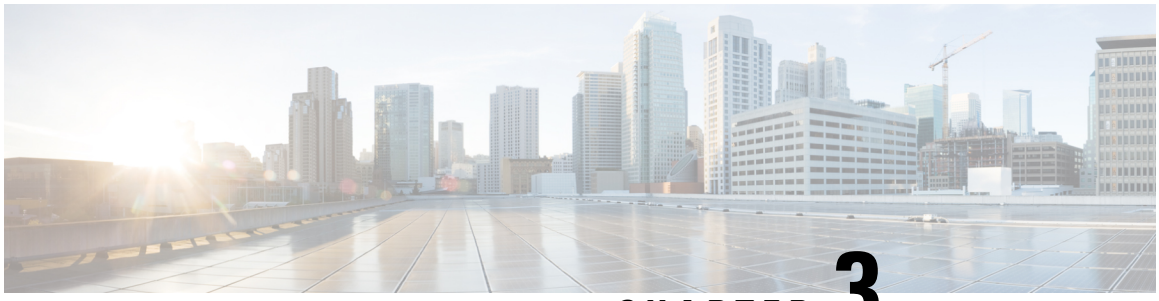
Open Caveats

Defect ID	Tittle
CSCvs41888	Configuration backup & restore is not working via SFTP GUI Transfer mode
CSCvs43516	Observed memory leakage in C9800-L-C-K9
CSCvs50296	mDNS service policy not able to configure in LocalPolicy->ServiceTemplate in Cisco Catalyst 9800 Series Wireless Controller
CSCvs53410	Client TDL auth_key_mgmt unmarshal fails causing not loading for open security client
CSCvs23453	Not able to configure MFP configuration through helping guide navigation in Cisco Catalyst 9800 Series Wireless Controller UI
CSCvs78121	NMSP_SSL_ERROR_DISCONNECT message is flooded in Cisco Catalyst 9800 Series Wireless Controller

CSCvs61119	Required Password encryption for config files in Cisco Catalyst 9800 Series Wireless Controller
CSCvs43415	Observed 9115 Ap crash

Resolved Caveats

Defect ID	Tittle
CSCvs21281	AP 1810 Crash due to OOM, apsw_watchdog: apsw_watchdog about to reboot with reason: oom
CSCvr33062	Samsung s10 client not able to connect to the WPA2+WPA3-SAE+PSK+FT PSK+PSK-SHA2 Mixed mode.
CSCvs53376	File Manager Options Not Working in Japanese UI.
CSCvs21105	Update & Apply to device button is not working after configure Ft-PSK with WPA2+WPA3 in GUI.
CSCvs29345	Observed error like "Error in Configuring WLAN" while modifying WLAN Configuration
CSCvs32392	User can able to create a WLAN with WPA3-PSK security without WPA2.
CSCvs59816	Pre-shared key option is not showing in GUI for PSK-SHA256.



CHAPTER 3

New Features

EWC HA

Logical ID	Title	Description	Status	Defect ID

EWCJ171S_HA_1	Converting Catalyst AP as EWC	To Convert the Catalyst AP as EWC and check if the AP comes Up as Primary EWC or not	Passed	
EWCJ171S_HA_2	Configuring EWC HA(Primary/Standby) Setup with two Catalyst APs	To configuring EWC HA(Primary/Standby) Setup with two Catalyst Aps and check if the primary and standby are in sync	Passed	
EWCJ171S_HA_3	Check Auto config of standby happens and verifying same in UI	To check if the auto-config for selection of standby EWC happens and verifying if the standby shown in UI or not	Passed	
EWCJ171S_HA_4	Verifying primary EWC failover to check behaviour of standby EWC	To check if the standby EWC comes as primary EWC after the Primary failover .	Passed	
EWCJ171S_HA_5	After Dual failover of primary and standby making preferred master as Primary EWC	To make the preferred master as primary after dual failover of primary and standby controller	Passed	
EWCJ171S_HA_6	Check the chassis number during and after failover	To check the chassis number during HA setup and after Primary failover	Failed	CSCvs48833
EWCJ171S_HA_7	Check the status of the EWC primary and standby in Cisco DNAC	To check the status of the EWC primary and standby in Cisco DNAC	Passed	
EWCJ171S_HA_8	Upgrading the image of the EWC after the primary switchover	To upgrade the image of the EWC after the primary failover and check if the upgrade of EWC is successful or not	Passed	

EWCJ171S_HA_9	Upgrading the image when the EWC is kept in HA setup and check image versions on both primary and standby	To upgrading the image when the EWC is kept in HA setup and check image versions on both primary and standby	Passed	
EWCJ171S_HA_10	Configuration backup and restore when the EWC is in HA setup	To make configuration backup when the EWC is in HA setup	Passed	
EWCJ171S_HA_11	Configuration backup and restore after primary failover with standby EWC	To make configuration backup after primary failover with standby EWC	Passed	
EWCJ171S_HA_12	Connecting a client to EWC when the EWC is in HA setup with primary and standby	To connect a client to EWC when the EWC is in HA setup with primary and standby	Passed	
EWCJ171S_HA_13	Connecting a client to EWC and making Primary failover and check if there is traffic loss during failover	To connect a client to EWC and making Primary failover and check if there is traffic loss during failover	Passed	
EWCJ171S_HA_14	Connecting a client to EWC when the EWC is in HA setup with primary and standby	To connect a client to EWC when the EWC is in HA setup with primary and standby	Passed	

iPSK Peer-2-Peer Blocking

Logical ID	Title	Description	Status	Defect ID
EWCJ171S_EWC_iPSK P2P blocking_1	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	

EWCJ171S_EWC_iPSK P2P blocking_2	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	
EWCJ171S_EWC_iPSK P2P blocking_3	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	
EWCJ171S_EWC_iPSK P2P blocking_4	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	
EWCJ171S_EWC_iPSK P2P blocking_5	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	
EWCJ171S_EWC_iPSK P2P blocking_6	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	
EWCJ171S_EWC_iPSK P2P blocking_7	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	
EWCJ171S_EWC_iPSK P2P blocking_8	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	

EWCJ171S_EWC_iPSK P2P blocking_9	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	
EWCJ171S_EWC_iPSK P2P blocking_10	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	
EWCJ171S_EWC_iPSK P2P blocking_11	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	
EWCJ171S_EWC_iPSK P2P blocking_12	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	
EWCJ171S_EWC_iPSK P2P blocking_13	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	
EWCJ171S_EWC_iPSK P2P blocking_14	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	

EWCJ171S_EWC_iPSK P2P blocking_15	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	
EWCJ171S_EWC_iPSK P2P blocking_16	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	
EWCJ171S_EWC_iPSK P2P blocking_17	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	
EWCJ171S_EWC_iPSK P2P blocking_18	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	
EWCJ171S_EWC_iPSK P2P blocking_19	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	
EWCJ171S_EWC_iPSK P2P blocking_20	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	Failed	CSCvs77751

EWCJ171S_EWC_iPSK P2P blocking_21	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	
EWCJ171S_EWC_iPSK P2P blocking_22	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	
EWCJ171S_EWC_iPSK P2P blocking_23	Verifying clients connectivity with iPSK tag while radius fall-back is enabled	To verify whether clients iPSK is being generated from secondary AAA server or not	Passed	
EWCJ171S_EWC_iPSK P2P blocking_24	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	
EWCJ171S_EWC_iPSK P2P blocking_25	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	
EWCJ171S_EWC_iPSK P2P blocking_26	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	
EWCJ171S_EWC_iPSK P2P blocking_27	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	

EWCJ171S_EWC_iPSK P2P blocking_28	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	
EWCJ171S_EWC_iPSK P2P blocking_29	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	
EWCJ171S_EWC_iPSK P2P blocking_30	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	
EWCJ171S_EWC_iPSK P2P blocking_31	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	
EWCJ171S_EWC_iPSK P2P blocking_32	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	
EWCJ171S_EWC_iPSK P2P blocking_33	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	

EWCJ171S_EWC_iPSK P2P blocking_34	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	
EWCJ171S_EWC_iPSK P2P blocking_35	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	
EWCJ171S_EWC_iPSK P2P blocking_36	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	
EWCJ171S_EWC_iPSK P2P blocking_37	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	
EWCJ171S_EWC_iPSK P2P blocking_38	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	
EWCJ171S_EWC_iPSK P2P blocking_39	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	

EWCJ171S_EWC_iPSK P2P blocking_40	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	
EWCJ171S_EWC_iPSK P2P blocking_41	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	
EWCJ171S_EWC_iPSK P2P blocking_42	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	
EWCJ171S_EWC_iPSK P2P blocking_43	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	
EWCJ171S_EWC_iPSK P2P blocking_44	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	

EWCJ171S_EWC_iPSK P2P blocking_45	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	
EWCJ171S_EWC_iPSK P2P blocking_46	Verifying clients roaming with same iPSK tag	To verify whether the client is roaming from one Ap to another Ap.	Passed	
EWCJ171S_EWC_iPSK P2P blocking_47	Verifying clients roaming with different iPSK tag	To verify whether the client is roaming from one Ap to another Ap.	Passed	
EWLCJ171S_iPSK_P2P_01	Verifying the iPSK tag generation for the Connected Window JOS Client in Cisco Catalyst 9800 Series Wireless Controller UI/CLI	To verify whether iPSK tag generated or not When Window JOS connected to iPSK enabled WLAN Profile	Passed	
EWLCJ171S_iPSK_P2P_02	Verifying the iPSK tag generation for the Connected MAC OS Client in Cisco Catalyst 9800 Series Wireless Controller UI/CLI	To verify whether iPSK tag generated or not When MAC OS connected to iPSK enabled WLAN Profile	Passed	
EWLCJ171S_iPSK_P2P_03	Verifying the iPSK tag generation for the Connected iOS Client in Cisco Catalyst 9800 Series Wireless Controller UI/CLI	To verify whether iPSK tag generated or not When iOS connected to iPSK enabled WLAN Profile	Passed	

EWLCJ171S_iPSK_P2P_04	Verifying the iPSK tag generation for the Connected Android Client in Cisco Catalyst 9800 Series Wireless Controller UI/CLI	To verify whether iPSK tag generated or not When Android connected to iPSK enabled WLAN Profile	Passed	
EWLCJ171S_iPSK_P2P_05	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	
EWLCJ171S_iPSK_P2P_06	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	
EWLCJ171S_iPSK_P2P_07	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	
EWLCJ171S_iPSK_P2P_08	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	
EWLCJ171S_iPSK_P2P_09	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	
EWLCJ171S_iPSK_P2P_10	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	

EWLCJ171S_iPSK_P2P_11	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	
EWLCJ171S_iPSK_P2P_12	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	
EWLCJ171S_iPSK_P2P_13	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	
EWLCJ171S_iPSK_P2P_14	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	
EWLCJ171S_iPSK_P2P_15	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	
EWLCJ171S_iPSK_P2P_16	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	

EWLCJ171S_iPSK_P2P_17	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	
EWLCJ171S_iPSK_P2P_18	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	
EWLCJ171S_iPSK_P2P_19	Verifying connected clients with the particular iPSK tag in CLI	To verify whether all the clients sharing iPSK tag are shown or not in Cisco Catalyst 9800 Series Wireless Controller CLI	Passed	
EWLCJ171S_iPSK_P2P_20	Verifying the wlan configuration with iPSK tag Configuration through Cisco Catalyst 9800 Series Wireless Controller Web	To verify whether wlan profile can be created or not with the iPSK configuration through the Cisco Catalyst 9800 Series Wireless Controller Web	Passed	
EWLCJ171S_iPSK_P2P_21	Verifying the wlan generation with iPSK tag Configuration through Cisco Catalyst 9800 Series Wireless Controller CLI	To verify whether wlan profile can be created or not with the iPSK configuration through the Cisco Catalyst 9800 Series Wireless Controller CLI	Passed	
EWLCJ171S_iPSK_P2P_22	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	

EWLCJ171S_iPSK_P2P_23	Verifying clients connectivity with iPSK tag while radius fall back is enabled	To verify whether clients iPSK is being generated from secondary AAA server or not	Passed	
EWLCJ171S_iPSK_P2P_24	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	
EWLCJ171S_iPSK_P2P_25	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	
EWLCJ171S_iPSK_P2P_26	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	
EWLCJ171S_iPSK_P2P_27	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	
EWLCJ171S_iPSK_P2P_28	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	
EWLCJ171S_iPSK_P2P_29	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	

EWLCJ171S_iPSK_P2P_30	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	
EWLCJ171S_iPSK_P2P_31	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	
EWLCJ171S_iPSK_P2P_32	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	
EWLCJ171S_iPSK_P2P_33	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	
EWLCJ171S_iPSK_P2P_34	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	
EWLCJ171S_iPSK_P2P_35	Verifying the iPSK tag generation for the Connected anyconnect Client in Cisco Catalyst 9800 Series Wireless Controller UI/CLI	To verify whether iPSK tag generated or not When Anyconnect client connected to iPSK enabled WLAN Profile	Passed	

EWLCJ171S_iPSK_P2P_36	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	
EWLCJ171S_iPSK_P2P_37	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	
EWLCJ171S_iPSK_P2P_38	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	
EWLCJ171S_iPSK_P2P_39	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	
EWLCJ171S_iPSK_P2P_40	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	
EWLCJ171S_iPSK_P2P_41	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	

EWLCJ171S_iPSK_P2P_42	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	
EWLCJ171S_iPSK_P2P_43	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	
EWLCJ171S_iPSK_P2P_44	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	
EWLCJ171S_iPSK_P2P_45	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	
EWLCJ171S_iPSK_P2P_46	Verifying clients roaming with same iPSK tag	To verify whether the client is roaming from one Ap to another Ap.	Passed	
EWLCJ171S_iPSK_P2P_47	Verifying clients roaming with different iPSK tag	To verify whether the client is roaming from one Ap to another Ap.	Passed	

EoGRE Support for ME

Logical ID	Title	Description	Status	Defect ID
EWCJ171S_EWC_EoGRE_1	Creating EoGRE Tunnel Gateway.	To check whether the tunnel gateway is created or not.	Passed	
EWCJ171S_EWC_EoGRE_2	Creating EoGRE Tunnel Domain	To check whether the tunnel Domain is created or not.	Passed	
EWCJ171S_EWC_EoGRE_3	Configuring the Global Parameter for the EoGRE.	To check whether the global parameters are configured or not.	Passed	
EWCJ171S_EWC_EoGRE_4	Configuring the tunnel Profile.	To check whether the tunnel profile is created or not.	Passed	
EWCJ171S_EWC_EoGRE_5	Associate the WLAN to the Wireless policy profile.	To check whether the wlan is associated with the policy profile.	Passed	
EWCJ171S_EWC_EoGRE_6	Adding a policy tag and site tag to AP	To check whether the policy and site tag is added to an AP.	Passed	
EWCJ171S_EWC_EoGRE_7	Checking the client connectivity.	To check whether the client is connected or not	Passed	
EWCJ171S_EWC_EoGRE_8	Getting the EoGRE tunnel from PI	To check whether the tunnel is exported from PI or not	Passed	
EWCJ171S_EWC_EoGRE_9	Connect the iOS clients and check the connectivity.	To check whether the iOS clients get connected successfully.	Passed	
EWCJ171S_EWC_EoGRE_10	Connect the mac os clients and check the connectivity.	To check whether the mac os clients get connected successfully.	Passed	
EWCJ171S_EWC_EoGRE_11	Checking the traffic in the tunnel.	To check whether the traffic in the tunnel is managed or not.	Passed	

BSS Coloring on AX APs

Logical ID	Title	Description	Status	Defect ID
EWCJ171S_EWC_BSS_01	Configuring Automatic BSS colouring for 2.4 ghz AP radios	To Check whether automatic BSS colouring is applied or not in 2.4 ghz Ap radio	Passed	
EWCJ171S_EWC_BSS_02	Configuring automatic BSS colour for 5ghz radio	To Check whether automatic BSS colouring is applied or not in 5 ghz Ap radio	Passed	
EWCJ171S_EWC_BSS_03	Configuring auto BSS colour appearing 2.4 to 5 Ghz radio or vice versa	To verify whether different BSS colouring is occur while Changing the AP radios 2.4 to 5 viseversa	Failed	CSCvs62656
EWCJ171S_EWC_BSS_04	Configuring Manual BSS colour configuration for 2.4/5 ghz radio	To Check whether Manual BSS colouring is applied or not in 2.4 ghz Ap radio	Passed	
EWCJ171S_EWC_BSS_05	Verifying the static BSS colour assignment for the 5 ghz radio in Flex-connect mode	To Check whether Static BSS colouring is applied or not in 5 ghz Ap radio	Passed	
EWCJ171S_EWC_BSS_06	Checking the manual BSS colouring while changing the AP radio from 2.4 ghz to 5 ghz	To verify whether different BSS colouring is occur while Changing the AP radios	Failed	CSCvs64155
EWCJ171S_EWC_BSS_07	Checking the BSS colour details are retained after AP and Controller reload	To Check whether the BSS colour retained after AP & Controller reload	Passed	
EWCJ171S_EWC_BSS_08	Verifying BSS colouring with Intra client roaming by using 9115AP	To verify whether BSS colouring with client roaming between AP's or not	Passed	

EWCJ171S_EWC_BSS_09	Verifying BSS colouring with inter roaming client using different radio	To check whether BSS colouring is appearing or not , when different radio clients are roaming between controllers	Passed	
EWCJ171S_EWC_BSS_10	Verifying BSS colouring with inter roaming client using same radio	To check whether BSS colouring is appearing or not , when same radio clients are roaming between controllers	Passed	
EWCJ171S_EWC_BSS_11	Capturing the Windows client connectivity & BSS colouring using Wireshark	To check the window client connectivity & BSS colouring using Wireshark	Passed	
EWCJ171S_EWC_BSS_12	Capturing the Android client connectivity & BSS colouring using Wireshark	To check the Android client connectivity & BSS colouring using Wireshark	Passed	
EWCJ171S_EWC_BSS_13	Capturing the Mac OS client connectivity & BSS colouring using Wireshark	To check the Mac OS client connectivity & BSS colouring using Wireshark	Passed	
EWCJ171S_EWC_BSS_14	Changing 9115 AP mode from local to Flex connect & check the BSS colouring Configuration	To change the mode of AP from local mode to Flexconnect mode and check the BSS colouring configuration in 9115 Ap	Passed	
EWCJ171S_EWC_BSS_15	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	

Scheduled Config Download

Logical ID	Title	Description	Status	Defect ID
EWCJ171S_EWC_Scheduled download_1	New Config should be applied when changes in old config through schedule download configuration using FTP server	To verify New Config should be applied when changes in old config through schedule download configuration using FTP server	Passed	
EWCJ171S_EWC_Scheduled download_2	New Config should be applied when changes in old config through schedule download configuration using SFTP server	To verify New Config should be applied when changes in old config through schedule download configuration using SFTP server	Passed	
EWCJ171S_EWC_Scheduled download_3	New Config should not applied when old config having no changes through schedule download configuration using FTP server	To verify New Config should not applied when old config having no changes through schedule download configuration using FTP server	Passed	
EWCJ171S_EWC_Scheduled download_4	New Config should not applied when old config having no changes through schedule download configuration using SFTP server	To verify New Config should not applied when old config having no changes through schedule download configuration using SFTP server	Passed	
EWCJ171S_EWC_Scheduled download_5	New config should not apply to the Device using FTP transfer mode when having bad config in server	To verify the new config should not apply to the Device using FTP transfer mode when having bad config in server	Passed	

EWCJ171S_EWC_Scheduled download_6	New config should not apply to the Device using SFTP transfer mode when having bad config in server	To verify the new config should not apply to the Device using SFTP transfer mode when having bad config in server	Passed	
EWCJ171S_EWC_Scheduled download_7	Getting error message when passing wrong CLI commands (Wrong format of server IP address) in schedule download configuration using FTP/SFTP server	To verify Getting error message when passing wrong CLI commands (Wrong format of server IP address) in schedule download configuration using FTP/SFTP server	Passed	
EWCJ171S_EWC_Scheduled download_8	Getting error message when passing wrong CLI commands (Wrong file path/ file name) in schedule download configuration using FTP/SFTP server	To verify Getting error message when passing wrong CLI commands (Wrong file path/file name) in schedule download configuration using FTP/SFTP server	Passed	
EWCJ171S_EWC_Scheduled download_9	New Config should be applied when changes in old config through schedule download configuration using FTP/SFTP server when passing domain name instead of server address in CLI command	To verify New Config should be applied when changes in old config through schedule download configuration using FTP/SFTP server when passing domain name instead of server address in CLI command	Passed	
EWCJ171S_EWC_Scheduled download_10	New Config should not apply when preferred Master AP is up after downloading config	To verify New Config should not apply when preferred Master AP is up after downloading config	Passed	

EWCJ171S_EWC_Scheduled download_11	New config should not apply when passing file name which is not available in the server	To verify New config should not apply when passing file name which is not available in the server	Passed	
EWCJ171S_EWC_Scheduled download_12	verify server reachable error message when FTP/SFTP sever is down	To verify server reachable error message when FTP/SFTP sever is down	Passed	
EWCJ171S_EWC_Scheduled download_13	Verify the behaviour of schedule config download when system time is changed after setting hourly schedule download	To Verify the behaviour of schedule config download when system time is changed after setting hourly schedule download	Passed	
EWCJ171S_EWC_Scheduled download_14	Verify EWC should be come up (after reset) after downloading new config	To Verify EWC should be come up (after reset) after downloading new config	Passed	
EWCJ171S_EWC_Scheduled download_15	Verify Ap join and client connectivity after new config downloaded	To verify Ap join and client connectivity after new config downloaded	Passed	
EWCJ171S_EWC_Scheduled download_16	Verify apply new config when Primary controller goes down and secondary controller is active (when both EWC on same model) after downloading config	To verify apply new config when Primary controller goes down and secondary controller is active (when both EWC on same model) after downloading config	Passed	

EWCJ171S_EWC_Scheduled download_17	Verify not apply new config when Primary controller goes down and secondary controller is active (when both EWC on different model) after downloading config	To verify not apply new config when Primary controller goes down and secondary controller is active (when both EWC on different model) after downloading config	Passed	
EWLCJ171S_Reg_88	Configure the Calendar Profile in open security WLAN with Start/End time.	To check whether WLAN is broadcasting or not on configured Start/End time	Passed	
EWLCJ171S_Reg_89	Configure the Calendar Profile in WPA2 security WLAN with Start/End time.	To check whether WLAN is broadcasting or not on configured Start/End time	Passed	
EWLCJ171S_Reg_90	Configure the Calendar Profile in WPA3 security WLAN with Start/End time.	To check whether WLAN is broadcasting or not on configured Start/End time	Passed	
EWLCJ171S_Reg_91	Configure the Calendar Profile in Static WEP security WLAN with Start/End time.	To check whether WLAN is broadcasting or not on configured Start/End time	Passed	
EWLCJ171S_Reg_92	Configure the Calendar Profile in Static WEP security WLAN with Start/End time with Monthly/Weekly/Daily option.	To check whether WLAN is broadcasting or not on configured Start/End time	Passed	
EWLCJ171S_Reg_93	Configure the Calendar Profile in Static WEP security WLAN with L3 Security,MAC Filtering and with Start/End time .	To check whether WLAN is broadcasting or not on configured Start/End time	Passed	

EWLCJ171S_Reg_94	Observe the Client Disassociation on Calendar Profile after end time	To check whether client is disassociating after end time.	Passed	

Cisco Catalyst 9800 Series Wireless Controller WebUI enhancements - Phase 2

Logical ID	Title	Description	Status	Defect ID
EWCJ171S_EWC_UI_Enhancement_1	Add the Ap Profile by Enabling the aWIPS in UI	To check whether the profile can be added by enable the aWIPS in Ap Join or not in eWC with Japanese UI	Passed	
EWCJ171S_EWC_UI_Enhancement_2	Edit the Default Profile and check weather we can able to enable the aWIPS	Edit the Default Profile and check weather we can able to enable the aWIPS or not in Cisco Catalyst 9800 Series Wireless Controller Japanese UI	Passed	
EWCJ171S_EWC_UI_Enhancement_3	To check weather the aWIPS alarms are displaying in Monitoring->aWIPS UI page	To check weather any aWIPS alarms are displaying or not under monitoring ->aWIPS page in Cisco Catalyst 9800 Series Wireless Controller Japanese UI	Passed	

EWCJ171S_EWC_UI_Enhancement_4	Create Guest LAN profile Cisco Catalyst 9800 Series Wireless Controller UI	To check weather the Guest LAN profile can be created or not in Cisco Catalyst 9800 Series Wireless Controller Japanese UI	Passed	
EWCJ171S_EWC_UI_Enhancement_5	Enable redundancy configuration to device	To Check weather Redundancy tab configuration can be applied by enabling the status in Cisco Catalyst 9800 Series Wireless Controller Japanese UI	Passed	
EWCJ171S_EWC_UI_Enhancement_6	Disable Redundancy Tab configuration to device	To Check weather Redundancy configuration can be Disabled by disabling the status in Cisco Catalyst 9800 Series Wireless Controller Japanese UI	Passed	
EWCJ171S_EWC_UI_Enhancement_7	Configure Enhanced URL filters to from existing URL filter page	Configure enhanced URL filters from existing URL filters page in Cisco Catalyst 9800 Series Wireless Controller Japanese UI	Passed	

EWCJ171S_EWC_UI_Enhancement_8	EoGRE support from UI	To check weather EoGRE domains and tunnels can be configured through Cisco Catalyst 9800 Series Wireless Controller in Japanese UI	Passed	
EWCJ171S_EWC_UI_Enhancement_9	WLAN Dashlets In Table view in UI	To check weather WLAN Dashlets table view changes are working or not in Cisco Catalyst 9800 Series Wireless Controller Japanese UI	Passed	
EWCJ171S_EWC_UI_Enhancement_10	WLAN Dashlets Graphical View in UI	To check weather the WLAN Dashlets Graphical view changes are working or not in Cisco Catalyst 9800 Series Wireless Controller Japanese UI	Passed	
EWCJ171S_EWC_UI_Enhancement_11	AP Dashlets in Table view in UI	To check weather the AP Dashlets Table view changes are working or not in Cisco Catalyst 9800 Series Wireless Controller Japanese UI	Passed	

EWCJ171S_EWC_UI_Enhancement_12	AP Dashlets in Chart view in UI	To check weather the AP Dashlets chart view changes are working or not in Cisco Catalyst 9800 Series Wireless ControllerJapanese UI	Passed	
EWCJ171S_EWC_UI_Enhancement_13	mDNS support in Service template page in UI	To check weather mDNS can be configure in Service template page in Cisco Catalyst 9800 Series Wireless Controller in Japanese UI	Passed	
EWCJ171S_EWC_UI_Enhancement_14	mDNS support in Guest LAN page	To check weather mDNS can be configure in Guest Lan page in Cisco Catalyst 9800 Series Wireless Controller in Japanese UI	Passed	
EWCJ171S_EWC_UI_Enhancement_15	mDNS support in RLAN page	To check weather mDNS can be configure in RLAN page in Cisco Catalyst 9800 Series Wireless Controller in Japanese UI	Passed	
EWCJ171S_EWC_UI_Enhancement_16	mDNS Service Policy Configuration on VLAN interface	To check weather mDNS can be configure in VLAN page in Cisco Catalyst 9800 Series Wireless Controller in Japanese UI	Failed	CSCvs50296

EWCJ171S_EWC_UI_Enhancement_17	mDNS Configuration in AP page	To check weather mDNS can be configure in AP page in Cisco Catalyst 9800 Series Wireless Controller in Japanese UI	Passed	
EWCJ171S_EWC_UI_Enhancement_18	Duplo AP Support	To check weather LAN Port Setting are displaying or not in AP Interface tab in Cisco Catalyst 9800 Series Wireless Controller Japanese UI	Passed	
EWCJ171S_EWC_UI_Enhancement_19	Cisco Catalyst 9800 Series Wireless Controller Flex & ME should natively support Umbrella integration	To check weather Umbrella integration support is applying in device or not in in Cisco Catalyst 9800 Series Wireless Controller Japanese UI	Passed	
EWCJ171S_EWC_UI_Enhancement_20	iPSK Peer-2-Peer Blocking	To check weather iPSK Peer-2-Peer Blocking configuration is applied in profile policy in Cisco Catalyst 9800 Series Wireless Controller in Japanese UI	Passed	

DNAC Support for EWC

Logical ID	Title	Description	Status	Defect ID

EWCJ171S_EWC_DNAc support_1	Verifying device details in inventory after added/discovered in cisco DNA	To verify whether the device details are showing in inventory after added in cisco DNA	Passed	
EWCJ171S_EWC_DNAc support_2	Monitoring the devices after adding in cisco DNA and verifying same in eWC	Verifying whether added devices properly assured or monitoring in cisco DNA	Passed	
EWCJ171S_EWC_DNAc support_3	Discovering multiple devices in cisco DNA and check for the same count in monitored devices	Checking whether count of wireless devices are added in Cisco DNA and they are monitored properly or not	Passed	
EWCJ171S_EWC_DNAc support_4	Checking AP devices in inventory after Wireless controller discovered in cisco DNA	To verify whether all AP's details showing in inventory after device discovered	Passed	
EWCJ171S_EWC_DNAc support_5	Checking the AP's count in network health after successfully added in inventory	To verify AP's count in Assurance dashboard after added in inventory	Passed	
EWCJ171S_EWC_DNAc support_6	Resync the cisco DNA and checking for the newly added AP's count in device	To verify newly added AP's count in cisco DNA after resync	Passed	
EWCJ171S_EWC_DNAc support_7	Exporting the inventory details from cisco DNA	To verify whether user able to export the device inventory details or not	Passed	
EWCJ171S_EWC_DNAc support_8	Importing the inventory details to device from computer in cisco DNA	To verify whether user able to import the device inventory details or not	Passed	

EWCJ171S_EWC_DNAcsupport_9	Running the commands in cisco DNA using command runner	To check the output for device commands after run in command runner in cisco DNA	Passed	
EWCJ171S_EWC_DNAcsupport_10	Deleting the device from inventory in cisco DNA	To check whether user able to delete the device from inventory or not	Passed	
EWCJ171S_EWC_DNAcsupport_11	Checking the device reachability status in inventory after make the device down	To check whether reachability status change to "unreachable" or not when device is down	Passed	
EWCJ171S_EWC_DNAcsupport_12	Adding site and provisioning device	To check whether user able to create site and provision device	Passed	
EWCJ171S_EWC_DNAcsupport_13	Positioning AP's on site with different radios	To check AP's positioning after positioned with different radios	Passed	
EWCJ171S_EWC_DNAcsupport_14	Checking for internal AP details after device added discover	To verify whether ME WC device showing as AP or not in inventory	Passed	
EWCJ171S_EWC_DNAcsupport_15	Connecting the clients to AP's and checking the client count in Dashboard	To verify the client details in client Health after connected to AP	Passed	
EWCJ171S_EWC_DNAcsupport_16	Provisioning the ME _WC in day0 via PnP profile and bring device day1	Verify that user is able to Provisioned the ME WC in day0 via PnP profile or not	Passed	

CMX Parity for Cisco Catalyst 9800 Series Wireless Controller ME

Logical ID	Title	Description	Status	Defect ID

EWCJ171S_EWC_CMX_01	Adding eWC-ME to CMX & CMX to DNAC	To Check Whether the Cisco Catalyst 9800 Series Wireless Controller -ME gets added to CMX & CMX added to DNAC successfully or not	Passed	
EWCJ171S_EWC_CMX_02	Connecting the IOS Client to the access point on the floor and check the details of the Client.	To connect a IOS Client to the access point on the floor and check if the details of the IOS Clients are shown correctly or not.	Passed	
EWCJ171S_EWC_CMX_03	Connecting the MacOS Client to the access point on the floor and check the details of the Client.	To connect a MacOS Client to the access point on the floor and check if the details of the MacOS Clients are shown correctly or not.	Passed	
EWCJ171S_EWC_CMX_04	Connecting the Android Client to the access point on the floor and check the details of the Client.	To connect a Android Client to the access point on the floor and check if the details of the IOS Clients are shown correctly or not.	Passed	
EWCJ171S_EWC_CMX_05	Connecting many Clients from different place and check the location of the Clients	To connect many Client from different place to the access points and check if the location of the Client are shown in CMX	Passed	
EWCJ171S_EWC_CMX_06	Connecting a 2.4 ghz Client to the access point which is placed in floor and checking the client details	To connect a 2.4 ghz Client to the access point on the floor and check if the details of the Clients are shown correctly or not.	Passed	

EWCJ171S_EWC_CMX_07	Connecting a 5 ghz Client to the access point which is placed in floor and checking the client details	To connect a 5 ghz Client to the access point on the floor and check if the details of the Clients are shown correctly or not.	Passed	
EWCJ171S_EWC_CMX_08	Connecting a Dual band Client to the access point which is placed in floor and checking the client details	To connect a Dual band Client to the access point on the floor and check if the details of the Clients are shown correctly or not.	Passed	
EWCJ171S_EWC_CMX_09	Verify the Disconnected client details in CMX	To check whether the client is disconnected or not in CMX	Passed	
EWCJ171S_EWC_CMX_10	Verifying the Intra client roaming in CMX	To verify whether the client is roaming between AP's or not	Passed	
EWCJ171S_EWC_CMX_11	Verifying the Inter client roaming in CMX	To verify whether the clients are roaming between controllers	Passed	
EWCJ171S_EWC_CMX_12	Verifying the Wired client details in CMX	To Check whether the Wired client details are showing or not in CMX	Passed	
EWCJ171S_EWC_CMX_13	Verifying the guest LAN client details in CMX	To Check whether the Guest LAN client details are showing or not in CMX	Passed	
EWCJ171S_EWC_CMX_14	Verifying MIMO client details using Wireshark	To check Whether all the clients getting same BW & data rate or not	Passed	

Browser rendering

Logical ID	Title	Description	Status	Defect ID

EWCJ171S_EWC_Browser _rendering_1	Capture the Console logs Dashboard Page	To Capture the warning and severe console logs in Dashboard Page	Passed	
EWCJ171S_EWC_Browser _rendering_2	Capture the Console logs on Monitoring Page	To Capture the warning and severe console logs in Monitoring Page	Passed	
EWCJ171S_EWC_Browser _rendering_3	Capture the Console logs Configuration Page	To Capture the warning and severe console logs in Configuration Page	Passed	
EWCJ171S_EWC_Browser _rendering_4	Capture the Console logs Administration Page	To check weather any JS failures or errors are their in the Administration page in Cisco Catalyst 9800 Series Wireless Controller Japanese UI	Passed	
EWCJ171S_EWC_Browser _rendering_5	Capture the Console logs on Troubleshooting Page	To check weather any JS failures or errors are their in the Troubleshooting page in Cisco Catalyst 9800 Series Wireless Controller Japanese UI	Passed	
EWLCJ171S_Chrome Rendring_01	Capture the Console logs Dashboard Page	To Capture the warning and severe console logs in Dashboard Page	Passed	
EWLCJ171S_Chrome Rendring_02	Capture the Console logs Dashboard AP link	To Capture the warning and severe console logs in Dashboard Aps link	Passed	

EWLCJ171S_Chrome Rendring_03	Capture the Console logs Dashboard WLAN link	To Capture the warning and severe console logs in Dashboard WLAN link	Passed	
EWLCJ171S_Chrome Rendring_04	Capture the Console logs Dashboard Clients link	To Capture the warning and severe console logs in Dashboard Clients link	Passed	
EWLCJ171S_Chrome Rendring_05	Capture the Console logs on Monitoring Page	To Capture the warning and severe console logs in Monitoring Page	Passed	
EWLCJ171S_Chrome Rendring_06	Capture the Console logs on Monitoring -> General Sub pages Page	To Capture the warning and severe console logs in Monitoring -> General Page	Passed	
EWLCJ171S_Chrome Rendring_07	Capture the Console logs on Monitoring -> Security Sub pages Page	To Capture the warning and severe console logs in Monitoring -> Security sub Pages	Passed	
EWLCJ171S_Chrome Rendring_08	Capture the Console logs on Monitoring -> Services Sub pages Page	To Capture the warning and severe console logs in Monitoring -> Services sub Pages	Passed	
EWLCJ171S_Chrome Rendring_09	Capture the Console logs on Monitoring -> Wireless Sub pages	To Capture the warning and severe console logs in Monitoring -> Wireless sub Pages	Passed	

EWLCJ171S_Chrome Rendring_10	Capture the Console logs Configuration Page	To Capture the warning and severe console logs in Configuration Page	Passed	
EWLCJ171S_Chrome Rendring_11	Capture the Console logs Configuration - >Interface sub Pages	To Capture the warning and severe console logs in Configuration -> Interface sub Pages	Passed	
EWLCJ171S_Chrome Rendring_12	Capture the Console logs Configuration - >Layer2 sub Pages	To Capture the warning and severe console logs in Configuration ->Layer 2 Page	Passed	
EWLCJ171S_Chrome Rendring_13	Capture the Console logs Configuration - >Interface sub Pages	To Capture the warning and severe console logs in Configuration Page	Passed	
EWLCJ171S_Chrome Rendring_14	Capture the Console logs Configuration - >Radio Configurations sub Pages	To Capture the warning and severe console logs in Configuration-> Radio Configurations Page	Passed	
EWLCJ171S_Chrome Rendring_15	Capture the Console logs Configuration - >Routing protocols sub Pages	To Capture the warning and severe console logs in Configuration -> Routing protocols Page	Passed	
EWLCJ171S_Chrome Rendring_16	Capture the Console logs Configuration - >Security sub Pages	To Capture the warning and severe console logs in Configuration->Security Page	Passed	

EWLCJ171S_Chrome Rendring_17	Capture the Console logs Configuration - >Services sub Pages	To Capture the warning and severe console logs in Configuration ->Services Page	Passed	
EWLCJ171S_Chrome Rendring_18	Capture the Console logs Configuration - > Tags & Profiles sub Pages	To Capture the warning and severe console logs in Configuration -> Tags & Profiles Page	Passed	
EWLCJ171S_Chrome Rendring_19	Capture the Console logs Configuration - > Wireless sub Pages	To Capture the warning and severe console logs in Configuration -> Wireless Page	Passed	
EWLCJ171S_Chrome Rendring_20	Capture the Console logs Configuration - > Wireless Setup sub Pages	To Capture the warning and severe console logs in Configuration -> Wireless Page	Passed	
EWLCJ171S_Chrome Rendring_21	Capture the Console logs Administration Page	To Capture the warning and severe console logs in Administration Page	Passed	
EWLCJ171S_Chrome Rendring_22	Capture the Console logs Administration -> Best Practices Page	To Capture the warning and severe console logs in Administration -> Best Practices Page	Passed	
EWLCJ171S_Chrome Rendring_23	Capture the Console logs Administration -> Command line interface Page	To Capture the warning and severe console logs in Administration -> Command line interface Page	Passed	

EWLCJ171S_Chrome Rendring_24	Capture the Console logs Administration -> Device Page	To Capture the warning and severe console logs in Administration ->Device Page	Passed	
EWLCJ171S_Chrome Rendring_25	Capture the Console logs Administration -> DHCP Pools Page	To Capture the warning and severe console logs in Administration -> DHCP Pools Page	Passed	
EWLCJ171S_Chrome Rendring_26	Capture the Console logs Administration -> DNS Page	To Capture the warning and severe console logs in Administration -> DNS Page	Passed	
EWLCJ171S_Chrome Rendring_27	Capture the Console logs Administration -> Licensing Page	To Capture the warning and severe console logs in Administration -> Licensing Page	Passed	
EWLCJ171S_Chrome Rendring_28	Capture the Console logs Administration -> Management Page	To Capture the warning and severe console logs in Administration -> Management Page	Passed	
EWLCJ171S_Chrome Rendring_29	Capture the Console logs Administration -> Reload Page	To Capture the warning and severe console logs in Administration -> Reload Page	Passed	
EWLCJ171S_Chrome Rendring_30	Capture the Console logs Administration -> Smart call Home Page	To Capture the warning and severe console logs in Administration ->Smart call Home Page	Passed	

EWLCJ171S_Chrome Rendring_31	Capture the Console logs Administration -> Software Management Page	To Capture the warning and severe console logs in Administration -> Software management Page	Passed	
EWLCJ171S_Chrome Rendring_32	Capture the Console logs Administration -> Time Page	To Capture the warning and severe console logs in Administration -> Time Page	Passed	
EWLCJ171S_Chrome Rendring_33	Capture the Console logs Administration ->User Administration Page	To Capture the warning and severe console logs in Administration-> User Administration Page	Passed	
EWLCJ171S_Chrome Rendring_34	Capture the Console logs on Troubleshooting Page	To Capture the warning and severe console logs in Troubleshooting Page	Passed	
EWLCJ171S_Chrome Rendring_35	Capture the Console logs on Troubleshooting -> Logs Page	To Capture the warning and severe console logs in Troubleshooting->Logs Page	Passed	
EWLCJ171S_Chrome Rendring_36	Capture the Console logs on Troubleshooting -> Core Dump and System report Page	To Capture the warning and severe console logs in Troubleshooting ->Core dump and System report Page	Passed	
EWLCJ171S_Chrome Rendring_37	Capture the Console logs on Troubleshooting ->Debug bundle Page	To Capture the warning and severe console logs in Troubleshooting -> Debug bundle Page	Passed	

EWLCJ171S_Chrome Rendring_38	Capture the Console logs on Troubleshooting -> Packet capture Page	To Capture the warning and severe console logs in Troubleshooting->packet capture Page	Passed	
EWLCJ171S_Chrome Rendring_39	Capture the Console logs on Troubleshooting -> Ping and trace route Page	To Capture the warning and severe console logs in Troubleshooting -> Ping and trace route Page	Passed	
EWLCJ171S_Chrome Rendring_40	Capture the Console logs on Troubleshooting ->Ap Packet capture Page	To Capture the warning and severe console logs in Troubleshooting ->Ap packet capture Page	Passed	
EWLCJ171S_Chrome Rendring_41	Capture the Console logs on Troubleshooting ->Ap Radio active trace Page	To Capture the warning and severe console logs in Troubleshooting ->radio active trace packet capture Page	Passed	

EWC Crashes(DHCP/Troubleshootings)

Logical ID	Title	Description	Status	Defect ID
EWCJ171S_EWC_Crash_1	Creating the DHCP scope form CLI with invalid IP address and observe crash while configuring	To verify whether invalid IP accepting in DHCP pool or not and eWC not crashing	Passed	
EWCJ171S_EWC_Crash_2	Mapping the DHCP pool to interface and observe crash while configuring	To verify whether DHCP pool mapped to interface or not and eWC not crashing	Passed	

EWCJ171S_EWC_Crash_3	Changing the RRM details after client connected to WLAN	To verify whether eWC going to Crash or not after changing the RRM details	Passed	
EWCJ171S_EWC_Crash_4	Creating more than 10 DHCP pool in eWC with Japanese UI	To verify whether more than 10 DHCP pools are created and eWC not crashing	Passed	
EWCJ171S_EWC_Crash_5	Clearing the eWC Configurations	To verify whether Controller Configurations are clearing or not	Passed	
EWCJ171S_EWC_Crash_6	Backup & Restore the eWC Configurations	To verify whether Controller Configurations are Backup & Restore or not and eWC not crashing	Passed	
EWCJ171S_EWC_Crash_7	Convert the CAPWAP to eWC	To verify whether AP can be converted to new eWC or not without crash	Failed	CSCvs43415
EWCJ171S_EWC_Crash_8	Invalid DNS server IP address configuration	To verify whether DNS IP address field accepting the Invalid IP address or not and eWC not crashing	Passed	
EWCJ171S_EWC_Crash_9	Checking the ping response	To verify whether ping response is getting without packet drop and eWC not crashing	Passed	
EWCJ171S_EWC_Crash_10	Checking the traceroute response	To verify whether traceroute response is getting with actual hop count and eWC not crashing	Passed	

EWC Day0 Elimination

Logical ID	Title	Description	Status	Defect ID
EWCJ171S_EWC_Day0_01	Provisioning the Cisco Catalyst 9800 Series Wireless Controller_ME in day0 via PnP profile	Verify that user is able to Provisioned the Cisco Catalyst 9800 Series Wireless Controller_ME in day0 via PnP profile or not	Passed	
EWCJ171S_EWC_Day0_02	Manually adding single device Pnp details and Provisioning the 9115AX Cisco Catalyst 9800 Series Wireless Controller_ME in day0	Verify that user is able to Provisioned the Cisco Catalyst 9800 Series Wireless Controller_ME in day0 after adding Pnp Details manually	Passed	
EWCJ171S_EWC_Day0_03	Adding the device details in PnP with importing the .csv file in Bulk devices option	Verify that user is able to Provisioned the 1815Cisco Catalyst 9800 Series Wireless Controller_ME in day0 after adding Pnp Details with importing .csv file	Passed	
EWCJ171S_EWC_Day0_04	Checking the image version after Provisioning Cisco Catalyst 9800 Series Wireless Controller_ME with PnP	Verifying the image version after Provisioning Cisco Catalyst 9800 Series Wireless Controller_ME with PnP	Passed	
EWCJ171S_EWC_Day0_05	Checking the AP details after Provisioning Cisco Catalyst 9800 Series Wireless Controller_ME with PnP	Verifying the AP details after ProvisioningCisco Catalyst 9800 Series Wireless Controller_ME with PnP	Passed	

EWCJ171S_EWC_Day0_06	Checking WLANs broadcasting or not after provisioning	To verify whether WLANs are broadcasting or not after provisioning	Passed	
EWCJ171S_EWC_Day0_07	Connecting client to created WLAN and checking the client details	Verifying the client details after connecting WLAN	Passed	
EWCJ171S_EWC_Day0_08	Configuring wrong DNAC IP address in switch and trying for the provisioning	To verify whether user is able to Provisioned theCisco Catalyst 9800 Series Wireless Controller_ME with providing wrong DNAC IP in Switch	Passed	
EWCJ171S_EWC_Day0_09	Configuring wrong details for PnP while claiming the device	To verify whether user is able to Provisioned the Cisco Catalyst 9800 Series Wireless Controller_ME with providing wrong PnP configuration in DNAC	Passed	
EWCJ171S_EWC_Day0_10	Checking the Cisco Catalyst 9800 Series Wireless Controller_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	

ISSU

Logical ID	Title	Description	Status	Defect ID
EWLCJ171S_ISSU_01	Performing Upgradation using ISSU	To check whether the upgradation is performed or not via ftp	Passed	

EWLCJ171S_ISSU_02	Performing Rollback for controller using ISSU.	To check whether the rollback happening for Controller image or not.	Passed	
EWLCJ171S_ISSU_03	Disabling the Rollback timer during upgrading controller using ISSU.	To check that the rollback doesn't happen for Controller image or not.	Passed	
EWLCJ171S_ISSU_04	Aborting the upgradation of Controller using ISSU.	To check whether the upgradation for Controller image is aborted or not.	Passed	
EWLCJ171S_ISSU_05	Performing Upgradation for controller using ISSU via tftp server.	To check whether the Controller Upgradation via tftp is happening or not.	Passed	
EWLCJ171S_ISSU_06	Performing Upgradation for Controller using ISSU via sftp server.	To check whether the Controller Upgradation via sftp is happening or not.	Passed	
EWLCJ171S_ISSU_07	Performing Upgradation for controller using ISSU via http server.	To check whether the Controller Upgradation via http is happening or not.	Passed	
EWLCJ171S_ISSU_08	Checking the client connectivity	To check whether the client continuously connecting during the upgrade of AP	Passed	

DNA Assurance

Logical ID	Title	Description	Status	Defect ID
EWLCJ171S_DNA_A_01	Verifying device details in inventory after added/discovered in cisco DNA	To verify whether the device details are showing in inventory after added in cisco DNA	Passed	

EWLCJ171S_DNA_A_02	Checking the Performance of APs in Cisco DNA	Verifying whether the Performance of APs are monitored correctly as per in the controller or not in Cisco DNA	Passed	
EWLCJ171S_DNA_A_03	Verifying number of wireless devices are added in Cisco DNA	Checking whether count of wireless devices are added in Cisco DNA and they are monitored properly or not	Passed	
EWLCJ171S_DNA_A_04	Monitoring to which AP clients are connected and their signal strength	Verifying whether all the clients are monitored or not according to their high interface along with the APs	Passed	
EWLCJ171S_DNA_A_05	Checking the Client connectivity status in Cisco DNA	Verifying whether the Client status are monitored correctly as per in the controller or not in Cisco DNA	Passed	
EWLCJ171S_DNA_A_06	Checking the Client On boarding Times in Cisco DNA	Verifying whether the Client On boarding Times are monitored correctly as per in the controller or not in Cisco DNA	Passed	
EWLCJ171S_DNA_A_07	Checking the Client Count per SSID in Cisco DNA	Verifying whether the Client Count per SSID are monitored correctly as per in the controller or not in Cisco DNA	Passed	
EWLCJ171S_DNA_A_08	Checking the Client Count per Band in Cisco DNA	Verifying whether the Client Count per Band are monitored correctly as per in the controller or not in Cisco DNA	Passed	

EWLCJ171S_DNA_A_09	Checking the Client RSSI & SNR values in Cisco DNA	Verifying whether the RSSI & SNR are monitored correctly as per in the controller or not in Cisco DNA	Passed	
EWLCJ171S_DNA_A_10	Performing Network Test in Sensor - Driven Test	Verifying the IP Addressing, DNS, Host Reachability & RADIUS Tests in Sensor - Driven Test	Passed	
EWLCJ171S_DNA_A_11	Capturing the Network Test from Wireless Sensor Dashboard	Monitoring the IP Addressing, DNS, Host Reachability & RADIUS Tests in Wireless Sensor Dashboard	Passed	
EWLCJ171S_DNA_A_12	Performing Performance Test in Sensor - Driven Test	Verifying the Speed Test & ISPLA Test in Sensor - Driven Test	Passed	
EWLCJ171S_DNA_A_13	Capturing the Performance Test from Wireless Sensor Dashboard	Monitoring the Speed Test & ISPLA Test in Wireless Sensor Dashboard	Passed	
EWLCJ171S_DNA_A_14	Performing Application Test in Sensor - Driven Test	Verifying the Email Test, Web Test & File Transfer Test in Sensor - Driven Test	Passed	
EWLCJ171S_DNA_A_15	Capturing the Application Test from Wireless Sensor Dashboard	Monitoring the Email Test, Web Test & File Transfer Test in Wireless Sensor Dashboard	Passed	
EWLCJ171S_DNA_A_16	Performing Scheduling On boarding Packet Capture Test	Checking whether the Scheduling On boarding Packet capture is done as per the schedule or not	Passed	

EWLCJ171S_DNA_A_17	Capturing Configured APs using Auto-Capture Settings	Testing whether the user able to capture or not the Configured APs using Auto-Capture Settings	Passed	
EWLCJ171S_DNA_A_18	Packet capture of client when the client is connected to AP with 2.4 GHz	To capture the Packet of the client when the client is connected to AP with radio as 2.4 GHz	Passed	
EWLCJ171S_DNA_A_19	Packet capture of client when the client is connected to AP with 5 GHz	To capture the Packet of the client when the client is connected to AP with radio as 5 GHz	Passed	
EWLCJ171S_DNA_A_20	Capturing of Packet of the client when the client is connected with WPA 2 PSK security	To capture packet when the client is connected to the AP with security as WPA 2 PSK	Passed	
EWLCJ171S_DNA_A_21	Capturing of Packet of the client when the client is connected with WPA 2 802.1x security	To capture packet when the client is connected to the AP with security as WPA 2 802.1x	Passed	
EWLCJ171S_DNA_A_22	Verifying the packet capture when the AP is in Flexconnect Local switching	To verify if the packet capture happens when the AP is in Flexconnect Local switching mode with a client connected to it	Passed	
EWLCJ171S_DNA_A_23	Verifying the packet capture when the AP is in Flexconnect Local switching with local authentication	To verify if the packet capture happens when the AP is in Flexconnect Local switching mode and local authentication with a client connected to it	Passed	

EWLCJ171S_DNA_A_24	Performing Intra controller roaming of client and capturing of packet using Intelligent capture	To check whether intra controller roaming of clients works properly or not and check if packet capture works properly or not	Passed	
EWLCJ171S_DNA_A_25	Performing Inter controller roaming of client and capturing the packet	To check whether inter controller roaming of Android clients works properly or not	Passed	
EWLCJ171S_DNA_A_26	Packet capture for the WGB based client using Intelligent Capture	To capture Packet for the WGB based client and check if packet capture for WGB based client is shown	Passed	
EWLCJ171S_DNA_A_27	Packet capture for Anyconnect client using Intelligent Capture option in AP page	To verify the packet capture for Anyconnect client using Intelligent capture in AP page	Passed	
EWLCJ171S_DNA_A_28	Packet capture for Windows JOS client using Intelligent Capture option in AP page	To verify the packet capture for Windows JOS client using Intelligent capture in AP page	Passed	
EWLCJ171S_DNA_A_29	Packet capture for Android client using Intelligent Capture option in AP page	To verify the packet capture for Android client using Intelligent capture in AP page	Passed	
EWLCJ171S_DNA_A_30	Packet capture for iOS client using Intelligent Capture option in AP page	To verify the packet capture for iOS client using Intelligent capture in AP page	Passed	
EWLCJ171S_DNA_A_31	Packet capture for MacOS client using Intelligent Capture option in AP page	To verify the packet capture for MacOS client using Intelligent capture in AP page	Passed	

EWLCJ171S_DNA_A_32	Capturing of Packet of the client when the client is connected with open security	To capture packet when the client is connected to the AP with security as OPEN	Passed	

Catalyst 9800 Crashes(DHCP/Troubleshootings)

Logical ID	Title	Description	Status	Defect ID
EWLCJ171S_EWLC_Crash_01	Creating the DHCP scope form CLI with invalid IP address and observe crash while configuring	To verify whether invalid IP accepting in DHCP pool or not and Cisco Catalyst 9800 Series Wireless Controller not crashing	Passed	
EWLCJ171S_EWLC_Crash_02	Mapping the DHCP pool to interface and observe crash while configuring	To verify whether DHCP pool mapped to interface or not and Cisco Catalyst 9800 Series Wireless Controller not crashing	Failed	CSCvs78121
EWLCJ171S_EWLC_Crash_03	Changing the RRM details after client connected to WLAN	To verify whether Cisco Catalyst 9800 Series Wireless Controller going to Crash or not after changing the RRM details	Passed	
EWLCJ171S_EWLC_Crash_04	Creating more than 10 DHCP pool inCisco Catalyst 9800 Series Wireless Controller with Japanese UI	To verify whether more than 10 DHCP pools are created and Cisco Catalyst 9800 Series Wireless Controller not crashing	Passed	

EWLCJ171S_EWLC_Crash_05	Clearing the Cisco Catalyst 9800 Series Wireless Controller Configurations	To verify whether Controller Configurations are clearing or not	Passed	
EWLCJ171S_EWLC_Crash_06	Backup & Restore the Cisco Catalyst 9800 Series Wireless Controller Configurations	To verify whether Controller Configurations are Backup & Restore or not and Cisco Catalyst 9800 Series Wireless Controller not crashing	Passed	
EWLCJ171S_EWLC_Crash_07	Convert the CAPWAP toCisco Catalyst 9800 Series Wireless Controller	To verify whether AP can be converted to new Cisco Catalyst 9800 Series Wireless Controller or not without crash	Passed	
EWLCJ171S_EWLC_Crash_08	Invalid DNS server IP address configuration	To verify whether DNS IP address field accepting the Invalid IP address or not and Cisco Catalyst 9800 Series Wireless Controller not crashing	Passed	
EWLCJ171S_EWLC_Crash_09	Checking the ping response	To verify whether ping response is getting without packet drop and Cisco Catalyst 9800 Series Wireless Controller not crashing	Passed	

EWLCJ171S_EWLC_Crash_10	Checking the traceroute response	To verify whether traceroute response is getting with actual hop count and Cisco Catalyst 9800 Series Wireless Controller not crashing	Passed	

mDNS Support for Wired Guest Ac

Logical ID	Title	Description	Status	Defect ID
EWLCJ171S_mDNS_WGA_01	Create the Guest Lan with mDNS Mode Bridging Gateway and Verify with Apple TV	Verify able to create the Guest Lan with mDNS Mode Bridging with Apple TV	Passed	
EWLCJ171S_mDNS_WGA_02	Create the Guest Lan with mDNS Mode Bridging.	Verify able to create the Guest Lan with mDNS Mode Bridging.	Passed	
EWLCJ171S_mDNS_WGA_03	Edit the Guest Lan with mDNS Mode Bridging.	Verify able to edit the Guest Lan with mDNS Mode Bridging.	Passed	
EWLCJ171S_mDNS_WGA_04	Delete the Guest Lan with mDNS Mode Bridging.	Verify able to Delete the Guest Lan with mDNS Mode Bridging.	Passed	
EWLCJ171S_mDNS_WGA_05	Create the Guest Lan with mDNS Mode Bridging with Guest LAN Map Configuration.	Verify able to create with the Guest Lan with mDNS Mode Bridging.	Passed	
EWLCJ171S_mDNS_WGA_06	Delete the Guest Lan with mDNS Mode Bridging with Guest LAN Map Configuration.	Verify able to Delete with the Guest Lan with mDNS Mode Bridging.	Passed	

EWLCJ171S_mDNS_WGA_07	Create the Guest Lan with mDNS Mode Gateway: .	Verify able to Create the Guest Lan with mDNS Mode Bridging Gateway: .	Passed	
EWLCJ171S_mDNS_WGA_08	Create the Guest Lan with mDNS Mode Bridging Drop.	verify able to Create the Guest Lan with mDNS Mode Drop.	Passed	

NAT Support for Mobility Tunnel

Logical ID	Title	Description	Status	Defect ID
EWLCJ171S_NAT_MT_01	Perform the roaming scenario and NAT with Windows client.	To Verify the roaming scenario and NAT with Windows client.	Passed	
EWLCJ171S_NAT_MT_02	Perform the roaming scenario and NAT with MAC client.	To Verify the roaming scenario and NAT with MAC client.	Passed	
EWLCJ171S_NAT_MT_03	Perform the roaming scenario and NAT with Android client.	To Verify the roaming scenario and NAT with Android client.	Passed	
EWLCJ171S_NAT_MT_04	Perform the roaming scenario and NAT with Apple client.	To Verify the roaming scenario and NAT with Apple client.	Passed	

Open DNS

Logical ID	Title	Description	Status	Defect ID
EWLCJ171S_OpenDNS_01	Verifying Cisco Catalyst 9800 Series Wireless Controller registered with open DNS server	To Verify whether the Cisco Catalyst 9800 Series Wireless Controller registered in open DNS and Cisco Catalyst 9800 Series Wireless Controller got the device ID or not	Passed	

EWLCJ171S_OpenDNS_02	Verifying the created profile mapped with Cisco Catalyst 9800 Series Wireless Controller GUI and CLI	To Verify whether the profile mapped with Cisco Catalyst 9800 Series Wireless Controller and reflected in Cisco Catalyst 9800 Series Wireless Controller GUI & CLI or not	Passed	
EWLCJ171S_OpenDNS_03	Verifying the WLAN created with open DNS configuration	To verify whether the WLAN created with open DNS configuration or not	Passed	
EWLCJ171S_OpenDNS_04	Verifying the open DNS configuration for the connected Windows Client in Cisco Catalyst 9800 Series Wireless Controller UI/CLI	To Verify whether the open DNS configured or not when Windows JOS connected to Umbrella enabled WLAN Profile	Passed	
EWLCJ171S_OpenDNS_05	Verifying the open DNS configuration for the connected MAC OS Client in Cisco Catalyst 9800 Series Wireless Controller UI/CLI	To Verify whether the open DNS configured or not when MAC OS connected to Umbrella enabled WLAN Profile	Passed	
EWLCJ171S_OpenDNS_06	Verifying the open DNS configuration for the connected iOS Client in Cisco Catalyst 9800 Series Wireless Controller UI/CLI	To Verify whether the open DNS configured or not when iOS client connected to Umbrella enabled WLAN Profile	Passed	
EWLCJ171S_OpenDNS_07	Verifying the open DNS configuration for the connected Android Client in Cisco Catalyst 9800 Series Wireless Controller UI/CLI	To Verify whether the open DNS configured or not when Android client connected to Umbrella enabled WLAN Profile	Passed	

EWLCJ171S_OpenDNS_08	clear the data plane stats in open DNS configuration	To verify whether the data plate stats is cleared or not	Passed	
EWLCJ171S_OpenDNS_09	Perform the roaming between 9115 & 9120 Aps	To verify the open DNs configuration after client roaming between 9115 & 9120 Aps	Passed	
EWLCJ171S_OpenDNS_10	Perform the roaming between two Cisco Catalyst 9800 Series Wireless Controller	To verify the open dns after Inter roaming	Passed	

RSSI and SNR in ASSOC request

Logical ID	Title	Description	Status	Defect ID
EWLCJ171S_RSSI_SNR_01	Adding Cisco Catalyst 9800 Series Wireless Controller to DNAC and connecting clients	To verify SNR and RSS values in DNA centre after connecting client	Passed	
EWLCJ171S_RSSI_SNR_02	Connecting client to AP flex connect mode ,authentication as open and verifying SNR and RSS details	To verify SNR and RSS connectivity in DNAcentre with AP mode flexconnect and authentication as open	Passed	
EWLCJ171S_RSSI_SNR_03	Connecting client to AP flex connect mode ,authentication as PSK and verifying SNR and RSS details	To verify SNR and RSS connectivity in DNAcentre with AP mode flexconnect and authentication as PSK	Passed	
EWLCJ171S_RSSI_SNR_04	Connecting client to AP flex connect mode ,authentication as dot11 and verifying SNR and RSS details	To verify SNR and RSS connectivity in DNAcentre with AP mode flexconnect and authentication as dot11	Passed	

EWLCJ171S_RSSI_SNR_05	verifying SNR and RSS details after connecting client to AP flex mode as standalone ,authentication as open	To verify SNR and RSS connectivity in DNAcentre with AP as Flex standalone and authentication as open	Passed	
EWLCJ171S_RSSI_SNR_06	verifying SNR and RSS details after connecting client to AP flex mode as standalone ,authentication as PSK	To verify SNR and RSS connectivity in DNAcentre with AP as Flex standalone and authentication as PSK	Passed	
EWLCJ171S_RSSI_SNR_07	verifying SNR and RSS details after connecting client to AP flex mode as standalone ,authentication as dot11	To verify SNR and RSS connectivity in DNAcentre with AP as Flex standalone and authentication as dot11	Passed	
EWLCJ171S_RSSI_SNR_08	Connecting client to AP local ,authentication as dot11 and verifying SNR and RSS details	To verify SNR and RSS connectivity in DNAcentre with AP mode as local and authentication as dot11	Passed	
EWLCJ171S_RSSI_SNR_09	Connecting client to AP mode as local verifying SNR and RSS details	To verify SNR and RSS connectivity in DNAcentre with AP mode as local	Passed	
EWLCJ171S_RSSI_SNR_10	Connecting client to AP mode as bridge ,authentication as dot11 and verifying SNR and RSS details	To verify SNR and RSS connectivity in DNAcentre with AP mode as bridge	Passed	
EWLCJ171S_RSSI_SNR_11	Checking the SNR and RSS values after performing intra roaming in Cisco Catalyst 9800 Series Wireless Controller	To verify SNR and RSS connectivity in DNAcentre after doing intra roaming in WLC	Passed	

EWLCJ171S_RSSI_SNR_12	Roaming client from 9115 & 9120 Aps and checking the SNR and RSS values	To Check the SNR and RSS values when client roam between 3800 & 1815 Aps	Passed	
EWLCJ171S_RSSI_SNR_13	Checking the SNR and RSS values after performing inter roaming in Cisco Catalyst 9800 Series Wireless Controller	To verify SNR and RSS connectivity in DNAcentre after doing inter roaming in Cisco Catalyst 9800 Series Wireless Controller	Passed	
EWLCJ171S_RSSI_SNR_14	Checking the SNR and RSS values after performing FT roaming roaming in Cisco Catalyst 9800 Series Wireless Controller	To verify SNR and RSS connectivity in DNAcentre after doing FT roaming in Cisco Catalyst 9800 Series Wireless Controller	Passed	
EWLCJ171S_RSSI_SNR_15	Verifying the AID values in client after connecting client	To check whether client getting AID value or not	Passed	

WGB

Logical ID	Title	Description	Status	Defect ID
EWLCJ171S_WGB_01	Configuring the Capwap Ap to autonomous AP	To change the Capwap Ap to autonomous Ap and check if the AP is converted	Passed	
EWLCJ171S_WGB_02	Configuring the Autonomous AP as the WGB	To configure the autonomous AP as WGB and check if the AP changes as WGB.	Passed	
EWLCJ171S_WGB_03	Configuring WGB in Cisco Catalyst 9800 Series Wireless Controller	To verify WGB configuration is successful or not in Cisco Catalyst 9800 Series Wireless Controller	Passed	

EWLCJ171S_WGB_04	Associating the WGB on open authentication with 9115 AP	To associate the WGB on open authentication and check if the WGB associates with the open WLAN or not.	Passed	
EWLCJ171S_WGB_05	Associating the WGB on WPA 2 with PSK with 9115 bridge AP	To associate the WGB on WPA 2 PSK security with 9115 bridge AP and check if the WGB associates with the WLAN or not.	Passed	
EWLCJ171S_WGB_06	Associating the WGB on WPA 2 with 802.1x with 9115 AP	To associate the WGB on WPA 2 802.1x security when AP in local mode and check if the WGB associates with the WLAN or not.	Passed	
EWLCJ171S_WGB_07	Associating the WGB on open authentication with flex+bridge	To associate the WGB on open authentication with 9115 AP flex+bridge AP and check if the WGB associates with the open WLAN or not.	Passed	
EWLCJ171S_WGB_08	Associating the WGB on WPA 2 with PSK with flex+bridge AP	To associate the WGB on WPA 2 PSK security with 9115 AP flex+bridge AP and check if the WGB associates with the WLAN or not.	Passed	
EWLCJ171S_WGB_09	Associating the WGB on WPA 2 with 802.1x with flex+bridge AP	To associate the WGB on WPA 2 802.1x security with 9115 flex+bridge AP and check if the WGB associates with the WLAN or not.	Passed	

EWLCJ171S_WGB_10	Checking of WGB roaming from one AP to another AP in bridge mode	To check the roaming of WGB from one AP to another AP when the AP is in bridge mode .	Passed	
EWLCJ171S_WGB_11	Checking of WGB roaming from one AP to another AP in flex+bridge mode	To check the roaming of WGB from one AP to another AP when Aps are in flex+bridge mode	Passed	
EWLCJ171S_WGB_12	Performing Inter controller roaming for WGB clients with OPEN security in AP flex+bridge mode	To check inter controller roaming for WGB clients with OPEN security in AP flex+bridge mode	Passed	
EWLCJ171S_WGB_13	Performing Inter controller roaming for WGB clients with WPA2 PSK security in AP flex+bridge mode	To check inter controller roaming for WGB clients with WPA2 PSK security in AP flex+bridge mode	Passed	
EWLCJ171S_WGB_14	Performing Inter controller roaming for WGB clients with WPA2 Dot1x security in AP flex+bridge mode	To check inter controller roaming for WGB clients with WPA2 Dot1x security in AP flex+bridge mode	Passed	
EWLCJ171S_WGB_15	Performing Inter controller roaming for WGB clients with OPEN security in AP bridge mode	To check inter controller roaming for WGB clients with OPEN security in AP bridge mode	Passed	
EWLCJ171S_WGB_16	Performing Inter controller roaming for WGB clients with WPA2 PSK security in AP bridge mode	To check inter controller roaming for WGB clients with WPA2 PSK security in AP bridge mode	Passed	
EWLCJ171S_WGB_17	Performing Inter controller roaming for WGB clients with WPA2 Dot1x security in AP bridge mode	To check inter controller roaming for WGB clients with WPA2 Dot1x security in AP bridge mode	Passed	

EWLCJ171S_WGB_18	Associating the WGB on open security with local authentication	To check WGB client association with OPEN security and local authentication	Passed	
EWLCJ171S_WGB_19	Checking Reassociation happens for WGB clients after session timeout	To verify reassociation for WGB clients after session timeout	Passed	
EWLCJ171S_WGB_20	Performing local switching for WGB clients with 9115 AP	To verify local switching traffic for client with 9115 AP	Passed	

Intelligent Capture

Logical ID	Title	Description	Status	Defect ID
EWLCJ171S_ic_01	Configuring Intelligent Capture parameter details on 9115/9120 AP	To configure Intelligent capture parameters in 9115/9120 Aps	Passed	
EWLCJ171S_ic_02	Check Configuration after the AP reboot	To Configure Intelligent capture parameters in different Aps 9115/9120 and check if the configuration remains same after the AP reboot.	Passed	
EWLCJ171S_ic_03	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	
EWLCJ171S_ic_04	Packet capture of client when the client is connected to 9115/9120 AP with 5 GHz	To capture the Packet of the client when the client is connected to AP with radio as 5 GHz	Passed	

EWLCJ171S_ic_05	Capturing of Packet of the client when the client is connected with open security.	To capture packet when the client is connected to the 9115/9120 AP with security as OPEN	Passed	
EWLCJ171S_ic_06	Capturing of Packet of the client when the client is connected with WPA 2 PSK security.	To capture packet when the client is connected to the 9115/9120 AP with security as WPA 2 PSK	Passed	
EWLCJ171S_ic_07	Capturing of Packet of the client when the client is connected with WPA 2 802.1x security.	To capture packet when the client is connected to the 9115/9120 AP with security as WPA 2 802.1x	Passed	
EWLCJ171S_ic_08	Capturing of Packet of the client when the client is connected with Static WEP security.	To capture packet when the client is connected to the 9115/9120 AP with security as Static WEP	Passed	
EWLCJ171S_ic_09	Verifying if the packet capture happens when the AP configured with different channel.	To verify if the packet capture happens when the AP is configured with different channel width and packet capture shows correct information.	Passed	
EWLCJ171S_ic_10	Verify the packet capture when the AP is in Flex connect Local switching .	To verify if the packet capture happens when the AP is in Flex connect Local switching mode with a client connected to it	Passed	

EWLCJ171S_ic_11	Verify the packet capture when the AP is in Flex connect Local switching with local authentication .	To verify if the packet capture happens when the AP is in Flex connect Local switching mode and local authentication with a client connected to it	Passed	
EWLCJ171S_ic_12	Performing Intra controller roaming of client and capturing of packet using Intelligent capture	To check whether intra controller roaming of clients works properly or not and check if packet capture works properly or not.	Passed	
EWLCJ171S_ic_13	Performing Inter controller roaming of client and capturing the packet .	To check whether inter controller roaming of Android clients works properly or not	Passed	
EWLCJ171S_ic_14	Capturing Packet of Windows client when the client connected to 9115/9120 AP	To capture packet when the Window client is connected to the 9115/9120 AP	Passed	
EWLCJ171S_ic_15	Capturing Packet of Android client when the client connected to 9115/9120 AP	To capture packet when the Android client is connected to the 9115/9120 AP	Passed	
EWLCJ171S_ic_16	Capturing Packet of Mac OS client when the client connected to 9115/9120 AP	To capture packet when the Mac OS client is connected to the 9115/9120 AP	Passed	
EWLCJ171S_ic_17	Capturing Packet of IOS client when the client connected to 9115/9120 AP	To capture packet when the IOS client is connected to the 9115/9120 AP	Passed	

DNAc support for Cisco Catalyst 9800 Series Wireless Controller

Logical ID	Title	Description	Status	Defect ID

EWLCJ171S_DNACSuppo_01	Verifying device details in inventory after added/discovered in cisco DNA	To verify whether the device details are showing in inventory after added in cisco DNA	Passed	
EWLCJ171S_DNACSuppo_02	Monitoring the devices after adding in cisco DNA and verifying same in Cisco Catalyst 9800 Series Wireless Controller	Verifying whether added devices properly assured or monitoring in cisco DNA	Passed	
EWLCJ171S_DNACSuppo_03	Discovering multiple devices in cisco DNA and check for the same count in monitored devices	Checking whether count of wireless devices are added in Cisco DNA and they are monitored properly or not	Passed	
EWLCJ171S_DNACSuppo_04	Checking AP devices in inventory after Wireless controller discovered in cisco DNA	To verify whether all AP's details showing in inventory after device discovered	Passed	
EWLCJ171S_DNACSuppo_05	Checking the AP's count in network health after successfully added in inventory	To verify AP's count in Assurance dashboard after added in inventory	Passed	
EWLCJ171S_DNACSuppo_06	Resync the cisco DNA and checking for the newly added AP's count in device	To verify newly added AP's count in cisco DNA after resync	Passed	
EWLCJ171S_DNACSuppo_07	Exporting the inventory details from cisco DNA	To verify whether user able to export the device inventory details or not	Passed	
EWLCJ171S_DNACSuppo_08	Importing the inventory details to device from computer in cisco DNA	To verify whether user able to import the device inventory details or not	Passed	

EWLCJ171S_DNACSuppo_09	Running the commands in cisco DNA using command runner	To check the output for device commands after run in command runner in cisco DNA	Passed	
EWLCJ171S_DNACSuppo_10	Deleting the device from inventory in cisco DNA	To check whether user able to delete the device from inventory or not	Passed	
EWLCJ171S_DNACSuppo_11	Checking the device reachability status in inventory after make the device down	To check whether reachability status change to "unreachable" or not when device is down	Passed	
EWLCJ171S_DNACSuppo_12	Adding site and provisioning device in cisco DNA	To check whether user able to create site and provision device	Passed	
EWLCJ171S_DNACSuppo_13	Positioning AP's on site with different radios in cisco DNA	To check AP's positioning after positioned with different radios	Passed	
EWLCJ171S_DNACSuppo_14	Connecting the wireless clients to AP's and checking the client count in Dashboard	To verify the wireless client details in client Health after connected to AP	Passed	
EWLCJ171S_DNACSuppo_15	Connecting the wired clients to AP's and checking the client count in Dashboard	To verify the wired clients details in client Health after connected to AP	Passed	
EWLCJ171S_DNACSuppo_16	Downloading the upgrade read lines report from inventory devices in cisco DNA	To check whether the user able to download the upgrade read lines report from inventory devices or not	Passed	

Support of Trap notification via SNMP3

Logical ID	Title	Description	Status	Defect ID

EWLCJ171S_Trap_ntfcn_01	Creating V3 user group with security level "Auth" and mapping to v3 user	To verify traps with v3 user group security level as "Auth" and v3 user with "AuthNoPriv"	Passed	
EWLCJ171S_Trap_ntfcn_02	Creating V3 user group with security level "No Auth" and mapping to v3 user	To verify traps with v3 user group security level as " No Auth" and v3 user with "NoAuthNoPriv"	Passed	
EWLCJ171S_Trap_ntfcn_03	Creating V3 user group with security level "Priv" and mapping to v3 user	To verify traps with v3 user group security level as "Priv" and v3 user with "AuthPriv"	Passed	
EWLCJ171S_Trap_ntfcn_04	Removing the v3 user group after mapped with SNMP v3 user	To check whether able to delete trap receiver with mapped SNMP v3 user	Passed	
EWLCJ171S_Trap_ntfcn_05	Checking the traps in trap host after configuring the SNMPv3 user with different authentication and privacy protocol	To verify whether user able to create SNMP V3 user and get the traps in trap host	Passed	
EWLCJ171S_Trap_ntfcn_06	Configuring the multiple SNMP trap hosts and verifying the traps	To verify whether user able to create SNMP V3 user and get the traps in trap host	Passed	
EWLCJ171S_Trap_ntfcn_07	Verifying traps in trap host after enabling wireless parameter	To verify traps in host after change the Ap modes in devices	Passed	
EWLCJ171S_Trap_ntfcn_08	Verifying traps in trap host after reloading device	To Check whether traps generating in host after reload the device	Passed	
EWLCJ171S_Trap_ntfcn_09	Observing the trap messages when performed switchover in device	To check traps in host after performing switchover in device	Passed	

EWLCJ171S_Trap_ntfcn_10	Verifying traps in trap host after enabling aaa_server parameter	To verify traps in host after create/delete radius servers in device	Passed	
EWLCJ171S_Trap_ntfcn_11	Disabling/not configuring the snmpv3 and checking for traps in trap host	To verify traps not showing when snmpv3 not mapped with trap host	Passed	

mDNS AP support

Logical Id	Title	Description	Status	Defect ID
EWLCJ171S_mDNSAp_01	Checking mDNS services are Applying to Mac OS and Apple Tv clients after enabling the mdns Ap to 9115Ap	To check whether the mdns services Applying to Mac OS and Apple Tv clients or not after enabling the mDNS-Ap to 9115Ap.	Passed	
EWLCJ171S_mDNSAp_02	Checking mDNS services are Applying to Mac OS and Apple Tv clients after enabling the mdns Ap to 9120Ap	To check whether the mdns services Applying to Mac OS and Apple Tv clients after enabling the mDNS-Ap to 9120Ap	Passed	
EWLCJ171S_mDNSAp_03	Checking mDNS services are Applying to Mac OS and Apple Tv clients after enabling the mdns Ap to 4800Ap	To check whether the mdns services Applying to Mac OS and Apple Tv clients or not after enabling the mDNS-Ap to 4800Ap.	Passed	
EWLCJ171S_mDNSAp_04	Checking mDNS services are Applying to Mac OS and Apple Tv clients after enabling the mdns Ap to 3700Ap	To check whether the mdns services Applying to Mac OS and Apple Tv clients or not after enabling the mDNS-Ap to 3700Ap	Passed	
EWLCJ171S_mDNSAp_05	Checking the mDNS Services and mDNS Ap configuration.	To check whether mDNS Services and mDNS Ap support configurations able to configure or not.	Passed	

EWLCJ171S_mDNSAp_06	Verifying the mDNS services and mDNS Ap support configurations after changing the Ap mode to Monitor from Local	To check whether mDNS Services and mDNS Ap support configurations after changing the Ap mode to Monitor from Local.	Passed	
EWLCJ171S_mDNSAp_07	Checking mDNS services are Applying to Apple iPad and IPhone and Apple Tv clients after enabling the mdns Ap to 9115Ap	To check whether the mdns services Applying to Apple iPad and IPhone, Apple Tv clients or not after enabling the mDNS-Ap to 9115Ap.	Passed	
EWLCJ171S_mDNSAp_08	Checking mDNS services are Applying to Apple iPad and IPhone and Apple Tv clients after enabling the mdns Ap to 4800Ap	To check whether the mdns services Applying to Apple iPad and IPhone, Apple Tv clients or not after enabling the mDNS-Ap to 4800Ap.	Passed	
EWLCJ171S_mDNSAp_09	Checking mDNS services are Applying to Apple iPad and IPhone and Apple Tv clients after enabling the mdns Ap to 9120Ap	To check whether the mdns services Applying to Apple iPad and IPhone, Apple Tv clients or not after enabling the mDNS-Ap to 9120Ap.	Passed	
EWLCJ171S_mDNSAp_10	Checking mDNS services are Applying to Apple iPad and IPhone and Apple Tv clients after enabling the mdns Ap to 3700Ap	To check whether the mdns services Applying to Apple iPad and IPhone, Apple Tv clients or not after enabling the mDNS-Ap to 3700Ap.	Passed	
EWLCJ171S_mDNSAp_11	Checking the mDNS Services and mDNS Ap configuration after export and importing the Configuration file.	To check the mDNS Services and mDNS Ap support configurations after export and importing the Configuration file.	Passed	

EWLCJ171S_mDNSAp_12	Checking mDNS services are Applying to Apple iPad and Mac os and Apple chromecast clients with WPA2-PSK security after enabling the mdns Ap to 9115/4800/9120/3700Ap	To check whether the mdns services Applying to Apple iPad and Mac os and Apple chromecast clients with WPA2-PSK security or not after enabling the mDNS-Ap to 9115/4800/9120/3700Ap.	Passed	
EWLCJ171S_mDNSAp_13	Checking mDNS services are Applying to Apple iPad and Mac os and Apple chromecast clients with WPA3-SAE security after enabling the mdns Ap to 9115/4800/9120/3700Ap's	To check whether the mdns services Applying to Apple iPad and Mac os and Apple chromecast clients with WPA2-SAE security or not after enabling the mDNS-Ap to 9115/4800/9120/3700Ap's.	Passed	
EWLCJ171S_mDNSAp_14	Checking mDNS services are Applying to Apple iPad and Mac os and Apple chromecast clients with Static WEP security after enabling the mdns Ap to9115/4800/9120/3700Ap's	To check whether the mdns services Applying to Apple iPad and Mac os and Apple chromecast clients with Static WEP security or not after enabling the mDNS-Ap to9115/4800/9120/3700Ap's.	Passed	

Psk Multi Auth Support

Logical ID	Title	Description	Status	Defect ID
EWCJ171S_EWC_MPSK_1	Creating Wlan with WPA2 Security with MPSK	Verify Wlan Creating with WPA2 Security with MPSK	Passed	
EWCJ171S_EWC_MPSK_2	Edit WPA2 Security PSK Keys on MPSK	Verify Wlan Edit with WPA2 Security with MPSK	Passed	
EWCJ171S_EWC_MPSK_3	Delete WPA2 Security PSK Keys on MPSK	Verify Wlan Delete with WPA2 Security with MPSK	Passed	

EWCJ171S_EWC_MPSK_4	Creating Wlan with WPA2 Security with MPSK - Format with Hexa:	Verify Creating Wlan with WPA2 Security with MPSK - Format with Hexa:	Failed	CSCvs61119
EWCJ171S_EWC_MPSK_5	Creating Wlan with WPA2 Security with MPSK - Password Type : AES :	Verify the Security Type with Advance Security	Passed	
EWCJ171S_EWC_MPSK_6	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	
EWCJ171S_EWC_MPSK_7	Connect the MAC Clients	Verify Connect the MAC Clients with all the 5 Key Combinations	Passed	
EWCJ171S_EWC_MPSK_8	Connect the Android Clients	Verify Connect the Android Clients with all the 5 Key Combinations:	Passed	
EWCJ171S_EWC_MPSK_9	Connect the Apple Mobile Clients with all the 5 Key Combinations:	Verify Connect the Apple Clients with all the 5 Key Combinations:	Passed	
EWCJ171S_EWC_MPSK_10	Connect the Windows Clients with all the 5 Key Combinations:	Verify Connect the Windows Clients with all the 5 Key Combinations:	Passed	
EWCJ171S_EWC_MPSK_11	MPSK with Ap Model 9115	Verify the Configurations with Ap Different Ap Model 9115	Passed	
EWCJ171S_EWC_MPSK_12	Connect Ap Model 9120	Verify the Configurations with Ap Different Ap Model 9120:	Passed	
EWCJ171S_EWC_MPSK_13	Connect Ap Model 4800	Verify the Configurations with Ap Different Ap Model 4800:	Passed	

EWCJ171S_EWC_MPSK_14	Connect Ap Model 3800	Verify the Configurations with Ap Different Ap Model 3800	Passed	
EWCJ171S_EWC_MPSK_15	Connect Ap Model 3700	Verify the Configurations with Ap Different Ap Model 3700	Passed	
EWCJ171S_EWC_MPSK_16	Connect Ap Model 1532	Verify the Configurations with Ap Different Ap Model 1532:	Passed	
EWLCJ171S_PSK_M_01	Creating Wlan with WPA2 Security with MPSK	Verify Wlan Creating with WPA2 Security with MPSK	Passed	
EWLCJ171S_PSK_M_02	Edit WPA2 Security PSK Keys on MPSK	Verify Wlan Edit with WPA2 Security with MPSK	Passed	
EWLCJ171S_PSK_M_03	Delete WPA2 Security PSK Keys on MPSK	Verify Wlan Delete with WPA2 Security with MPSK	Passed	
EWLCJ171S_PSK_M_04	Creating Wlan with WPA2 Security with MPSK - Format with Hexa:	Verify Creating Wlan with WPA2 Security with MPSK - Format with Hexa:	Passed	
EWLCJ171S_PSK_M_05	Creating Wlan with WPA2 Security with MPSK - Password Type : AES :	Verify the Security Type with Advance Security	Passed	
EWLCJ171S_PSK_M_06	Verify WPA2 Security with MPSK Applied in Wlan's with Window's Clients with all the 5 Key Combinations	Verify WPA2 Security with MPSK Applied in Wlan's with Window's Clients with all the 5 Key Combinations	Passed	
EWLCJ171S_PSK_M_07	Connect the MAC Clients	Verify Connect the MAC Clients with all the 5 Key Combinations	Passed	

EWLCJ171S_PSK_M_08	Connect the Android Clients	Verify Connect the Android Clients with all the 5 Key Combinations:	Passed	
EWLCJ171S_PSK_M_09	Connect the Apple Mobile Clients with all the 5 Key Combinations:	Verify Connect the Apple Clients with all the 5 Key Combinations:	Passed	
EWLCJ171S_PSK_M_10	Connect the Windows Clients with all the 5 Key Combinations:	Verify Connect the Windows Clients with all the 5 Key Combinations:	Passed	
EWLCJ171S_PSK_M_11	MPSK with Ap Model 9115	Verify the Configurations with Ap Different Ap Model 9115	Passed	
EWLCJ171S_PSK_M_12	Connect Ap Model 9120	Verify the Configurations with Ap Different Ap Model 9120:	Passed	
EWLCJ171S_PSK_M_13	Connect Ap Model 4800	Verify the Configurations with Ap Different Ap Model 4800:	Passed	
EWLCJ171S_PSK_M_14	Connect Ap Model 3800	Verify the Configurations with Ap Different Ap Model 3800	Passed	
EWLCJ171S_PSK_M_15	Connect Ap Model 3700	Verify the Configurations with Ap Different Ap Model 3700	Passed	
EWLCJ171S_PSK_M_16	Connect Ap Model 1532	Verify the Configurations with Ap Different Ap Model 1532:	Passed	

Inter Release Controller Mobility

Logical Id	Title	Description	Status	Defect ID

EWLCJ171S_iRCM_01	Setting UP the secure mobility tunnel between 9800 Controller & 5520 WLC	To check whether both Control & Data path gets UP or not between 9800 Controller & 5520 Controller	Passed	
EWLCJ171S_iRCM_02	Checking the mobility groups configuration after upload/download the config file in 5520 WLC via TFTP	To check whether mobility groups configurations gets retained or not after upload/download the config file via TFTP in 5520 WLC	Passed	
EWLCJ171S_iRCM_03	Checking the mobility groups configuration after backup/restore the config file in 9800 Controller via TFTP	To check whether mobility groups configurations gets retained or not after backup/restore the config file via TFTP in Cat 9800 Controller	Passed	
EWLCJ171S_iRCM_04	Configuring the Anchor controller option in a WLAN in 5520 WLC UI	To check whether Anchor option can be configured or not in a WLAN for WLC's	Passed	
EWLCJ171S_iRCM_05	Configuring the Anchor controller option in 9800 WLC UI	To check whether Anchor option can be configured or not in a 9800 Controller.	Passed	
EWLCJ171S_iRCM_06	Performing Inter Controller roaming of Windows client between 9800 Controller and 5520 WLC	To check whether Inter Controller roaming works properly or not for Windows clients between 5520 WLC and 9800 Controller with secure mobility tunnel config	Passed	

EWLCJ171S_iRCM_07	Performing Inter Controller roaming of Android client between 9800 Controller and 5520 WLC	To check whether Inter Controller roaming works properly or not for Android clients between 5520 WLC and 9800 Controller with secure mobility tunnel config	Passed	
EWLCJ171S_iRCM_08	Checking Inter Controller roaming of Mac Os client between 9800 Controller and 5520 WLC	To check whether Inter Controller roaming works properly or not for Mac os clients between 5520 WLC and 9800 Controller with secure mobility tunnel config	Passed	
EWLCJ171S_iRCM_09	Verifying Inter Controller roaming of different OS clients between 9800 Controller and 5520 WLC with WPA2+dot1x (PEAP)	To check whether Inter Controller roaming works properly or not for clients between 5520 WLC and 9800 Controller with security type WPA2+dot1x (PEAP)	Passed	
EWLCJ171S_iRCM_10	Checking the Anchor controller functionality during the roaming of Windows Client with L2 security-WEP	To check whether Anchor controller functionality works properly or not in Cat 9800 Controller during the roaming of Windows Client	Passed	
EWLCJ171S_iRCM_11	Checking the Anchor controller functionality during the roaming of Android Client with L2 security-WEP	To check whether Anchor controller functionality works properly or not in Cat 9800 Controller during the roaming of Android Client	Passed	

EWLCJ171S_iRCM_12	Checking the Anchor controller functionality during the roaming of IOS Client with L2 security-WEP	To check whether Anchor controller functionality works properly or not in Cat 9800 Controller during the roaming of IOS Client	Passed	
EWLCJ171S_iRCM_13	Checking the Mobility groups configuration in Active/Standby HA WLC	To check whether mobility group configurations gets synced or not in Standby WLC during HA	Passed	
EWLCJ171S_iRCM_14	Checking the Mobility groups configuration in Active/Standby HA WLC	To check whether mobility group configurations gets synced or not in Standby WLC during HA	Passed	
EWLCJ171S_iRCM_15	Checking the Anchor controller functionality during the roaming of Windows Client with L2 security-WPA3-SAE	To check whether Anchor controller functionality works properly or not in Cat 9800 Controller during the roaming of Windows Client with WPA3-SAE security	Passed	
EWLCJ171S_iRCM_16	Checking the Anchor controller functionality during the roaming of Android Client with L2 security-WPA3-SAE	To check whether Anchor controller functionality works properly or not in Cat 9800 Controller during the roaming of Android Client with WPA3-SAE security	Passed	
EWLCJ171S_iRCM_17	Checking the Anchor controller functionality during the roaming of IOS Client with L2 security-WPA3-SAE	To check whether Anchor controller functionality works properly or not in Cat 9800 Controller during the roaming of IOS Client with WPA3-SAE security	Passed	

EWLCJ171S_iRCM_18	Checking Inter Controller roaming of Windows client between 9800 Controller and 3504 WLC	To check whether Anchor controller functionality works properly or not in Cat 9800 Controller during the roaming of Windows Client with WPA3-SAE security	Passed	
EWLCJ171S_iRCM_19	Checking Inter Controller roaming of Android client between 9800 Controller and 3504 WLC	To check whether Anchor controller functionality works properly or not in Cat 9800 Controller during the roaming of Android Client with WPA3-SAE security	Passed	
EWLCJ171S_iRCM_20	Checking Inter Controller roaming of IOS client between 9800 Controller and 3504 WLC	To check whether Anchor controller functionality works properly or not in Cat 9800 Controller during the roaming of IOS Client with WPA3-SAE security	Passed	
EWLCJ171S_iRCM_21	Checking Inter Controller roaming of Windows client between 9800 Controller and 8540 WLC	To check whether Anchor controller functionality works properly or not in Cat 9800 Controller during the roaming of Windows Client with WPA3-SAE security	Passed	
EWLCJ171S_iRCM_22	Checking Inter Controller roaming of Android client between 9800 Controller and 8540 WLC	To check whether Anchor controller functionality works properly or not in Cat 9800 Controller during the roaming of Android Client with WPA3-SAE security	Passed	

EWLCJ171S_iRCM_23	Checking Inter Controller roaming of IOS client between 9800 Controller and 8540 WLC	To check whether Anchor controller functionality works properly or not in Cat 9800 Controller during the roaming of IOS Client with WPA3-SAE security	Passed	

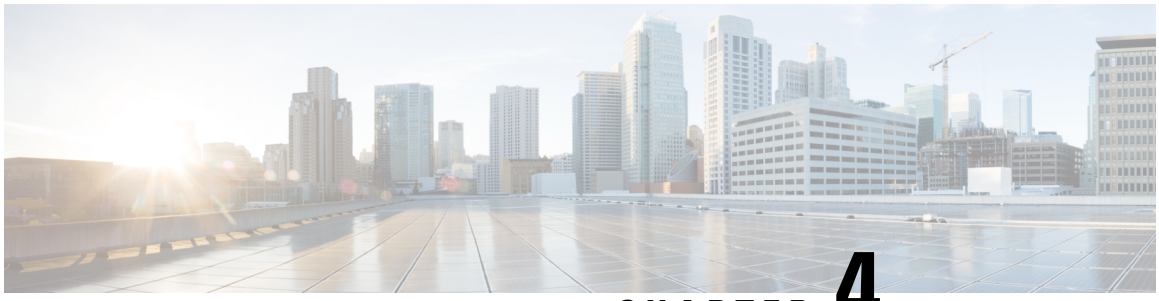
Mesh and Flex+Bridge Support on all Indoor Wave 2 AP's

Logical Id	Title	Description	Status	Defect ID
EWLCJ171S_Mesh_01	Verifying the Mesh configuration.	To check whether the Mesh configurations are configuring correct or not.	Passed	
EWLCJ171S_Mesh_02	Check the Joining of 3800Ap in to Cisco Catalyst 9800 Series Wireless Controller with Mesh /Bridge Mode	To check the Mesh/Bridge support of 3800 Ap after joining in to Cisco Catalyst 9800 Series Wireless Controller	Passed	
EWLCJ171S_Mesh_03	Check the Joining of 3800Ap in to Cisco Catalyst 9800 Series Wireless Controller with Flex+Bridge Mode	To check the Flex+Bridge Mode support of 3800 Ap in to Cisco Catalyst 9800 Series Wireless Controller	Passed	
EWLCJ171S_Mesh_04	Check the Joining of 4800Ap in to Cisco Catalyst 9800 Series Wireless Controller with Mesh/Bridge Mode	To check the Mesh/Bridge support of 4800 Ap after joining in to Cisco Catalyst 9800 Series Wireless Controller	Passed	
EWLCJ171S_Mesh_05	Check the Joining of 4800Ap in to Cisco Catalyst 9800 Series Wireless Controller with Flex+Bridge Mode	To check the Flex+Bridge Mode support of 4800 Ap in to Cisco Catalyst 9800 Series Wireless Controller	Passed	

EWLCJ171S_Mesh_06	Verify the Windows clients connection for bridge mode Ap's with WEP security	To check whether the windows client is connected or not to bridge mode Ap's	Passed	
EWLCJ171S_Mesh_07	Verify the Android clients connection for bridge mode Ap's with WEP security	To check whether the Android client is connected or not to bridge mode Ap's	Passed	
EWLCJ171S_Mesh_08	Verify the IOS clients connection for bridge mode Ap's with WEP security	To check whether the IOS client is connected or not to bridge mode Ap's	Passed	
EWLCJ171S_Mesh_09	Verify the Windows clients connection for Flex+bridge mode Ap's with WEP security	To check whether the windows client is connected or not to Flex+bridge mode Ap's	Passed	
EWLCJ171S_Mesh_10	Verify the Android clients connection for Flex+bridge mode Ap's with WEP security	To check whether the Android client is connected or not to Flex+bridge mode Ap's	Passed	
EWLCJ171S_Mesh_11	Verify the IOS clients connection for Flex+bridge mode Ap's with WEP security	To check whether the IOS client is connected or not to Flex+bridge mode Ap's	Passed	
EWLCJ171S_Mesh_12	Verify the Windows clients connection for bridge mode Ap's with WPA2-PSk security	To check whether the windows client is connected or not to bridge mode Ap's with WPA2-PSK security	Passed	
EWLCJ171S_Mesh_13	Verify the Android clients connection for bridge mode Ap's with WPA2-PSK security	To check whether the Android client is connected or not to bridge mode Ap's with WPA2-PSK security	Passed	

EWLCJ171S_Mesh_14	Verify the IOS clients connection for bridge mode Ap's with WPA2-PSK security	To check whether the IOS client is connected or not to bridge mode Ap's with WPA2-PSK security	Passed	
EWLCJ171S_Mesh_15	Verify the Windows clients connection for Flex+bridge mode Ap's with WPA2-PSK security	To check whether the windows client is connected or not to Flex+bridge mode Ap's with WPA2-PSK security	Passed	
EWLCJ171S_Mesh_16	Verify the Android clients connection for Flex+bridge mode Ap's with WPA2-PSK security	To check whether the Android client is connected or not to Flex+bridge mode Ap's with WPA2-PSK security	Passed	
EWLCJ171S_Mesh_17	Verify the IOS clients connection for Flex+bridge mode Ap's with WPA2-PSK security	To check whether the IOS client is connected or not to Flex+bridge mode Ap's with WPA2-PSK security	Passed	
EWLCJ171S_Mesh_18	Verify the Windows clients connection for bridge mode Ap's with WPA3-SAE security	To check whether the windows client is connected or not to bridge mode Ap's with WPA3-SAE security	Passed	
EWLCJ171S_Mesh_19	Verify the Android clients connection for bridge mode Ap's with WPA3-SAE security	To check whether the Android client is connected or not to bridge mode Ap's with WPA3-SAE security	Passed	
EWLCJ171S_Mesh_20	Verify the IOS clients connection for bridge mode Ap's with WPA3-SAE security	To check whether the IOS client is connected or not to bridge mode Ap's with WPA3-SAE security	Passed	

EWLCJ171S_Mesh_21	Verify the Windows clients connection for Flex+bridge mode Ap's with WPA3-SAE security	To check whether the windows client is connected or not to Flex+bridge mode Ap's with WPA3-SAE security	Passed	
EWLCJ171S_Mesh_22	Verify the Android clients connection for Flex+bridge mode Ap's with WPA3-SAE security	To check whether the Android client is connected or not to Flex+bridge mode Ap's with WPA3-SAEsecurity	Passed	
EWLCJ171S_Mesh_23	Verify the IOS clients connection for Flex+bridge mode Ap's with WPA3-SAE security	To check whether the IOS client is connected or not to Flex+bridge mode Ap's with WPA3-SAE security	Passed	
EWLCJ171S_Mesh_24	Check and verify the Ap mode changes by changing From bridge mode to local	To check whether Ap mode changing or not from bridge to local	Passed	
EWLCJ171S_Mesh_25	Check and verify the Ap mode changes by changing From Flex+bridge mode to Flexconnect.	To check whether Ap mode changing or not from Flex+bridge to Flexconnect.	Passed	
EWLCJ171S_Mesh_26	Check and verify the intra roaming with bridge mode Ap	To check whether intra roaming hAppening or not with bridge mode Ap's	Passed	
EWLCJ171S_Mesh_27	Check and verify the intra roaming with Flex+bridge mode Ap	To check whether intra roaming hAppening or not with Flex+bridge mode Ap's	Passed	



CHAPTER 4

Regression Features - Test Summary

TACACS

Logical ID	Title	Description	Status	Defect ID
EWCJ171S__Reg_01	Allowing the user for complete access to ME Cisco Catalyst 9800 Series Wireless Controller network via TACACS	To check whether user can able to read-write access the complete ME Cisco Catalyst 9800 Series Wireless Controller network or not via TACACS	Passed	
EWCJ171S__Reg_02	Providing the user for lobby admin access to the ME Cisco Catalyst 9800 Series Wireless Controller via TACACS	To check whether user can able to have lobby admin access or not to ME Cisco Catalyst 9800 Series Wireless Controller via TACACS	Passed	
EWCJ171S__Reg_03	Providing the user for monitoring access to the ME Cisco Catalyst 9800 Series Wireless Controller via TACACS	To check whether user can able to have monitoring access (which is read-only) or not to ME Cisco Catalyst 9800 Series Wireless Controller via TACACS	Passed	
EWCJ171S__Reg_04	Trying to login ME Cisco Catalyst 9800 Series Wireless Controller via TACACS with invalid credentials	To check whether user can able to login or not in ME Cisco Catalyst 9800 Series Wireless Controller via TACACS with invalid credentials	Passed	
EWCJ171S__Reg_05	Providing the user for selected access to the ME Cisco Catalyst 9800 Series Wireless Controller via TACACS	To check whether user can able to have access with the selected checkbox's like "WLAN" and "Controller" checkboxes.	Passed	
EWCJ171S__Reg_06	Providing the user for selected access to the ME Cisco Catalyst 9800 Series Wireless Controller via TACACS	To check whether user can able to have access with the selected checkbox's like "Wireless" and "Security" checkboxes.	Passed	
EWCJ171S__Reg_07	Providing the user for selected access to the ME Cisco Catalyst 9800 Series Wireless Controller via TACACS	To check whether user can able to have access with the selected checkbox's like "Command" and "Management" checkboxes.	Passed	

EWCJ171S__Reg_08	Providing the user for selected access to the ME Cisco Catalyst 9800 Series Wireless Controller 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	
EWCJ171S__Reg_09	Trying to login ME Cisco Catalyst 9800 Series Wireless Controller network via TACACS with Invalid credentials.	To verify whether user can able to login or not in ME Cisco Catalyst 9800 Series Wireless Controller via TACACS with invalid credentials	Passed	
EWLCJ171S_Reg_99	Allowing the user for complete access to ME Cisco Catalyst 9800 Series Wireless Controller network via TACACS	To check whether user can able to read-write access the complete ME Cisco Catalyst 9800 Series Wireless Controller network or not via TACACS	Passed	
EWLCJ171S_Reg_100	Providing the user for lobby admin access to the ME Cisco Catalyst 9800 Series Wireless Controller via TACACS	To check whether user can able to have lobby admin access or not to ME Cisco Catalyst 9800 Series Wireless Controller via TACACS	Passed	
EWLCJ171S_Reg_101	Providing the user for monitoring access to the ME Cisco Catalyst 9800 Series Wireless Controller via TACACS	To check whether user can able to have monitoring access (which is read-only) or not to ME Cisco Catalyst 9800 Series Wireless Controller via TACACS	Passed	
EWLCJ171S_Reg_102	Trying to login ME Cisco Catalyst 9800 Series Wireless Controller via TACACS with invalid credentials	To check whether user can able to login or not in ME Cisco Catalyst 9800 Series Wireless Controller via TACACS with invalid credentials	Passed	
EWLCJ171S_Reg_103	Providing the user for selected access to the ME Cisco Catalyst 9800 Series Wireless Controller via TACACS	To check whether user can able to have access with the selected checkbox's like "WLAN" and "Controller" checkboxes.	Passed	
EWLCJ171S_Reg_104	Providing the user for selected access to the ME Cisco Catalyst 9800 Series Wireless Controller via TACACS	To check whether user can able to have access with the selected checkbox's like "Wireless" and "Security" checkboxes.	Passed	
EWLCJ171S_Reg_105	Providing the user for selected access to the ME Cisco Catalyst 9800 Series Wireless Controller via TACACS	To check whether user can able to have access with the selected checkbox's like "Command" and "Management" checkboxes.	Passed	

EWLCJ171S_Reg_106	Providing the user for selected access to the ME Cisco Catalyst 9800 Series Wireless Controller via TACACS	To check whether user can able to have access with the selected checkbox's like"WLAN,Controller,Wireless and "Management" checkboxes.	Passed	
EWLCJ171S_Reg_107	Trying to login ME Cisco Catalyst 9800 Series Wireless Controller network via TACACS with Invalid credentials.	To verify whether user can able to login or not in ME Cisco Catalyst 9800 Series Wireless Controller via TACACS with invalid credentials	Passed	

Hotspot 2.0

Logical ID	Title	Description	Status	Defect ID
EWCJ171S__Reg_55	Enabling the Internet Access WLAN and connecting a client	To verify whether Internet Access mode is enabled or not	Passed	
EWCJ171S__Reg_56	Configuring the Network type from one to another	To verify whether client connecting or not with network type changes from one to other	Passed	
EWCJ171S__Reg_57	Configuring the Network Authentication	To verify whether Client is connecting after Network Authentication or not	Passed	
EWCJ171S__Reg_58	Checking with IPv4 type details	To verify whether Client connecting or not after IPv4 type changes from one to another	Passed	
EWCJ171S__Reg_59	Creating OUI with Duplicate name	To verify whether OUI is creating with duplicate name or not	Passed	
EWCJ171S__Reg_60	Configuring the NAI-relam and Eap-methods.	To verify whether client will connect with NAI-relam credentials or not	Passed	
EWCJ171S__Reg_61	Adding cellular network information with duplicate name	To verify whether Cellular network information added successfully	Passed	

EWCJ171S__Reg_62	Configuring the OSU SSID	To verify whether OSU SSID applying or not	Passed	
EWCJ171S__Reg_63	Configuring the OSU Provider information	To verify whether OSU Provider information applying or not	Passed	
EWCJ171S__Reg_64	Configure the WAN metrics.	To verify whether WAN status is varying or not	Passed	
EWCJ171S__Reg_65	Varying Port configurations	To verify whether Port configurations can vary after client connect	Passed	
EWCJ171S__Reg_66	Downgrading the AP after Hotspot configurations	To verify whether Client connected or not after downgrade with Hotspot	Passed	
EWCJ171S__Reg_67	Upgrading the AP after Hotspot configurations	To verify whether all hotspot details are showing properly or not	Passed	
EWCJ171S__Reg_68	Changing the AP modes after Client connect to Hotspot	To verify whether client will connect or not after modes changes in AP	Passed	
EWCJ171S__Reg_69	Configure the Venue name and URL.	To verify whether venue name or Url applying or not.	Passed	
EWCJ171S__Reg_70	Configure the Domain name.	To verify whether Domain name applying or not.	Passed	
EWCJ171S__Reg_71	Checking the Roaming after roaming-oi configurations	To verify whether client will roam between hotspots or not	Passed	
EWCJ171S__Reg_72	Configure the Operating class	To verify whether operating class configured or not.	Passed	
EWCJ171S__Reg_73	Configure the Icon for the Hotspot	To verify whether Icon configured successfully or not.	Passed	

EWLCJ171S_Reg_07	Configure Mesh setup and the Network type from one to another	To verify that Mesh setup configured and client connecting or not with network type changes from one to other	Passed	
EWLCJ171S_Reg_08	Enabling the Internet Access WLAN and connecting client	To verify whether Internet Access mode is enabled or not	Passed	
EWLCJ171S_Reg_09	Configuring the Network type from one to another	To verify whether client connecting or not with network type changes from one to other	Passed	
EWLCJ171S_Reg_10	Configuring the Network Authentication	To verify whether Client is connecting after Network Authentication or not	Passed	
EWLCJ171S_Reg_11	Checking with IPv4 type details	To verify whether Client connecting or not after IPv4 type changes from one to another	Passed	
EWLCJ171S_Reg_12	Creating OUI with Duplicate name	To verify whether OUI is creating with duplicate name or not	Passed	
EWLCJ171S_Reg_13	Configuring the NAI-relam and Eap-methods.	To verify whether client will connect with NAI-relam credentials or not	Passed	
EWLCJ171S_Reg_14	Adding cellular network information with duplicate name	To verify whether Cellular network information added successfully	Passed	
EWLCJ171S_Reg_15	Configuring the OSU SSID	To verify whether OSU SSID applying or not	Passed	
EWLCJ171S_Reg_16	Configuring the OSU Provider information	To verify whether OSU Provider information applying or not	Passed	

EWLCJ171S_Reg_17	Configure the WAN metrics.	To verify whether WAN status is varying or not	Passed	
EWLCJ171S_Reg_18	Varying Port configurations	To verify whether Port configurations can vary after client connect	Passed	
EWLCJ171S_Reg_19	Downgrading the AP after Hotspot configurations	To verify whether Client connected or not after downgrade with Hotspot	Passed	
EWLCJ171S_Reg_20	Upgrading the AP after Hotspot configurations	To verify whether all hotspot details are showing properly or not	Passed	
EWLCJ171S_Reg_21	Changing the AP modes after Client connect to Hotspot	To verify whether client will connect or not after modes changes in AP	Passed	
EWLCJ171S_Reg_22	Configure the Venue name and URL.	To verify whether venue name or Url applying or not.	Passed	
EWLCJ171S_Reg_23	Configure the Domain name.	To verify whether Domain name applying or not.	Passed	
EWLCJ171S_Reg_24	Checking the Roaming after roaming-oi configurations	To verify whether client will roam between hotspots or not	Passed	
EWLCJ171S_Reg_25	Configure the Operating class	To verify whether operating class configured or not.	Passed	

Mac filtering (for L2 security)

Logical ID	Title	Description	Status	Defect ID
EWCJ171S__Reg_101	Adding Windows 10 Client mac address in eWC and checking the connection of Clients	To add the windows Client mac address in mac filtering in eWC and checking whether Clients gets associated or not successfully in	Passed	

EWCJ171S__Reg_102	Uploading the empty CSV file in eWC UI	To check whether an blank CSV file could be uploaded in eWC UI	Passed	
EWCJ171S__Reg_103	Importing the .CSV file with modifications in eWC	To check whether .CSV file gets imported or not after importing the updated file with some changes in it	Passed	
EWCJ171S__Reg_104	Connecting the Client with wlan security mac filtering + WPA personal	To Connect the Client with wlan security mac filtering + WPA personal	Passed	
EWCJ171S__Reg_105	Connecting the Client with wlan security mac filtering + WPA enterprise	To Connect the Client with wlan security mac filtering + WPA enterprise	Passed	
EWCJ171S__Reg_106	Connecting the Client with Wlan Security Type as WPA Enterprise enabling MAC Filtering option Choosing Authentication Server as External Radius and RADIUS Compatibility as other	To Connect the Client with MAC Filtering using WPA Enterprise as security type choosing Authentication Server as External Radius and RADIUS Compatibility as other	Passed	
EWCJ171S__Reg_107	Connecting the client after client identity account expired in ISE	To Connect the Client after client identity account expired in ISE	Passed	
EWCJ171S__Reg_108	Connecting the Client and then moving it to block using MAC address	To Connect the client and then blocking it using the MAC address	Failed	CSCvs43441

EWLCJ171S_Reg_138	Adding Windows 10 Client mac address in Cisco Catalyst 9800 Series Wireless Controller-ME and checking the connection of Clients in 1800 Series ME	To add the windows Client mac address in mac filtering in Cisco Catalyst 9800 Series Wireless Controller UI and checking whether Clients gets associated or not successfully	Passed	
EWLCJ171S_Reg_139	Uploading the empty CSV file in Cisco Catalyst 9800 Series Wireless Controller UI	To check whether an blank CSV file could be uploaded in Cisco Catalyst 9800 Series Wireless Controller UI	Passed	
EWLCJ171S_Reg_140	Importing the .CSV file with modifications in Cisco Catalyst 9800 Series Wireless Controller UI	To check whether .CSV file gets imported or not after importing the updated file with some changes in it	Passed	
EWLCJ171S_Reg_141	Connecting the Client with wlan security mac filtering + WPA personal	To Connect the Client with wlan security mac filtering + WPA personal	Passed	
EWLCJ171S_Reg_142	Connecting the Client with wlan security mac filtering + WPA enterprise	To Connect the Client with wlan security mac filtering + WPA enterprise	Passed	
EWLCJ171S_Reg_143	Connecting the Client with WLAN as MAC Filtering+WPA Enterprise Choosing Authentication Server as AP	To Connect the Client with MAC Filtering using WPA Enterprise as security type choosing Authentication Server as AP	Passed	

EWLCJ171S_Reg_144	Connecting the Client with Wlan Security Type as WPA Enterprise enabling MAC Filtering option Choosing Authentication Server as External Radius and RADIUS Compatibility as other	To Connect the Client with MAC Filtering using WPA Enterprise as security type choosing Authentication Server as External Radius and RADIUS Compatibility as other	Passed	
EWLCJ171S_Reg_145	Connecting the client after client identity account expired in ISE	To Connect the Client after client identity account expired in ISE	Passed	
EWLCJ171S_Reg_146	Connecting the Client and then moving it to block using MAC address	To Connect the client and then blocking it using the MAC address	Passed	

Syslogs

Logical ID	Title	Description	Status	Defect ID
EWCJ171S__Reg_185	Enabling logging for Errors in Cisco Catalyst 9800 Series Wireless Controller-ME	To check whether log can be generated or not for Error Message in Cisco Catalyst 9800 Series Wireless Controller-ME GUI	Passed	
EWCJ171S__Reg_186	Disabling logging for Errors in Cisco Catalyst 9800 Series Wireless Controller-ME	To check whether logging for Errors disabled or not in Cisco Catalyst 9800 Series Wireless Controller-ME	Passed	
EWCJ171S__Reg_187	Enabling logging for Debugging in Cisco Catalyst 9800 Series Wireless Controller-ME	To check whether log can be generated or not for Debug Message in Cisco Catalyst 9800 Series Wireless Controller-ME GUI	Passed	

EWCJ171S__Reg_188	Enabling logging server for Emergencies	To check whether log can be generated or not for Emergencies in Cisco Catalyst 9800 Series Wireless Controller-ME GUI	Passed	
EWCJ171S__Reg_189	Enabling logging for Alerts	To check whether log can be generated or not for alerts in Cisco Catalyst 9800 Series Wireless Controller-ME GUI	Passed	
EWCJ171S__Reg_190	Enabling logging for Warning	To check whether log can be generated or not for warning in Cisco Catalyst 9800 Series Wireless Controller-ME GUI	Passed	
EWCJ171S__Reg_191	Enabling logging for Critical	To check whether log can be generated or not for critical events in Cisco Catalyst 9800 Series Wireless Controller-ME GUI	Passed	
EWCJ171S__Reg_192	Enabling logging for Notification	To check whether log can be generated or not for notification in Cisco Catalyst 9800 Series Wireless Controller-ME GUI	Passed	
EWCJ171S__Reg_193	Enabling logging for Information message	To check whether log can be generated or not for Informational message in Cisco Catalyst 9800 Series Wireless Controller-ME GUI	Passed	
EWCJ171S__Reg_194	Checking the validation of syslog errors in PI	To check whether the syslog errors are displayed in PI	Passed	

EWCJ171S_Reg_195	Checking the validation of syslog information in PI	To check whether the syslog information are displayed in PI	Passed	
EWCJ171S_Reg_196	Checking the historic information about syslog in PI	To check whether the historic information about syslog in PI	Passed	
EWCJ171S_Reg_197	Validating the syslog warning message in PI	To check whether the syslog warning message in PI	Passed	
EWCJ171S_Reg_198	Validating the syslog notification in PI	To check whether syslog notification in PI	Passed	
EWCJ171S_Reg_199	Verifying the severity filtering for syslog in PI	To verify the severity filtering for syslog in PI	Passed	
EWCJ171S_Reg_200	Verifying the Device IP address filtering for syslog in PI	To verify the Device IP address filtering for syslog in PI	Passed	
EWLCJ171S_Reg_281	Adding syslog server in Cisco Catalyst 9800 Series Wireless Controller and checking the syslog messages in syslog server	To check whether syslog's are generating in syslog server after adding in Cisco Catalyst 9800 Series Wireless Controller	Passed	
EWLCJ171S_Reg_282	Configuring multiple syslog servers in Cisco Catalyst 9800 Series Wireless Controller and checking the syslog messages in syslog server	To verify whether syslog's are generating in syslog server after adding multiple servers in Cisco Catalyst 9800 Series Wireless Controller	Passed	
EWLCJ171S_Reg_283	Downloading the syslog's after generated in Cisco Catalyst 9800 Series Wireless Controller	To check whether able to download the syslog's from Cisco Catalyst 9800 Series Wireless Controller	Passed	

EWLCJ171S_Reg_284	Clearing the logs in controller after generated successfully	To verify whether user able to clear the all generated logs in Cisco Catalyst 9800 Series Wireless Controller	Passed	
EWLCJ171S_Reg_285	Checking the alert messages after configured syslog server level as "alert"	To check the alert syslog's in syslog server after configured severity level as alert	Passed	
EWLCJ171S_Reg_286	Configuring syslog servers in Cisco Catalyst 9800 Series Wireless Controller with log level setting as critical	To verify the critical logs in syslog server after configuration in device	Passed	
EWLCJ171S_Reg_287	Checking the information messages after configured syslog server level as "information"	To check the information syslog's in syslog server after configured severity level as information	Passed	
EWLCJ171S_Reg_288	Checking the debugging messages after configured syslog server level as "debugging"	To check the debugging syslog's in syslog server after configured severity level as debugging	Passed	

NAT

Logical ID	Title	Description	Status	Defect ID
EWCJ171S__Reg_212	Associating the DHCP Interface	To verify whether DHCP Scope is associate the Interface or not	Passed	
EWCJ171S__Reg_213	Peer-to-peer blocking the configuration on DHCP through CLI	To verify whether Peer-to-peer blocking applied successfully or not	Passed	
EWCJ171S__Reg_214	Configuring the NAT functionality in radio 2.4GHZ band for AP	To verify whether NATing working or not in 2.4 GHZ radio band	Passed	

EWCJ171S__Reg_215	Configuring the NAT functionality in radio 5GHZ band AP	To verify whether NATing working or not in 5 GHZ radio band	Passed	
EWCJ171S__Reg_216	Cheking Client performance in Monitoring page after client connect	To verify whether Client performance is showing or not in monitoring page	Passed	
EWCJ171S__Reg_217	Checking the Connection and event log after client connect	To verify whether Connection showing properly or not	Passed	

Rogue AP

Logical ID	Title	Description	Status	Defect ID
EWCJ171S__Reg_280	Configuring the rogue AP rule in eWC via CLI	To verify that user is able to configure the rogue AP rule in eWC via CLI or not	Passed	
EWCJ171S__Reg_281	Enabling/disabling rogue detection on eWC CLI	To verify that user is able to enable/disable rogue detection on eWC or not	Passed	
EWCJ171S__Reg_282	Classifying the rogue Client on eWC after Client connect	To verify that user is able to classify rogue Client on eWC or not	Passed	
EWCJ171S__Reg_283	Verifying that on the basis of rogue AP rule	To verify that user is able to classify rogue AP on the basis of rogue rule or not	Passed	
EWCJ171S__Reg_284	Verifying the special character names rogue devices	To verifying that special character names rogue devices are Appearing under rogue AP or not	Passed	
EWCJ171S__Reg_285	After Appearing the rogue AP in eWC ,Updating the their class	To verifying that user is able to update the rogue AP's class or not	Passed	

EWCJ171S__Reg_286	Manual mitigation of rogue device	Verify that user is able to manually mitigate the rogue AP or not	Passed	
EWCJ171S__Reg_287	Auto mitigation of rogue device	Verify that user is able to auto mitigate the rogue AP or not	Passed	
EWCJ171S__Reg_288	Classifying the rogue Adhoc on eWC	Verify that user is able to classify rogue Adhoc on eWC or not	Passed	
EWCJ171S__Reg_289	Deleting the specific rogue AP or all rogue from eWC	Verify that user is able to delete the rogue specific rogue AP or all rogue AP from eWC or not	Passed	

Internal DHCP Server

Logical ID	Title	Description	Status	Defect ID
EWCJ171S__Reg_133	Mapping a Internal DHCP pool to WLAN and verifying Windows Client IP Address and vlan id	To verify whether a window client get Ip address and vlan id from a specified DHCP pool or not	Passed	
EWCJ171S__Reg_134	Mapping a Internal DHCP pool to WLAN and verifying Android Client IP Address and vlan id	To verify whether a Android client get Ip address and vlan id from a specified DHCP pool or not	Passed	
EWCJ171S__Reg_135	Mapping a Internal DHCP pool to WLAN and verifying MAC Client IP Address and vlan id	To verify whether a MAC Os client get Ip address and vlan id from a specified DHCP pool or not	Passed	
EWCJ171S__Reg_136	Mapping a Internal DHCP pool to WLAN and verifying iOS Client IP Address and vlan id	To verify whether a iOS client get Ip address and vlan id from a specified DHCP pool or not	Passed	

EWCJ171S__Reg_137	Checking lease period for connected Client through a DHCP pool	To verify whether DHCP release a particular IP address or not after a certain lease period for client	Passed	
EWLCJ171S_Reg_211	Mapping a Internal DHCP pool to WLAN and verifying Windows Client IP Address and vlan id	To verify whether a window client get Ip address and vlan id from a specified DHCP pool or not	Passed	
EWLCJ171S_Reg_212	Mapping a Internal DHCP pool to WLAN and verifying Android Client IP Address and vlan id	To verify whether a Android client get Ip address and vlan id from a specified DHCP pool or not	Passed	
EWLCJ171S_Reg_213	Mapping a Internal DHCP pool to WLAN and verifying MAC Client IP Address and vlan id	To verify whether a MAC Os client get Ip address and vlan id from a specified DHCP pool or not	Passed	
EWLCJ171S_Reg_214	Mapping a Internal DHCP pool to WLAN and verifying iOS Client IP Address and vlan id	To verify whether a iOS client get Ip address and vlan id from a specified DHCP pool or not	Passed	
EWLCJ171S_Reg_215	Checking lease period for connected Client through a DHCP pool	To verify whether DHCP release a particular IP address or not after a certain lease period for client	Passed	

Open DNS

Logical ID	Title	Description	Status	Defect ID

EWLCJ171S_OpenDNS_01	Verifying Cisco Catalyst 9800 Series Wireless Controller registered with open DNS server	To Verify whether the Cisco Catalyst 9800 Series Wireless Controller registered in open DNS and Cisco Catalyst 9800 Series Wireless Controller got the device ID or not	Passed	
EWLCJ171S_OpenDNS_02	Verifying the created profile mapped with Cisco Catalyst 9800 Series Wireless Controller GUI and CLI	To Verify whether the profile mapped with Cisco Catalyst 9800 Series Wireless Controller and reflected in Cisco Catalyst 9800 Series Wireless Controller GUI & CLI or not	Passed	
EWLCJ171S_OpenDNS_03	Verifying the WLAN created with open DNS configuration	To verify whether the WLAN created with open DNS configuration or not	Passed	
EWLCJ171S_OpenDNS_04	Verifying the open DNS configuration for the connected Windows Client in Cisco Catalyst 9800 Series Wireless Controller UI/CLI	To Verify whether the open DNS configured or not when Windows JOS connected to Umbrella enabled WLAN Profile	Passed	
EWLCJ171S_OpenDNS_05	Verifying the open DNS configuration for the connected MAC OS Client in Cisco Catalyst 9800 Series Wireless Controller UI/CLI	To Verify whether the open DNS configured or not when MAC OS connected to Umbrella enabled WLAN Profile	Passed	
EWLCJ171S_OpenDNS_06	Verifying the open DNS configuration for the connected iOS Client in Cisco Catalyst 9800 Series Wireless Controller UI/CLI	To Verify whether the open DNS configured or not when iOS client connected to Umbrella enabled WLAN Profile	Passed	

EWLCJ171S_OpenDNS_07	Verifying the open DNS configuration for the connected Android Client in Cisco Catalyst 9800 Series Wireless Controller UI/CLI	To Verify whether the open DNS configured or not when Android client connected to Umbrella enabled WLAN Profile	Passed	
EWLCJ171S_OpenDNS_08	clear the data plane stats in open DNS configuration	To verify whether the data plate stats is cleared or not	Passed	
EWLCJ171S_OpenDNS_09	Perform the roaming between 9115 & 9120 Aps	To verify the open DNs configuration after client roaming between 9115 & 9120 Aps	Passed	
EWLCJ171S_OpenDNS_10	Perform the roaming between two Cisco Catalyst 9800 Series Wireless Controller	To verify the open dns after Inter roaming	Passed	

Maximum number of clients per WLAN/radio

Logical ID	Title	Description	Status	Defect ID
EWCJ171S__Reg_274	Configuring maximum Allowed Clients Per AP Radio as 4 and connecting client with WPA 2 Personal security.	To configure maximum allowed client Per AP radio as 4 and connecting 5 different client with radio policy as ALL and check if the number of client that is configured alone gets connected to the WLAN	Passed	

EWCJ171S__Reg_275	Configuring maximum Allowed Clients Per AP Radio as 3 and connecting client with WPA 2 Enterprise security .	To configure maximum allowed client Per AP radio as 3 and connecting 4 different client with radio policy as ALL and now after 3 client disconnect one client and check if other client get authenticated to the WLAN	Passed	
EWCJ171S__Reg_276	Configuring maximum Allowed Clients Per AP Radio in RF profile as 4 and in WLAN as 3 and connecting the client	To configure maximum allowed client Per AP radio in RF profile and also setting the same in WLAN and check which of the configured number of clients gets connected .	Passed	
EWCJ171S__Reg_277	Creating WPA 2 Personal security WLAN with radio policy as 5 GHz and configuring Maximum Allowed Clients Per AP Radio	To configure maximum allowed client per AP radio setting the WLAN security with WPA 2 Personal and radio policy as 5 GHz and check if only the defined number of client alone connect to the WLAN.	Passed	
EWCJ171S__Reg_278	Creating WPA 2 Enterprise security WLAN with radio policy as 5 GHz and configuring Maximum Allowed Clients Per AP Radio	To configure maximum allowed client per AP radio setting the WLAN security with WPA 2 Enterprise and radio policy as 5 GHz and check if only the defined number of client alone connect to the WLAN.	Passed	

EWCJ171S__Reg_279	Creating WPA 2 Personal security WLAN with radio policy as 2.4 GHz and configuring Maximum Allowed Clients Per AP Radio	To create WPA 2 Personal security WLAN configuring Maximum allowed client per AP radio with radio policy as 2.4 GHz and check if only the defined number of client alone connect to the WLAN.	Passed	
EWLCJ171S_Reg_250	Configuring maximum Allowed Clients Per AP Radio as 4 and connecting client with WPA 2 Personal security.	To configure maximum allowed client Per AP radio as 4 and connecting 5 different client with radio policy as ALL and check if the number of client that is configured alone gets connected to the WLAN	Passed	
EWLCJ171S_Reg_251	Configuring maximum Allowed Clients Per AP Radio as 3 and connecting client with WPA 2 Enterprise security .	To configure maximum allowed client Per AP radio as 3 and connecting 4 different client with radio policy as ALL and now after 3 client disconnect one client and check if other client get authenticated to the WLAN	Passed	
EWLCJ171S_Reg_252	Configuring maximum Allowed Clients Per AP Radio in RF profile as 4 and in WLAN as 3 and connecting the client	To configure maximum allowed client Per AP radio in RF profile and also setting the same in WLAN and check which of the configured number of clients gets connected .	Passed	

EWLCJ171S_Reg_253	Creating WPA 2 Personal security WLAN with radio policy as 5 GHz and configuring Maximum Allowed Clients Per AP Radio	To configure maximum allowed client per AP radio setting the WLAN security with WPA 2 Personal and radio policy as 5 GHz and check if only the defined number of client alone connect to the WLAN.	Passed	
EWLCJ171S_Reg_254	Creating WPA 2 Enterprise security WLAN with radio policy as 5 GHz and configuring Maximum Allowed Clients Per AP Radio	To configure maximum allowed client per AP radio setting the WLAN security with WPA 2 Enterprise and radio policy as 5 GHz and check if only the defined number of client alone connect to the WLAN.	Passed	
EWLCJ171S_Reg_255	Creating WPA 2 Personal security WLAN with radio policy as 2.4 GHz and configuring Maximum Allowed Clients Per AP Radio	To create WPA 2 Personal security WLAN configuring Maximum allowed client per AP radio with radio policy as 2.4 GHz and check if only the defined number of client alone connect to the WLAN.	Passed	

SNMP trap receivers

Logical ID	Title	Description	Status	Defect ID
EWCJ171S__Reg_179	Create the SNMP trap receiver name with invalid IP address.	To check whether the SNMP trap receiver is created with invalid IP address or not in CME GUI	Passed	

EWCJ171S__Reg_180	Create the SNMP trap receiver name is the more than 31 characters in CME ui.	To check whether the SNMP trap receiver is created with more than 31 characters or not in CME GUI	Passed	
EWCJ171S__Reg_181	Checking the validation of SNMP trap receiver information.	To check whether the SNMP trap receiver is received the information or not.	Passed	
EWCJ171S__Reg_182	Verifying the severity filtering for SNMP trap receiver information.	To verify the severity filtering for SNMP trap receiver information.	Passed	
EWCJ171S__Reg_183	Verifying the Device IP address filtering for SNMP trap receiver in PI	To verify the Device IP address filtering for SNMP trap receiver in PI	Passed	
EWCJ171S__Reg_184	Create the SNMP trap receiver by using the invalid IP address in CME CLI.	To check whether the SNMP trap receiver is created or not in CME CLI	Passed	
EWLCJ171S_Reg_205	Create the SNMP trap receiver name with invalid IP address.	To check whether the SNMP trap receiver is created with invalid IP address or not in CME GUI	Passed	
EWLCJ171S_Reg_206	Create the SNMP trap receiver name is the more than 31 characters in CME ui.	To check whether the SNMP trap receiver is created with more than 31 characters or not in CME GUI	Passed	
EWLCJ171S_Reg_207	Checking the validation of SNMP trap receiver information.	To check whether the SNMP trap receiver is received the information or not.	Passed	
EWLCJ171S_Reg_208	Verifying the severity filtering for SNMP trap receiver information.	To verify the severity filtering for SNMP trap receiver information.	Passed	

EWLCJ171S_Reg_209	Verifying the Device IP address filtering for SNMP trap receiver in PI	To verify the Device IP address filtering for SNMP trap receiver in PI	Passed	
EWLCJ171S_Reg_210	Create the SNMP trap receiver by using the invalid IP address in CME CLI.	To check whether the SNMP trap receiver is created or not in CME CLI	Passed	

CWA (Central Web Authentication)

Logical ID	Title	Description	Status	Defect ID
EWCJ171S__Reg_224	Creating a CWA along with ACL Configuration in eWC UI	To check Whether CWA along with ACL Configuration in eWC UI created or not	Passed	
EWCJ171S__Reg_225	Associating a Japanese Windows Client to a SSID which is mapped with ISE	To verify whether Japanese Windows Client which is mapped to ISE is redirected successfully or not	Passed	
EWCJ171S__Reg_226	Associating a iOS Client to a SSID which is mapped with ISE	To verify whether iOS Client which is mapped to ISE is redirected successfully or not	Passed	
EWCJ171S__Reg_227	Associating a Android Client to a SSID which is mapped with ISE	To verify whether Android Client which is mapped to ISE is redirected successfully or not	Passed	
EWCJ171S__Reg_228	Associating a MAC OS Client to a SSID which is mapped with ISE	To verify whether MAC Client which is mapped to ISE is redirected successfully or not	Passed	

EWCJ171S__Reg_229	Associating a different Clients to SSID which is mapped with ISE and redirecting to Guest portal page with invalid credentials	To verify whether client connected to ssid redirecting to Guest portal page with invalid credentials	Passed	
EWCJ171S__Reg_230	Associating a different Clients to a SSID which is mapped with ISE by creating AVC profile	To verify whether different Clients is redirected successfully and checking that particular application is dropped or not	Passed	
EWCJ171S__Reg_231	Associating a different Clients to a SSID which is mapped with ISE by denying the action in ACL	To verify whether Clients gets denied when it is connected to SSID which is mapped with ISE	Passed	
EWCJ171S__Reg_232	Associating a different Clients to a SSID which is mapped with ISE by permitting the action in ACL using TCP protocol	To verify whether Clients gets connected to SSID which is mapped with ISE by permitting the action in ACL using TCP protocol	Passed	
EWCJ171S__Reg_233	Associating a different Clients to a SSID which is mapped with ISE by permitting the action in ACL using UDP protocol	To verify whether Clients gets connected to SSID which is mapped with ISE by permitting the action in ACL using UDP protocol	Passed	
EWCJ171S__Reg_234	Associating a different Clients to a SSID which is mapped with ISE by permitting the action in ACL using ICMP protocol	To verify whether Clients gets connected to SSID which is mapped with ISE by permitting the action in ACL using ICMP protocol	Passed	

EWCJ171S__Reg_235	Checking the expired Radius Guest User for proper error message	To verify whether the expired Guest user gets proper Error messages when he logging in	Passed	
EWCJ171S__Reg_236	Validate whether eWC is switch between configured Radius servers	To verify whether AAA authentication is occurring when one radius server goes down	Passed	
EWCJ171S__Reg_237	Reboot the Controller after CWA enabling	To verify whether Configurations are showing same or different after controller reboot	Passed	
EWCJ171S__Reg_238	Creating a CWA along with ACL Configuration through CLI	To verify whether ACL rule is created or not through CLI	Passed	
EWCJ171S__Reg_239	Checking the configuration of CWA when the user is in Read-only	To verify whether configuration display error message or not when the user is in Read-only	Passed	
EWCJ171S__Reg_240	Exporting/Importing configuration of CWA	To verify whether export and import is done successfully	Passed	
EWLCJ171S_Reg_216	Creating a CWA along with ACL Configuration in Cisco Catalyst 9800 Series Wireless Controller UI	To check Whether CWA along with ACL Configuration in Cisco Catalyst 9800 Series Wireless Controller UI created or not	Passed	
EWLCJ171S_Reg_217	Associating a Japanese Windows Client to a SSID which is mapped with ISE	To verify whether Japanese Windows Client which is mapped to ISE is redirected successfully or not	Passed	
EWLCJ171S_Reg_218	Associating a iOS Client to a SSID which is mapped with ISE	To verify whether iOS Client which is mapped to ISE is redirected successfully or not	Passed	

EWLCJ171S_Reg_219	Associating a Android Client to a SSID which is mapped with ISE	To verify whether Android Client which is mapped to ISE is redirected successfully or not	Passed	
EWLCJ171S_Reg_220	Associating a MAC OS Client to a SSID which is mapped with ISE	To verify whether MAC Client which is mapped to ISE is redirected successfully or not	Passed	
EWLCJ171S_Reg_221	Associating a different Clients to SSID which is mapped with ISE and redirecting to Guest portal page with invalid credentials	To verify whether client connected to ssid redirecting to Guest portal page with invalid credentials	Passed	
EWLCJ171S_Reg_222	Associating a different Clients to a SSID which is mapped with ISE by creating AVC profile	To verify whether different Clients is redirected successfully and checking that particular application is dropped or not	Passed	
EWLCJ171S_Reg_223	Associating a different Clients to a SSID which is mapped with ISE by denying the action in ACL	To verify whether Clients gets denied when it is connected to SSID which is mapped with ISE	Passed	
EWLCJ171S_Reg_224	Associating a different Clients to a SSID which is mapped with ISE by permitting the action in ACL using TCP protocol	To verify whether Clients gets connected to SSID which is mapped with ISE by permitting the action in ACL using TCP protocol	Passed	
EWLCJ171S_Reg_225	Associating a different Clients to a SSID which is mapped with ISE by permitting the action in ACL using UDP protocol	To verify whether Clients gets connected to SSID which is mapped with ISE by permitting the action in ACL using UDP protocol	Passed	

EWLCJ171S_Reg_226	Associating a different Clients to a SSID which is mapped with ISE by permitting the action in ACL using ICMP protocol	To verify whether Clients gets connected to SSID which is mapped with ISE by permitting the action in ACL using ICMP protocol	Passed	
EWLCJ171S_Reg_227	Checking the expired Radius Guest User for proper error message	To verify whether the expired Guest user gets proper Error messages when he logging in	Passed	
EWLCJ171S_Reg_228	Validate whether Cisco Catalyst 9800 Series Wireless Controller is switch between configured Radius servers	To verify whether AAA authentication is occurring when one radius server goes down	Passed	
EWLCJ171S_Reg_229	Reboot the Controller after CWA enabling	To verify whether Configurations are showing same or different after controller reboot	Passed	
EWLCJ171S_Reg_230	Creating a CWA along with ACL Configuration through CLI	To verify whether ACL rule is created or not through CLI	Passed	
EWLCJ171S_Reg_231	Checking the configuration of CWA when the user is in Read-only	To verify whether configuration display error message or not when the user is in Read-only	Passed	
EWLCJ171S_Reg_232	Exporting/Importing configuration of CWA	To verify whether export and import is done successfully	Passed	

AAA Override of VLAN Name-id template

Logical ID	Title	Description	Status	Defect ID

EWCJ171S_Reg_109	Enable AAA override and connecting a JOS window 7 client to the AAA override enabled WLAN with WPA 2 Personal security .	To enable AAA override and connecting a JOS window 7 client to the AAA override enabled with WPA 2 Personal security WLAN and check if the VLAN from AAA server is overridden to the client	Passed	
EWCJ171S_Reg_110	Enable AAA override and connecting a Android client to the AAA override enabled WLAN with WPA 2 Personal security .	To enable AAA override and connecting a Android client to the AAA override enabled with WPA 2 Personal security WLAN and check if the VLAN from AAA server is overridden to the client	Passed	
EWCJ171S_Reg_111	Enable AAA override and connecting a IOS client to the AAA override enabled WLAN with WPA 2 Personal security .	To enable AAA override and connecting a IOS client to the AAA override enabled with WPA 2 Personal security WLAN and check if the VLAN from AAA server is overridden to the client	Passed	
EWCJ171S_Reg_112	Enable AAA override and connecting a Mac OS client to the AAA override enabled WLAN with WPA 2 Personal security .	To enable AAA override and connecting a Mac OS client to the AAA override enabled with WPA 2 Personal security WLAN and check if the VLAN from AAA server is overridden to the client	Passed	

EWCJ171S__Reg_113	Connecting a JOS window 7 client to the AAA override enabled WLAN with WPA 2 Enterprise security enabled with AAA override .	To connect a JOS Window 7 client to AAA override enabled WLAN with WPA 2 Enterprise security and check if the Native VLAN is overridden or not.	Passed	
EWCJ171S__Reg_114	Connecting a Android client to the AAA override enabled WLAN with WPA 2 Enterprise security enabled with AAA override .	To connect a Android client to AAA override enabled WLAN with WPA 2 Enterprise security and check if the Native VLAN is overridden or not.	Passed	
EWCJ171S__Reg_115	Connecting a IOS client to the AAA override enabled WLAN with WPA 2 Enterprise security enabled with AAA override .	To connect a IOS client to AAA override enabled WLAN with WPA 2 Enterprise security and check if the Native VLAN is overridden or not.	Passed	
EWCJ171S__Reg_116	Connecting a MacOS client to the AAA override enabled WLAN with WPA 2 Enterprise security enabled with AAA override .	To connect a Mac OS client to AAA override enabled WLAN with WPA 2 Enterprise security and check if the Native VLAN is overridden or not.	Passed	
EWLCJ171S_Reg_289	Enable AAA override and connecting a JOS window 10 client to the AAA override enabled WLAN with WPA 2 Personal security .	To enable AAA override and connecting a JOS window 10 client to the AAA override enabled with WPA 2 Personal security WLAN and check if the VLAN from AAA server is overridden to the client	Passed	

EWLCJ171S_Reg_290	Enable AAA override and connecting a Android client to the AAA override enabled WLAN with WPA 2 Personal security .	To enable AAA override and connecting a Android client to the AAA override enabled with WPA 2 Personal security WLAN and check if the VLAN from AAA server is overridden to the client	Passed	
EWLCJ171S_Reg_291	Enable AAA override and connecting a IOS client to the AAA override enabled WLAN with WPA 2 Personal security .	To enable AAA override and connecting a IOS client to the AAA override enabled with WPA 2 Personal security WLAN and check if the VLAN from AAA server is overridden to the client	Passed	
EWLCJ171S_Reg_292	Enable AAA override and connecting a Mac OS client to the AAA override enabled WLAN with WPA 2 Personal security .	To enable AAA override and connecting a Mac OS client to the AAA override enabled with WPA 2 Personal security WLAN and check if the VLAN from AAA server is overridden to the client	Passed	
EWLCJ171S_Reg_293	Connecting a window 10 client to the AAA override enabled WLAN with WPA 2 Enterprise security enabled with AAA override .	To connect a JOS Window 10 client to AAA override enabled WLAN with WPA 2 Enterprise security and check if the Native VLAN is overridden or not.	Passed	

EWLCJ171S_Reg_294	Connecting a more than one window 10 client to the AAA override enabled WLAN with WPA 2 security enabled with AAA override .	To connect a more no of JOS Window 10 client to AAA override enabled WLAN with WPA 2 Enterprise security and check if the Native VLAN is overridden or not.	Passed	
EWLCJ171S_Reg_295	Connecting a Android client to the AAA override enabled WLAN with WPA 2 Enterprise security enabled with AAA override .	To connect a Android client to AAA override enabled WLAN with WPA 2 Enterprise security and check if the Native VLAN is overridden or not.	Passed	
EWLCJ171S_Reg_296	Connecting a IOS client to the AAA override enabled WLAN with WPA 2 Enterprise security enabled with AAA override .	To connect a IOS client to AAA override enabled WLAN with WPA 2 Enterprise security and check if the Native VLAN is overridden or not.	Passed	
EWLCJ171S_Reg_297	Connecting a MacOS client to the AAA override enabled WLAN with WPA 2 Enterprise security enabled with AAA override .	To connect a Mac OS client to AAA override enabled WLAN with WPA 2 Enterprise security and check if the Native VLAN is overridden or not.	Passed	
EWLCJ171S_Reg_298	Connecting a 2 or 3 MacOS client to the AAA override enabled WLAN with WPA 2 Enterprise security enabled with AAA override .	To connect a Mac OS client to AAA override enabled WLAN with WPA 2 Enterprise security and check if the Native VLAN is overridden or not.	Passed	
EWLCJ171S_Reg_299	Connecting a client to the AAA override enabled with the macfiltering.	To connect a client to the AAA override enabled with the macfiltering.	Passed	

EWLCJ171S_Reg_300	Connecting Combination of different client to the AAA override enabled WLAN with WPA 2 Enterprise security enabled with AAA override .	To connect combination of different client to AAA override enabled WLAN with WPA 2 Enterprise security and check if the Native VLAN is overridden or not.	Passed	
EWLCJ171S_Reg_301	Connecting a 2 or 3 IOS client to the AAA override enabled WLAN with WPA 2 Enterprise security enabled with AAA override .	To connect more number of client to AAA override enabled WLAN with WPA 2 Enterprise security and check if the Native VLAN is overridden or not.	Passed	

802.1x support with EAP-TLS and EAP-PEAP

Logical ID	Title	Description	Status	Defect ID
EWCJ171S__Reg_251	Enabling dot1x auth for AP and joining AP to WLC	To check whether AP joins WLC or not after dot1x authentication from Switch/ISE	Passed	
EWCJ171S__Reg_252	Associating Windows clients to AP joined via Dot1x authentication	To check whether Windows clients associated successfully or not once AP joined via dot1x authentication from Switch/ISE	Passed	
EWCJ171S__Reg_253	Joining COS AP to WLC through Dot1x+PEAP authentication	To check whether COS AP joins WLC or not after dot1x authentication from Switch/ISE via EAP method PEAP	Passed	

EWCJ171S__Reg_254	Joining iOS AP to WLC through Dot1x+EAP TLS authentication	To check whether iOS AP joins WLC or not after dot1x authentication from Switch/ISE via EAP method TLS	Passed	
EWCJ171S__Reg_255	Trying to join AP's through Dot1x authentication with LSC provisioning	To check whether AP's joins WLC or not through LSC provisioning & dot1x authentication	Passed	
EWCJ171S__Reg_256	Providing invalid credentials for AP authentication and checking the status of AP in console	To check whether AP throws error message or not when invalid credentials provided during dot1x authentication	Passed	
EWCJ171S__Reg_257	Disabling dot1x support in Switch and trying to associate AP via Dot1x authentication to WLC	To check whether AP joins WLC or not even dot1x is disabled in switch	Passed	
EWCJ171S__Reg_258	Enabling dot1x auth for AP in 3850 Switch	Configuring the 3850 Switch for Dot1x authentication by mapping the identity profiles to a port.	Passed	
EWCJ171S__Reg_259	Checking the configuration of 802.1x authentication parameters after export/import the config file	To check whether 802.1x auth parameters restores or not after export/import the config file in WLC UI via TFTP	Passed	
EWCJ171S__Reg_260	Associating Mac OS clients to AP joined via Dot1x authentication	To check whether Mac OS clients associated successfully or not once AP joined via dot1x authentication from Switch/ISE	Passed	

EWCJ171S__Reg_261	Associating Android clients to AP joined via Dot1x authentication	To check whether Android clients associated successfully or not once AP joined via dot1x authentication from Switch/ISE	Passed	
EWCJ171S__Reg_262	Associating iOS clients to AP joined via Dot1x authentication	To check whether iOS clients associated successfully or not once AP joined via dot1x authentication from Switch/ISE	Passed	
EWCJ171S__Reg_263	Trying to configure of 802.1x authentication parameters via Read-only User	To check whether Read only user can be able to configure or not the 802.1x auth parameters in WLC UI	Passed	

Software update using SFTP

Logical ID	Title	Description	Status	Defect ID
EWCJ171S__Reg_117	eWC Software updating via SFTP server	Verifying eWC software updating or not via SFTP server	Passed	
EWCJ171S__Reg_118	Invalid eWC Software updating via SFTP server	Verifying eWC software updating or not via SFTP server	Passed	
EWCJ171S__Reg_119	eWC .bin Software updating via SFTP server	Checking the eWC .bin software updating or not via SFTP server	Passed	
EWCJ171S__Reg_120	eWC .SSH Software updating via SFTP server	Checking the eWC .bin software updating or not via SFTP server	Passed	
EWCJ171S__Reg_121	eWC Software updating through Invalid SFTP IP	To check whether software is upgrading or not through Invalid SFTP IP	Passed	

EWCJ171S__Reg_122	eWC Software updating through Invalid SFTP user name/password	Verifying eWC software is upgrading or not through Invalid SFTP user name/password	Passed	
EWLCJ171S_Reg_01	Cisco Catalyst 9800 Series Wireless ControllerSoftware updating via SFTP server	Verifying Cisco Catalyst 9800 Series Wireless Controller software updating or not via SFTP server	Passed	
EWLCJ171S_Reg_02	Invalid Cisco Catalyst 9800 Series Wireless Controller Software updating via SFTP server	VerifyingCisco Catalyst 9800 Series Wireless Controller software updating or not via SFTP server	Passed	
EWLCJ171S_Reg_03	Cisco Catalyst 9800 Series Wireless Controller .bin Software updating via SFTP server	Checking the Cisco Catalyst 9800 Series Wireless Controller.bin software updating or not via SFTP server	Passed	
EWLCJ171S_Reg_04	Cisco Catalyst 9800 Series Wireless Controller .SSH Software updating via SFTP server	Checking the Cisco Catalyst 9800 Series Wireless Controller .bin software updating or not via SFTP server	Passed	
EWLCJ171S_Reg_05	Cisco Catalyst 9800 Series Wireless Controller Software updating through Invalid SFTP IP	To check whether software is upgrading or not through Invalid SFTP IP	Passed	
EWLCJ171S_Reg_06	Cisco Catalyst 9800 Series Wireless Controller Software updating through Invalid SFTP user name/password	Verifying Cisco Catalyst 9800 Series Wireless Controller software is upgrading or not through Invalid SFTP user name/password	Passed	

Capwap Image Conversion

Logical ID	Title	Description	Status	Defect ID

EWCJ171S__Reg_158	Joining the AP image with less than other than eWC and checking the details	To verify whether AP join to the Cisco Catalyst 9800 Series Wireless Controller eWC and downloading the image or not	Passed	
EWCJ171S__Reg_159	Joining the AP after Efficient join enable/Disable state	To verify whether AP is joining & downloading image from eWC or not after efficient join enable state	Passed	
EWCJ171S__Reg_160	CAPWAP image joins to eWC	To verify whether COS AP is joining to the eWC with eWC capable or not	Passed	
EWCJ171S__Reg_161	CAPWAP image joins to eWC	To verify whether IOS AP is joining to the eWC with AP & eWC different version and not downloading the image	Passed	
EWCJ171S__Reg_162	Upgrading the eWC image and making the capwap Aps to eWC capable	To verify whether Aps converting the eWC capable or not after upgrade the eWC image	Passed	
EWCJ171S__Reg_163	Downgrading the eWC image and making the capwap Aps to eWC capable	To verify whether Aps converting the eWC capable or not after downgrade the eWC image	Passed	
EWCJ171S__Reg_164	Removing the Master AP at the time of AP downloading the image	To verify whether it is possible to remove the Master AP at the time of AP downloading the image	Passed	
EWCJ171S__Reg_165	Changing the eWC time and trying to join the AP	To verify whether AP joining to the eWC or not with AP and eWC times are different	Passed	

EWCJ171S__Reg_166	Performing the Master AP failover	To verify whether after Master Ap failover, Ap is again downloading the images or not	Passed	
EWCJ171S__Reg_167	Interchanging the eWC image	To verify whether after image interchange eWC coming as changed version or not	Passed	
EWCJ171S__Reg_168	Interchanging the AP image and making as eWC Controller	To verify whether after AP interchange, AP is coming as changed image with eWC capable controller or not	Passed	

ME AP convert to CAPWAP via DHCP Option

Logical ID	Title	Description	Status	Defect ID
EWCJ171S__Reg_201	Change the 1852 ME AP type to capwap using DHCP 43	To change the AP type to capwap using DHCP 43	Passed	
EWCJ171S__Reg_202	Change the 2800 ME AP type to capwap using DHCP 43	To change the AP type to capwap using DHCP 43	Passed	
EWCJ171S__Reg_203	Change the 1542 ME AP type to capwap using DHCP 43	To change the AP type to capwap using DHCP 43	Passed	
EWCJ171S__Reg_204	Change the 1815i ME AP type to capwap using DHCP 43	To change the AP type to capwap using DHCP 43	Passed	
EWCJ171S__Reg_205	Change the AP mode after converting in to capwap	To change the AP mode after converting in to CAPWAP	Passed	

EWCJ171S_Reg_206	Connect iOS client to Capwap converted AP from ME with WPA2-PSK security	To connect the iOS client to capwap converted AP from ME with WPA2-PSK security	Passed	
EWCJ171S_Reg_207	Connect Android client to Capwap converted AP from ME with WPA2-PSK security	To connect the Android client to capwap converted AP from ME with WPA2-PSK security	Passed	
EWCJ171S_Reg_208	Config primary, secondary controller in AP and reload ME controller	To verify that ME changed to capwap and send join request to controller that configured using DHCP option 43	Passed	
EWCJ171S_Reg_209	Config two controller ip in dhcp option 43 and first should be wrong ip	To verify that AP joined to second controller if first ip is wrong in dhcp	Passed	
EWCJ171S_Reg_210	Change the 1815i ME AP type to capwap using DHCP 43 and join in to vWLC	To change the AP type to capwap using DHCP 43and join in to vWLC	Passed	
EWCJ171S_Reg_211	Make the Preferred Master one ME capable AP and reload ME Controller	To verify that ME Controller changed to capwap after make Preferred master as another ME capable AP	Passed	

CMX Support

Logical ID	Title	Description	Status	Defect ID

EWCJ171S__Reg_169	Adding Cisco Cisco Catalyst 9800 Series Wireless Controller_ME to CMX	To add a Cisco Cisco Catalyst 9800 Series Wireless Controller_ME to CMX and check if the Cisco Catalyst 9800 Series Wireless Controller_ME gets added to the CMX with the Cisco Catalyst 9800 Series Wireless Controller_ME status showing	Passed	
EWCJ171S__Reg_170	Importing maps from prime infrastructure	To import maps from prime infrastructure and check if the maps gets imported to the cmx .	Passed	
EWCJ171S__Reg_171	Importing the maps with Access points from PI to CMX	To import the maps from prime infra to CMX with Access points and check if the access point details are shown correctly including Clients connected .	Passed	
EWCJ171S__Reg_172	Connecting the Client to the access point on the floor and check if the details of the Client.	To connect a Client to the access point on the floor and check if the details of the Clients are shown correctly or not.	Passed	
EWCJ171S__Reg_173	Connecting many Clients from different place and check the location of the Clients	To connect many Client from different place to the access points and check if the location of the Client are shown in CMX	Passed	
EWCJ171S__Reg_174	Using MAC address the Client devices are searched	To check whether Client device can be searched by specifying its MAC address or not	Passed	

EWCJ171S__Reg_175	Using IP address the Client devices are searched	To check whether Client device can be searched by specifying its IP address or not	Passed	
EWCJ171S__Reg_176	Using SSID the Client devices are searched	To verify whether Client device can be searched by specifying the SSID or not	Passed	
EWCJ171S__Reg_177	Number of Clients visiting the building and floor in hourly and daily basis	Verifying the number of Clients visiting the building or floor on hourly and daily basis	Passed	
EWCJ171S__Reg_178	Number of Client visits to the building and the floor	To check the number of new Clients and repeated Clients to the building or floor .	Passed	
EWLCJ171S_Reg_118	Adding Cisco Cisco Catalyst 9800 Series Wireless Controller_ME to CMX	To add a Cisco Cisco Catalyst 9800 Series Wireless Controller_ME to CMX and check if the Cisco Catalyst 9800 Series Wireless Controller_ME gets added to the CMX with the Cisco Catalyst 9800 Series Wireless Controller_ME status showing	Passed	
EWLCJ171S_Reg_119	Importing maps from prime infrastructure	To import maps from prime infrastructure and check if the maps gets imported to the cmx .	Passed	

EWLCJ171S_Reg_120	Importing the maps with Access points from PI to CMX	To import the maps from prime infra to CMX with Access points and check if the access point details are shown correctly including Clients connected .	Passed	
EWLCJ171S_Reg_121	Connecting the Client to the access point on the floor and check if the details of the Client.	To connect a Client to the access point on the floor and check if the details of the Clients are shown correctly or not.	Passed	
EWLCJ171S_Reg_122	Connecting many Clients from different place and check the location of the Clients	To connect many Client from different place to the access points and check if the location of the Client are shown in CMX	Passed	
EWLCJ171S_Reg_123	Using MAC address the Client devices are searched	To check whether Client device can be searched by specifying its MAC address or not	Passed	
EWLCJ171S_Reg_124	Using IP address the Client devices are searched	To check whether Client device can be searched by specifying its IP address or not	Passed	
EWLCJ171S_Reg_125	Using SSID the Client devices are searched	To verify whether Client device can be searched by specifying the SSID or not	Passed	
EWLCJ171S_Reg_126	Number of Clients visiting the building and floor in hourly and daily basis	Verifying the number of Clients visiting the building or floor on hourly and daily basis	Passed	
EWLCJ171S_Reg_127	Number of Client visits to the building and the floor	To check the number of new Clients and repeated Clients to the building or floor .	Passed	

Aging Test Cases

Logical ID	Title	Description	Status	Defect ID
EWCJ171S_Reg_123	Connecting a JOS client to a 1815I AP and enable debug log and check RSSI value for the client for 2 to 3 hours.	To connect JOS client to 1815I and check the debug log for the client and check the RSSI value for 2 to 3 hours.	Passed	
EWCJ171S_Reg_124	Connecting a Window client to a 1815I AP and enable debug log and check RSSI value for the client for 2 to 3 hours.	To connect Window client to 1815I and check the debug log for the client and check the RSSI value for 2 to 3 hours.	Passed	
EWCJ171S_Reg_125	Connecting a Android client to a 1815I AP and enable debug log and check RSSI value for the client for 2 to 3 hours.	To connect Android client to 1815I and check the debug log for the client and check the RSSI value for 2 to 3 hours.	Passed	
EWCJ171S_Reg_126	Connecting a IOS client to a 1815I AP and enable debug log and check RSSI value for the client for 2 to 3 hours.	To connect IOS client to 1815I and check the debug log for the client and check the RSSI value for 2 to 3 hours.	Passed	
EWCJ171S_Reg_127	Connecting a MAC OS client to a 1815I AP and enable debug log and check RSSI value for the client for 2 to 3 hours.	To connect MAC OS client to 1815I and check the debug log for the client and check the RSSI value for 2 to 3 hours.	Passed	
EWCJ171S_Reg_128	Checking the JOS Client details when the client is connected to 2802/3802 AP and check the Average rate for the client for more than 2 hours	To check the JOS Client details when the client is connected to 2802/3802 AP and check the Average rate for the client for more than 2 hours	Passed	

EWCJ171S__Reg_129	Checking the Android Client details when the client is connected to 2802/3802 AP and check the Average rate for the client for more than 2 hours	To check the Android Client details when the client is connected to 2802/3802 AP and check the Average rate for the client for more than 2 hours	Passed	
EWCJ171S__Reg_130	Checking the Window Client details when the client is connected to 2802/3802 AP and check the Average rate for the client for more than 2 hours	To check the Window Client details when the client is connected to 2802/3802 AP and check the Average rate for the client for more than 2 hours	Passed	
EWCJ171S__Reg_131	Checking the IOS Client details when the client is connected to 2802/3802 AP and check the Average rate for the client for more than 2 hours	To check the IOS Client details when the client is connected to 2802/3802 AP and check the Average rate for the client for more than 2 hours	Passed	
EWCJ171S__Reg_132	Checking the Air Quality data for different AP with JOS client and check the health of the AP in a regular interval.	To check the Air quality data for different AP with JOS client and check the health of the particular AP in a regular interval	Passed	
EWLCJ171S_Reg_128	Connecting a JOS client to a 1815I AP and enable debug log and check RSSI value for the client for 2 to 3 hours.	To connect JOS client to 1815I and check the debug log for the client and check the RSSI value for 2 to 3 hours.	Passed	
EWLCJ171S_Reg_129	Connecting a Window client to a 1815I AP and enable debug log and check RSSI value for the client for 2 to 3 hours.	To connect Window client to 1815I and check the debug log for the client and check the RSSI value for 2 to 3 hours.	Passed	

EWLCJ171S_Reg_130	Connecting a Android client to a 1815I AP and enable debug log and check RSSI value for the client for 2 to 3 hours.	To connect Android client to 1815I and check the debug log for the client and check the RSSI value for 2 to 3 hours.	Passed	
EWLCJ171S_Reg_131	Connecting a IOS client to a 1815I AP and enable debug log and check RSSI value for the client for 2 to 3 hours.	To connect IOS client to 1815I and check the debug log for the client and check the RSSI value for 2 to 3 hours.	Passed	
EWLCJ171S_Reg_132	Connecting a MAC OS client to a 1815I AP and enable debug log and check RSSI value for the client for 2 to 3 hours.	To connect MAC OS client to 1815I and check the debug log for the client and check the RSSI value for 2 to 3 hours.	Passed	
EWLCJ171S_Reg_133	Checking the JOS Client details when the client is connected to 2802/3802 AP and check the Average rate for the client for more than 2 hours	To check the JOS Client details when the client is connected to 2802/3802 AP and check the Average rate for the client for more than 2 hours	Passed	
EWLCJ171S_Reg_134	Checking the Android Client details when the client is connected to 2802/3802 AP and check the Average rate for the client for more than 2 hours	To check the Android Client details when the client is connected to 2802/3802 AP and check the Average rate for the client for more than 2 hours	Passed	
EWLCJ171S_Reg_135	Checking the Window Client details when the client is connected to 2802/3802 AP and check the Average rate for the client for more than 2 hours	To check the Window Client details when the client is connected to 2802/3802 AP and check the Average rate for the client for more than 2 hours	Passed	

EWLCJ171S_Reg_136	Checking the IOS Client details when the client is connected to 2802/3802 AP and check the Average rate for the client for more than 2 hours	To check the IOS Client details when the client is connected to 2802/3802 AP and check the Average rate for the client for more than 2 hours	Passed	
EWLCJ171S_Reg_137	Checking the Air Quality data for different AP with JOS client and check the health of the AP in a regular interval.	To check the Air quality data for different AP with JOS client and check the health of the particular AP in a regular interval	Passed	

SFTP Domain Name support

Logical ID	Title	Description	Status	Defect ID
EWCJ171S__Reg_152	eWC Software updating via SFTP server	Verifying eWC software updating or not via SFTP server	Passed	
EWCJ171S__Reg_153	Invalid eWC Software updating via SFTP server	Verifying eWC software updating or not via SFTP server	Passed	
EWCJ171S__Reg_154	eWC .bin Software updating via SFTP server	Checking the eWC .bin software updating or not via SFTP server	Passed	
EWCJ171S__Reg_155	eWC .SSH Software updating via SFTP server	Checking the eWC .bin software updating or not via SFTP server	Passed	
EWCJ171S__Reg_156	eWC Software updating through Invalid SFTP IP	To check whether software is upgrading or not through Invalid SFTP IP	Passed	
EWCJ171S__Reg_157	eWC Software updating through Invalid SFTP user name/password	Verifying eWC software is upgrading or not through Invalid SFTP user name/password	Passed	

EWLCJ171S_Reg_199	Cisco Catalyst 9800 Series Wireless Controller Software updating via SFTP server	Verifying Cisco Catalyst 9800 Series Wireless Controller software updating or not via SFTP server	Passed	
EWLCJ171S_Reg_200	Invalid Cisco Catalyst 9800 Series Wireless Controller Software updating via SFTP server	Verifying Cisco Catalyst 9800 Series Wireless Controller software updating or not via SFTP server	Failed	CSCvs41888
EWLCJ171S_Reg_201	Cisco Catalyst 9800 Series Wireless Controller.bin Software updating via SFTP server	Checking the Cisco Catalyst 9800 Series Wireless Controller .bin software updating or not via SFTP server	Passed	
EWLCJ171S_Reg_202	Cisco Catalyst 9800 Series Wireless Controller .SSH Software updating via SFTP server	Checking the Cisco Catalyst 9800 Series Wireless Controller .bin software updating or not via SFTP server	Passed	
EWLCJ171S_Reg_203	Cisco Catalyst 9800 Series Wireless Controller Software updating through Invalid SFTP IP	To check whether software is upgrading or not through Invalid SFTP IP	Passed	
EWLCJ171S_Reg_204	Cisco Catalyst 9800 Series Wireless Controller Software updating through Invalid SFTP user name/password	Verifying Cisco Catalyst 9800 Series Wireless Controller software is upgrading or not through Invalid SFTP user name/password	Passed	

MC2UC (Videostreaming)

Logical ID	Title	Description	Status	Defect ID
EWCJ171S__Reg_90	MC2UC traffic to local-switching client	To verify that the local-switching client subscribed to video streaming receives MC2UC traffic	Passed	

EWCJ171S__Reg_91	MC2UC traffic to local-switching client when MC2UC is disabled	To verify the local switching client receiving MC traffic when MC2UC is disabled at the WLAN	Passed	
EWCJ171S__Reg_92	MC2UC traffic to local-switching client when Media stream is removed at AP	To verify the local switching client receiving MC traffic when Media Stream is disabled at AP	Passed	
EWCJ171S__Reg_93	Multiple LS clients in same vlan, same wlan, receiving MC2UC traffic	To verify whether the multiple local-switching clients receives MC2UC traffic when subscribed to video stream	Passed	
EWCJ171S__Reg_94	Client disassociates when receiving MC2UC traffic	To verify whether AP stops sending traffic when client disassociates	Passed	
EWCJ171S__Reg_95	LS client receiving MC2UC traffic roam between radios at the AP	To verify the local-switching client receiving MC2UC traffic roaming between radios of the AP	Passed	
EWCJ171S__Reg_96	Flex LS client receiving MC2UC traffic when AP move from connected > SA > connected with same config	To verify whether the LS client receives continuous MC2UC traffic when AP moves from connected > SA > connected with same config	Passed	
EWCJ171S__Reg_97	Flex LS client receiving MC2UC traffic when AP move from connected > SA > connected with different config	To verify whether the LS client receives continuous MC2UC traffic when AP moves from connected > SA > connected with different config	Passed	

EWCJ171S__Reg_98	Flex AP reboot in connected mode when Flex LS client receiving MC2UC traffic	To verify whether client reassociates and receives MC2UC traffic when flex AP is rebooted in connected mode.	Passed	
EWCJ171S__Reg_99	Video stream config sync for LS WLAN in HA setup	To verify whether the video streaming config for LS WLAN has been synced between the Active and Standby in HA setup	Passed	
EWCJ171S__Reg_100	LS client with MC2UC enabled receiving traffic after switchover in HA pair	To verify whether LS client with MC2UC enabled receives unicast traffic after switchover	Passed	
EWLCJ171S_Reg_34	MC2UC traffic to local-switching client	To verify that the local-switching client subscribed to video streaming receives MC2UC traffic	Passed	
EWLCJ171S_Reg_35	MC2UC traffic to local-switching client when MC2UC is disabled	To verify the local switching client receiving MC traffic when MC2UC is disabled at the WLAN	Passed	
EWLCJ171S_Reg_36	MC2UC traffic to local-switching client when Media stream is removed at AP	To verify the local switching client receiving MC traffic when Media Stream is disabled at AP	Passed	
EWLCJ171S_Reg_37	Multiple LS clients in same vlan, same wlan, receiving MC2UC traffic	To verify whether the multiple local-switching clients receives MC2UC traffic when subscribed to video stream	Passed	

EWLCJ171S_Reg_38	Client disassociates when receiving MC2UC traffic	To verify whether AP stops sending traffic when client disassociates	Passed	
EWLCJ171S_Reg_39	LS client receiving MC2UC traffic roam between radios at the AP	To verify the local-switching client receiving MC2UC traffic roaming between radios of the AP	Passed	
EWLCJ171S_Reg_40	Flex LS client receiving MC2UC traffic when AP move from connected > SA > connected with same config	To verify whether the LS client receives continuous MC2UC traffic when AP moves from connected > SA > connected with same config	Passed	
EWLCJ171S_Reg_41	Flex LS client receiving MC2UC traffic when AP move from connected > SA > connected with different config	To verify whether the LS client receives continuous MC2UC traffic when AP moves from connected > SA > connected with different config	Passed	
EWLCJ171S_Reg_42	Flex AP reboot in connected mode when Flex LS client receiving MC2UC traffic	To verify whether client reassociates and receives MC2UC traffic when flex AP is rebooted in connected mode.	Passed	
EWLCJ171S_Reg_43	Video stream config sync for LS WLAN in HA setup	To verify whether the video streaming config for LS WLAN has been synced between the Active and Standby in HA setup	Passed	
EWLCJ171S_Reg_44	LS client with MC2UC enabled receiving traffic after switchover in HA pair	To verify whether LS client with MC2UC enabled receives unicast traffic after switchover	Passed	

mDNS Support

Logical ID	Title	Description	Status	Defect ID
EWCJ171S_Reg_264	Checking mDNS services are applied to MAC OS with wlan open security	Verifying mDNS services are applied to Mac OS with open ssid	Passed	
EWCJ171S_Reg_265	Checking mDNS services are applied to MacOS and IOS with wlan WPA2 personal security	Verifying mDNS services are applied to MacOS and IOS with WPA2 personal security	Passed	
EWCJ171S_Reg_266	Checking mDNS services are applied to Apple TV and IOS with wlan WPA2 Enterprise security and authentication server as radius	Verifying mDNS services are applied to AppleTV and IOS with WPA2 Enterprise security and radius as authentication server	Passed	
EWCJ171S_Reg_267	Checking mDNS services are applied to MacOS and IOS with wlan WPA3-SAE security	Verifying mDNS services are applied to MacOS and IOS with WPA3-SAE security	Passed	
EWCJ171S_Reg_268	Checking mDNS services are applied to Apple Devices with Fast transition enabled	Verifying mDNS services are applied to Apple Devices with fast transition enabled	Passed	
EWCJ171S_Reg_269	Performing client communication between two clients connected two different vlan	Checking client communication between two clients connected to different vlan	Passed	
EWCJ171S_Reg_270	Performing roaming operation when mDNS is applied	Checking roaming when mDNS is applied	Passed	
EWCJ171S_Reg_271	Exporting config file after upgrading eWC	Checking mDNS config after exporting config file	Passed	

EWCJ171S__Reg_272	Creating mDNS profile by adding required services	Verifying mDNS profile is creating with required services	Passed	
EWCJ171S__Reg_273	Checking mDNS services are applied to IOS with wlan Static WEP security	Verifying mDNS services are applied to IOS with Static WEP ssid	Passed	
EWLCJ171S_Reg_271	Checking mDNS services are applied to MAC OS with wlan open security	Verifying mDNS services are applied to Mac OS with open ssid	Passed	
EWLCJ171S_Reg_272	Checking mDNS services are applied to MacOS and IOS with wlan WPA2 personal security	Verifying mDNS services are applied to MacOS and IOS with WPA2 personal security	Passed	
EWLCJ171S_Reg_273	Checking mDNS services are applied to Apple TV and IOS with wlan WPA2 Enterprise security and authentication server as radius	Verifying mDNS services are applied to AppleTV and IOS with WPA2 Enterprise security and radius as authentication server	Passed	
EWLCJ171S_Reg_274	Checking mDNS services are applied to MacOS and IOS with wlan WPA3-SAE security	Verifying mDNS services are applied to MacOS and IOS with WPA3-SAE security	Passed	
EWLCJ171S_Reg_275	Checking mDNS services are applied to Apple Devices with Fast transition enabled	Verifying mDNS services are applied to Apple Devices with fast transition enabled	Passed	
EWLCJ171S_Reg_276	Performing client communication between two clients connected two different vlan	Checking client communication between two clients connected to different vlan	Passed	
EWLCJ171S_Reg_277	Performing roaming operation when mDNS is applied	Checking roaming when mDNS is applied	Passed	

EWLCJ171S_Reg_278	Exporting config file after upgrading Cisco Catalyst 9800 Series Wireless Controller	Checking mDNS config after exporting config file	Passed	
EWLCJ171S_Reg_279	Creating mDNS profile by adding required services	Verifying mDNS profile is creating with required services	Passed	
EWLCJ171S_Reg_280	Checking mDNS services are applied to IOS with wlan Static WEP security	Verifying mDNS services are applied to IOS with Static WEP ssid	Passed	

Schedule WLAN Support (Calendar Profile on CLI)

Logical ID	Title	Description	Status	Defect ID
EWCJ171S__Reg_10	Configure the Calendar Profile in open security WLAN with Start/End time.	To check whether WLAN is broadcasting or not on configured Start/End time	Passed	
EWCJ171S__Reg_11	Configure the Calendar Profile in WPA2 security WLAN with Start/End time.	To check whether WLAN is broadcasting or not on configured Start/End time	Passed	
EWCJ171S__Reg_12	Configure the Calendar Profile in WPA3 security WLAN with Start/End time.	To check whether WLAN is broadcasting or not on configured Start/End time	Passed	
EWCJ171S__Reg_13	Configure the Calendar Profile in Static WEP security WLAN with Start/End time.	To check whether WLAN is broadcasting or not on configured Start/End time	Passed	
EWCJ171S__Reg_14	Configure the Calendar Profile in Static WEP security WLAN with Start/End time with Monthly/Weekly/Daily option.	To check whether WLAN is broadcasting or not on configured Start/End time	Passed	

EWCJ171S__Reg_15	Configure the Calendar Profile in Static WEP security WLAN with L3 Security,MAC Filtering and with Start/End time .	To check whether WLAN is broadcasting or not on configured Start/End time	Passed	
EWCJ171S__Reg_16	Observe the Client Disassociation on Calendar Profile after end time	To check whether client is disassociating after end time.	Passed	
EWLCJ171S_Reg_88	Configure the Calendar Profile in open security WLAN with Start/End time.	To check whether WLAN is broadcasting or not on configured Start/End time	Failed	CSCvs53410
EWLCJ171S_Reg_89	Configure the Calendar Profile in WPA2 security WLAN with Start/End time.	To check whether WLAN is broadcasting or not on configured Start/End time	Passed	
EWLCJ171S_Reg_90	Configure the Calendar Profile in WPA3 security WLAN with Start/End time.	To check whether WLAN is broadcasting or not on configured Start/End time	Passed	
EWLCJ171S_Reg_91	Configure the Calendar Profile in Static WEP security WLAN with Start/End time.	To check whether WLAN is broadcasting or not on configured Start/End time	Passed	
EWLCJ171S_Reg_92	Configure the Calendar Profile in Static WEP security WLAN with Start/End time with Monthly/Weekly/Daily option.	To check whether WLAN is broadcasting or not on configured Start/End time	Passed	
EWLCJ171S_Reg_93	Configure the Calendar Profile in Static WEP security WLAN with L3 Security,MAC Filtering and with Start/End time .	To check whether WLAN is broadcasting or not on configured Start/End time	Passed	

EWLCJ171S_Reg_94	Observe the Client Disassociation on Calendar Profile after end time	To check whether client is disassociating after end time.	Passed	

Optimized Roaming

Logical ID	Title	Description	Status	Defect ID
EWCJ171S__Reg_138	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	
EWCJ171S__Reg_139	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	
EWCJ171S__Reg_140	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	
EWCJ171S__Reg_141	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	
EWCJ171S__Reg_142	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	

EWCJ171S__Reg_143	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	
EWCJ171S__Reg_144	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	
EWCJ171S__Reg_145	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	
EWCJ171S__Reg_146	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	
EWCJ171S__Reg_147	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	
EWCJ171S__Reg_148	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	
EWCJ171S__Reg_149	Connect iOS client from where SSID signal is week	To verify that iOS client connecting or not from where SSID signal is week	Passed	

EWCJ171S__Reg_150	Restarting the ME eWC after optimized roaming configuration	To verify that optimization roaming configuration remain same after reboot	Passed	
EWCJ171S__Reg_151	Importing/exporting configuration file after optimized roaming configuring	To verify that optimization roaming configuration remain same after import and export configuration file	Passed	
EWLCJ171S_Reg_147	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	
EWLCJ171S_Reg_148	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	
EWLCJ171S_Reg_149	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	
EWLCJ171S_Reg_150	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	

EWLCJ171S_Reg_151	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	
EWLCJ171S_Reg_152	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	
EWLCJ171S_Reg_153	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	
EWLCJ171S_Reg_154	Moving the Android client from AP after enable optimized roaming with interference availability	To verify that client got disassociated when signal is poor while moving from AP with interference availability	Passed	
EWLCJ171S_Reg_155	Connect iOS client from where SSID signal is week	To verify that iOS client connecting or not from where SSID signal is week	Passed	
EWLCJ171S_Reg_156	Restarting the Cisco Catalyst 9800 Series Wireless Controller after optimized roaming configuration	To verify that optimization roaming configuration remain same after reboot	Passed	
EWLCJ171S_Reg_157	Importing/exporting configuration file after optimized roaming configuring	To verify that optimization roaming configuration remain same after import and export configuration file	Passed	

Authentication Survivability Support

Logical ID	Title	Description	Status	Defect ID

EWCJ171S__Reg_17	Creating WLAN with Radius server and connecting client	To verify whether Client is connecting to WLAN with Radius server or not	Passed	
EWCJ171S__Reg_18	Guest WLAN with Radius survivability	To verify whether Client able to connect Guest WLAN with Radius survivability o not	Passed	
EWCJ171S__Reg_19	Captive network enabled WLAN with Radius survivability	To verify whether Client able to connect captive network enabled WLAN with Radius survivability or not	Passed	
EWCJ171S__Reg_20	MAC filter enabled WLAN with Radius survivability	To verify whether Client able to connect MAC filter enabled WLAN with Radius survivability or not	Passed	
EWCJ171S__Reg_21	WPA+WPA2 enabled WLAN with Radius survivability	To verify whether Client able to connect Guest+MAC enabled WLAN with Radius survivability or not	Passed	
EWCJ171S__Reg_22	WPA2+WPA3 enabled WLAN with Radius survivability	To verify whether Client able to connect Guest+Capative+MAC enabled WLAN with Radius survivability or not	Passed	
EWCJ171S__Reg_23	Static web enabled WLAN with Radius survivability	To verify whether Client able to connect Guest+Capative+MAC enabled WLAN with Radius survivability or not	Passed	
EWCJ171S__Reg_24	AVC configured WLAN with Radius survivability	To verify whether AVC rules are applying to WLAN with Radius survivability or not	Passed	

EWCJ171S__Reg_25	Assigning DHCP Radius survivability enabled WLAN	To verify whether Client is getting the IP address from DHCP pool or not with Radius survivability	Passed	
EWCJ171S__Reg_26	Enabling Fast Transition on WLAN with Radius survivability	To verify whether Client is connecting to Hotspot enabled WLAN with Radius survivability or not	Passed	
EWCJ171S__Reg_27	Check Authorization details in ISE	To verify whether Client details are showing proper in ISE or not	Passed	
EWCJ171S__Reg_28	Making ISE down and check client is using cache details or not	To verify whether Client are using cache details or not when ISE went down	Passed	
EWCJ171S__Reg_29	Upgrading Cisco Catalyst 9800 Series Wireless Controller-ME and checking Radius survivability details	To verify whether Radius survivability details showing or not after image downgrade	Passed	
EWCJ171S__Reg_30	Downgrading Cisco Catalyst 9800 Series Wireless Controller-ME and checking Radius survivability details	To verify whether Radius survivability details showing or not after image Downgrade	Passed	
EWCJ171S__Reg_31	Validating Radius survivability details after ME down and UP	To verify whether Radius survivability details are showing proper or not after ME came UP	Passed	
EWCJ171S__Reg_32	Changing Security details after client connected to Radius survivability	To verify whether Security details are possible to change or not when client connected with Radius survivability	Passed	
EWCJ171S__Reg_33	Configuring Invalid Radius server details and trying to connect clients	To verify whether Client is able to connect with Invalid radius server details or not	Passed	

EWLCJ171S_Reg_233	Creating WLAN with Radius server and connecting client	To verify whether Client is connecting to WLAN with Radius server or not	Passed	
EWLCJ171S_Reg_234	Guest WLAN with Radius survivability	To verify whether Client able to connect Guest WLAN with Radius survivability o not	Passed	
EWLCJ171S_Reg_235	Captive network enabled WLAN with Radius survivability	To verify whether Client able to connect captive network enabled WLAN with Radius survivability or not	Passed	
EWLCJ171S_Reg_236	MAC filter enabled WLAN with Radius survivability	To verify whether Client able to connect MAC filter enabled WLAN with Radius survivability or not	Passed	
EWLCJ171S_Reg_237	WPA+WPA2 enabled WLAN with Radius survivability	To verify whether Client able to connect Guest+MAC enabled WLAN with Radius survivability or not	Passed	
EWLCJ171S_Reg_238	WPA2+WPA3 enabled WLAN with Radius survivability	To verify whether Client able to connect Guest+Capative+MAC enabled WLAN with Radius survivability or not	Passed	
EWLCJ171S_Reg_239	Static web enabled WLAN with Radius survivability	To verify whether Client able to connect Guest+Capative+MAC enabled WLAN with Radius survivability or not	Passed	
EWLCJ171S_Reg_240	AVC configured WLAN with Radius survivability	To verify whether AVC rules are applying to WLAN with Radius survivability or not	Passed	

EWLCJ171S_Reg_241	Assigning DHCP Radius survivability enabled WLAN	To verify whether Client is getting the IP address from DHCP pool or not with Radius survivability	Passed	
EWLCJ171S_Reg_242	Enabling Fast Transition on WLAN with Radius survivability	To verify whether Client is connecting to Hotspot enabled WLAN with Radius survivability or not	Passed	
EWLCJ171S_Reg_243	Check Authorization details in ISE	To verify whether Client details are showing proper in ISE or not	Passed	
EWLCJ171S_Reg_244	Making ISE down and check client is using cache details or not	To verify whether Client are using cache details or not when ISE went down	Passed	
EWLCJ171S_Reg_245	Upgrading Cisco Catalyst 9800 Series Wireless Controller and checking Radius survivability details	To verify whether Radius survivability details showing or not after image downgrade	Passed	
EWLCJ171S_Reg_246	Downgrading Cisco Catalyst 9800 Series Wireless Controller and checking Radius survivability details	To verify whether Radius survivability details showing or not after image Downgrade	Passed	
EWLCJ171S_Reg_247	Validating Radius survivability details after ME down and UP	To verify whether Radius survivability details are showing proper or not after ME came UP	Passed	
EWLCJ171S_Reg_248	Changing Security details after client connected to Radius survivability	To verify whether Security details are possible to change or not when client connected with Radius survivability	Passed	
EWLCJ171S_Reg_249	Configuring Invalid Radius server details and trying to connect clients	To verify whether Client is able to connect with Invalid radius server details or not	Passed	

Master AP Failover Issues

Logical ID	Title	Description	Status	Defect ID
EWCJ171S_Reg_218	Changing the next preferred Cisco Catalyst 9800 Series Wireless Controller ME capable AP to Controller from UI	To verify whether Next preferred Master AP can changing the Cisco Catalyst 9800 Series Wireless Controller ME or not by using the UI	Passed	
EWCJ171S_Reg_219	Changing the next preferred Cisco Catalyst 9800 Series Wireless Controller ME capable AP to Controller from CLI	To verify whether Next preferred Master AP can changing the Cisco Catalyst 9800 Series Wireless Controller ME or not by using the CLI	Passed	
EWCJ171S_Reg_220	Making the More than 5 Aps to Cisco Catalyst 9800 Series Wireless Controller ME capable	To verify whether more than 5 Aps are changing the state to Cisco Catalyst 9800 Series Wireless Controller ME capable or not	Passed	
EWCJ171S_Reg_221	Deleting the Master Prepared AP from CLI	To verify whether Master preferred AP is deleting from CLI or not	Passed	
EWCJ171S_Reg_222	Configuring the Controller IP address with DHCP server	To verify whether DHCP server IP address is assign to the Controller and come up with same IP address or not	Passed	
EWCJ171S_Reg_223	Assigning the Global AP Configurations	To verify whether Global AP Configurations authenticate to the AP or not	Passed	

Intelligent Capture-eWC

Logical ID	Title	Description	Status	Defect ID
EWCJ171S__Reg_74	Packet capture for Android client using Intelligent Capture option in Campgroup	To verify the packet capture for Android client using Intelligent capture in Campgroup	Passed	
EWCJ171S__Reg_75	Packet capture for Windows JOS client using Intelligent Capture option in Campgroup	To verify the packet capture for Windows client using Intelligent capture in Campgroup	Passed	
EWCJ171S__Reg_76	Packet capture for IOS client using Intelligent Capture option in Campgroup	To verify the packet capture for IOS client using Intelligent capture in Campgroup	Passed	
EWCJ171S__Reg_77	Packet capture for Mac OS client using Intelligent Capture option in Campgroup	To verify the packet capture for MAC OS client using Intelligent capture in Campgroup	Passed	
EWCJ171S__Reg_78	Packet capture of client when the client is connected to AP with 2.4 GHz	To capture the Packet of the client when the client is connected to AP with radio as 2.4 GHz in Cisco Catalyst 9800 Series Wireless Controller ME	Passed	
EWCJ171S__Reg_79	Packet capture of client when the client is connected to AP with 5 GHz	To capture the Packet of the client when the client is connected to AP with radio as 5 GHz inCisco Catalyst 9800 Series Wireless Controller ME	Passed	

EWCJ171S__Reg_80	Capturing of Packet of the client when the client is connected with open security	To capture packet when the client is connected to the iOS AP with security as OPEN in Cisco Catalyst 9800 Series Wireless Controller ME	Passed	
EWCJ171S__Reg_81	Capturing of Packet of the client when the client is connected with WPA 2 PSK security	To capture packet when the client is connected to the iOS AP with security as WPA 2 PSK in Cisco Catalyst 9800 Series Wireless Controller ME	Passed	
EWCJ171S__Reg_82	Capturing of Packet of the client when the client is connected with WPA 2 Enterprise security	To capture packet when the client is connected to the iOS AP with security as WPA 2 Enterprise in Cisco Catalyst 9800 Series Wireless Controller ME	Passed	
EWCJ171S__Reg_83	Capturing of Packet of the client when the client is connected with captive portal-web consent	To capture packet when the client is connected to the AP with security as Captive portal-web consent	Passed	
EWCJ171S__Reg_84	Packet capture for Anyconnect client using Intelligent Capture option in Campgroup page	To verify the packet capture for Anyconnect client using Intelligent capture in Campgroup page	Passed	
EWCJ171S__Reg_85	Packet capture for Windows JOS client using Intelligent Capture option in AP page	To verify the packet capture for Windows JOS client using Intelligent capture in AP page	Passed	
EWCJ171S__Reg_86	Packet capture for Android client using Intelligent Capture option in AP page	To verify the packet capture for Android client using Intelligent capture in AP page	Passed	

EWCJ171S__Reg_87	Packet capture for iOS client using Intelligent Capture option in AP page	To verify the packet capture for iOS client using Intelligent capture in AP page	Passed	
EWCJ171S__Reg_88	Packet capture for MacOS client using Intelligent Capture option in AP page	To verify the packet capture for MacOS client using Intelligent capture in AP page	Passed	
EWCJ171S__Reg_89	Packet capture for Anyconnect client using Intelligent Capture option in AP page	To verify the packet capture for Anyconnect client using Intelligent capture in AP page	Passed	

Captive Portal with Internal, External

Logical ID	Title	Description	Status	Defect ID
EWLCJ171S_Reg_95	Configuring the Email address in Internal /External splash page and associating different types clients to a WLAN	To check whether JOS client gets associated successfully or not to a WLAN in which captive portal enabled as Internal splash page with mapping username as Email address	Passed	
EWLCJ171S_Reg_96	Configuring the Web Consent in Internal/External splash page and associating JOS clients to a WLAN	To check whether JOS client gets associated successfully or not to a WLAN in which captive portal enabled as Internal splash page with mapping access type as Web consent	Passed	

EWLCJ171S_Reg_97	Associating MacOS clients to a WLAN with captive portal and mac filtering enabled	To check whether MacOS clients get associated successfully or not to a WLAN in which captive portal mapped to Internal/external splash page with access type Email address	Passed	
EWLCJ171S_Reg_98	Associating MacOS clients to a WLAN created with UTF-8 Char with providing invalid email address as username	To check whether MacOS clients get associated successfully or not to a WLAN by providing invalid email address as username during captive portal mapped to internal/external splash page	Passed	

Lobby Ambassador

Logical ID	Title	Description	Status	Defect ID
EWLCJ171S_Reg_26	Create and verify Lobby user account and try to login GUI with lobby credentials.	To verify the user able to login GUI with the lobby user credentials.	Passed	
EWLCJ171S_Reg_27	Create 3 lobby users and try to login GUI with all 3 lobby users with different browsers.	To verify the user able to login GUI with the all 3 lobby user credentials with different browsers.	Passed	
EWLCJ171S_Reg_28	Delete the Created lobby users and try to login GUI with lobby user credentials.	To verify the user able to login GUI with the deleted lobby user credentials .	Passed	
EWLCJ171S_Reg_29	Create the Lobby user and try to login CLI with lobby credentials.	To verify the user able to login CLI with the lobby credentials.	Passed	

EWLCJ171S_Reg_30	Create 3 lobby users and try to login CLI with all 3 lobby users with Telnet.	To verify the user able to login CLI with the all 3 lobby credentials with Telnet	Passed	
EWLCJ171S_Reg_31	Create 3 lobby users and try to login CLI with all 3 lobby users with SSh	To verify the user able to login CLI with the all 3 lobby credentials with SSH	Passed	
EWLCJ171S_Reg_32	Delete the Created lobby users and try to login CLI with lobby user credentials.	To verify the user able to login CLI with the deleted lobby user credentials .	Passed	
EWLCJ171S_Reg_33	Create and verify the lobby user in CLI	To verify the User able to login with Lobby credentials	Passed	

AP 4800 Support

Logical ID	Title	Description	Status	Defect ID
EWLCJ171S_Reg_158	Association of 4800 AP with different Cisco Catalyst 9800 Series Wireless Controller model	To associate 4800 AP to Cisco Catalyst 9800 Series Wireless Controller with latest image and check if the AP gets associated or not	Passed	
EWLCJ171S_Reg_159	Associating 4800 AP with different country code as with Cisco Catalyst 9800 Series Wireless Controller	To associate 4800 AP with different country code and check if the AP does not get joined to Cisco Catalyst 9800 Series Wireless Controller	Passed	

EWLCJ171S_Reg_160	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 Cisco Catalyst 9800 Series Wireless Controller	Passed	
EWLCJ171S_Reg_161	Check if the AP with MIC authorization alone joins the Cisco Catalyst 9800 Series Wireless Controller	To check if the AP with MIC authorization alone joins the controller and check if other AP do not join	Passed	
EWLCJ171S_Reg_162	Rebooting the 4800 AP	To check if the AP gets Rebooted or not and check if the AP joins the controller again.	Passed	
EWLCJ171S_Reg_163	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	
EWLCJ171S_Reg_164	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	
EWLCJ171S_Reg_165	Connecting a Window client to the 4800 AP	To connect a window client to the AP and check if the client gets connected to the AP without any errors.	Passed	
EWLCJ171S_Reg_166	Connecting a Android client to the 4800 AP	To connect a Android client to the AP and check if the client gets connected to the AP without any errors.	Passed	

EWLCJ171S_Reg_167	Connecting a IOS client to the 4800 AP	To connect a IOS client to the AP and check if the client gets connected to the AP without any errors.	Passed	
EWLCJ171S_Reg_168	Connecting a MAC client to the 4800 AP	To connect a MAC client to the AP and check if the client gets connected to the AP without any errors.	Passed	
EWLCJ171S_Reg_169	Configure 802.1x Supplicant Credentials for 4800 AP	To configure 802.1x Supplicant Credentials for AP and check if the credentials work correctly or not	Passed	
EWLCJ171S_Reg_170	AP failover priority with critical	To check AP failover priority with critical and check if the AP gets connected to the next controller .	Passed	
EWLCJ171S_Reg_171	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	
EWLCJ171S_Reg_172	Moving AP from 3504 controller to 5520 through High availability	To check if the AP moves from 3504 Cisco Catalyst 9800 Series Wireless Controller to 5520 Cisco Catalyst 9800 Series Wireless Controller through high availability.	Passed	
EWLCJ171S_Reg_173	Reassociation of client to the AP after reboot	To verify if the client gets reassociated to the to the AP .	Passed	

EWLCJ171S_Reg_174	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	
EWLCJ171S_Reg_175	Performing Intra controller roaming of Windows J OS client	To check whether intra controller roaming of windows clients works properly or not in Cisco Catalyst 9800 Series Wireless Controller	Passed	
EWLCJ171S_Reg_176	Performing Intra controller roaming of Android client	To check whether intra controller roaming of Android clients works properly or not	Passed	
EWLCJ171S_Reg_177	Performing Intra controller roaming of IOS client	To check whether intra controller roaming of IOS clients works properly or not in Cisco Catalyst 9800 Series Wireless Controller	Passed	
EWLCJ171S_Reg_178	Performing Intra controller roaming of Mac OS client	To check whether intra controller roaming of MacOS clients works properly or not	Passed	
EWLCJ171S_Reg_179	Performing Inter controller roaming of Windows J OS client	To check whether inter controller roaming of windows clients works properly or not	Passed	
EWLCJ171S_Reg_180	Performing Inter controller roaming of Android client	To check whether inter controller roaming of Android clients works properly or not	Passed	

EWLCJ171S_Reg_181	Performing Inter controller roaming of IOS client	To check whether inter controller roaming of IOS clients works properly or not	Passed	
EWLCJ171S_Reg_182	Performing Inter controller roaming of Mac OS client	To check whether inter controller roaming of Mac OS clients works properly or not	Passed	
EWLCJ171S_Reg_183	Change AP mode from local to Flex connect in 4800 AP.	To change the mode of AP from local mode to Flex connect mode and check if the AP does not reboot.	Passed	
EWLCJ171S_Reg_184	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	
EWLCJ171S_Reg_185	Adding two 4800 AP in the AP group and connecting a client to the AP with specific WLAN	To add two 4800 AP in AP group and map a WLAN to group and connect a client to the WLAN and check the client connectivity	Passed	
EWLCJ171S_Reg_186	Adding 4800 AP in the Flex Connect group and connecting a client to the AP with specific WLAN	To add 4800 Ap to Flex Connect group and check if the AP gets added to the AP group	Passed	
EWLCJ171S_Reg_187	Checking Flex Connect Local Switching and Local Auth works properly	To check if Flex Connect Local Switching and Local Auth works in 4800 Ap and check if the clients gets locally authenticated and switched locally	Passed	

EWLCJ171S_Reg_188	Upgrading a correct ME image to the 4800 AP and check if the ME image is upgraded	To check if a correct ME image is upgraded to 4800 AP and check if it reboots in the day 0 config	Passed	
EWLCJ171S_Reg_189	Upgrading a incorrect ME image to the 4800 AP and check if the ME image is upgrading	To check if ME image is upgrading with the wrong ME image or not	Passed	
EWLCJ171S_Reg_190	Connecting a Window J OS client to the ME image upgraded 4800 AP	To verify if the Window J OS clients gets connected to the ME image Upgraded 4800 AP	Passed	
EWLCJ171S_Reg_191	Connecting a Android client to the ME image upgraded 4800 AP	To verify if the Android clients gets connected to the ME image Upgraded 4800 AP	Passed	
EWLCJ171S_Reg_192	Connecting a IOS client to the ME image upgraded 4800 AP	To verify if the IOS clients gets connected to the ME image Upgraded 4800 AP	Passed	
EWLCJ171S_Reg_193	Connecting a Mac OS client to the ME image upgraded 4800 AP	To verify if the Mac OS clients gets connected to the ME image Upgraded 4800 AP	Passed	
EWLCJ171S_Reg_194	Converting the 4800 AP to a autonomous AP	To convert the 4800 AP into autonomous AP and check if the AP is converted into autonomous AP or not	Passed	
EWLCJ171S_Reg_195	Connecting client to 4800 AP with different Channel Width	To connect client to 4800 AP with different channel width and check if the clients gets connected to the different Channel Width .	Passed	

EWLCJ171S_Reg_196	Connecting a client using Indian extended channels enabled in DCA channels.	To connect a client enabling the Indian extended channels and check if the clients is connected in the channel allocated for the extended one or not.	Passed	
EWLCJ171S_Reg_197	Verifying AP-Image Pre-download with primary image to the 4800 AP	To verify the AP-Pre download with primary images is successful or not.	Passed	
EWLCJ171S_Reg_198	Verifying AP-Image Pre-download with primary image to the 4800 AP	To verify the AP-Pre download with primary images is successful or not.	Passed	

WPA3 Support

Logical ID	Title	Description	Status	Defect ID
EWLCJ171S_Reg_45	Verifying the WPA3 support with SAE security key.	To verify the WPA3 support with SAE security Configuration.	Passed	
EWLCJ171S_Reg_46	Verifying the WPA3 support with SAE security key by connecting the windows client.	To verify the the Client packets by connecting the windows client to WPA3 and SAE supported SSID	Passed	
EWLCJ171S_Reg_47	Verifying the WPA3 support with SAE security key by connecting the Android client.	To verify the the Client packets by connecting the Android client to WPA3 and SAE supported SSID	Passed	
EWLCJ171S_Reg_48	Verifying the WPA3 support with SAE security key by connecting the Mac os client.	To verify the the Client packets by connecting the Mac os client to WPA3 and SAE supported SSID	Passed	

EWLCJ171S_Reg_49	Verifying the WPA3 support with SAE and PSK security key.	To verify the Client packets by connecting the client to WPA3 and SAE and PSK supported SSID	Passed	
EWLCJ171S_Reg_50	Verifying the WPA3 support with SAE and 802.1x security key.	To verify the WPA3 Configuration with SAE and 802.1x supported SSID	Passed	
EWLCJ171S_Reg_51	Validating the WPA3 support with SAE and Layer 3 Splash page web redirect	To verify the WPA3 support with SAE and Layer3 Splash page web redirect	Passed	
EWLCJ171S_Reg_52	Validating the WPA3 support with SAE and Layer 3 On Mac filter failure.	To verify the WPA3 support with SAE and Layer3 On Mac filter failure	Passed	
EWLCJ171S_Reg_53	verifying the WPA3 support with SAE and PMF PSK Auth key.	To verify the WPA3 support with SAE and PMF PSK Auth key.	Passed	
EWLCJ171S_Reg_54	verifying the WPA3 support with SAE and PSK Auth key and Layer3 Splash page web redirect.	To verify the WPA3 support with SAE and PSK Auth key and Layer3 Splash page web redirect.	Passed	
EWLCJ171S_Reg_55	Verifying the WPA3 support with 802.1x security.	To verify the WPA3 support with 802.1x security for the different clients.	Passed	
EWLCJ171S_Reg_56	Verifying the WPA3 support with 802.1x and CCKM security.	To verify the WPA3 support with 802.1x and CCKM security for the different clients.	Passed	
EWLCJ171S_Reg_57	Verifying the WPA3 support with Ft+802.1x security.	To verify the WPA3 support with +Ft_802.1x security for the different clients.	Passed	
EWLCJ171S_Reg_58	Verifying the WPA3 support with Intra client roaming by using 9115AP	To verify the Intra client roaming by using WPA3 support with 9115AP	Passed	

EWLCJ171S_Reg_59	Verifying the WPA3 support and SAE security with Inter WLC Roaming	To verify inter WLC Roaming between WLANs with WPA3 support and SAE support	Passed	
EWLCJ171S_Reg_60	Verifying the WPA3 support with Roaming between Controllers with Different Radio types	To verify whether Client is Moving between Controllers with Different Radio type or not with WPA3 WLAN.	Passed	
EWLCJ171S_Reg_61	Verifying the WPA3 support Roaming between Controllers with same Radio types	To verify whether Client is Moving between Controllers with same Radio type or not with WPA3 WLAN.	Passed	

OWE Support

Logical ID	Title	Description	Status	Defect ID
EWLCJ171S_Reg_62	Verifying WPA3 and OWE support for the Windows client	To verify the OWE Auth key support to the WPA3 security for the Windows client.	Passed	
EWLCJ171S_Reg_63	Verifying WPA3 and OWE support for the Android client	To verify the OWE Auth key support to the WPA3 security for the Android client.	Passed	
EWLCJ171S_Reg_64	Verifying WPA3 and OWE support for the Mac os client	To verify the OWE Auth key support to the WPA3 security for the Mac os client.	Passed	
EWLCJ171S_Reg_65	Verifying WPA3 and OWE-Transition mode support for the Windows client	To verify the OWE-Transition mode support to the WPA3 security for the Windows client.	Passed	

EWLCJ171S_Reg_66	Verifying WPA3 and OWE-Transition mode support for the Android client	To verify the OWE-Transition mode support to the WPA3 security for the Android client.	Passed	
EWLCJ171S_Reg_67	Verifying WPA3 and OWE-Transition mode support for the Mac os client	To verify the OWE-Transition mode support to the WPA3 security for the Mac os client.	Passed	
EWLCJ171S_Reg_68	Checking the WPA3 and OWE support with Layer3 Splash page web redirect	To check the Client packets by connecting the client to WPA3 and OWE support SSID with Layer3 Splash page Web redirect.	Passed	
EWLCJ171S_Reg_69	Verifying theWPA3 and OWE Support with Layer3 On Mac filter failure.	To verify the WPA3 and OWE Support with OWE transition mode and Layer3On Mac filter failure.	Passed	
EWLCJ171S_Reg_70	Verifying the WPA3 support with OWE security with Inter WLC Roaming	To verify inter WLC Roaming between WLANs with WPA3 support and OWE support	Passed	
EWLCJ171S_Reg_71	Verifying the WPA3 support and OWE with Intra client roaming by using 9115AP	To verify the Intra client roaming by using WPA3 support with 9115AP	Passed	
EWLCJ171S_Reg_72	Verifying the WPA3 support and OWE security with Inter WLC Roaming	To verify inter WLC Roaming between WLANs with WPA3 support and OWE support	Passed	
EWLCJ171S_Reg_73	Verifying the WPA3 and OWE support with Roaming between Controllers with Different Radio types	To verify whether Client is Moving between Controllers with Different Radio type or not with WPA3 WLAN.	Passed	

EWLCJ171S_Reg_74	Verifying the WPA3 and OWE support Roaming between Controllers with same Radio types	To verify whether Client is Moving between Controllers with same Radio type or not with WPA3 WLAN.	Passed	

Best Practices WebUI

Logical ID	Title	Description	Status	Defect ID
EWLCJ171S_Reg_75	Enable/Disable the http/https for management	Verify the web UI is able to open or not through http/https after modification	Passed	
EWLCJ171S_Reg_76	Configure the NTP server	To check whether NTP server is able to configure or not for WEB UI	Passed	
EWLCJ171S_Reg_77	Configure the Client Exclusion policies[fix button is not available need to check in latest build]	To check whether Client Exclusion Policies is enabled or not	Passed	
EWLCJ171S_Reg_78	Create the WLAN with WPA2	Verify the WLAN with WPA2 after configuring via best practice	Passed	
EWLCJ171S_Reg_79	Enable the User Login Policies	Checking the User Login Policies is enabled or not	Passed	
EWLCJ171S_Reg_80	Enable the Local Profiling on one or more active WLANs	Verify the enabled Local Profile on Active WLAN	Passed	
EWLCJ171S_Reg_81	Configure the client band for all Active WLANs	To check whether client Band is applied or not for Active WLANs	Passed	
EWLCJ171S_Reg_82	Enable the 5ghz band for Active WLAN	Verify the 5ghz client band on active WLANs	Passed	
EWLCJ171S_Reg_83	Enable the 2.4ghz band for Active WLAN	Checking the 2.4ghz client band on active WLANs	Passed	

EWLCJ171S_Reg_84	Configure the Best channel width	To check whether Best channel width is configured or not on both radios	Passed	
EWLCJ171S_Reg_85	Enable the Flexible Radio Assignment	To check whether Flexible Radio Assignment is enabled or not	Passed	
EWLCJ171S_Reg_86	Configure the Load balance for one or more active WLAN	Verify the Load balance enabled or not on Active WLAN	Passed	
EWLCJ171S_Reg_87	Enable the Auto Dynamic Channel Assignment	To check whether global channel is enabled or not	Passed	

Image Predownload

Logical ID	Title	Description	Status	Defect ID
EWLCJ171S_Reg_302	Cisco Catalyst 9800 Series Wireless Controller Software updating via SFTP server	Verifying Cisco Catalyst 9800 Series Wireless Controller software updating or not via SFTP server	Passed	
EWLCJ171S_Reg_303	Invalid Cisco Catalyst 9800 Series Wireless Controller Software updating via SFTP server.	Verifying Cisco Catalyst 9800 Series Wireless Controller software updating or not via SFTP server	Passed	
EWLCJ171S_Reg_304	Cisco Catalyst 9800 Series Wireless Controller Software updating via SFTP server using different browser.	Verifying Cisco Catalyst 9800 Series Wireless Controller software updating or not via SFTP server using different browser.	Passed	
EWLCJ171S_Reg_305	Software updating via tftp server	Checking theCisco Catalyst 9800 Series Wireless Controller software updating or not via tftp server	Passed	

EWLCJ171S_Reg_306	Cisco Catalyst 9800 Series Wireless Controller Software updating via SFTP server using 9880 port.	Verifying Cisco Catalyst 9800 Series Wireless Controller software updating or not via SFTP server	Passed	
EWLCJ171S_Reg_307	Cisco Catalyst 9800 Series Wireless Controller Software updating via SFTP server using 9840 port.	Verifying Cisco Catalyst 9800 Series Wireless Controller software updating or not via SFTP server	Passed	
EWLCJ171S_Reg_308	Invalid Cisco Catalyst 9800 Series Wireless Controller Software updating via tftp server	To check whether Cisco Catalyst 9800 Series Wireless Controller software upgrading or not via tftp server	Passed	
EWLCJ171S_Reg_309	Cisco Catalyst 9800 Series Wireless Controller Software upgrading through Invalid SFTP user name/password	VerifyingCisco Catalyst 9800 Series Wireless Controller software is upgrading or not through Invalid SFTP user name/password	Passed	
EWLCJ171S_Reg_310	Cisco Catalyst 9800 Series Wireless Controller software upgrading through invalid tftp file path	Checking Cisco Catalyst 9800 Series Wireless Controllersoftware upgrading or not through invalid tftp file path	Passed	
EWLCJ171S_Reg_311	Cisco Catalyst 9800 Series Wireless Controller software upgrading through valid tftp file path using 9880 port	Checking Cisco Catalyst 9800 Series Wireless Controller software upgrading or not through valid tftp file path	Passed	
EWLCJ171S_Reg_312	Cisco Catalyst 9800 Series Wireless Controller software upgrading through valid tftp file path 9840	Checking Cisco Catalyst 9800 Series Wireless Controller software upgrading or not through valid tftp file path	Passed	

EWLCJ171S_Reg_313	Cisco Catalyst 9800 Series Wireless ControllerSoftware upgrading via Desktop(HTTP)	Verifying Cisco Catalyst 9800 Series Wireless Controller software upgrading or not via Desktop(HTTP) server	Passed	
EWLCJ171S_Reg_314	Invalid Cisco Catalyst 9800 Series Wireless Controller Software updating via Desktop(HTTP) mode	Verifying Cisco Catalyst 9800 Series Wireless Controller software upgrading or not via Desktop(HTTP) mode	Passed	
EWLCJ171S_Reg_315	ME Software upgrading via webserver	Verifying Cisco Catalyst 9800 Series Wireless Controller software upgrading or not via webserver	Passed	
EWLCJ171S_Reg_316	Invalid Cisco Catalyst 9800 Series Wireless Controller Software updating via webserver	To check whether Invalid Cisco Catalyst 9800 Series Wireless Controller software upgrading or not via webserver	Passed	
EWLCJ171S_Reg_317	ME Software upgrading via webserver using different browser	Verifying Cisco Catalyst 9800 Series Wireless Controller software upgrading or not via webserver using different browser.	Passed	

Image Download Method : HTTP Upload

Logical ID	Title	Description	Status	Defect ID
EWLCJ171S_Reg_256	Cisco Catalyst 9800 Series Wireless Controller Software images upgrading via HTTP Upload	Verifying Cisco Catalyst 9800 Series Wireless Controller -ME software images upgrading or not via HTTP Upload	Passed	

EWLCJ171S_Reg_257	Invalid Cisco Catalyst 9800 Series Wireless Controller Controller image upgrading via HTTP server	Verifying Cisco Catalyst 9800 Series Wireless Controller-ME invalid controller image is upgrading or not via HTTP server	Passed	
EWLCJ171S_Reg_258	Invalid Cisco Catalyst 9800 Series Wireless Controller AP image upgrading via HTTP server	Verifying Cisco Catalyst 9800 Series Wireless Controller invalid AP image is upgrading or not via HTTP server	Passed	
EWLCJ171S_Reg_259	Joining different model AP to Cisco Catalyst 9800 Series Wireless Controller and upgrade the device with latest image	To check whether software image are upgrading or not through different AP Models	Passed	
EWLCJ171S_Reg_260	Joining different model AP's to Cisco Catalyst 9800 Series Wireless Controller and downgrade the image	To check whether software images are Downgrading or not through different AP Models	Passed	
EWLCJ171S_Reg_261	Upgrading Cisco Catalyst 9800 Series Wireless Controller controller with wrong image and checking the error message	Verifying Cisco Catalyst 9800 Series Wireless Controller device is upgrading or not with wrong image and check the error message	Passed	
EWLCJ171S_Reg_262	Upgrading Cisco Catalyst 9800 Series Wireless Controllerwith wrong AP image and checking the error message	Verifying Cisco Catalyst 9800 Series Wireless Controller device is upgrading or not with wrong AP image and check the error message	Passed	
EWLCJ171S_Reg_263	Upgrading Cisco Catalyst 9800 Series Wireless Controller controller image alone and checking the error messages	Verifying Cisco Catalyst 9800 Series Wireless Controller software is upgrading or not with controller image alone	Passed	

EWLCJ171S_Reg_264	Upgrading Cisco Catalyst 9800 Series Wireless Controller AP image alone and checking the error messages	Verifying Cisco Catalyst 9800 Series Wireless Controller software is upgrading or not with AP image alone	Passed	
EWLCJ171S_Reg_265	Upgrading the Cisco Catalyst 9800 Series Wireless Controller with latest image and checking if any crash happen	To check whether user getting any crash log while upgrading with latest image	Passed	
EWLCJ171S_Reg_266	Downgrading the Cisco Catalyst 9800 Series Wireless Controller with latest image and checking if any crash happen	To check whether user getting any crash log while Downgrading with latest image	Passed	
EWLCJ171S_Reg_267	Checking the memory leaks while upgrading the Cisco Catalyst 9800 Series Wireless Controller	To check whether any memory leaks while upgrading with Cisco Catalyst 9800 Series Wireless Controller image	Passed	
EWLCJ171S_Reg_268	Checking the memory leaks while Downgrading the Cisco Catalyst 9800 Series Wireless Controller	To check whether any memory leaks while downgrading with Cisco Catalyst 9800 Series Wireless Controller image	Passed	
EWLCJ171S_Reg_269	Checking the Error messages while upgrading the Cisco Catalyst 9800 Series Wireless Controller	To check whether any interrupted error messages coming or not while upgrading Cisco Catalyst 9800 Series Wireless Controller Image	Passed	
EWLCJ171S_Reg_270	Checking the behaviour of AP while moving from WLC toCisco Catalyst 9800 Series Wireless Controller	To Check whether the behaviour of AP while moving from WLC to Cisco Catalyst 9800 Series Wireless Controller	Passed	

Config Wireless

Logical ID	Title	Description	Status	Defect ID
EWLCJ171S_config_1	Verify the WLAN configuration with PSK and Ft-802.1x AKM's	To verify the WLAN configuration with PSK and Ft-802.1x AKM's	Failed	CSCvs40319
EWLCJ171S_config_2	Verify the behaviour of 1810AP in Cisco Catalyst 9800 Series Wireless Controller	To verifying the behaviour of 1810 AP	Passed	
EWLCJ171S_config_6	Static-WEP configuration with 104 key throws error.	To verifying the static-WEP configuration with 104 key	Failed	CSCvs47124
EWLCJ171S_config_13	Observed memory leakage in C9800-L-C-K9	To observing memory leakage in C9800-L-C-K9	Failed	CSCvs43516

SR Cases

Logical ID	Title	Description	Status	Defect ID
EWLCJ171S_SR_01	Mapping multiple WLAN's to policies and verify same in running configuration	To verify whether user able to see the WLAN information when mapped policies	Passed	
EWLCJ171S_SR_02	Mapping policy to AP and checking for the configuration in running configuration	To verify WLAN's information in running configuration after mapping policy to AP	Passed	
EWLCJ171S_SR_03	Mapping policy to multiple AP's and checking for the configuration in running config	To check WLAN's information after mapping policy to multiple Aps	Passed	

EWLCJ171S_SR_04	Checking the AP configuration details after switchover scenario	To verify the AP configuration details in standby switch after primary down	Passed	
EWLCJ171S_SR_05	Reloading the AP multiple times and checking for the configuration details	To verify the AP configuration details after AP reloaded multiple time	Passed	
EWLCJ171S_SR_06	Enable/disable the AP all configuration parameter (Radio Core Mode, Static Ip Failover) and check for same after the switchover	To verify the AP configuration details in standby switch after enable/disable the AP config	Passed	
EWLCJ171S_SR_07	Joining day0 AP to the controller without PnP configuration	To verify whether day0 AP Joins controller without PnP or not	Passed	
EWLCJ171S_SR_08	Resetting the AP and joining to the controller without PnP configuration	To verify whether AP joining to controller after reset the configuration	Passed	
EWLCJ171S_SR_09	Doing PnP successfully and joining AP to the controller	To verify whether AP joining to controller after PnP done successfully	Passed	
EWLCJ171S_SR_10	Checking the 802.1x client connection with flex COS/IOS AP after	To verify whether client connecting to flex connect AP with 802.1x security or not	Passed	
EWLCJ171S_SR_11	Upgrade/downgrade the Cisco Catalyst 9800 Series Wireless Controller and check for the 802.1x client authentication	To check the connected 802.1x client authentication after the device upgrade/downgrade	Passed	
EWLCJ171S_SR_12	Reload the Flex AP and check for the 802.1x authenticated client	To Verify whether client connected to radius server successfully after AP reloaded	Passed	

EWLCJ171S_SR_13	Checking the Android client by associating to AP9115 with EAP security methods.	To check whether Android client able to associate the 9115AP with EAP security	Passed	
EWLCJ171S_SR_14	Checking the IOS client by associating to AP4800 with EAP security methods.	To check whether IOS client able to associate the 4800AP with EAP security	Passed	
EWLCJ171S_SR_15	Checking the Windows client by associating to AP9120 with EAP security methods.	To check whether Windows client able to associate the 9120AP with EAP security	Passed	
EWLCJ171S_SR_16	Performing the Cisco Catalyst 9800 Series Wireless Controller Power Off/On after downloading the config file from GUI and verify the behaviour.	To check whether Factory reset happening or not after downloading the config file from GUI and performing the Cisco Catalyst 9800 Series Wireless Controller power off/on	Passed	
EWLCJ171S_SR_17	Performing the Cisco Catalyst 9800 Series Wireless Controller reload after downloading the config file and verify the behaviour.	To check whether Factory reset happening or not after downloading the config file and performing the Cisco Catalyst 9800 Series Wireless Controller reload	Passed	
EWLCJ171S_SR_18	Performing the Cisco Catalyst 9800 Series Wireless Controller Power Off/On for HA after downloading the config file from GUI and verify the behaviour.	To check whether Factory reset happening or not after downloading the config file from Cisco Catalyst 9800 Series Wireless Controller-HA device GUI and performing the Cisco Catalyst 9800 Series Wireless Controller power off/on	Passed	
EWLCJ171S_SR_19	Verify the 9115AP behaviour in Flex/local mode with 80/160Mhz bandwidth	To check whether 9115AP got crashed or not in Flex/local mode with 80/160Mhz bandwidth	Passed	

EWLCJ171S_SR_20	Verify the 2800AP behaviour in Flex/local mode with 80/160Mhz bandwidth	To check whether 2800AP got crashed or not in Flex/local mode with 80/160Mhz bandwidth	Passed	
EWLCJ171S_SR_21	Verify the 3702AP behaviour in Flex/local mode with 80/160Mhz bandwidth	To check whether 3702AP got crashed or not in Flex/local mode with 80/160Mhz bandwidth	Passed	
EWLCJ171S_SR_22	Change the Active switch Priority and observe the Cisco Catalyst 9800 Series Wireless Controller HA.	To check whether Cisco Catalyst 9800 Series Wireless Controller HA failover happening or not by changing the Active switch priority.	Passed	
EWLCJ171S_SR_23	Change the Active switch renumber and observe the Cisco Catalyst 9800 Series Wireless Controller HA.	To check whether Cisco Catalyst 9800 Series Wireless Controller HA failover happening or not by changing the Active switch renumber.	Passed	
EWLCJ171S_SR_24	Create the WLAN with central dhcp/ central switching	Verify the central dhcp/central switching conifg after AP reboot	Passed	
EWLCJ171S_SR_25	Create the Coverage Areas, Obstacles, Location Regions in site maps	To check whether Coverage Areas, Obstacles, Location Regions are created or not in MAPS	Passed	
EWLCJ171S_SR_26	Verify the client Coverage Areas, Obstacles, Location Regions	Checking the client Coverage Areas, Obstacles, Location Regions in PI floor maps	Passed	
EWLCJ171S_SR_27	Verify the wave2 AP's health after controller downgrading/upgrading	Validate the EWC controller is upgrading/downgrading successfully and WAVE2 AP's health	Passed	
EWLCJ171S_SR_28	Converting the 9115AP to EWC-ME	Verify the 9115 AP to EWC-ME converting or not	Passed	

EWLCJ171S_SR_29	Rename the user defined dashboard in Japanese UI	To check whether successfully user defined dashboard renamed or not	Passed	
EWLCJ171S_SR_30	Rename the default dashboard in Japanese UI	Verify the successfully default dashboard renamed or not	Passed	
EWLCJ171S_SR_31	Install the new SSL certificate in CMX	To check whether SSL certificate is installed successfully or not in CMX	Passed	
EWLCJ171S_SR_32	Configuring HA Setup check the client connectivity after master failover	To verify the client connectivity after master failover	Passed	
EWLCJ171S_SR_33	Configuring HA Setup and upgrading the image through TFTP server	To verify the image upgrade through TFTP Server after master failover	Passed	
EWLCJ171S_SR_34	Downgrading Cisco Catalyst 9800 Series Wireless Controller-ME and checking Radius server details	To verify whether Radius server details showing or not after image Downgrade	Passed	
EWLCJ171S_SR_35	Changing Security details after client connected to Radius server	To verify whether Security details are possible to change or not when client connected with Radius server	Passed	
EWLCJ171S_SR_36	Configuring Invalid Radius server details and trying to connect clients	To verify whether Client is able to connect with Invalid radius server details or not	Passed	
EWLCJ171S_SR_37	Associate the multiple clients to the flex profile WLAN	Verify the clients connectivity in flex profile WLAN	Passed	
EWLCJ171S_SR_38	Create the flex profile on 9800 HA setup	To check whether flex profile is created or not on HA setup	Passed	

EWLCJ171S_SR_39	Importing SSL Certificate in Cisco Catalyst 9800 Series Wireless Controller & checking the client connectivity	To check whether the SSL Certificate upload & the client able to connect or not in Cisco Catalyst 9800 Series Wireless Controller	Passed	
EWLCJ171S_SR_40	Verifying the 5ghz client throughput in 9115 AP	validate the 5ghz client throughput in 9115 AP	Passed	
EWLCJ171S_SR_41	Verifying the 2.4 ghz client throughput in 9120 AP	validate the 2.4 ghz client throughput in 9120 AP	Passed	
EWLCJ171S_SR_42	Checking Flex ACL present or not in c9115 Flex connect AP	Verify the Flex Acl presenence in c9115 flexconenct AP or not	Passed	
EWLCJ171S_SR_43	Checking Flex ACL present or not in 4800 Flex connect AP	Verify the Flex Acl presence in 4800 flexconenct AP or not	Passed	
EWLCJ171S_SR_44	Removing Syslog server config from AP profile	Verify that Syslog host removed from AP profile or not	Passed	
EWLCJ171S_SR_45	Disabling Syslog in Cisco Catalyst 9800 Series Wireless ControllerGlobally	Verify that Syslog disabled from Cisco Catalyst 9800 Series Wireless Controller globally	Passed	
EWLCJ171S_SR_46	Configuring auto duplex for catalyst gig port and connect AP	Verify that there is no Duplex mismatch message in switch console	Passed	
EWLCJ171S_SR_47	Configuring full duplex for IOS-XE gig port and AP port	Verify that there is no Duplex mismatch message in switch console	Passed	
EWLCJ171S_SR_48	Verifying MacOS client PEM state while moving client from CWA_SSID-1 to CWA_SSID-2	Verify the MacOS client PEM state is 'Central_WEB_AUTH' after moving to new CWA config SSID	Passed	
EWLCJ171S_SR_49	Verifying MacOS client PEM state with invalid user	Verify the MacOS client PEM state is 'CENTRAL_WEB_AUTH' with invalid user	Passed	

EWLCJ171S_SR_50	Downloading the Recommended CCO build for c9115 eWC	Verify the Recommended CCO build only downloaded in eWC	Passed	
EWLCJ171S_SR_51	Downloading the latest CCO build for c9115 eWC	Verify the latest CCO build only downloaded in eWC	Passed	
EWLCJ171S_SR_52	Checking the 1810 AP's SSH connection status after changing AP mode	To verify the SSH connection working for 1815 AP after changing AP mode	Passed	
EWLCJ171S_SR_53	Checking the 9115 AP's SSH connection status after download/upload config file	To verify that SSH connection working for 9115 AP after download/upload config file	Passed	
EWLCJ171S_SR_54	Checking the client connection during the roaming of AP.	To verify the SSH connection during the AP roaming.	Passed	
EWLCJ171S_SR_55	Checking the 1810 AP's SSH connection after changing from connected to standalone mode.	To verify whether the SSH is enable after changing from connected to standalone.	Passed	
EWLCJ171S_SR_56	Checking the service health of applications in PI	To Verify whether the Service health information is shown in PI or not	Passed	
EWLCJ171S_SR_57	checking the metrics in the PI application.	To verify whether metrics in the application of PI is shown properly or not.	Passed	
EWLCJ171S_SR_58	checking the client connection and status of it.	To verify whether the client metrics in PI is Proper or not.	Passed	
EWLCJ171S_SR_59	checking the SPID and Serial number on PI	To check whether the spid and serial no details are displayed or not.	Passed	
EWLCJ171S_SR_60	Configuring some operation in PI and checking the status of it	To check whether the status of the PI is working fine.	Passed	

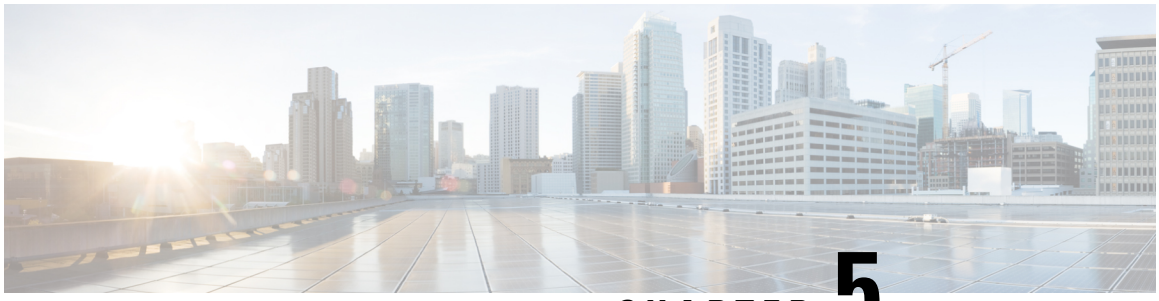
EWLCJ171S_SR_61	Checking the SNMP status after adding the device.	To check whether the SNMP is enabled after adding the device in PI	Passed	
EWLCJ171S_SR_62	Checking the SNMP status after deleting the device.	To check whether the SNMP is enabled after deleting the device in PI	Passed	
EWLCJ171S_SR_63	Checking the SNMP status after rebooting the device.	To check whether the SNMP is enabled after rebooting the device in PI	Passed	
EWLCJ171S_SR_64	Checking the SNMP status in HA mode.	To check whether the SNMP state	Passed	
EWLCJ171S_SR_65	Checking the status of SNMP while exporting template from PI and rebooting.	To check whether the exporting and reboot is happened without changing snmp status.	Passed	
EWLCJ171S_SR_66	Checking the connectivity of the CMX and its status	To check whether the CMX is enabled and generating logs	Passed	
EWLCJ171S_SR_67	Checking the functionality of CMX when it is in disabled state.	To check that the CMX does not provide logs when it is in disabled state.	Passed	
EWLCJ171S_SR_68	GUI/SSH of the primary wlc when we do a HA failover in a pair of Cisco Catalyst 9800 Series Wireless Controller in Chrome Browser.	Verify able to access the GUI/SSH of the primary wlc when we do a HA failover in a pair of Cisco Catalyst 9800 Series Wireless Controller in any browser. Disconnect and Reconnect the wireless client, it works fine in Chrome Browser.	Passed	

EWLCJ171S_SR_69	GUI/SSH of the primary wlc when we do a HA failover in a pair of Cisco Catalyst 9800 Series Wireless Controller in IE Browser.	Verify able to access the GUI/SSH of the primary wlc when we do a HA failover in a pair of Cisco Catalyst 9800 Series Wireless Controller in any browser. Disconnect and Reconnect the wireless client, it works fine in IE Browser.	Passed	
EWLCJ171S_SR_70	Licencing count with different device on virtual Appliance.	To Verify the Licence with respect to device type and count - Virtual Application	Passed	
EWLCJ171S_SR_71	Licencing count with different device on Physical Appliance.	To Verify the Licence with respect to device type and count - Physical Appliance	Passed	
EWLCJ171S_SR_72	Performance Dashboard able to show all the data's properly.	Verify Performance Dashboard able to show all the data's properly.	Passed	
EWLCJ171S_SR_73	Wireless Dashboard able to show all the data's properly.	Verify Wireless Dashboard able to show all the data's properly.	Passed	
EWLCJ171S_SR_74	Network device Export option with selected device	Verify export of network devices properly with selected devices.	Passed	
EWLCJ171S_SR_75	Network device Export option with Bulk export option.	Verify export of network devices properly with Bulk Option.	Passed	
EWLCJ171S_SR_76	OFDM Parameter keeps showing 'Automatic' or manual allocation	To Verify the 'Configuration' of 'Phy OFDM Parameters' on AP3802E	Passed	
EWLCJ171S_SR_77	To Verify the 'Configuration' of 'Phy OFDM Parameters'	To Verify the 'Configuration' of 'Phy OFDM Parameters' on AP2802	Passed	

EWLCJ171S_SR_78	Upgrading PI from 3.7 CCO build to 3.8 and check if the device details before and after upgrade are same .	To upgrade PI from 3.7 CCO to 3.8 and check if the device details are same as before and after upgrade	Passed	
EWLCJ171S_SR_79	Restoring the backed up data in PI and check if the details are restored completely or not	To restore the backed up data in PI and check if the restoration of data is successful also Check the device details and configuration	Passed	
EWLCJ171S_SR_80	Restoring backed up data after fresh installation .	To restore backup data to PI making a fresh install.	Passed	
EWLCJ171S_SR_81	Making schedule archive configuration for particular Cisco Catalyst 9800 Series Wireless Controller device happens when scheduled	To check if the schedule archive configuration for the Cisco Catalyst 9800 Series Wireless Controller device happens successfully when scheduled or not	Passed	
EWLCJ171S_SR_82	Schedule Archive for all network devices through inventory device	To check if Schedule Archive for all network devices through inventory page works or not	Passed	
EWLCJ171S_SR_83	Generating a custom report related to AP and check different details of the AP	To generate a custom report related to AP and check if the details of the AP and Sub details of the AP are shown correctly.	Passed	
EWLCJ171S_SR_84	Generating a custom report related to Rogue AP and check different details of the AP	To generate a custom report related to Rogue AP and check if the details of the AP and Sub details of the AP are shown correctly.	Passed	
EWLCJ171S_SR_85	Generating a custom report related to Clients and check different details of the AP	To generate a custom report related to Clients and check if the details of the AP and Sub details of the AP are shown correctly.	Passed	

EWLCJ171S_SR_86	Check if the HA happens when the connectivity is made through Eth1	To check if the HA pairing happens when the connectivity is made through Eth1	Passed	
EWLCJ171S_SR_87	Check if the HA happens when the connectivity is made through Eth0	To check if the HA pairing happens when the connectivity is made through Eth1	Passed	
EWLCJ171S_SR_88	Check if the HA happens when the connectivity is made through Eth0 port in Primary and Eth1 in secondary	To check if the HA happens when the connectivity is made through Eth0 port in Primary and Eth1 in secondary	Passed	
EWLCJ171S_SR_89	Upload the backup config file via TFTP method	To verify whether config file uploaded or not via FTP method	Passed	
EWLCJ171S_SR_90	Upload the backup config file via HTTP method	To verify whether config file uploaded or not via HTTP method	Passed	
EWLCJ171S_SR_91	Upload the backup config file via PI	To verify whether config file uploaded or not via PI	Passed	
EWLCJ171S_SR_92	Checking Client connectivity while primary goes down in HA	To check whether client associate properly or not	Passed	
EWLCJ171S_SR_93	Checking Client connectivity while roaming	To check whether client associate properly or not	Passed	
EWLCJ171S_SR_94	Checking VLAN details after configuring flex profile and Central Switching	To Check whether VLAN details shown or not while configuring AP flex mode and Central Switching	Passed	
EWLCJ171S_SR_95	Checking VLAN details without AAA override	To Check whether VLAN details shown or not while configuring AP flex mode and without AAA override	Passed	
EWLCJ171S_SR_96	Checking the Ap crash while changing the Ap radios(2.4 GHz /5GHz)	To Check whether ap crashed or not while changing the radios(2.4 & 5GHz)	Passed	

EWLCJ171S_SR_97	Checking the Ap crash after Ap Reset	To Check whether ap crashed or not after Ap reload	Passed	
EWLCJ171S_SR_98	Checking the Ap crash while disable the MFP configuration	To Check whether ap crashed or not after disabling MFP	Failed	CSCvs23453
EWLCJ171S_SR_99	Associate client and checking AID value while doing inter roaming with Aps in Local/flex	To verify whether clients getting AID value after the inter roaming or not	Passed	
EWLCJ171S_SR_100	Associate client and checking AID value while doing intra roaming with Aps in Local/flex	To verify whether clients getting AID value after doing intra roaming or not	Passed	
EWLCJ171S_SR_101	Associate client and checking AID value while doing FT roaming with Aps in Local/flex	To verify whether clients getting AID value after the FT roaming or not	Passed	



CHAPTER 5

Related Documentation

Related Documentation

CME 8.10 Rlease Notes

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

WLC 8.10 Configuration Guide

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

CMX 10.6 Configuration Guide

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

PI 3.7 User Guide

https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-7/user/guide/bk_CiscoPrimeInfrastructure_3_7_0_User_Guide.html

ISE 2.6 Release Notes

https://www.cisco.com/c/en/us/td/docs/security/ise/2-6/release_notes/b_ise_26_RN.html

Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide

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

Cisco Catalyst 9800 Series Wireless Controller 17.1 Configuration Guide

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-1/config-guide/b_wl_17_11_cg/mac-authentication-bypass.html

Cisco Catalyst 9800 Series Wireless Controller 17.1 Release Notes

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-1/release-notes/rn-17-1-9800.html

Related Documentation