Test Results Summary for Cisco Wireless LAN Controller AireOS 8.10 ,CME 8.10 & IOS XE 16.12 for Japan (Release Version AireOS 8.10.105.0 ,CME 8.10.105.0,IOX XE 16.12.1)

First Published: 2019-10-23

Last Modified: 2019-10-24

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

CONTENTS

CHAPTER 1

Overview

Cisco Wireless LAN Solution Test

Cisco Wireless LAN Solution 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 Wireless LAN Solution Test 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 WLC 8.10 & eWLC 16.12 and CME 8.10
- 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 Wireless LAN Controller 8540
- Cisco Wireless LAN Controller 5520
- Cisco Wireless LAN Controller 3504
- Virtual Wireless LAN Controller
- Cisco Mobility Express 1850
- Cisco Mobility Express 1830
- Cisco Mobility Express 1815I
- Cisco Mobility Express 4800
- Cisco Mobility Express 3800
- Cisco Mobility Express 2800

- Cisco Mobility Express 1562
- Cisco Mobility Express 1542
- Catalyst Mobility Express 9115/9120
- Cisco Elastic Wireless LAN Controller 9800-L (Lite)
- Virtual Elastic Wireless LAN Controller
- DNAC
- CMX
- APIC-EM Controller appliance
- ISE(VM)
- Access Point 3700
- Access Point 2700
- Access Point 1700
- Access Point 1570
- Access Point 1542
- Access Point 1530
- Access Point 702
- Access Point 1850
- Access Point 1830
- Access Point 4800
- Access Point 3800
- Access Point 2800
- Access Point 1810
- Access Point 1815I
- Access Point 1815W
- Access Point 9115
- Access Point 9120
- Cisco Prime Infrastructure (Physical-UCS,VM)

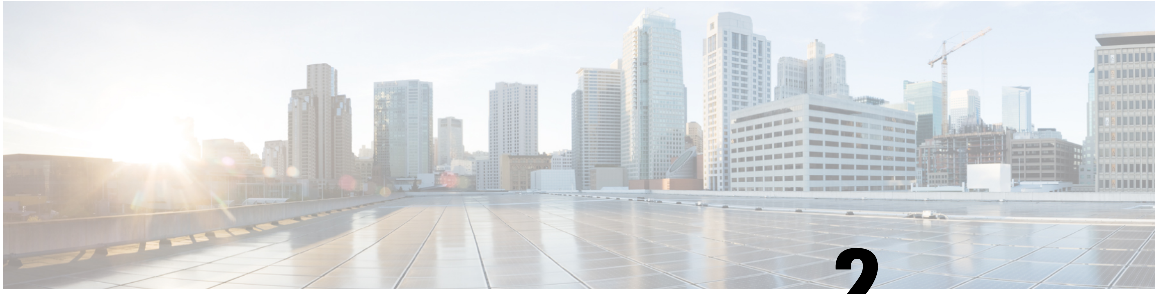
Acronyms

Acronym	Description
AAA	Authentication Authorization and Accounting
ACL	Access Control List

Acronym	Description
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
DNAC	Cisco Digital Network Architecture Center
DNS	Domain Name System
DTIM	Delivery Traffic Indication Map
DSCP	Differentiated Services Code Point
DTLS	Datagram Transport Layer Security
EAP	Extensible Authentication Protocol
EULA	End User Licence Agreement
EWLC	Elastic Wireless LAN Controller
FLA	Flex Local Authentication

Acronym	Description
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
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
MC2UC	Multicast to Unicast
MFP	Management Frame Protection
mDNS	multicast Domain Name System
MIC	Message Integrity Check
MSE	Mobility Service Engine
MTU	Maximum Transmission Unit
NAC	Network Admission Control
NAT	Network Address Translation
NBAR	Network Based Application Recognition
NCS	Network Control System
NGWC	Next Generation Wiring closet
NMSP	Network Mobility Services Protocol
OEAP	Office Extended Access Point
PEAP	Protected Extensible Authentication Protocol
PEM	Policy Enforcement Module
PI	Prime Infrastructure
PMF	Protected Management Frame
PnP	Plug n Play

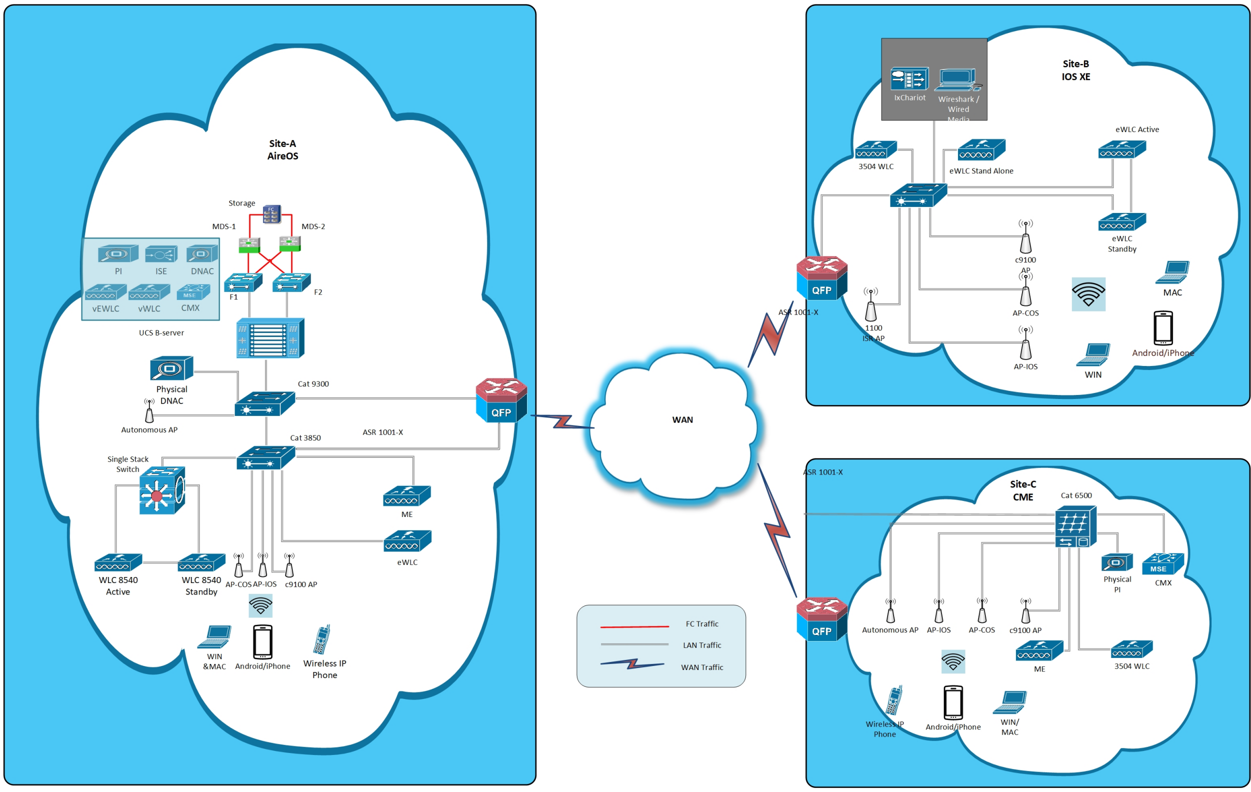
Acronym	Description
POI	Point of Interest
PPPoE	Point-to-Point Protocol over Ethernet
PSK	Pre-shared Key
QOS	Quality of service
RADIUS	Remote Authentication Dial-In User Service
RAP	Root Access Point
RP	Redundancy Port
RRM	Radio Resource Management
SDN	Software Defined Networking
SOAP	Simple Object Access 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
TACACS	Terminal Access Controller Access Control System
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
vWLC	Virtual Wireless LAN Controller
VPC	Virtual port channel
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WGB	Workgroup Bridge
wIPS	Wireless Intrusion Prevention System
WLAN	Wireless LAN
WLC	Wireless LAN Controller
WPA	Wi-Fi Protected Access
WSM	Wireless Security Module



CHAPTER 2

Test Topology and Environment Matrix

Test Topology



Component Matrix

Category	Component	Version
Controller	Wireless LAN Controller 8540	8.10.105.0
	Wireless LAN controller 5520	8.10.105.0
	Wireless LAN controller 3504	8.10.105.0
	IOS-XE 9800	16.12.1
	9800 Controller (VM)	16.12.1
	Virtual Controller	8.10.105.0
	CME 1562/1850/1830	8.10.105.0
	CME 4800/3800/2800	8.10.105.0
	Catalyst Mobility Express 9115	16.12.1
	Catalyst Mobility Express 9120	16.12.1
	Virtual Elastic Wireless LAN Controller	16.12.1
	Cisco Elastic Wireless LAN Controller 9800-L	16.12.1
Applications	Prime Infrastructure (Virtual Appliance, UCS based)	3.7.0.1.59
	ISE(VM)	2.6
	CMX(Physical (3375), VM)	10.6
	DNAC	1.3.2
	APIC-EM Controller appliance	1.6
	MSE(Physical (3365),VM)	8.0.140.0
	Cisco Jabber for Windows, iPhone	12.6.0
	Cisco Air Provisioning App	1.4

Category	Component	Version
Access Point	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 1815/1815W	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
	Catalyst 9115 AX AP	16.12
	Cisco AP 1540/1530	15.3
	Cisco AP 9120	15.3
	Cisco AP 9115	15.3
	Cisco ISR 1100 AP	16.12
Switch	Cisco 3750V2 switch	15.0(2)SE2
	Cisco Cat 6509-E	15.1(1)SY1
	Cisco Cat 9300	16.11.1
	Cisco Cat 9200L	16.12
	Cisco Cat 9800	16.12.2
Chipset	5300, 6300 AGN	15.18.0.1
	7265 AC	21.40.2
	Airport Extreme	7.9.1

Category	Component	Version
Client	Operating System(JOS)	Windows 7 Enterprise
		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 13.1.3
	iPhone 6, 6S & 7,10 (JP Locale)	iOS 13.1.3
	Samsung Galaxy S4 ,S7 & S10, Nexus 6P, Sony Xperia XZ	Android 9.0 Pie
	Wireless IP Phone 8821	11-0-5MN-102
	End points	Windows 7 Enterprise
		Apple Mac 10.15
		Windows 8 & 8.1
		iPhone 6,6S & 7,10
		Windows 10
		Samsung Galaxy S4, S7,S10 Nexus 6P,SonyXperia
	Cisco AnyConnect VPN Client	4.8.175
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	69.0
	Safari	13.0
	Chrome	77.0
Antenna	Hyperlocation	NA
Access Point	Autonomous AP	15.3.3-JI3

What's New ?

WLC AireOS

- AireOS AP Accounting
- CPU ACL

- Indoor Mesh
- Master key WLC Encryption
- ATF Wave 2
- Per AP Group NTP Server Config
- Flexconnect Post Auth ACL Per WLAN
- ATF for All Modes(Mesh and ME)
- Intelligent Capture for 1850 AP
- Intelligent Capture for 9115 AP
- Nbar Upgrade
- Password Encryption in running Configuration
- Support of Trap notification via SNMP3
- RSSI and SNR in ASSOC request
- WPA3 Support
- OWE Support
- DNA Spaces
- DNAC Assurance
- Browser Rendering Coverage

CME

- ME Config download Enhancement
- Mesh support on ALL Indoor wave 2 APS including ME

IOS XE

- Intelligent Capture for 1850 AP
- ATF for All Modes
- WEBUI : Best Practices
- ATF support for Wave-2 APs
- WPA3 Support
- OWE Support

Open Caveats

Defect ID	Title
CSCvr82264	AP 3802 Crashed due Systemd critical process crash
CSCvp98478	1562 AP got crashed After upgrading WLC
CSCvr33062	Samsung s10 client not able to connect to the WPA2+WPA3-SAE+PSK+FT PSK+PSK-SHA2 Mixed mode.
CSCvq37536	Flex AVC rules are not deployed to WLC from PI
CSCvq24204	Getting false beacon stuck logs for both radio 0 and radio 1 in AP 9115AX
CSCvr33178	OWE-TM settings under open WLAN gets discarded after editing the enhanced open WLAN configurations

CSCvr60426	Not able to configure the Radius NAC after configuring the Tunneling profile.
CSCvp90962	AAA method list-name accepting invalid input in eWLC CLI.
CSCvr31372	Configured Preferred master is not showing in Monitoring Page
CSCvr78271	Not able to perform HTTP/HTTPS secure mode configuration in eWLC-ME UI
CSCvr63290	Samsung s10 client not able to connect to the 3702 AP with WPA2+WPA3 Mixed mode.
CSCvr70785	Not able to configure http/https web secure mode in Best practice page
CSCvq35277	Need to remove Sensor mode support for this AP model C9115AXI-D
CSCvq39055	Able to enable the WLAN with out configuring the Pre-shared key for PMF-PSK.
CSCvq45149	Able to configure ATF optimization in monitor mode
CSCvr51021	Getting error popup while changing Flexconnect/Local to Bridge or Flex+Brige AP mode in PI
CSCvr63038	Clean Air NSI key is not showing for AP in eWLC ME -- not seen in oper table
CSCvr14732	Bridge mode not reflecting when APC9115AXI-D mode changed from flex to Bridge in eWLC UI
CSCvr31335	Preferred Master AP reboots when selected with Convert to CAPWAP option.
CSCvr31441	Accounting Identity list name has no restriction in eWLC CLI

Resolved Caveats

Defect ID	Title
CSCvp51557	System crash happend while configuring min and max polling intervals in NTP
CSCvp59502	Controller reloads unexpectedly during de-authenticating client in multiple times[10-15] on UI page
CSCvp94967	Policy type Mismatch in client when Local Authentication enabled
CSCvq54175	System got crashed due to "commandConfigVapSplitTunnel+448"
CSCvq55777	Controller crashed due to spamReceiveTask
CSCvq66507	Controller crashed on configuring NTP server
CSCvq18615	OWE Transition mode and Open SSID aren't configuring after Downloaded the Configuration file
CSCvq23619	Documentation issue for AP 9115AX
CSCvq40750	AP9115 crashed while upgrading WLC with 2 different images(8.10.104.63,8.10.204.21)
CSCvr40861	WPA2 security policy is showing for WPA3-802.1x clients.
CSCvq48510	Unable to enable mesh battery state from WLC CLI

CSCvr16538	UI status showing wrong after device provisioned successfully
CSCvr14947	WLAN security page redirecting to None security page after configuring the WPA3-SAE security
CSCvr55261	Unable to create guest user with auto generated password having special character "double quotes“
CSCvr62028	Documentation issue for Interim Interval in WLC
CSCvp96838	eWLC Controller crashed @ linux_iosd-image has been held down (rc 139)
CSCvq37633	Wired clients are not displaying in eWLC UI
CSCvp78775	While adding Policy Map-Local Policy in Move To option Ok button is not working in eWLC UI
CSCvq01705	Not able to modify the WLAN with static wep security.
CSCvq33289	WLAN is created and saved successfully without PSK while configuring FT+PSK
CSCvq63217	Media stream Clients are not showing in eWLC GUI (caused by TDL Model change CSCvj79379)
CSCvq60933	While enabling the OWE AKM AES is disabled
CSCvo85672	User can able to enable the Optimization for the monitor mode profiles in CLI
CSCvp88842	Able to configure the PSK with OSEN security in CLI.
CSCvr35036	Need validation on session announcement phone textbox.
CSCvq14560	Rogue AP rules after creating shows empty
CSCvq29075	BP - 2.4GHz Low Data Rates manual Configuration link redirected to 5GHz Band
CSCvq53705	ME UI not operational due to "error in setting port number"
CSCvq39003	Not able to change the Security type from Enhanced Open to Personal WPA3
CSCvq39168	Access type is redirecting to WPA2 Enterprise even configured with WPA2 Personal
CSCvq57979	Not able to upload and download the configuration file from CME CLI by using FTP

CHAPTER 3

New Features

CME

ME Config download Enhancement

Logical ID	Title	Description	Status	Defect ID
MEJ810S_CDE_01	Perform Day0 and upload config file through TFTP	To check whether previous config file uploaded and reflected successfully through TFTP after day0	Passed	
MEJ810S_CDE_02	Perform Day0 and upload config file through FTP	To check whether previous config file uploaded and reflected successfully through FTP after day0	Passed	
MEJ810S_CDE_03	Perform ME failover after uploading config file from TFTP	To check whether configurations reflected successfully through TFTP after ME failover	Passed	
MEJ810S_CDE_04	Configure preferred master and upload config file from FTP	To check whether preferred master comes up after rebooting through config update	Passed	

MEJ810S_CDE_05	Perform roll-back by uploading invalid config file from HTTP	To check whether ME automatically rollback to old config after uploading invalid file	Passed	
MEJ810S_CDE_06	Perform config update through CLI	To check whether config file uploading successfully through CLI	Passed	
MEJ810S_CDE_07	Upgrade/downgrade and upload the config file simultaneously	To verify whether error displays when both upgrade/downgrade and uploading done simultaneously	Passed	
MEJ810S_CDE_08	Scheduling config update with frequency hourly using FTP	To verify whether config files scheduled hourly using FTP and uploaded successfully	Passed	
MEJ810S_CDE_09	Uploading config file from HTTP to controller	To check whether config files uploaded successfully from HTTP to controller	Passed	
MEJ810S_CDE_10	Transfer config file from FTP to controller	To Check whether config files uploaded successfully from FTP to controller	Passed	
MEJ810S_CDE_11	Checking ME will reboot after uploading config through TFTP	To Check whether config files uploaded successfully from TFTP to controller after rebooting	Passed	
MEJ810S_CDE_12	Uploading config file from SFTP to controller	To Check whether config files uploaded successfully from SFTP to controller	Passed	

MEJ810S_CDE_13	Uploading config file when TFTP/FTP not accessible	To check whether error message displaying successfully when TFTP/FTP not accessible	Passed	
MEJ810S_CDE_14	Checking FTP details after performing Day0	To Check whether FTP details are clearing after Day0	Passed	
MEJ810S_CDE_15	Checking TFTP details after performing Day0	To Check whether TFTP details are clearing after Day0	Passed	
MEJ810S_CDE_16	Downloading config file from controller to external source	To Check whether config files downloaded successfully from controller to external source	Passed	
MEJ810S_CDE_17	Scheduling config update with frequency once using TFTP	To verify whether config files scheduled once using TFTP and uploaded successfully	Passed	
MEJ810S_CDE_18	Scheduling config update with frequency weekly using SFTP	To verify whether config files scheduled weekly using SFTP and uploaded successfully	Passed	
MEJ810S_CDE_19	Scheduling config update with frequency monthly using TFTP	To verify whether config files scheduled monthly using TFTP and uploaded successfully	Passed	

Mesh support on ALL Indoor wave 2 APS including ME

Logical ID	Title	Description	Status	Defect ID
MEJ810S_Mesh_01	Configuring mesh in ME	To verify Mesh configuration is successful or not without any error	Passed	

MEJ810S_Mesh_02	Checking windows client connecting to RAP with OPEN security	To Verify windows client is connecting to RAP or not with open security	Passed	
MEJ810S_Mesh_03	Checking android client connecting to mesh AP with WPA personal security	To Verify windows client is connecting to MESH AP or not with WPA Personal security	Passed	
MEJ810S_Mesh_04	Checking MACOS client connecting to mesh AP with WPA Enterprise security	To Verify windows client is connecting to MESH AP or not with WPA Enterprise security	Passed	
MEJ810S_Mesh_05	Checking WLAN scheduling for client with MESH configuration	To Verify WLAN scheduling is applying to client or not with MESH configuration	Passed	
MEJ810S_Mesh_06	Checking client roaming between RAP to CAPWAP MAP with OPEN security	To Verify client roaming between RAP to CAPWAP MAP with OPEN security	Passed	
MEJ810S_Mesh_07	Checking client roaming between RAP to CAPWAP MAP with WPA Personal security	To Verify client roaming between RAP to CAPWAP MAP with WPA Personal security	Passed	
MEJ810S_Mesh_08	Checking client roaming between RAP to CAPWAP MAP with WPA Enterprise security and Radius as Authentication server	To Verify client roaming between RAP to CAPWAP MAP with WPA Enterprise security and Radius as Authentication server	Passed	
MEJ810S_Mesh_09	Checking client roaming between RAP to CAPWAP MAP with WPA Enterprise security and AP as Authentication server	To Verify client roaming between RAP to CAPWAP MAP with WPA Enterprise security and AP as Authentication server	Passed	

MEJ810S_Mesh_10	Checking client roaming between RAP to ME-Capable MAP with OPEN security	To Verify client roaming between RAP to ME-Capable MAP with OPEN security	Passed	
MEJ810S_Mesh_11	Checking client roaming between RAP to ME-Capable MAP with WPA Personal security	To Verify client roaming between RAP to ME-Capable MAP with WPA Personal security	Passed	
MEJ810S_Mesh_12	Checking client roaming between RAP to ME-Capable MAP with WPA Enterprise security and Radius as Authentication server	To Verify client roaming between RAP to ME-Capable MAP with WPA Enterprise security and Radius as Authentication server	Passed	
MEJ810S_Mesh_13	Checking client roaming between RAP to ME-Capable MAP with WPA Enterprise security and AP as Authentication server	To Verify client roaming between RAP to ME-Capable MAP with WPA Enterprise security and AP as Authentication server	Passed	
MEJ810S_Mesh_14	Configuring ACL with mesh configuration to client	To verify ACL is applying to client or not with mesh configuration	Passed	
MEJ810S_Mesh_15	Configuring AVC to client with mesh configuration	To verify AVC is applying to client or not with mesh configuration	Passed	
MEJ810S_Mesh_16	Converting ME-capable MAP to CAPWAP MAP	To Verify ME-Capable MAP is converting to CAPWAP MAP or not	Passed	
MEJ810S_Mesh_17	Converting CAPWAP MAP to ME-Capable MAP	To Verify CAPWAP MAP is converting to ME-Capable MAP or not	Passed	

MEJ810S_Mesh_18	Checking client connection with Guest Network in Internal splash page+Web consent	To Verify client connection with Guest Network in Internal splash page+Web consent	Passed	
MEJ810S_Mesh_19	Checking client connection with Guest Network in Internal splash page+Local User	To Verify client connection with Guest Network in Internal splash page+Local User	Passed	
MEJ810S_Mesh_20	Checking client connection with Guest Network in Internal splash page+Email Address	To Verify client connection with Guest Network in Internal splash page+Email Address	Passed	
MEJ810S_Mesh_21	Checking Mesh configuration after reset ME	Verifying mesh configuration is proper or not after ME reset	Passed	
MEJ810S_Mesh_22	Checking MESH configuration after preforming Day0	Verifying MESH configuration got removed after performing Day0	Passed	
MEJ810S_Mesh_23	Performing ME failover with mesh config	To verify Mesh config reflects same after ME failover	Passed	
MEJ810S_Mesh_24	Performing ME failover with MAP AP	To verify Mesh config reflects same after ME failover with MAP AP	Passed	
MEJ810S_Mesh_25	Checking MESH configuration for ME-Capable AP after changing AP group	To Verify MESH configuration reflecting for ME-Capable after changing AP-group	Passed	
MEJ810S_Mesh_26	Checking MESH configuration for CAPWAP AP after changing AP group	To Verify MESH configuration reflecting for CAPWAP after changing AP-group	Passed	

IOS-XE

Intelligent Capture for 1850 AP

Logical ID	Title	Description	Status	Defect ID
WLJ1612S_IC_01	Configuring Intelligent Capture parameter details on 1800 AP	To configure Intelligent capture parameters in 1800 Aps	Passed	
WLJ1612S_IC_02	Check Configuration after the AP reboot	To Configure Intelligent capture parameters in different Aps 1800 and check if the configuration remains same after the AP reboot.	Passed	
WLJ1612S_IC_03	Packet capture of client when the client is connected to 1800 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	
WLJ1612S_IC_04	Packet capture of client when the client is connected to 1800 AP with 5 GHz	To capture the Packet of the client when the client is connected to AP with radio as 5 GHz	Passed	
WLJ1612S_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 1800 AP with security as OPEN	Passed	
WLJ1612S_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 1800 AP with security as WPA 2 PSK	Passed	

WLJ1612S_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 1800 AP with security as WPA 2 802.1x	Passed	
WLJ1612S_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 1800 AP with security as Static WEP	Passed	
WLJ1612S_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	
WLJ1612S_IC_10	Verify 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	
WLJ1612S_IC_11	Verify 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	
WLJ1612S_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	

WLJ1612S_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	
WLJ1612S_IC_14	Capturing Packet of Windows client when the client connected to 1800 AP	To capture packet when the Window client is connected to the 1800 AP	Passed	
WLJ1612S_IC_15	Capturing Packet of Android client when the client connected to 1800 AP	To capture packet when the Android client is connected to the 1800 AP	Passed	
WLJ1612S_IC_16	Capturing Packet of Mac OS client when the client connected to 1800 AP	To capture packet when the Mac OS client is connected to the 1800 AP	Passed	
WLJ1612S_IC_17	Capturing Packet of IOS client when the client connected to 1800 AP	To capture packet when the IOS client is connected to the 1800 AP	Passed	

ATF for All Modes

Logical ID	Title	Description	Status	Defect ID
WLJ1612S_ATF_01	Creating ATF policy and checking After configured	To verify whether user able to create ATF policies with out any issues or not	Passed	
WLJ1612S_ATF_02	Modifying ATF policy by enabling client sharing in policy	To verify whether able to modify ATF policy without any issues	Passed	
WLJ1612S_ATF_03	deleting the existing ATF policy and verifying in running config	To verify whether user able to delete ATF policy without any issues or not	Passed	
WLJ1612S_ATF_04	Attaching ATF Policies to Policy-Profile with 2.4Ghz and 5Ghz	To check whether user able to Attach ATF Policies to Policy-Profile or not	Passed	

WLJ1612S_ATF_05	Configuring the Airtime Fairness Global Configuration with 2.5 GHZ and mode as monitor and connecting client to WLAN	To check whether Airtime Fairness Global Configuration able to done with 2.4 GHZ and able to monitor WLAN air time fairness with mode as monitor	Passed	
WLJ1612S_ATF_06	Configuring the Airtime Fairness Global Configuration with 5 GHZ and mode as monitor and connecting client to WLAN	To check whether Airtime Fairness Global Configuration able to done with 5 GHZ and able to monitor WLAN air time fairness with mode as monitor	Passed	
WLJ1612S_ATF_07	Configuring the Airtime Fairness Global Configuration with 2.5 GHZ & 5 Ghz and mode as monitor and connecting client to WLAN	To check whether Airtime Fairness Global Configuration able to done with 2.4 GHZ & 5GHZ and able to monitor WLAN air time fairness with mode as monitor	Passed	
WLJ1612S_ATF_08	Creating Airtime Fairness Global Configuration with enforcement mode and enabling optimization	To verify whether able to configure Global Configuration with enforcement mode and enabling optimization	Failed	CSCvq45149/CSCvp66376
WLJ1612S_ATF_09	Mapping policy to the WLAN and connecting client to enforced mode ATF	To verify client statistics After client connected to WLAN with ATF mode as enforced	Passed	
WLJ1612S_ATF_10	Configure two ATF policies with different weights and map to different WLANs and connecting 2 clients	To verify whether speed test performance is showing as changed with different weights	Passed	

WLJ1612S_ATF_11	Connecting three or more clients to created ATF policy without client fair sharing and checking the whether all the clients associated to SSID gets equal air time	To verify whether connected clients showing un equal fair time or not when client fair is disabled	Passed	
WLJ1612S_ATF_12	Connecting three or more clients to created ATF policy with client fair sharing and checking the whether all the clients associated to SSID gets equal air time	To verify whether connected clients showing equal fair time or not with client fair	Passed	
WLJ1612S_ATF_13	Configure two ATF policies with different weights and map to different WLANs and connecting 2 clients	To verify clients capability, interference and other factors able to see After connected with different weights and map to different WLANs	Passed	
WLJ1612S_ATF_14	Configuring mesh on AP and connecting client with ATF enforcement mode and optimaization	To check client statistics with Mesh AP connect the client with 2.5 GHZ with optimazation enabled	Passed	
WLJ1612S_ATF_15	Configuring mesh on AP and connecting client with ATF enforcement mode and optimaization	To check client statistics with Mesh AP connect the client with 5 GHZ with optimazation enabled	Passed	
WLJ1612S_ATF_16	Configuring mesh on AP and connecting client with ATF enforcement mode	To verify client statistics with mesh AP and connect the client with enforcement with 2.5 GHZ	Failed	CSCvq61543

WLJ1612S_ATF_17	Configuring mesh on AP and connecting client with ATF enforcement mode	To verify client statistics with mesh AP and connect the client with enforcement with 5 Ghz	Failed	CSCvq59528

OWE Support

Logical ID	Title	Description	Status	Defect ID
EWLCJ1612S_OWE_02	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	
EWLCJ1612S_OWE_05	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	
EWLCJ1612S_OWE_07	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	
EWLCJ1612S_OWE_08	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	
EWLCJ1612S_OWE_09	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	
EWLCJ1612S_OWE_10	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	

EWLCJ1612S_OWE_11	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	
EWLCJ1612S_OWE_12	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	
EWLCJ1612S_OWE_13	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

Logical ID	Title	Description	Status	Defect ID
WLJ1612S_Best_Pract_01	Enable/Disable the http/https for management	Verify the web UI is able to open or not through http/https after modification	Failed	CSCvr78271
WLJ1612S_Best_Pract_02	Configure the NTP server	To check whether NTP server is able to configure or not for WEB UI	Passed	
WLJ1612S_Best_Pract_03	Create the WLAN with WPA2	Verify the WLAN with WPA2 after configuring via best practice	Failed	CSCvq27735/CSCvr70785
WLJ1612S_Best_Pract_04	Enable the User Login Policies	Checking the User Login Policies is enabled or not	Passed	
WLJ1612S_Best_Pract_05	Configure the Client Exclusion policies	To check whether Client Exclusion Policies is enabled or not	Passed	

WLJ1612S_Best_Pract_06	Configure the client band for all Active WLANs	To check whether client Band is applied or not for Active WLANs	Passed	
WLJ1612S_Best_Pract_07	Enable the 5ghz band for Active WLAN	Verify the 5ghz client band on active WLANs	Passed	
WLJ1612S_Best_Pract_08	Enable the 2.4ghz band for Active WLAN	Checking the 2.4ghz client band on active WLANs	Passed	
WLJ1612S_Best_Pract_09	Configure the Best channel width	To check whether Best channel width is configured or not on both radios	Passed	
WLJ1612S_Best_Pract_10	Enable the Local Profiling on one or more active WLANs	Verify the enabled Local Profile on Active WLAN	Passed	
WLJ1612S_Best_Pract_11	Enable the Flexible Radio Assignment	To check whether Flexible Radio Assignment is enabled or not	Passed	
WLJ1612S_Best_Pract_12	Configure the Load balance for one or more active WLAN	Verify the Load balance enabled or not on Active WLAN	Passed	
WLJ1612S_Best_Pract_13	Enable the Auto Dynamic Channel Assignment	To check whether global channel is enabled or not	Passed	

ATF support for Wave-2 APs

Logical ID	Title	Description	Status	Defect ID
WLJ1612S_ATF_01	Creating ATF policy and checking After configured	To verify whether user able to create ATF policies with out any issues or not	Passed	
WLJ1612S_ATF_02	Modifying ATF policy by enabling client sharing in policy	To verify whether able to modify ATF policy without any issues	Passed	

WLJ1612S_ATF_03	deleting the existing ATF policy and verifying in running config	To verify whether user able to delete ATF policy without any issues or not	Passed	
WLJ1612S_ATF_04	Attaching ATF Policies to Policy-Profile with 2.4GHZ and 5GHZ	To check whether user able to Attach ATF Policies to Policy-Profile or not	Passed	
WLJ1612S_ATF_05	Configuring the Airtime Fairness Global Configuration with 2.5 GHZ and mode as monitor and connecting client to WLAN	To check whether Airtime Fairness Global Configuration able to done with 2.4 GHZ and able to monitor WLAN air time fairness with mode as monitor	Passed	
WLJ1612S_ATF_06	Configuring the Airtime Fairness Global Configuration with 5 GHZ and mode as monitor and connecting client to WLAN	To check whether Airtime Fairness Global Configuration able to done with 5 GHZ and able to monitor WLAN air time fairness with mode as monitor	Passed	
WLJ1612S_ATF_07	Configuring the Airtime Fairness Global Configuration with 2.5 GHZ & 5 GHZ and mode as monitor and connecting client to WLAN	To check whether Airtime Fairness Global Configuration able to done with 2.4 GHZ & 5GHZ and able to monitor WLAN air time fairness with mode as monitor	Passed	
WLJ1612S_ATF_08	Creating Airtime Fairness Global Configuration with enforcement mode and enabling optimization	To verify whether able to configure Global Configuration with enforcement mode and enabling optimization	Passed	
WLJ1612S_ATF_09	Mapping policy to the WLAN and connecting client to enforced mode ATF	To verify client statistics After client connected to WLAN with ATF mode as enforced	Passed	

WLJ1612S_ATF_10	Configure two ATF policies with different weights and map to different WLANs and connecting 2 clients	To verify whether speed test performance is showing as changed with different weights	Passed	
WLJ1612S_ATF_11	Connecting three or more clients to created ATF policy without client fair sharing and checking the whether all the clients associated to SSID gets equal air time	To verify whether connected clients showing un equal fair time or not when client fair is disabled	Passed	
WLJ1612S_ATF_12	Connecting three or more clients to created ATF policy with client fair sharing and checking the whether all the clients associated to SSID gets equal air time	To verify whether connected clients showing equal fair time or not with client fair	Passed	
WLJ1612S_ATF_13	Configure two ATF policies with different weights and map to different WLANs and connecting 2 clients	To verify clients capability, interference and other factors able to see After connected with different weights and map to different WLANs	Passed	

WPA3 Support

Logical ID	Title	Description	Status	Defect ID
EWLCJ1612S_WPA3_01	Verifying the WPA3 support with SAE security key.	To verify the WPA3 support with SAE security Configuration.	Passed	

EWLCJ1612S_WPA3_03	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	
EWLCJ1612S_WPA3_05	Verifying the WPA3 support with SAE and PSK security key.	To verify the the Client packets by connecting the client to WPA3 and SAE and PSK supported SSID	Failed	CSCvr50970 ,CSCvr63290
EWLCJ1612S_WPA3_06	Verifying the WPA3 support with SAE and 802.1x security key.	To verify the WPA3 Configuration with SAE and 802.1x supported SSID	Passed	
EWLCJ1612S_WPA3_07	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	
EWLCJ1612S_WPA3_08	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	
EWLCJ1612S_WPA3_09	verifying the WPA3 support with SAE and PMF PSK Auth key.	To verify the WPA3 support with SAE and PMF PSK Auth key.	Passed	
EWLCJ1612S_WPA3_10	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	
EWLCJ1612S_WPA3_11	Verifying the WPA3 support with 802.1x security.	To verify the WPA3 support with 802.1x security for the different clients.	Passed	

EWLCJ1612S_WPA3_12	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	
EWLCJ1612S_WPA3_13	Verifying the WPA3 support with Ft+802.1x security.	To verify the WPA3 support with +Ft_802.1x security for the different clients.	Passed	
EWLCJ1612S_WPA3_14	Verifying the WPA3 support with Intra client roaming by using 9115AP	To verify the Intra client roaming by using WPA3 support with 9115AP	Passed	
EWLCJ1612S_WPA3_15	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	
EWLCJ1612S_WPA3_16	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	
EWLCJ1612S_WPA3_17	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	

WLC AireOS

AireOS AP Accounting

Logical ID	Title	Description	Status	Defect ID

WLJ810S_APacc_01	Adding a radius accounting server to WLC	To add accounting server to WLC UI and check if the accounting server is added to WLC ,check the same in WLC CLI also .	Passed	
WLJ810S_APacc_02	Connecting COS AP to WLC by enabling radius accounting	To connect COS AP to WLC and check if Radius accounting log in radius server is generated for AP joining or not	Passed	
WLJ810S_APacc_03	Disconnecting a COS AP connected to WLC by enabling radius accounting .	To disconnect a COS AP which is connected to WLC by enabling Radius accounting and check if the accounting logs for AP disconnecting is generated or not	Passed	
WLJ810S_APacc_04	Disabling Radius accounting for AP and joining COS AP to WLC	To connect COS AP to WLC without enabling Radius accounting and check if there is a log generated or not in radius server.	Passed	
WLJ810S_APacc_05	Connecting a AP through dot1x authentication and check the accounting message in radius server after the AP joins to WLC	To connect a AP through wired dot1x authentication and check if a accounting message is shown in radius server when a AP joins to the controller.	Passed	
WLJ810S_APacc_06	Disconnecting a AP which is connected through dot1x authentication to check the accounting log in radius server	To disconnect a AP which is connected through dot1x authentication to the WLC and check if accounting log is generated in radius server or not	Passed	

WLJ810S_APacc_07	Connecting IOS AP to WLC by enabling radius accounting	To connect IOS AP to WLC and check if Radius accounting log in radius server is generated for AP joining or not	Passed	
WLJ810S_APacc_08	Disconnecting a IOS AP connected to WLC by enabling radius accounting .	To disconnect a IOS AP which is connected to WLC by enabling Radius accounting and check if the accounting logs for AP disconnecting is generated or not	Passed	
WLJ810S_APacc_09	Disabling Radius accounting for AP and joining IOS AP to WLC	To connect IOS AP to WLC without enabling Radius accounting and check if there is a log generated or not in radius server.	Passed	
WLJ810S_APacc_10	Restarting the COS AP through PI and check for the accounting logs	To restart the COS AP connected to WLC through PI and check if the Radius accounting log are generated or not.	Passed	
WLJ810S_APacc_11	Restarting the IOS AP through PI and check for the accounting logs	To restart the IOS AP connected to WLC through PI and check if the Radius accounting log are generated or not.	Passed	
WLJ810S_APacc_12	Adding a COS AP in Active controller and making the active controller down to check for the accounting logs	To join a COS AP to the Active controller and make the active controller down and disconnect the COS AP and check if the Radius accounting log are generated or not.	Passed	

WLJ810S_APacc_13	Adding a IOS AP in Active controller and making the active controller down to check for the accounting logs	To join a IOS AP to the Active controller and make the active controller down and disconnect the COS AP and check if the Radius accounting log are generated or not.	Passed	
WLJ810S_APacc_14	Connecting COS AP to WLC by enabling radius accounting in Flex connect mode	To connect COS AP to WLC in flex connect mode and check if Radius accounting log in radius server is generated for AP joining or not	Passed	
WLJ810S_APacc_15	Connecting IOS AP to WLC by enabling radius accounting in Flex connect mode	To connect IOS AP to WLC in flex connect mode and check if Radius accounting log in radius server is generated for AP joining or not	Passed	
WLJ810S_APacc_16	Connecting a Window client to a AP enabling radius accounting	To connect a Window client to a AP enabling Radius accounting for AP and check if the radius accounting logs are generated also check the client behaviour.	Passed	
WLJ810S_APacc_17	Connecting a Android client to a AP enabling radius accounting	To connect a Android client to a AP enabling Radius accounting for AP and check if the radius accounting logs are generated also check the client behaviour.	Passed	

WLJ810S_APacc_18	Connecting a IOS client to a AP enabling radius accounting	To connect a IOS client to a AP enabling Radius accounting for AP and check if the radius accounting logs are generated also check the client behaviour.	Passed	
WLJ810S_APacc_19	Connecting a Mac OS client to a AP enabling radius accounting	To connect a Mac OS client to a AP enabling Radius accounting for AP and check if the radius accounting logs are generated also check the client behaviour.	Passed	
WLJ810S_APacc_20	Connecting AP to WLC by enabling radius accounting disabling WLC in network device	To connect COS AP to WLC disabling WLC in network device and check if Radius accounting log in radius server is generated for AP joining or not	Passed	
WLJ8102S_Reg_350	Adding a radius accounting server to WLC	To add accounting server to WLC UI and check if the accounting server is added to WLC ,check the same in WLC CLI also .	Passed	
WLJ8102S_Reg_351	Connecting COS AP to WLC by enabling radius accounting	To connect COS AP to WLC and check if Radius accounting log in radius server is generated for AP joining or not	Passed	
WLJ8102S_Reg_352	Disconnecting a COS AP connected to WLC by enabling radius accounting .	To disconnect a COS AP which is connected to WLC by enabling Radius accounting and check if the accounting logs for AP disconnecting is generated or not	Passed	

WLJ8102S_Reg_353	Disabling Radius accounting for AP and joining COS AP to WLC	To connect COS AP to WLC without enabling Radius accounting and check if there is a log generated or not in radius server.	Passed	
WLJ8102S_Reg_354	Connecting a AP through dot1x authentication and check the accounting message in radius server after the AP joins to WLC	To connect a AP through wired dot1x authentication and check if a accounting message is shown in radius server when a AP joins to the controller.	Passed	
WLJ8102S_Reg_355	Disconnecting a AP which is connected through dot1x authentication to check the accounting log in radius server	To disconnect a AP which is connected through dot1x authentication to the WLC and check if accounting log is generated in radius server or not	Passed	
WLJ8102S_Reg_356	Connecting IOS AP to WLC by enabling radius accounting	To connect IOS AP to WLC and check if Radius accounting log in radius server is generated for AP joining or not	Passed	
WLJ8102S_Reg_357	Disconnecting a IOS AP connected to WLC by enabling radius accounting .	To disconnect a IOS AP which is connected to WLC by enabling Radius accounting and check if the accounting logs for AP disconnecting is generated or not	Passed	
WLJ8102S_Reg_358	Disabling Radius accounting for AP and joining IOS AP to WLC	To connect IOS AP to WLC without enabling Radius accounting and check if there is a log generated or not in radius server.	Passed	

WLJ8102S_Reg_359	Restrating the COS AP through PI and check for the accounting logs	To restart the COS AP connected to WLC through PI and check if the Radius accounting log are generated or not.	Passed	
WLJ8102S_Reg_360	Restrating the IOS AP through PI and check for the accounting logs	To restart the IOS AP connected to WLC through PI and check if the Radius accounting log are generated or not.	Passed	
WLJ8102S_Reg_361	Adding a COS AP in Active controller and making the active controller down to check for the accounting logs	To join a COS AP to the Active controller and make the active controller down and disconnect the COS AP and check if the Radius accounting log are generated or not.	Passed	
WLJ8102S_Reg_362	Adding a IOS AP in Active controller and making the active controller down to check for the accounting logs	To join a IOS AP to the Active controller and make the active controller down and disconnect the COS AP and check if the Radius accounting log are generated or not.	Passed	
WLJ8102S_Reg_363	Connecting COS AP to WLC by enabling radius accounting in Flexconnect mode	To connect COS AP to WLC in flexconnect mode and check if Radius accounting log in radius server is generated for AP joining or not	Passed	

WLJ8102S_Reg_364	Connecting IOS AP to WLC by enabling radius accounting in Flexconnect mode	To connect IOS AP to WLC in flexconnect mode and check if Radius accounting log in radius server is generated for AP joining or not	Passed	
WLJ8102S_Reg_365	Connecting a Window client to a AP enabling radius accounting	To connect a Window client to a AP enabling Radius accounting for AP and check if the radius accounting logs are generated also check the client behaviour.	Passed	
WLJ8102S_Reg_366	Connecting a Android client to a AP enabling radius accounting	To connect a Android client to a AP enabling Radius accounting for AP and check if the radius accounting logs are generated also check the client behaviour.	Passed	
WLJ8102S_Reg_367	Connecting a IOS client to a AP enabling radius accounting	To connect a IOS client to a AP enabling Radius accounting for AP and check if the radius accounting logs are generated also check the client behaviour.	Passed	
WLJ8102S_Reg_368	Connecting a Mac OS client to a AP enabling radius accounting	To connect a Mac OS client to a AP enabling Radius accounting for AP and check if the radius accounting logs are generated also check the client behaviour.	Passed	

WLJ8102S_Reg_369	Connecting AP to WLC by enabling radius accounting disabling WLC in network device	To connect COS AP to WLC disabling WLC in network device and check if Radius accounting log in radius server is generated for AP joining or not	Passed	

CPU ACL

Logical ID	Title	Description	Status	Defect ID
WLJ810S_CPUACL_01	Configuring ACL policy to be applied for CPU ACL	To create a ACL policy to be applied for CPU ACL	Passed	
WLJ810S_CPUACL_02	Configuring CPU ACL by mapping the ACL created in WLC GUI	To map the ACL created to the CPU ACL and check if the ACL is mapped to CPU ACL or not in WLC GUI.	Passed	
WLJ810S_CPUACL_03	Configuring CPU ACL by mapping the ACL created in WLC CLI	To map the ACL created to the CPU ACL and check if the ACL is mapped to CPU ACL or not in WLC CLI.	Passed	
WLJ810S_CPUACL_04	Enabling High priority CPU Acl in WLC 3504	To enable High priority CPU ACL in WLC 3504 and check if the High priority ACL is enabled or not.	Passed	
WLJ810S_CPUACL_05	Enabling High priority CPU Acl in WLC 5520	To enable High priority CPU ACL in WLC 5520 and check if the High priority ACL is enabled or not.	Passed	
WLJ810S_CPUACL_06	Enabling High priority CPU Acl in WLC 8540	To enable High priority CPU ACL in WLC 8540 and check if the High priority ACL is enabled or not.	Passed	

WLJ810S_CPUACL_07	Allowing virtual IP in ACL and connecting a client to check if redirection happens or not.	To allow virtual IP in ACL and check if the redirection for web auth client happens successfully .	Passed	
WLJ810S_CPUACL_08	Blocking the Virtual IP and check if the redirection of web auth happens or not.	To block the virtual IP address and check if the redirection to webauth fails .	Passed	
WLJ810S_CPUACL_09	Allowing SNMP using IP address enabling High priority CPU ACL	To allow SNMP using IP address enabling High priority CPU acl and check if the WLC when added in SNMP server should show as reachable.	Passed	
WLJ810S_CPUACL_10	Denying SNMP server in ACL enabling HCA .	To deny SNMP using IP address enabling High priority CPU acl and check if the WLC when added in SNMP server should show as Not reachable.	Passed	
WLJ810S_CPUACL_11	Blocking telnet to a particular device enabling CPU ACL with high priority	To block the telnet access to device enabling HCA and check if the telnet is not accessible to the particular device.	Passed	
WLJ810S_CPUACL_12	Allowing radius authentication for clients enabling HCA	To Allow radius authentication for client enabling HCA for the particular WLC	Passed	
WLJ810S_CPUACL_13	Restricting the radius authentication for the clients enabling HCA	To restrict radius authentication for client enabling HCA for the particular WLC	Passed	

WLJ8102S_Reg_370	Configuring ACL policy to be applied for CPU ACL	To create a ACL policy to be applied for CPU ACL	Passed	
WLJ8102S_Reg_371	Configuring CPU ACL by mapping the ACL created in WLC GUI	To map the ACL created to the CPU ACL and check if the ACL is mapped to CPU ACL or not in WLC GUI.	Passed	
WLJ8102S_Reg_372	Configuring CPU ACL by mapping the ACL created in WLC CLI	To map the ACL created to the CPU ACL and check if the ACL is mapped to CPU ACL or not in WLC CLI.	Passed	
WLJ8102S_Reg_373	Enabling High priority CPU Acl in WLC 3504	To enable High priority CPU ACL in WLC 3504 and check if the High priority ACL is enabled or not.	Passed	
WLJ8102S_Reg_374	Enabling High priority CPU Acl in WLC 5520	To enable High priority CPU ACL in WLC 5520 and check if the High priority ACL is enabled or not.	Passed	
WLJ8102S_Reg_375	Enabling High priority CPU Acl in WLC 8540	To enable High priority CPU ACL in WLC 8540 and check if the High priority ACL is enabled or not.	Passed	
WLJ8102S_Reg_376	Allowing virtual IP in ACL and connecting a client to check if redirection happens or not.	To allow virtual IP in ACL and check if the redirection for web auth client happens succesfully .	Passed	
WLJ8102S_Reg_377	Blocking the Virtual IP and check if the redirection of web auth happens or not.	To block the virtual IP address and check if the redirection to webauth fails .	Passed	

WLJ8102S_Reg_378	Allowing SNMP using IP address enabling High priority CPU ACL	To allow SNMP using IP address enabling High priority CPU acl and check if the WLC when added in SNMP server should show as reachable.	Passed	
WLJ8102S_Reg_379	Denying SNMP server in ACL enabling HCA .	To deny SNMP using IP address enabling High priority CPU acl and check if the WLC when added in SNMP server should show as Not reachable.	Passed	
WLJ8102S_Reg_380	Blocking telnet to a particular device enabling CPU ACL with high priority	To block the telnet access to device enabling HCA and check if the telnet is not accessible to the particular device.	Passed	
WLJ8102S_Reg_381	Allowing radius authentication for clients enabling HCA	To Allow radius authentication for client enabling HCA for the particular WLC	Passed	
WLJ8102S_Reg_382	Restricting the radius authentication for the clients enabling HCA	To restrict radius authentication for client enabling HCA for the particular WLC	Passed	

Indoor Mesh

Logical ID	Title	Description	Status	Defect ID
WLJ810S_IM_01	Checking indoor mesh AP is configured as RAP	Verifying indoor mesh AP configured as RAP role or not	Passed	
WLJ810S_IM_02	Checking indoor mesh AP is configured as MAP	Verifying indoor mesh AP configured as MAP role or not	Passed	

WLJ810S_IM_03	Checking windows client connection with open security in AP bridge mode	Verifying windows client is connecting or not with open security in AP bridge mode	Passed	
WLJ810S_IM_04	Checking IOS client connection with WPA Personal security in AP bridge mode	Verifying IOS client is connecting or not with WPA Personal security in AP bridge mode	Passed	
WLJ810S_IM_06	Checking MacOS client connection with Dot1x security in AP bridge mode	Verifying MacOS client is connecting or not with Dot1x security in AP bridge mode	Passed	
WLJ810S_IM_07	Checking JOS client connection with Static web security in AP bridge mode	Verifying JOS client is connecting or not with Static web security in AP bridge mode	Passed	
WLJ810S_IM_08	Checking client connection with open security in AP flex+bridge mode	Verifying client is connecting or not with open security in AP flex+bridge mode	Passed	
WLJ810S_IM_09	Checking client connection with WPA Personal security in AP flex+bridge mode	Verifying client is connecting or not with WPA Personal security in AP flex+bridge mode	Passed	
WLJ810S_IM_11	Checking client connection with Dot1x security in AP flex+bridge mode	Verifying client is connecting or not with Dot1x security in AP flex+bridge mode	Passed	
WLJ810S_IM_12	Checking client connection with Static web security in AP flex+bridge mode	Verifying client is connecting or not with Static web security in AP flex+bridge mode	Passed	
WLJ810S_IM_13	Creating mesh setup with indoor and outdoor mesh AP's	Verifying mesh AP is able to create or not with indoor and outdoor mesh AP's	Passed	
WLJ810S_IM_14	Checking mesh AP joining to WLC authenticating via ISE	Verifying mesh AP is able to join to WLC or not authenticating via ISE	Passed	

WLJ810S_IM_15	Checking mesh setup by configuring RAP downlink with 2.4GhZ	Verifying mesh setup is proper or not by setting RAP downlink to 2.4GhZ	Passed	
WLJ810S_IM_16	Checking mesh setup by configuring RAP downlink with 5GhZ	Verifying mesh setup is proper or not by setting RAP downlink to 5GhZ	Passed	
WLJ810S_IM_17	Checking client connection by configuring backhaul client access	Verifying client connecting properly or not by configuring backhaul client access	Passed	
WLJ810S_IM_18	Checking client connection by disabling backhaul client access	Verifying client connecting properly or not by disabling backhaul client access	Passed	
WLJ810S_IM_19	Performing the Intra roaming of clients between 2 AP's	To check whether clients can be roamed or not between 2 AP's (mode should be different) in a WLC	Passed	
WLJ810S_IM_20	Performing Inter roaming of clients between 2 WLC's with Indoor and Outdoor AP's	To check whether clients can be roamed or not between Indoor and Outdoor in different WLC	Passed	
WLJ810S_IM_21	Checking mesh configuration after rebooting WLC	Verifying mesh setup is configured same as before after rebooting WLC	Passed	
WLJ810S_IM_22	Checking mesh configuration after upgrading/downgrading the controller	Verifying mesh configuration after upgrading/downgrading the controller	Passed	
WLJ810S_IM_23	Checking mesh configuration after performing Day0	Verifying mesh configuration exists or not after performing day0	Passed	
WLJ8102S_Reg_383	Checking indoor mesh AP is configured as RAP	Verfying indoor mesh AP configured as RAP role or not	Passed	
WLJ8102S_Reg_384	Checking indoor mesh AP is configured as MAP	Verfying indoor mesh AP configured as MAP role or not	Passed	

WLJ8102S_Reg_385	Checking windows client connection with open security in AP bridge mode	Verifying windows client is connecting or not with open security in AP bridge mode	Passed	
WLJ8102S_Reg_386	Checking IOS client connection with WPA Personal security in AP bridge mode	Verifying IOS client is connecting or not with WPA Personal security in AP bridge mode	Passed	
WLJ8102S_Reg_387	Checking android client connection with WPA3 security in AP bridge mode	Verifying android client is connecting or not with WPA3 security in AP bridge mode	Passed	
WLJ8102S_Reg_388	Checking MacOS client connection with Dot1x security in AP bridge mode	Verifying MacOS client is connecting or not with Dot1x security in AP bridge mode	Passed	
WLJ8102S_Reg_389	Checking JOS client connection with Static wep security in AP bridge mode	Verifying JOS client is connecting or not with Static wep security in AP bridge mode	Passed	
WLJ8102S_Reg_390	Checking client connection with open security in AP flex+bridge mode	Verifying client is connecting or not with open security in AP flex+bridge mode	Passed	
WLJ8102S_Reg_391	Checking client connection with WPA Personal security in AP flex+bridge mode	Verifying client is connecting or not with WPA Personal security in AP flex+bridge mode	Passed	
WLJ8102S_Reg_392	Checking client connection with WPA3 security in AP flex+bridge mode	Verifying client is connecting or not with WPA3 security in AP flex+bridge mode	Passed	
WLJ8102S_Reg_393	Checking client connection with Dot1x security in AP flex+bridge mode	Verifying client is connecting or not with Dot1x security in AP flex+bridge mode	Passed	
WLJ8102S_Reg_394	Checking client connection with Static wep security in AP flex+bridge mode	Verifying client is connecting or not with Static wep security in AP flex+bridge mode	Passed	

WLJ8102S_Reg_395	Creating mesh setup with indoor and outdoor mesh AP's	Verfying mesh AP is able to create or not with indoor and outdoor mesh AP's	Passed	
WLJ8102S_Reg_396	Checking mesh AP joining to WLC authenticating via ISE	Verfying mesh AP is able to join to WLC or not authenticating via ISE	Passed	
WLJ8102S_Reg_397	Checking mesh setup by configuring RAP downlink with 2.4GhZ	Verfying mesh setup is proper or not by setting RAP downlink to 2.4GhZ	Passed	
WLJ8102S_Reg_398	Checking mesh setup by configuring RAP downlink with 5GhZ	Verfying mesh setup is proper or not by setting RAP downlink to 5GhZ	Passed	
WLJ8102S_Reg_399	Checking client connection by configuring backhaul client access	Verfying client connecting properly or not by configuring backhaul client access	Passed	
WLJ8102S_Reg_400	Checking client connection by disabling backhaul client access	Verfying client connecting properly or not by disabling backhaul client access	Passed	
WLJ8102S_Reg_401	Performing the Intra roaming of clients between 2 AP's	To check whether clients can be roamed or not between 2 AP's (mode should be different) in a WLC	Passed	
WLJ8102S_Reg_402	Performing Inter roaming of clients between 2 WLC's with Indoor and Outdoor AP's	To check whether clients can be roamed or not between Indoor and Outdoor in different WLC	Passed	
WLJ8102S_Reg_403	Checking mesh configuration after rebooting WLC	Verfying mesh setup is configured same as before after rebooting WLC	Passed	
WLJ8102S_Reg_404	Checking mesh configuration after upgrading/downgrading the controller	Verfying mesh configuration after upgrading/downgrading the controller	Passed	
WLJ8102S_Reg_405	Checking mesh configuration after performing Day0	Verfying mesh configuration exists or not after performing day0	Passed	

Master key WLC Encryption

Logical ID	Title	Description	Status	Defect ID
WLJ810S_MKE_01	Verify the configuration file after downloaded from Controller by using the ftp server	To download the configuration file from controller by using ftp server and verify whether it is encrypted or not	Passed	
WLJ810S_MKE_02	Verify the configuration file after downloaded from Controller by using the TFTP server	To download the configuration file from controller by using TFTP server and verify whether it is encrypted or not	Passed	
WLJ810S_MKE_03	Verify the configuration file after downloaded from Controller by using the SFTP server	To download the configuration file from controller by using SFTP server and verify whether it is encrypted or not	Passed	
WLJ810S_MKE_04	Verify the Controller Configurations after uploaded the Configuration file to Controller by using ftp server	To upload the configuration file to Controller by using ftp server and check the controller configurations configured successfully or not	Passed	
WLJ810S_MKE_05	Verify the Controller after uploaded the Configuration file to Controller by using TFTP server	To upload the configuration file to Controller by using TFTP server and check the controller configurations configured successfully or not	Passed	
WLJ810S_MKE_06	Verify the Controller after uploaded the Configuration file to Controller by using SFTP server	To upload the configuration file to Controller by using SFTP server and check the controller configurations configured successfully or not	Passed	

WLJ810S_MKE_07	Access the Controller with TACACS profile and Check the configuration file after downloaded from Controller by using the ftp server	To verify the user can able to Access Controller with TACACS profile and Check the configuration file after downloaded from Controller by using the ftp server	Passed	
WLJ810S_MKE_08	Access the Controller with TACACS profile and Check the configuration file after downloaded from Controller by using the TFTP server	To verify the user can able to Access Controller with TACACS profile and Check the configuration file after downloaded from Controller by using the TFTP server	Passed	
WLJ810S_MKE_09	Access the Controller with TACACS profile and Check the configuration file after downloaded from Controller by using the SFTP server	To verify the user can able to Access Controller with TACACS profile and Check the configuration file after downloaded from Controller by using the SFTP server	Passed	
WLJ810S_MKE_10	Access the Controller with TACACS profile and Verify the Controller Configurations after uploaded the Configuration file to Controller by using ftp server	To verify the user can able to Access the Controller with TACACS profile and Check the Controller configurations after Uploading the Configuration file to Controller by using the ftp server	Passed	

WLJ810S_MKE_11	Access the Controller with TACACS profile and Check the configuration file after downloaded from Controller by using the TFTP server	To verify the user can able to Access the Controller with TACACS profile and Check the Controller configurations after Uploading the Configuration file to Controller by using the TFTP server	Passed	
WLJ810S_MKE_12	Access the Controller with TACACS profile and Check the configuration file after downloaded from Controller by using the SFTP server	To verify the user can able to Access the Controller with TACACS profile and Check the Controller configurations after Uploading the Configuration file to Controller by using the SFTP server	Passed	
WLJ810S_MKE_13	Verify the Error message of Encryption key with Less than 16 Characters	To Configure the Encryption key with less than 16 Characters and verify the Error message	Passed	
WLJ810S_MKE_14	Check the Error message for Encryption key with Less than 16 Characters	To Configure the Encryption key with less than 16 Characters and verify the Error message	Passed	
WLJ810S_MKE_15	Verify the Encryption key by including the special characters while downloading the file from Controller	To configure the Encryption key by including the special characters and download configuration file from controller and verify the file whether it is encrypted or not	Passed	

WLJ810S_MKE_16	Check the Encryption Key by including the special characters while uploading the file to Controller	To configure the Encryption key by including the special characters and Upload the Configuration file to controller and verify the Controller Configurations.	Passed	
WLJ810S_MKE_17	Verify the Encryption key by including the Japanese characters while downloading the file from Controller	To configure the Encryption key by including the Japanese characters and download configuration file from controller and verify the file whether it is encrypted or not	Passed	
WLJ810S_MKE_18	Check the Encryption Key by including the Japanese characters while uploading the file to Controller	To configure the Encryption key by including the Japanese characters and Upload the Configuration file to controller and verify the Controller Configurations.	Passed	
WLJ810S_MKE_19	Check the Encryption key and download the configuration file by configuring the file format as .txt and .as and .csv	To configure the file format as .txt and .as and .csv and download the configure file from Controller.	Passed	
WLJ810S_MKE_20	Verify the Encryption key and upload the configuration file by configuring the file format as .txt and .as and .csv	To configure the file format as .txt and .as and .csv and Upload the configure file to Controller.	Passed	

WLJ810S_MKE_21	Verify the Encryption key and upload the different model controller configuration file.	To verify the Encryption key and controller configurations after uploaded the different model controller configurations file.	Passed	
WLJ810S_MKE_22	Verify the Encryption key and upload the downgraded build controller configuration file.	To verify the Encryption key and controller configurations after uploaded the downgraded build controller configurations file.	Passed	
WLJ810S_MKE_23	Verify the Encryption key and upload the Upgraded build controller configuration file.	To verify the Encryption key and controller configurations after uploaded the Upgraded build controller configurations file.	Passed	
WLJ810S_MKE_24	Check the Encryption key and Upload the Modified configuration file to controller	To verify the Encryption Key and Controller configurations after uploaded the Modified Configuration file.	Passed	
WLJ810S_MKE_25	Check the Encryption key while uploading the Configuration file to controller make down the primary Controller.	To check the Encryption key and make down the primary controller while uploading the Configuration file and observe the behaviour.	Passed	
WLJ810S_MKE_26	Check the Encryption key while Downloading the Configuration file from controller make down the primary Controller.	To check the Encryption key and make down the primary controller while Downloading the Configuration file and observe the behaviour.	Passed	

WLJ8102S_Reg_406	Verify the configuration file after downloaded from Controller by using the ftp server	To download the configuration file from controller by using ftp server and verify whether it is encrypted or not	Passed	
WLJ8102S_Reg_407	Verify the configuration file after downloaded from Controller by using the TFTP server	To download the configuration file from controller by using TFTP server and verify whether it is encrypted or not	Passed	
WLJ8102S_Reg_408	Verify the configuration file after downloaded from Controller by using the SFTP server	To download the configuration file from controller by using SFTP server and verify whether it is encrypted or not	Passed	
WLJ8102S_Reg_409	Verify the Controller Configurations after uploaded the Configuration file to Controller by using ftp server	To upload the configuration file to Controller by using ftp server and check the controller configurations configured sucessfully or not	Passed	
WLJ8102S_Reg_410	Verify the Controller after uploaded the Configuration file to Controller by using TFTP server	To upload the configuration file to Controller by using TFTP server and check the controller configurations configured sucessfully or not	Passed	
WLJ8102S_Reg_411	Verify the Controller after uploaded the Configuration file to Controller by using SFTP server	To upload the configuration file to Controller by using SFTP server and check the controller configurations configured sucessfully or not	Passed	

WLJ8102S_Reg_412	Access the Controller with TACACS profile and Check the configuration file after downloaded from Controller by using the ftp server	To verify the user can able to Access Controller with TACACS profile and Check the configuration file after downloaded from Controller by using the ftp server	Passed	
WLJ8102S_Reg_413	Access the Controller with TACACS profile and Check the configuration file after downloaded from Controller by using the TFTP server	To verify the user can able to Access Controller with TACACS profile and Check the configuration file after downloaded from Controller by using the TFTP server	Passed	
WLJ8102S_Reg_414	Access the Controller with TACACS profile and Check the configuration file after downloaded from Controller by using the SFTP server	To verify the user can able to Access Controller with TACACS profile and Check the configuration file after downloaded from Controller by using the SFTP server	Passed	
WLJ8102S_Reg_415	Access the Controller with TACACS profile and Verify the Controller Configurations after uploaded the Configuration file to Controller by using ftp server	To verify the user can able to Access the Controller with TACACS profile and Check the Controller configurations after Uploading the Configuration file to Controller by using the ftp server	Passed	

WLJ8102S_Reg_416	Access the Controller with TACACS profile and Check the configuration file after downloaded from Controller by using the TFTP server	To verify the user can able to Access the Controller with TACACS profile and Check the Controller configurations after Uploading the Configuration file to Controller by using the TFTP server	Passed	
WLJ8102S_Reg_417	Access the Controller with TACACS profile and Check the configuration file after downloaded from Controller by using the SFTP server	To verify the user can able to Access the Controller with TACACS profile and Check the Controller configurations after Uploading the Configuration file to Controller by using the SFTP server	Passed	
WLJ8102S_Reg_418	Verify the Error message of Encryption key with Less than 16 Characters	To Configure the Encryption key with less than 16 Characters and verify the Error message	Passed	
WLJ8102S_Reg_419	Check the Error message for Encryption key with Less than 16 Characters	To Configure the Encryption key with less than 16 Characters and verify the Error message	Passed	
WLJ8102S_Reg_420	Verify the Encryption key by including the special characters while downloading the file from Controller	To configure the Encryption key by including the special characters and download configuration file from controller and verify the file whether it is encrypted or not	Passed	

WLJ8102S_Reg_421	Check the Encryption Key by including the special characters while uploading the file to Controller	To configure the Encryption key by including the special characters and Upload the Configuration file to controller and verify the Controller Configurations.	Passed	
WLJ8102S_Reg_422	Verify the Encryption key by including the Japanese characters while downloading the file from Controller	To configure the Encryption key by including the Japanese characters and download configuration file from controller and verify the file whether it is encrypted or not	Passed	
WLJ8102S_Reg_423	Check the Encryption Key by including the Japanese characters while uploading the file to Controller	To configure the Encryption key by including the Japanese characters and Upload the Configuration file to controller and verify the Controller Configurations.	Passed	
WLJ8102S_Reg_424	Check the Encryption key and download the configuration file by configuring the file formate as .txt and .aes and .csv	To configure the file formate as .txt and .aes and .csv and download the configure file from Controller.	Passed	
WLJ8102S_Reg_425	Verify the Encryption key and upload the configuration file by configuring the file formate as .txt and .aes and .csv	To configure the file formate as .txt and .aes and .csv and Upload the configure file to Controller.	Passed	

WLJ8102S_Reg_426	Verify the Encryption key and upload the different model controller configuration file.	To verify the Encryption key and controller configurations after uploaded the different model controller configurations file.	Passed	
WLJ8102S_Reg_427	Verify the Encryption key and upload the downgraded build controller configuration file.	To verify the Encryption key and controller configurations after uploaded the downgraded build controller configurations file.	Passed	
WLJ8102S_Reg_428	Verify the Encryption key and upload the Upgraded build controller configuration file.	To verify the Encryption key and controller configurations after uploaded the Upgraded build controller configurations file.	Passed	
WLJ8102S_Reg_429	Check the Encryption key and Upload the Modified configuration file to controller	To verify the Encryption Key and Controller configurations after uploaded the Modified Configuration file.	Passed	
WLJ8102S_Reg_430	Check the Encryption key while uploading the Configuration file to controller make down the primary Controller.	To check the Encryption key and make down the primary controller while uploading the Configuration file and observe the behaviour.	Passed	
WLJ8102S_Reg_431	Check the Encryption key while Downloading the Configuration file from controller make down the primary Controller.	To check the Encryption key and make down the primary controller while Downloading the Configuration file and observe the behaviour.	Passed	

ATF Wave 2

Logical ID	Title	Description	Status	Defect ID
WLJ810S_ATFW2_01	Creating Policy with different weights and enabling/disabling client pair sharing	To verify whether user able to create Policy configuration with different weights and enabling/disabling client pair sharing	Passed	
WLJ810S_ATFW2_02	Configuring ATF monitor mode configuration with 802.11ac Wave2 AP in AP name and checking the ATF statistics per WLAN	To check whether ATF statistics showing or not per WLAN in monitor mode	Passed	
WLJ810S_ATFW2_03	Checking the ATF statistics per WLAN with enabling radio modes as monitor	To check whether user able to view Instantaneous and Accumulated Values in ATF statistics	Passed	
WLJ810S_ATFW2_04	Checking the ATF statistics per WLAN with disabling radio modes	To check whether user able to view Instantaneous and Accumulated time as 0 sec in ATF statistics after disabled radio modes	Passed	
WLJ810S_ATFW2_05	Configuring ATF enforce mode with AP name and mapping WLAN with policy ID	To verify whether able to configure ATF enforcement with AP name and mapping WLAN with policy ID	Passed	
WLJ810S_ATFW2_06	Connecting client to the WLAN with ATF enforcement mode configuration with Ap name and check the client statistics	To verify Client statistics after client connected to the WLAN with ATF enforcement mode	Passed	

WLJ810S_ATFW2_07	Connecting client to the WLAN with ATF enforcement mode configuration with AP group name and check the client statistics	To verify client statistics after connected to the WLAN with ATF enforcement mode configuration with AP group name	Passed	
WLJ810S_ATFW2_08	Connecting client to the WLAN with ATF enforcement mode configuration with network and check the client statistics	To verify client statistics after connected to the WLAN with ATF enforcement mode configuration with network	Passed	
WLJ810S_ATFW2_09	Config Mesh setup and apply config on Mesh Aps	To verify that Mesh setup configured and mesh Aps added in ATF	Passed	
WLJ810S_ATFW2_10	Apply ATF Enforcement mode on MESH AP	To verify that ATF Enforcement mode applied on MESH AP or not	Passed	
WLJ810S_ATFW2_11	Apply ATF policy on wlan and connect Android client for mesh configured AP	To verify that policy applied on WLAN and connect client to the mesh configured AP successfully or not	Passed	
WLJ810S_ATFW2_12	Apply ATF Enforcement mode on AP group	To verify that ATF Enforcement mode applied on AP group or not	Passed	
WLJ810S_ATFW2_13	Airtime allocation override on universal client access radio 802.11a	To verify that ATF override on universal client access radio 802.11a is enable or not	Passed	
WLJ810S_ATFW2_14	Airtime allocation override on universal client access radio 802.11b	To verify that ATF override on universal client access radio 802.11b is enable or not	Failed	CSCvq39338

WLJ810S_ATFW2_15	Connecting three or more clients to created AFT policy without client fair sharing and checking the whether all the clients associated to SSID gets un equal air time	To verify whether connected clients showing unequal fair time or not without client fair	Passed	
WLJ810S_ATFW2_16	Connecting three or more clients to created AFT policy with client fair sharing and checking the whether all the clients associated to SSID gets equal air time	To verify whether connected clients showing equal fair time or not with client fair	Passed	
WLJ810S_ATFW2_17	Configure two AFT policies with different weights and map to diffent WLANs and connecting 2 clients	To verify clients capability, interference and other factors able to see after connected with different weights and map to diffent WLANs	Passed	

Per AP Group NTP Server Config

Logical ID	Title	Description	Status	Defect ID
WLJ810S_NTP_01	Config the AP-Group NTP IPv4 server at a index	To verify whether user able to create NTP server without any issues	Passed	
WLJ810S_NTP_02	Validating boundary value range for key index,also providing keys with special/UTF/Japanese Characters and creating keys	To verify whether user able to create key index with the given range <1 to 65535> and key with all special and Japanese characters	Passed	
WLJ810S_NTP_03	Config NTP server without enabling auth key	To verify whether AP synced with NTP server without auth key	Passed	

WLJ810S_NTP_04	Config NTP server with auth enabled for a Ap-Group with auth enabled	To verify whether user able to create NTP serverConfig NTP server with auth enabled for a Ap-Group without any issues	Passed	
WLJ810S_NTP_05	Changing the key index after NTP server added in AP group	To verify user able to Map new key index to the added NTP server in AP group	Passed	
WLJ810S_NTP_06	Delete configured AP-Group NTP server	To check whether user able to delete configured AP-Group NTP server	Passed	
WLJ810S_NTP_07	Connecting client to the NTP mapped AP group WLANs	To check whether user able to connect client to the AP which is in AP group and synced with NTP server	Passed	
WLJ810S_NTP_08	Verify time is synced with all ap's present in group corresponding to NTPserver	To Validate the Aps present in that apgroup synced with that NTP server or not	Passed	
WLJ810S_NTP_09	Checking NTP logs in AP Console after synced WLC to AP	To verify whether debugging logs are able to get or not in WLC	Passed	
WLJ810S_NTP_10	Verify max number of NTP servers(no.32)	To Validate whether user able to Configure max(32) number of NTP servers or not	Passed	
WLJ810S_NTP_11	Validate NTP config on AP after changing mode of AP	Configure NTP server and key map to apgroup and change the mode of the AP and validate time is synced with NTP server	Passed	

WLJ810S_NTP_12	Verify able to delete NTP server and key when it is mapped to apgroup	Configure NTP server, keys and add it to apgroup and try to delete NTP server and key	Passed	
WLJ810S_NTP_13	Delete existed NTP server from AP group and add new NTP server to ap group and validate all the AP's time is synced with new server	Configure NTP servers and keys and map it to apgroup. After deletion of existed NTP server and configure new NTP and validate the new NTP time is synced to all aps in that group	Passed	
WLJ810S_NTP_14	Validating whether AP is synced with a present in group corresponding to NTPserver with AP console logs	To monitor whether AP is synced with AP group NTP server or not	Passed	
WLJ810S_NTP_15	Validate NTP configs are present in running config	Configure max NTP servers, key and map to apgroup and validate confits exists in running config	Passed	
WLJ810S_NTP_16	Move AP from one group to another and validate ap time is updated with new NTP server	Configure multiple NTP servers,keys and map to different apgroups. Move ap from group to another and validate the time on AP	Passed	
WLJ810S_NTP_17	Validate NTP configuration after uploading and downloading the WLC config	Configure max NTP servers, key and map to apgroup and save the config and upload and download WLC and validate the confits on wlc	Passed	
WLJ810S_NTP_18	Connecting client to IOS AP and checking NTP status	To verify whether IOS AP sync with the NTP server or not	Passed	

WLJ810S_NTP_19	Connecting client to COS AP and checking NTP status	To verify whether COS AP sync with the NTP server or not	Passed	
WLJ810S_NTP_20	Validate NTP configurations on WLC after rebooting WLC	Configure the NTP server, key and map those to apgroup and reboot the WLC and validate all the confits retains in WLC	Passed	
WLJ810S_NTP_21	Validate NTP configuration synced with secondary WLC	Configure the NTP server, key and map those to apgroup and verify the confits are synced to standby WLC	Passed	
WLJ810S_NTP_22	Validate NTP configuration after WLC failover happened and validate time on AP	Configure the NTP server, key and map those to apgroup do a switchover and verify the confits are present and ap's are getting proper NTP time	Passed	
WLJ810S_NTP_23	Validating time after doing intra roaming with COS and IOS Aps Aps and connecting client	To verify whether time showing same after intra roaming	Passed	
WLJ810S_NTP_24	Verifying NTP synchronization with ISR APS	To check whether ISR Aps are showing proper time or not after sync	Passed	
WLJ810S_NTP_25	Rebooting AP and checking the sync details	To verify whether Aps synch time properly after rebooting	Passed	
WLJ810S_NTP_26	Checking the NTP status with mess support Aps	To verify whether Mess AP synchronize with NTP server or not	Passed	
WLJ8102S_Reg_432	Config the AP-Group NTP IPv4 server at a index	To verify whether user able to create NTP server without any issues	Passed	

WLJ8102S_Reg_433	Validating boundary value range for key index,also providing keys with special/UTF/Japanese Characters and creating keys	To verify whether user able to create key index with the given range <1 to 65535> and key with all special and japanese characters	Passed	
WLJ8102S_Reg_434	Config NTP server without enabling auth key	To verify whether AP synced with NTP server without auth key	Passed	
WLJ8102S_Reg_435	Config NTP server with auth enabled for a Ap-Group with auth enabled	To verify whether user able to create NTP serverConfig NTP server with auth enabled for a Ap-Group without any issues	Passed	
WLJ8102S_Reg_436	Changing the key index after NTP server added in AP group	To verify user able to Map new key index to the added NTP server in AP group	Passed	
WLJ8102S_Reg_437	Delete configured AP-Group NTP server	To check whether user able to delete configured AP-Group NTP server	Passed	
WLJ8102S_Reg_438	Connecting client to the NTP mapped AP group WLANs	To check whether user able to connect client to the AP which is in AP group and synced with NTP server	Passed	
WLJ8102S_Reg_439	Verify time is synced with all ap's present in agroup corresponding to NTPserver	To Validate the Aps present in that apgroup synced with that NTP server or not	Passed	
WLJ8102S_Reg_440	Checking NTP logs in AP Console after synced WLC to AP	To verify whether debugging logs are able to get or not in WLC	Passed	

WLJ8102S_Reg_441	Verify max number of NTP servers(no.32)	To Validate whether user able to Configure max(32) number of NTP servers or not	Passed	
WLJ8102S_Reg_442	Validate NTP config on AP after changing mode of AP	Configure NTP server and key map to apgroup and change the mode of the AP and validate time is synced with NTP server	Passed	
WLJ8102S_Reg_443	Verify able to delete NTP server and key when it is mapped to apgroup	Configure NTP server, keys and add it to apgroup and try to delete NTP server and key	Passed	
WLJ8102S_Reg_444	Delete existed NTP server from AP group and add new NTP server to ap group and validate all the AP's time is synced with new server	Configure NTP servers and keys and map it to apgroup. After deletion of existed NTP server and configure new NTP and validate the new NTP time is synced to all aps in that group	Passed	
WLJ8102S_Reg_445	Validating whether AP is synced with a present in agroup corresponding to NTPserver with AP console logs	To monitor whether AP is synced with AP group NTP server or not	Passed	
WLJ8102S_Reg_446	Validate NTP configs are present in running config	Configure max NTP servers, key and map to apgroup and validate configs exists in running config	Passed	
WLJ8102S_Reg_447	Move AP from one group to another and validate ap time is updated with new NTP server	Configure multiple NTP servers,keys and map to different apgroups. Move ap from group to another and validate the time on AP	Passed	

WLJ8102S_Reg_448	Validate NTP configuration after uploading and downloading the WLC config	Configure max NTP servers, key and map to apgroup and save the config and upload and download WLC and validate the configs on wlc	Passed	
WLJ8102S_Reg_449	Connecting client to IOS AP and checking NTP status	To verify whether IOS AP sync with the NTP server or not	Passed	
WLJ8102S_Reg_450	Connecting client to COS AP and checking NTP status	To verify whether COS AP sync with the NTP server or not	Passed	
WLJ8102S_Reg_451	Validate NTP configurations on WLC after rebooting WLC	Configure the NTP server,key and map those to apgroup and reboot the WLC and validate all the configs retains in WLC	Passed	
WLJ8102S_Reg_452	Validate NTP configuration synced with secondary WLC	Configure the NTP server,key and map those to apgroup and verify the configs are synced to standby WLC	Passed	
WLJ8102S_Reg_453	Validate NTP configuration after WLC failover happened and validate time on AP	Configure the NTP server,key and map those to apgroup do a switchover and verify the configs are present and ap's are getting proper NTP time	Passed	
WLJ8102S_Reg_454	Validating time after doing intra roaming with COS and IOS Aps Aps and connecting client	To verify whether time showing same after intra roaming	Passed	
WLJ8102S_Reg_455	Verifying NTP synchronization with ISR APS	To check whether ISR Aps are showing proper time or not after sync	Passed	

WLJ8102S_Reg_456	Rebooting AP and checking the sync details	To verify whether Aps synch time properly after rebooting	Passed	
WLJ8102S_Reg_457	Checking the NTP status with mess support Aps	To verify whether Mess AP synchronize with NTP server or not	Passed	

Flexconnect Post Auth ACL Per WLAN

Logical ID	Title	Description	Status	Defect ID
WLJ810S_FPA_01	Creating WLAN with L2 as WPA+WPA2 and L3 as authentication and map post auth ACL in WLAN	To verify whether client connected successfully and applied Post auth ACL in WLAN	Passed	
WLJ810S_FPA_02	Mapping ACL in WLAN using L2 as WP2+WPA3 and L3 as pass-through	To verify whether client connected successfully and applied Post auth ACL in WLAN	Passed	
WLJ810S_FPA_03	Checking the clients dissociation in post auth state after logout from web-auth	To verify whether clients gets disassociated after successful logout from web-auth	Passed	
WLJ810S_FPA_04	Checking pre-auth ACL's gets deleted after client switching from web-auth to post auth state	To verify whether pre-auth ACL's gets deleted after client switching from web-auth to post-auth	Passed	
WLJ810S_FPA_05	Removing mapped ACL in WLAN after client gets connected	To verify whether ACL's removes from AP and controller after removing ACL's	Passed	
WLJ810S_FPA_06	Mapping ACL in WLAN using L2 as WPA+WPA2 and L3 as on MAC failure	To verify whether ACL applied post auth ACL successfully in WLAN	Passed	

WLJ810S_FPA_07	Creating WLAN with L2 as WPA+WPA2 and L3 as authentication and map ACL in flex connect group	To verify whether WLAN redirected and flex connect group applied successfully in post-auth ACL	Passed	
WLJ810S_FPA_08	Creating WLAN with L2 as WPA+WPA3 and L3 as pass-through and map ACL in flex connect group	To verify whether client connected successfully and applied Post auth ACL in flex connect group	Passed	
WLJ810S_FPA_09	Creating WLAN with L2 as Static WEP and L3 as on MAC failure and map ACL in flex connect group	To verify whether client connected successfully and applied Post auth ACL in flex connect group	Passed	
WLJ810S_FPA_10	Creating WLAN with L2 as WPA+WPA2 and L3 as authentication and mapping ACL in flex connect group and WLAN	To verify whether client connected successfully and flex connect group applied in post-auth ACL	Passed	
WLJ810S_FPA_11	Creating WLAN with L2 as WPA+WPA2 and L3 as pass-through and mapping ACL in flex connect group and WLAN	To verify whether client connected successfully and flex connect group applied in post-auth ACL	Passed	
WLJ810S_FPA_12	Creating WLAN with L2 as WPA+WPA2 and L3 as authentication and mapping ACL in AP	To verify whether client connected successfully and AP level applied in post-auth ACL	Passed	
WLJ810S_FPA_13	Mapping ACL in AP using L2 as WP2+WPA3 and L3 as pass-through	To verify whether client connected successfully and AP level applied successfully in post-auth ACL	Passed	

WLJ810S_FPA_14	Mapping ACL flex connect group and AP with L2 as WPA+WPA2 and L3 as authentication	To verify whether client connected successfully and AP level applied in post-auth ACL	Passed	
WLJ810S_FPA_15	Creating WLAN with L2 as static WEP and L3 as pass-through and mapping ACL in AP and WLAN	To verify whether client connected successfully and AP level applied in post-auth ACL	Passed	
WLJ810S_FPA_16	Creating WLAN with L2 as WPA+WPA3 and L3 as on MAC failure and mapping ACL in AP ,WLAN and flex connect group	To verify the priority of WLAN,flexconnect and WLAN	Passed	
WLJ810S_FPA_17	Configure flex connect ACL on the controller map with local policy and connect the clients	To verify whether local policy overrides flex connect ACL	Passed	
WLJ8102S_Reg_458	Creating WLAN with L2 as WPA+WPA2 and L3 as authentication and map post auth ACL in WLAN	To verify whether client connected successflly and applied Post auth ACL in WLAN	Passed	
WLJ8102S_Reg_459	Mapping ACL in WLAN using L2 as WP2+WPA3 and L3 as passthrough	To verify whether client connected successflly and applied Post auth ACL in WLAN	Passed	
WLJ8102S_Reg_460	Checking the clients dissociation in post auth state after logout from web-auth	To verify whether clients gets disassociated after successful logout from web-auth	Passed	
WLJ8102S_Reg_461	Checking pre-auth ACL's gets deleted after client switching from web-auth to post auth state	To verify whether pre-auth ACL's gets deleted after client switching from web-auth to post-auth	Passed	

WLJ8102S_Reg_462	Removing mapped ACL in WLAN after client gets connected	To verify whether ACL's removes from AP and controller after removing ACL's	Passed	
WLJ8102S_Reg_463	Mapping ACL in WLAN using L2 as WPA+WPA2 and L3 as on MAC failure	To verify whether ACL applied post auth ACL successfully in WLAN	Passed	
WLJ8102S_Reg_464	Creating WLAN with L2 as WPA+WPA2 and L3 as authentication and map ACL in flexconnect group	To verify whether WLAN redirected and flexconnect group applied successfully in post-auth ACL	Passed	
WLJ8102S_Reg_465	Creating WLAN with L2 as WPA+WPA3 and L3 as passthrough and map ACL in flexconnect group	To verify whether client connected successflly and applied Post auth ACL in flexconnect group	Passed	
WLJ8102S_Reg_466	Creating WLAN with L2 as Static WEP and L3 as on MAC failure and map ACL in flexconnect group	To verify whether client connected successflly and applied Post auth ACL in flexconnect group	Passed	
WLJ8102S_Reg_467	Creating WLAN with L2 as WPA+WPA2 and L3 as authentication and mapping ACL in flexconnect group and WLAN	To verify whether client connected successfully and flexconnect group applied in post-auth ACL	Passed	
WLJ8102S_Reg_468	Creating WLAN with L2 as WPA+WPA2 and L3 as passthrough and mapping ACL in flexconnect group and WLAN	To verify whether client connected successfully and flexconnect group applied in post-auth ACL	Passed	

WLJ8102S_Reg_469	Creating WLAN with L2 as WPA+WPA2 and L3 as authentication and mapping ACL in AP	To verify whether client connected successfully and AP level applied in post-auth ACL	Passed	
WLJ8102S_Reg_470	Mapping ACL in AP using L2 as WP2+WPA3 and L3 as passthrough	To verify whether client connected successfully and AP level applied successfully in post-auth ACL	Passed	
WLJ8102S_Reg_471	Mapping ACL flexconnect group and AP with L2 as WPA+WPA2 and L3 as authentication	To verify whether client connected successfully and AP level applied in post-auth ACL	Passed	
WLJ8102S_Reg_472	Creating WLAN with L2 as static WEP and L3 as passthrough and mapping ACL in AP and WLAN	To verify whether client connected successfully and AP level applied in post-auth ACL	Passed	
WLJ8102S_Reg_473	Creating WLAN with L2 as WPA+WPA3 and L3 as on MAC failure and mapping ACL in AP ,WLAN and flexconnect group	To verify the priority of WLAN,flexconnect and WLAN	Passed	
WLJ8102S_Reg_474	Configure flexconnect ACL on the controller map with local policy and connect the clients	To verify whether local policy overrides flexconnect ACL	Passed	

ATF for All Modes(Mesh and ME)

Logical ID	Title	Description	Status	Defect ID

WLJ810S_ATF_01	Creating Policy with different weights and enabling/disabling client pair sharing	To verify whether user able to create Policy configuration with different weights and enabling/disabling client pair sharing	Passed	
WLJ810S_ATF_02	Configuring ATF monitor mode configuration with AP name and checking the ATF statistics per WLAN	To check whether ATF statistics showing or not per WLAN in monitor mode	Passed	
WLJ810S_ATF_03	Checking the ATF statistics per WLAN with enabling radio modes as monitor	To check whether user able to view Instantaneous and Accumulated Values in ATF statistics	Passed	
WLJ810S_ATF_04	Checking the ATF statistics per WLAN with disabling radio modes	To check whether user able to view Instantaneous and Accumulated time as 0 sec in ATF statistics after disabled radio modes	Passed	
WLJ810S_ATF_05	Configuring ATF enforce mode with AP name and mapping WLAN with policy ID	To verify whether able to configure ATF enforcement with AP name and mapping WLAN with policy ID	Passed	
WLJ810S_ATF_06	Connecting client to the WLAN with ATF enforcement mode configuration with Ap name and check the client statistics	To verify Client statistics after client connected to the WLAN with ATF enforcement mode	Passed	
WLJ810S_ATF_07	Connecting client to the WLAN with ATF enforcement mode configuration with AP group name and check the client statistics	To verify client statistics after connected to the WLAN with ATF enforcement mode configuration with AP group name	Passed	

WLJ810S_ATF_08	Connecting client to the WLAN with ATF enforcement mode configuration with network and check the client statistics	To verify client statistics after connected to the WLAN with ATF enforcement mode configuration with network	Paased	
WLJ810S_ATF_09	Config Mesh setup and apply config on Mesh Aps	To verify that Mesh setup configured and mesh Aps added in ATF	Passed	
WLJ810S_ATF_10	Apply ATF Enforcement mode on MESH AP	To verify that ATF Enforcement mode applied on MESH AP or not	Passed	
WLJ810S_ATF_11	Apply ATF policy on wlan and connect Android client for mesh configured AP	To verify that policy applied on WLAN and connect client to the mesh configured AP successfully or not	Passed	
WLJ810S_ATF_12	Apply ATF Enforcement mode on AP group	To verify that ATF Enforcement mode applied on AP group or not	Passed	
WLJ810S_ATF_13	Airtime allocation override on universal client access radio 802.11a	To verify that ATF override on universal client access radio 802.11a is enable or not	Passed	
WLJ810S_ATF_14	Airtime allocation override on universal client access radio 802.11b	To verify that ATF override on universal client access radio 802.11b is enable or not	Passed	
WLJ810S_ATF_15	Connecting three or more clients to created AFT policy without client fair sharing and checking the whether all the clients associated to SSID gets un equal air time	To verify whether connected clients showing unequal fair time or not without client fair	Passed	

WLJ810S_ATF_16	Connecting three or more clients to created AFT policy with client fair sharing and checking the whether all the clients associated to SSID gets equal air time	To verify whether connected clients showing equal fair time or not with client fair	Passed	
WLJ810S_ATF_17	Configure two AFT policies with different weights and map to diffent WLANs and connecting 2 clinets	To verify clients capability, interference and other factors able to see after connected with different weights and map to diffent WLANs	Passed	
WLJ8102S_Reg_475	Creating Policy with different weights and enabling/disabling client pair sharing	To verify whether user able to create Policy configuration with different weights and enabling/disabling client pair sharing	Passed	
WLJ8102S_Reg_476	Configuring ATF monitor mode configuration with AP name and checking the ATF statistics per WLAN	To check whether ATF statistics showing or not per WLAN in monitor mode	Failed	CSCvr08928
WLJ8102S_Reg_477	Checking the ATF statistics per WLAN with enabling radio modes as monitor	To check whether user able to view Instantaneous and Accumulated Values in ATF statistics	Passed	
WLJ8102S_Reg_478	Checking the ATF statistics per WLAN with disabling radio modes	To check whether user able to view Instantaneous and Accumulated time as 0 sec in ATF statistics after disabled radio modes	Passed	

WLJ8102S_Reg_479	Configuring ATF enforce mode with AP name and mapping WLAN with policy ID	To verify whether able to configure ATF enforcement with AP name and mapping WLAN with policy ID	Passed	
WLJ8102S_Reg_480	Connecting client to the WLAN with ATF enforcement mode configuration with Ap name and check the client statstics	To verify Client statistics after clinet connected to the WLAN with ATF enforcement mode	Passed	
WLJ8102S_Reg_481	Connecting client to the WLAN with ATF enforcement mode configuration with AP group name and check the client statstics	To verify client statistics after connected to the WLAN with ATF enforcement mode configuration with AP group name	Passed	
WLJ8102S_Reg_482	Connecting client to the WLAN with ATF enforcement mode configuration with network and check the client statstics	To verify client statistics after connected to the WLAN with ATF enforcement mode configuration with network	Passed	
WLJ8102S_Reg_483	Config Mesh setup and apply config on Mesh Aps	To verify that Mesh setup configured and mesh Aps added in ATF	Passed	
WLJ8102S_Reg_484	Apply ATF Enforcement mode on MESH AP	To verify that ATF Enforcement mode applied on MESH AP or not	Passed	
WLJ8102S_Reg_485	Apply ATF policy on wlan and connect Android client for mesh configured AP	To verify that policy applied on WLAN and connect client to the mesh configured AP succesfully or not	Passed	
WLJ8102S_Reg_486	Apply ATF Enforcement mode on AP group	To verify that ATF Enforcement mode applied on AP group or not	Passed	

WLJ8102S_Reg_487	Airtime allocation override on universal client access radio 802.11a	To verify that ATF override on universal client access radio 802.11a is enable or not	Passed	
WLJ8102S_Reg_488	Airtime allocation override on universal client access radio 802.11b	To verify that ATF override on universal client access radio 802.11b is enable or not	Passed	
WLJ8102S_Reg_489	Connecting three or more clients to created AFT plocy without client fair sharing and checking the whether all the clients associated to SSID gets un equal air time	To verify whether connected clients showing unequal fair time or not without client fair	Passed	
WLJ8102S_Reg_490	Connecting three or more clients to created AFT plocy with client fair sharing and checking the whether all the clients associated to SSID gets equal air time	To verify whether connected clients showing equal fair time or not with client fair	Passed	
WLJ8102S_Reg_491	Configure two AFT policies with different weights and map to diffent WLANs and connecting 2 clinets	To verify clients capability, interference and other factors able to see after connected with different weights and map to diffent WLANs	Passed	

Intelligent Capture for 1850 AP

Logical ID	Title	Description	Status	Defect ID
WLJ810S_ICAPC_01	Packet capture for Android client using Intelligent Capture option in Apgroup	To verify the packet capture for Android client using Intelligent capture in Apgroup	Passed	

WLJ810S_ICAPC_02	Packet capture of client when the client is connected to 1850AP 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	
WLJ810S_ICAPC_03	Packet capture of client when the client is connected to 1850AP with 5 GHz	To capture the Packet of the client when the client is connected to AP with radio as 5 GHz	Passed	
WLJ810S_ICAPC_04	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 1850AP with security as WPA 2 PSK	Passed	
WLJ810S_ICAPC_05	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 1850AP with security as WPA 2 802.1x	Passed	
WLJ810S_ICAPC_06	Verifying 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	
WLJ810S_ICAPC_07	Verifying 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	
WLJ810S_ICAPC_08	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	

WLJ810S_ICAPC_09	Performing Inter controller roaming of client and capturing the packet	To check whether inter controller roaming of Android clients works properly or not	Passed	
WLJ810S_ICAPC_10	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	
WLJ810S_ICAPC_11	Packet capture using roaming scenario in APgroup using different Aps	To capture the Packet by using different AP in APgroup and check if the client roams between different Aps	Passed	
WLJ810S_ICAPC_12	Packet capture for Any connect client using Intelligent Capture option in AP page	To verify the packet capture for Any connect client using Intelligent capture in AP page	Passed	
WLJ810S_ICAPC_13	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	
WLJ810S_ICAPC_14	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	
WLJ810S_ICAPC_15	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	
WLJ810S_ICAPC_16	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	

WLJ810S_ICAPC_17	Packet capture for Windows client using Intelligent Capture option in APgroup	To verify the packet capture for Windows client using Intelligent capture in APgroup	Passed	
WLJ810S_ICAPC_18	Packet capture for IOS client using Intelligent Capture option in APgroup	To verify the packet capture for IOS client using Intelligent capture in APgroup	Passed	
WLJ810S_ICAPC_19	Packet capture for Mac OS client using Intelligent Capture option in APgroup	To verify the packet capture for Mac OS client using Intelligent capture in APgroup	Passed	
WLJ810S_ICAPC_20	Capturing of Packet of the client when the client is connected with open security	To capture packet when the client is connected to the 1850AP with security as OPEN	Passed	

Intelligent Capture for 9115 AP

Logical ID	Title	Description	Status	Defect ID
WLJ810S_ICAPax_01	Packet capture for Android client using Intelligent Capture option in Apgroup	To verify the packet capture for Android client using Intelligent capture in Apgroup	Passed	
WLJ810S_ICAPax_02	Configuring the Intelligent Capture parameters via WLC CLI	To configure Intelligent Capture parameters on WLC CLI and check if all the parameters can be configured using CLI or not	Passed	
WLJ810S_ICAPax_03	Packet capture of client when the client is connected to 9115AP 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	

WLJ810S_ICAPax_04	Packet capture of client when the client is connected to 9115AP with 5 GHz	To capture the Packet of the client when the client is connected to AP with radio as 5 GHz	Passed	
WLJ810S_ICAPax_05	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 9115AP with security as WPA 2 PSK	Passed	
WLJ810S_ICAPax_06	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 9115AP with security as WPA 2 802.1x	Passed	
WLJ810S_ICAPax_07	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	
WLJ810S_ICAPax_08	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	
WLJ810S_ICAPax_09	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	
WLJ810S_ICAPax_10	Performing Inter controller roaming of client and capturing the packet	To check whether inter controller roaming of Android clients works properly or not	Passed	

WLJ810S_ICAPax_11	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	
WLJ810S_ICAPax_12	Packet capture using APgroup without a AP in it	To check if packet capture occurs or not if no AP is in the APgroup	Passed	
WLJ810S_ICAPax_13	Packet capture using roaming scenario in APgroup using different Aps	To capture the Packet by using different AP in APgroup and check if the client roams between different Aps	Passed	
WLJ810S_ICAPax_14	Packet capture for Any connect client using Intelligent Capture option in AP page	To verify the packet capture for Any connect client using Intelligent capture in AP page	Passed	
WLJ810S_ICAPax_15	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	
WLJ810S_ICAPax_16	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	
WLJ810S_ICAPax_17	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	
WLJ810S_ICAPax_18	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	

WLJ810S_ICAPax_19	Packet capture for Windows client using Intelligent Capture option in APgroup	To verify the packet capture for Windows client using Intelligent capture in APgroup	Passed	
WLJ810S_ICAPax_20	Packet capture for IOS client using Intelligent Capture option in APgroup	To verify the packet capture for IOS client using Intelligent capture in APgroup	Passed	
WLJ810S_ICAPax_21	Packet capture for Mac OS client using Intelligent Capture option in APgroup	To verify the packet capture for Mac OS client using Intelligent capture in APgroup	Passed	
WLJ810S_ICAPax_22	Capturing of Packet of the client when the client is connected with open security	To capture packet when the client is connected to the 9115AP with security as OPEN	Passed	
WLJ810S_ICAPax_23	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 9115AP with security as Static WEP	Passed	
WLJ810S_ICAPax_24	Verifying the packet capture happen 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	

DNA Spaces

Logical ID	Title	Description	Status	Defect ID
WLJ810S_DNAS_01	Configuring token for WLC to connect to Cisco DNA Spaces	To configuring token for WLC to connect to Cisco DNA Spaces	Passed	

WLJ810S_DNAS_02	Adding a Wireless Network in DNA Spaces	To add a wireless network in DNA spaces and check if the wireless network is added to the DNA Spaces.	Passed	
WLJ810S_DNAS_03	Importing the DigiCert CA Root Certificate	To import a DigiCert CA Root Certificate	Passed	
WLJ810S_DNAS_04	Connect a WLC to DNA Spaces via Aireos WLC Direct connector	To connect a WLC to DNA Spaces via Aireos WLC direct connector.	Passed	
WLJ810S_DNAS_05	Connect a WLC to DNA Spaces via Aireos WLC Direct connector using wrong token or certificate.	To connect a WLC to DNA Spaces via Aireos WLC direct connector using wrong token or certificate and check if the WLC is showing in location hierarchy or not.	Passed	
WLJ810S_DNAS_06	Adding the WLC to the Group	To add a group to the WLC and check if the access points are listed in the group .	Passed	
WLJ810S_DNAS_07	Connecting CMX to DNA Spaces using CMX Tethering	To connect CMX to DNA spaces using CMX tethering and check if the CMX is added	Passed	
WLJ810S_DNAS_08	Connecting CMX to DNA Spaces using CMX Tethering and adding Campuses	To connect CMX to DNA spaces using CMX tethering and add campuses. check if the CMX is added and campuses are added to it.	Passed	
WLJ810S_DNAS_09	Adding a space connector to DNA Spaces	To add a space connector to DNA spaces.	Passed	

WLJ810S_DNAS_10	Adding a controller to DNA Space using Space connector	To add a controller to DNA space using space connecter and check if the controller is added or not.	Passed	
WLJ810S_DNAS_11	Upgrading the DNA Space connector	To upgrade the DNA space connector and check if the connector is upgraded or not	Passed	
WLJ810S_DNAS_12	Adding a AP to the already configured WLC in DNA Space	Adding a AP to the already configured WLC and check if the AP count gets added increased	Passed	
WLJ810S_DNAS_13	Checking the location update in DNA Space	To check the location update for the controller and CMX in Monitoring and Support page	Passed	

Nbar Upgrade

Logical ID	Title	Description	Status	Defect ID
WLJ810S_Nbar_01	Create a AVC profile and add rule to drop the YouTube application	To check whether "YouTube" application getting dropped or not	Passed	
WLJ810S_Nbar_02	Add the rate limit rule for YouTube application	Verify the YouTube application rate limit traffic	Passed	
WLJ810S_Nbar_03	Configure the rule mark for AVC YouTube application	Checking YouTube Application is getting marked with correct DSCP value or not	Passed	
WLJ810S_Nbar_04	Create a AVC profile and add rule to drop the skype application	To check whether "skype" application getting dropped or not	Passed	
WLJ810S_Nbar_05	Add the rate limit rule for "skype" application	Verify the "skype" application rate limit traffic	Passed	

WLJ810S_Nbar_06	Create the AVC profile and add a rule mark to the "skype" application	Checking "skype" Application is getting marked with correct DSCP value or not	Passed	
WLJ810S_Nbar_07	Create a AVC profile and add rule to drop the webex-meeting application	To check whether webex-meeting application getting dropped or not	Passed	
WLJ810S_Nbar_08	Add the rate limit rule for webex-meeting application	Verify the webex-meeting application rate limit traffic	Passed	
WLJ810S_Nbar_09	Create the AVC profile and add a rule mark to the webex-meeting application	Checking webex-meeting Application is getting marked with correct DSCP value or not	Passed	
WLJ810S_Nbar_10	Create a AVC profile and add rule to drop the facebook application	To check whether facebook application getting dropped or not	Passed	
WLJ810S_Nbar_11	Add the rate limit rule for facebook application	Verify the facebook application rate limit traffic	Passed	
WLJ810S_Nbar_12	Create the AVC profile and add a rule mark to the facebook application	Checking facebook Application is getting marked with correct DSCP value or not	Passed	
WLJ810S_Nbar_13	Create a AVC profile and add rule to drop the LinkedIn application	To check whether LinkedIn application getting dropped or not	Passed	
WLJ810S_Nbar_14	Add the rate limit rule for LinkedIn application	Verify the LinkedIn application rate limit traffic	Passed	
WLJ810S_Nbar_15	Create the AVC profile and add a rule mark to the LinkedIn application	Checking LinkedIn Application is getting marked with correct DSCP value or not	Passed	

WLJ810S_Nbar_16	Create a AVC profile and add rule to drop the twitter application	To check whether twitter application getting dropped or not	Passed	
WLJ810S_Nbar_17	Add the rate limit rule for twitter application	Verify the twitter application rate limit traffic	Passed	
WLJ810S_Nbar_18	Create the AVC profile and add a rule mark to the twitter application	Checking twitter Application is getting marked with correct DSCP value or not	Passed	
WLJ810S_Nbar_19	Create a AVC profile and add rule to drop the http application	To check whether http application getting dropped or not	Passed	
WLJ810S_Nbar_20	Add the rate limit rule for http application	Verify the http application rate limit traffic	Passed	
WLJ810S_Nbar_21	Create the AVC profile and add a rule mark to the http application	Checking http Application is getting marked with correct DSCP value or not	Passed	
WLJ810S_Nbar_22	Create a flex AVC profile and add rule to drop the webex-meeting application	To check whether webex-meeting application getting dropped or not	Passed	
WLJ810S_Nbar_23	Add the rate limit rule for flex AVC webex-meeting application	Verify the flex AVC "webex-meeting" application rate limit traffic	Passed	
WLJ810S_Nbar_24	Configure the flex AVC profile and add a rule mark to the "webex-meeting" application	Checking webex-meeting Application is getting marked with correct DSCP value or not	Passed	
WLJ810S_Nbar_25	Create a flex AVC profile and add rule to drop the Wi-Fi-calling application	To check whether Wi-Fi-calling application getting dropped or not	Passed	

WLJ810S_Nbar_26	Add the rate limit rule for flex AVC Wi-Fi-calling application	Verify the flex AVC Wi-Fi-calling application rate limit traffic	Passed	
WLJ810S_Nbar_27	Configure the flex AVC profile and add a rule mark to the "Wi-Fi-calling" application	Checking Wi-Fi-calling Application is getting marked with correct DSCP value or not	Passed	
WLJ810S_Nbar_28	Create a flex AVC profile and add rule to drop the cisco-spark application	To check whether cisco-spark application getting dropped or not	Passed	
WLJ810S_Nbar_29	Add the rate limit rule for flex AVC cisco-spark application	Verify the flex AVC cisco-spark application rate limit traffic	Passed	
WLJ810S_Nbar_30	Configure the flex AVC profile and add a rule mark to the "cisco-spark" application	Checking flex AVC cisco-spark Application is getting marked with correct DSCP value or not	Passed	
WLJ810S_Nbar_31	Create a flex AVC profile and add rule to drop the Verizon-wireless-web application	To check whether flex AVC Verizon-wireless-web application getting dropped or not	Passed	
WLJ810S_Nbar_32	Add the rate limit rule for flex AVC Verizon-wireless-web application	Verify the flex AVC Verizon-wireless-web application rate limit traffic	Passed	
WLJ810S_Nbar_33	Configure the flex AVC profile and add a rule mark to the "Verizon-wireless-web" application	Checking flex AVC Verizon-wireless-web Application is getting marked with correct DSCP value or not	Passed	
WLJ810S_Nbar_34	Create a flex AVC profile and add rule to drop the time-news application	To check whether flex AVC time-news application getting dropped or not	Passed	

WLJ810S_Nbar_35	Add the rate limit rule for flex AVC time-news application	Verify the flex AVC time-news application rate limit traffic	Passed	
WLJ810S_Nbar_36	Configure the flex AVC profile and add a rule mark to the "time-news" application	Checking flex AVC time-news Application is getting marked with correct DSCP value or not	Passed	

Password Encryption in running Configuration

Logical ID	Title	Description	Status	Defect ID
WLJ8102S_PWD_01	Validate if all the password in running configuration of 3504 WLC are encrypted or not	To validate if the passwords in running configuration are encrypted in 3504 WLC	Passed	
WLJ8102S_PWD_02	Validate if all the password in running configuration of 5520 WLC are encrypted or not	To validate if the passwords in running configuration are encrypted in 5520 WLC	Passed	
WLJ8102S_PWD_03	Validate if all the password in running configuration of 8540 WLC are encrypted or not	To validate if the passwords in running configuration are encrypted in 8540 WLC	Passed	
WLJ8102S_PWD_04	Exporting running configuration through Tftp to check if all passwords encrypted or not.	To check if all the password in running configuration of WLC are encrypted when exported through tftp from WLC UI	Passed	
WLJ8102S_PWD_05	Exporting running configuration through ftp to check if all passwords encrypted or not.	To check if all the password in running configuration of WLC are encrypted when exported through tftp from WLC UI	Passed	

WLJ8102S_PWD_06	Exporting running configuration through Sftp to check if all passwords encrypted or not.	To check if all the password in running configuration of WLC are encrypted when exported through tftp from WLC UI	Passed	
WLJ8102S_PWD_07	Check the password encryption for ssid with WPA2 PSK security in running config and validate if the password are encrypted or not	To verify if the password is encrypted for ssid with WPA2 PSK security in running config or not	Passed	
WLJ8102S_PWD_08	Check the password encryption for ssid with WPA3 PSK security in running config and validate if the password are encrypted or not	To verify if the password is encrypted for ssid with WPA3 PSK security in running config or not	Passed	
WLJ8102S_PWD_09	Check if the password encrypted for ssid with Static WEP with 40 bit key security in running config and validate if the password are encrypted or not	To verify if the password is encrypted in running config for WLAN with Static WEP with 40 bit key or not	Passed	
WLJ8102S_PWD_10	Check if the password encrypted for ssid with Static WEP 104 bit key security in running config and validate if the password are encrypted or not	To check if the password for WLAN with Static WEP with 104 bit key is encrypted or not.	Passed	
WLJ8102S_PWD_11	Configuring HA for WLC to check if the password is encrypted in both active and standy WLC	To configure HA for WLC and check if the passwords in running configuration is encrypted	Passed	

Support of Trap notification via SNMP3

Logical ID	Title	Description	Status	Defect ID

WLJ8102S_SNMP_01	Creating SNMP V3 user with authentication & privacy protocol as none	To verify whether user able to create SNMP V3 user without any issues or not	Passed	
WLJ8102S_SNMP_02	Configuring the maximum SNMP trap receiver with mapping SNMP V3 username	To check whether able to configure six(max) SNMP trap receivers with mapping SNMP V3 username or not	Passed	
WLJ8102S_SNMP_03	Removing the trap receiver with after mapped SNMP v3 user	To check whether able to delete trap receiver with mapped SNMP v3 user	Passed	
WLJ8102S_SNMP_04	Checking the SNMP trap messages in receiver after configuring client side parameters in trap controls	To verify whether user able to get SNMP V3 traps after configuring client parameters	Passed	
WLJ8102S_SNMP_05	Checking the SNMP trap messages in receiver after configuring AP parameters in trap controls	To verify whether user able to get SNMP V3 traps after configuring AP parameters	Passed	
WLJ8102S_SNMP_06	Checking the SNMP trap messages in receiver after configuring security parameters in trap controls	To verify whether user able to get SNMP V3 traps after configuring security parameters	Passed	
WLJ8102S_SNMP_07	Checking the SNMP trap messages in receiver after configuring auto RF parameters in trap controls	To verify whether user able to get SNMP V3 traps after configuring RF parameters	Passed	

WLJ8102S_SNMP_08	Checking the SNMP trap messages in receiver after configuring mesh parameters in trap controls	To verify whether user able to get SNMP V3 traps after configuring Mesh parameters	Passed	
WLJ8102S_SNMP_09	Checking the SNMP trap messages in receiver after configuring general parameters in trap controls	To verify whether user able to get SNMP V3 traps after configuring general parameters	Passed	
WLJ8102S_SNMP_10	Creating SNMP V3 user with authentication & privacy protocol as none	To verify whether user able to create SNMP V3 user without any issues or not	Passed	
WLJ8102S_SNMP_11	Creating SNMP V3 user with authentication as MD5 & privacy protocol as AES	To verify whether user able to create SNMP V3 user without any issues or not	Passed	
WLJ8102S_SNMP_12	Creating SNMP V3 user with authentication SHA & privacy protocol as AES	To verify whether user able to create SNMP V3 user without any issues or not	Passed	
WLJ8102S_SNMP_13	Creating SNMP V3 user with authentication & privacy protocol as none and access mode as read only	To verify whether user able to create SNMP V3 user without any issues or not	Passed	
WLJ8102S_SNMP_14	Creating SNMP V3 user with authentication & privacy protocol as none and access mode as read and write	To verify whether user able to create SNMP V3 user without any issues or not	Passed	
WLJ8102S_SNMP_15	Creating the trap receiver and snmp template in PI and deploying to WLC	To check whether user able to deploy template to WLC without any issues or not	Passed	

RSSI and SNR in ASSOC Request

Logical ID	Title	Description	Status	Defect ID
WLJ8102S_SNR & RSS_01	Adding WLC to DNAC and connecting clients	To verify SNR and RSS logs in DNA center after connecting client	Passed	
WLJ8102S_SNR & RSS_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 flex connect and authentication as open	Passed	
WLJ8102S_SNR & RSS_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 flex connect and authentication as PSK	Passed	
WLJ8102S_SNR & RSS_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 flex connect and authentication as dot11	Passed	
WLJ8102S_SNR & RSS_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	
WLJ8102S_SNR & RSS_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	
WLJ8102S_SNR & RSS_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	

WLJ8102S_SNR & RSS_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	
WLJ8102S_SNR & RSS_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	
WLJ8102S_SNR & RSS_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	
WLJ8102S_SNR & RSS_11	Checking the SNR and RSS values after performing intra roaming in WLC	To verify SNR and RSS connectivity in DNAcentre after doing intra roaming in WLC	Passed	
WLJ8102S_SNR & RSS_12	Roaming client from 3800 & 1815 Aps and checking the SNR and RSS values	To Check the SNR and RSS values when client roam between 3800 & 1815 Aps	Passed	
WLJ8102S_SNR & RSS_13	Checking the SNR and RSS values after performing inter roaming in WLC	To verify SNR and RSS connectivity in DNAcentre after doing inter roaming in WLC	Passed	
WLJ8102S_SNR & RSS_14	Checking the SNR and RSS values after performing FT roaming roaming in WLC	To verify SNR and RSS connectivity in DNAcentre after doing FT roaming in WLC	Passed	
WLJ8102S_SNR & RSS_15	Verifying the AID values in client after connecting client	To check whether client getting AID value or not	Passed	

WPA3 Support

Logical ID	Title	Description	Status	Defect ID

WLJ8102S_WPA3_01	Checking the WPA3 configurations	To check the SAE and WPA3 security support.	Passed	
WLJ8102S_WPA3_03	Verifying WPA3 and dot1x support for the Android client	To verify the dot1x Auth key support to the WPA3 security for the Android client.	Passed	
WLJ8102S_WPA3_06	Verifying the WPA3 and PSK security support for the Android client	To verify the Psk Auth key support to the WPA3 security for the Android client.	Passed	
WLJ8102S_WPA3_09	Check the WPA3 support for SAE security for the Android client	To verify the SAE and WPA3 security support for the Android client	Passed	
WLJ8102S_WPA3_12	Verify the CCKM security key to the WPA3 for the Android client	To verify the CCKM and WPA3 security support for the Android client	Passed	
WLJ8102S_WPA3_17	Verifying the WPA3 security support for the Ft-dot1x security	To verify the Ft-dot1x Auth key support to the WPA3 security	Passed	
WLJ8102S_WPA3_18	Validate the Ft-Psk Auth key support to the WPA3 security	To validate the Ft-Psk auth key support to the WPA3 security.	Failed	CSCvr33062
WLJ8102S_WPA3_19	Validate the WPA3 support for the Layer 3 Authentication security type	To validate the Layer 3 Authentication security type support for the WPA3 security	Passed	
WLJ8102S_WPA3_20	Verifying the WPA3 support for the Layer 3 Pass-through security type	To verify the Layer 3 Pass-through security type support for the WPA3 security	Passed	
WLJ8102S_WPA3_21	Checking the WPA3 support for the Layer 3 Conditional web redirect security type	To check the Layer 3 Conditional web redirect security type support for the WPA3 security	Passed	

WLJ8102S_WPA3_22	Checking the WPA3 support for the Layer 3 Splash page web redirect security type	To check the Layer 3 Splash page web redirect security type support for the WPA3 security	Passed	
WLJ8102S_WPA3_23	Checking the WPA3 support for the Layer 3 On Mac Filter Failure security type	To check the Layer 3 On Mac Filter Failure Security type support for the WPA3 security	Passed	
WLJ8102S_WPA3_24	Verify the WPA3 security support for the Sleeping Client	To verify the WPA3 support for the Sleeping client	Passed	
WLJ8102S_WPA3_25	Verifying the WPA3 security support for the Pre Auth ACl	To verify the WPA3 security support by mapping the Pre Auth Acl	Passed	
WLJ8102S_WPA3_26	Verifying the WPA3 security support for the Web Auth ACl	To verify the WPA3 security support by mapping the Web Auth Acl	Passed	
WLJ8102S_WPA3_27	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	
WLJ8102S_WPA3_28	Verifying the WPA3 support with Intra AP Roaming with same AP group	To verify the Intra AP Roaming with same AP group with WPA3 support WLAN	Passed	
WLJ8102S_WPA3_29	Verifying the WPA3 support with Intra Controller Roaming between Different AP-Groups	To verify the Intra AP Roaming with Different AP group with WPA3 support WLAN	Passed	
WLJ8102S_WPA3_30	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	

WLJ8102S_WPA3_31	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
WLJ8102S_OWE_01	Checking the OWE configurations	To check the OWE support by configuring the WLAN with OWE	Passed	
WLJ8102S_OWE_02	Checking the OWE with OWE transition mode configurations	To check the OWE support with OWE transition mode by configuring the WLAN with OWE	Failed	CSCvr33178
WLJ8102S_OWE_03	Checking the OWE support for the Windows client.	To check the Client packets by connecting the windows client to OWE support SSID	Passed	
WLJ8102S_OWE_04	Checking the OWE support for the Android client.	To check the Client packets by connecting the Android client to OWE support SSID	Passed	
WLJ8102S_OWE_05	Checking the OWE support for the MAC Os client.	To check the Client packets by connecting the MAC oS client to OWE support SSID	Passed	
WLJ8102S_OWE_06	Verifying the OWE support with OWE transition mode for the Windows client	To verify the Client packets by connecting the windows client to OWE support SSID with OWE transition mode.	Passed	

WLJ8102S_OWE_07	Verifying the OWE support with OWE transition mode for the Android client	To verify the Client packets by connecting the Android client to OWE support SSID with OWE transition mode.	Passed	
WLJ8102S_OWE_08	Verifying the OWE support with OWE transition mode for the MAC OS client	To verify the Client packets by connecting the Mac os client to OWE support SSID with OWE transition mode.	Passed	
WLJ8102S_OWE_09	Validate the OWE Support with Layer3 Authentication	To Validate the Client packets by connecting the client to OWE support SSID with Layer3 Authentication	Passed	
WLJ8102S_OWE_10	Checking the OWE Support with Layer3 Pass-through	To check the Client packets by connecting the client to OWE support SSID with Layer3 Pass-through	Passed	
WLJ8102S_OWE_11	Validate the OWE Support with Layer3 Conditional web redirect	To check the Client packets by connecting the client to OWE support SSID with Layer3 Conditional Web redirect.	Passed	
WLJ8102S_OWE_12	Verifying the OWE Support with Layer3 Splash page web redirect.	To verify the OWE Support with Layer3 Splash page web redirect.	Passed	
WLJ8102S_OWE_13	Validate the OWE Support with Layer3 On MAC filter failure.	To check the Client packets by connecting the client to OWE support SSID with Layer3 On MAC filter failure.	Passed	

WLJ8102S_OWE_14	Mapping the Pre Auth Acl to the OWE security SSID	To verify the Client packets by mapping the Pre Auth Acl to the OWE Security SSID.	Passed	
WLJ8102S_OWE_15	Mapping the Web Auth Acl to the OWE security SSID	To verify the Client packets by mapping the Web Auth Acl to the OWE Security SSID.	Passed	
WLJ8102S_OWE_16	Validate the OWE Support with OWE transition mode and Layer3 Authentication	To Validate the Client packets by connecting the client to OWE support SSID with OWE transition mode and Layer3 Authentication	Passed	
WLJ8102S_OWE_17	Checking the OWE Support with OWE transition mode and Layer3 Pass-through	To check the Client packets by connecting the client to OWE support SSID with OWE transition mode and Layer3 Pass-through	Passed	
WLJ8102S_OWE_18	Validate the OWE Support with OWE transition mode and Layer3 Conditional web redirect	To check the Client packets by connecting the client to OWE support SSID with OWE transition mode and Layer3 Conditional Web redirect.	Passed	
WLJ8102S_OWE_19	Checking the OWE Support with OWE transition mode and Layer3 Splash page web redirect.	To check the OWE Support with OWE transition mode and Layer3 Splash page web redirect.	Passed	

WLJ8102S_OWE_20	Validate the OWE Support with OWE transition mode and Layer3 On MAC filter failure.	To check the Client packets by connecting the client to OWE support SSID with OWE transition mode and Layer3 On MAC filter failure.	Passed	
WLJ8102S_OWE_21	Mapping the Pre Auth Acl to the OWE security with OWE transition mode.	To verify the Client packets by mapping the Pre Auth Acl to the OWE Security SSID with OWE transition mode.	Passed	
WLJ8102S_OWE_22	Mapping the Web Auth Acl to the OWE security with OWE transition mode.	To verify the Client packets by mapping the Web Auth Acl to the OWE Security SSID with OWE transition mode	Passed	
WLJ8102S_OWE_23	Verifying the OWE support with Inter WLC Roaming	To verify inter WLC Roaming between WLANs with OWE support	Passed	
WLJ8102S_OWE_24	Verifying the OWE support with Intra AP Roaming with same AP group	To verify the Intra AP Roaming with same AP group with OWE support WLAN	Passed	
WLJ8102S_OWE_25	Verifying the OWE support with Intra Controller Roaming between Different AP-Groups	To verify the Intra AP Roaming with Different AP group with OWE support WLAN	Passed	
WLJ8102S_OWE_26	Verifying the OWE support with Inter WLC Roaming	To verify inter WLC Roaming between WLANs with OWE support and OWE transition mode WLAN.	Passed	

WLJ8102S_OWE_27	Verifying the OWE support with Intra AP Roaming with same AP group	To verify the Intra AP Roaming with same AP group with OWE support and OWE transition mode WLAN	Passed	
WLJ8102S_OWE_28	Verifying the OWE support with Intra Controller Roaming between Different AP-Groups	To verify the Intra AP Roaming with Different AP group with OWE support and OWE transition mode WLAN	Passed	
WLJ8102S_OWE_29	Verifying the 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 OWE support and OWE transition mode WLAN WLAN.	Passed	
WLJ8102S_OWE_30	Verifying the OWE support Roaming between Controllers with same Radio types	To verify whether Client is Moving between Controllers with same Radio type or not with OWE support and OWE transition mode WLAN WLAN.	Passed	
WLJ8102S_OWE_31	Verifying the IRCM Configuration with OWE Support	To Verifying the IRCM Configuration with OWE Support and OWE transition mode WLAN WLAN.	Passed	
WLJ8102S_OWE_32	Verifying the OWE support in Mesh network	To verify the OWE Support and OWE transition mode WLAN with Mesh network.	Passed	

DNAC Assurance

Logical ID	Title	Description	Status	Defect ID

WLJ8102S_Assurance_01	Adding the controller in Cisco DNAC	Provisioning the controller in Cisco DNAC	Passed	
WLJ8102S_Assurance_02	Upgrading WLC from Cisco DNAC	Verifying whether the user is able to upgrade the controller or not from Cisco DNAC	Passed	
WLJ8102S_Assurance_03	Checking the Performance of APs in Cisco DNAC	Verifying whether the Performance of APs are monitored correctly as per in the controller or not in Cisco DNAC	Passed	
WLJ8102S_Assurance_04	Verifying how many wireless devices are added in Cisco DNAC	Checking whether how many wireless devices are added in Cisco DNAC and they are monitored properly or not	Passed	
WLJ8102S_Assurance_05	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	
WLJ8102S_Assurance_06	Checking the Client connectivity status in Cisco DNAC	Verifying whether the Client status are monitored correctly as per in the controller or not in Cisco DNAC	Passed	
WLJ8102S_Assurance_07	Checking the Client Onboarding Times in Cisco DNAC	Verifying whether the Client Onboarding Times are monitored correctly as per in the controller or not in Cisco DNAC	Passed	

WLJ8102S_Assurance_08	Checking the Client Count per SSID in Cisco DNAC	Verifying whether the Client Count per SSID are monitored correctly as per in the controller or not in Cisco DNAC	Passed	
WLJ8102S_Assurance_09	Checking the Client Count per Band in Cisco DNAC	Verifying whether the Client Count per Band are monitored correctly as per in the controller or not in Cisco DNAC	Passed	
WLJ8102S_Assurance_10	Checking the Client RSSI & SNR values in Cisco DNAC	Verifying whether the RSSI & SNR are monitored correctly as per in the controller or not in Cisco DNAC	Passed	
WLJ8102S_Assurance_11	Checking the throughput & Packet loss details for the wireless devices	Verifying the Usage of Bytes, Average throughput & Packet loss details for the wireless devices	Passed	
WLJ8102S_Assurance_12	Performing Network Test in Sensor - Driven Test	Verifying the IP Addressing, DNS, Host Reachability & RADIUS Tests in Sensor - Driven Test	Passed	
WLJ8102S_Assurance_13	Capturing the Network Test from Wireless Sensor Dashboard	Mentoring the IP Addressing, DNS, Host Reachability & RADIUS Tests in Wireless Sensor Dashboard	Passed	
WLJ8102S_Assurance_14	Performing Performance Test in Sensor - Driven Test	Verifying the Speed Test & ISPLA Test in Sensor - Driven Test	Passed	

WLJ8102S_Assurance_15	Capturing the Performance Test from Wireless Sensor Dashboard	Monitoring the Speed Test & ISPLA Test in Wireless Sensor Dashboard	Passed	
WLJ8102S_Assurance_16	Performing Application Test in Sensor - Driven Test	Verifying the Email Test, Web Test & File Transfer Test in Sensor - Driven Test	Passed	
WLJ8102S_Assurance_17	Capturing the Application Test from Wireless Sensor Dashboard	Monitoring the Email Test, Web Test & File Transfer Test in Wireless Sensor Dashboard	Passed	
WLJ8102S_Assurance_18	Performing Scheduling Onboarding Packet Capture Test	Checking whether the Scheduling Onboarding Packet capture is done as per the schedule or not	Passed	
WLJ8102S_Assurance_19	Capturing Configured APs using Auto-Capture Settings	Testing whether the user able to capture or not the Configured APs using Auto-Capture Settings	Passed	
WLJ8102S_Assurance_20	Packet capture for Android client using Intelligent Capture option in Apgroup	To verify the packet capture for Android client using Intelligent capture in Apgroup	Passed	
WLJ8102S_Assurance_21	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	
WLJ8102S_Assurance_22	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	

WLJ8102S_Assurance_23	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	
WLJ8102S_Assurance_24	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	
WLJ8102S_Assurance_25	Verifying 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	
WLJ8102S_Assurance_26	Verifying 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	
WLJ8102S_Assurance_27	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	
WLJ8102S_Assurance_28	Performing Inter controller roaming of client and capturing the packet	To check whether inter controller roaming of Android clients works properly or not	Passed	

WLJ8102S_Assurance_29	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	
WLJ8102S_Assurance_30	Packet capture using roaming scenario in APgroup using different Aps	To capture the Packet by using different AP in APgroup and check if the client roams between different Aps	Passed	
WLJ8102S_Assurance_31	Packet capture for Any connect client using Intelligent Capture option in AP page	To verify the packet capture for Any connect client using Intelligent capture in AP page	Passed	
WLJ8102S_Assurance_32	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	
WLJ8102S_Assurance_33	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	
WLJ8102S_Assurance_34	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	
WLJ8102S_Assurance_35	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	
WLJ8102S_Assurance_36	Packet capture for Windows client using Intelligent Capture option in APgroup	To verify the packet capture for Windows client using Intelligent capture in APgroup	Passed	

WLJ8102S_Assurance_37	Packet capture for IOS client using Intelligent Capture option in APgroup	To verify the packet capture for IOS client using Intelligent capture in APgroup	Passed	
WLJ8102S_Assurance_38	Packet capture for Mac OS client using Intelligent Capture option in APgroup	To verify the packet capture for Mac OS client using Intelligent capture in APgroup	Passed	
WLJ8102S_Assurance_39	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	

Browser Rendering Coverage

Logical ID	Title	Description	Status	Defect ID
WLJ8102S_Rendering_1	Capture the Console logs in Network Summary page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_2	Capture the Console logs in Access Points under Network Summary page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_3	Capture the Console logs in Clients under Network Summary page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_4	Capture the Console logs in Access Points under Rogues page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_5	Capture the Console logs in Clients under Rogues page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_6	Capture the Console logs in Interferers page	To verify console logs are captured or not	Passed	

WLJ8102S_Rendering_7	Capture the Console logs in Wireless Dashboard page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_8	Capture the Console logs in Client Performance page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_9	Capture the Console logs in AP Performance page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_10	Capture the Console logs in Best Practices page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_11	Capture the Console logs in Summary under Monitor page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_12	Capture the Console logs in Access Points under Monitor page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_13	Capture the Console logs in Cisco CleanAir under Monitor page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_14	Capture the Console logs in Statistics under Monitor page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_15	Capture the Console logs in CDP under Monitor page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_16	Capture the Console logs in Rogues under Monitor page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_17	Capture the Console logs in Clients under Monitor page	To verify console logs are captured or not	Passed	

WLJ8102S_Rendering_18	Capture the Console logs in Sleeping Clients under Monitor page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_19	Capture the Console logs in Multicast under Monitor page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_20	Capture the Console logs in Applications under Monitor page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_21	Capture the Console logs in Lync under Monitor page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_22	Capture the Console logs in Local Profiling under Monitor page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_23	Capture the Console logs in Cloud Services under Monitor page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_24	Capture the Console logs in WLANs under WLANs page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_25	Capture the Console logs in Edit WLANs under WLANs page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_26	Capture the Console logs in Advanced-> AP Groups under WLANs page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_27	Capture the Console logs in Advanced-> Edit AP Groups under WLANs page	To verify console logs are captured or not	Passed	

WLJ8102S_Rendering_28	Capture the Console logs in General under CONTROLLER page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_29	Capture the Console logs in Icons under CONTROLLER page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_30	Capture the Console logs in Inventory under CONTROLLER page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_31	Capture the Console logs in Interfaces under CONTROLLER page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_32	Capture the Console logs in Interface Groups under CONTROLLER page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_33	Capture the Console logs in Multicast under CONTROLLER page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_34	Capture the Console logs in Network Routes under CONTROLLER page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_35	Capture the Console logs in Fabric Configuration under CONTROLLER page	To verify console logs are captured or not	Passed	

WLJ8102S_Rendering_36	Capture the Console logs in Redundancy under CONTROLLER page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_37	Capture the Console logs in Mobility Management under CONTROLLER page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_38	Capture the Console logs in Ports under CONTROLLER page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_39	Capture the Console logs in NTP under CONTROLLER page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_40	Capture the Console logs in CDP under CONTROLLER page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_41	Capture the Console logs in PMIPv6 under CONTROLLER page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_42	Capture the Console logs in Tunnelling under CONTROLLER page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_43	Capture the Console logs in IPv6 under CONTROLLER page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_44	Capture the Console logs in WLANs under CONTROLLER page	To verify console logs are captured or not	Passed	

WLJ8102S_Rendering_45	Capture the Console logs in Lawful Interception under CONTROLLER page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_46	Capture the Console logs in Advanced under CONTROLLER page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_47	Capture the Console logs in Access Points under WIRELESS page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_48	Capture the Console logs in Edit Access Points under WIRELESS page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_49	Capture the Console logs in Advanced under WIRELESS page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_50	Capture the Console logs in Mesh under WIRELESS page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_51	Capture the Console logs in AP Group NTP under WIRELESS page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_52	Capture the Console logs in ATF under WIRELESS page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_53	Capture the Console logs in RF Profiles under WIRELESS page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_54	Capture the Console logs in Flex Connect Groups under WIRELESS page	To verify console logs are captured or not	Passed	

WLJ8102S_Rendering_55	Capture the Console logs in Edit RF Profiles under WIRELESS page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_56	Capture the Console logs in Edit Flex Connect Groups under WIRELESS page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_57	Capture the Console logs in Flex Connect ACLs under WIRELESS page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_58	Capture the Console logs in Flex Connect VLAN Templates under WIRELESS page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_59	Capture the Console logs in Network Lists under WIRELESS page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_60	Capture the Console logs in 802.11a/n/ac/ax under WIRELESS page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_61	Capture the Console logs in 802.11b/g/n/ax under WIRELESS page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_62	Capture the Console logs in Media Stream under WIRELESS page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_63	Capture the Console logs in Application Visibility And Control under WIRELESS page	To verify console logs are captured or not	Failed	CSCvr29632

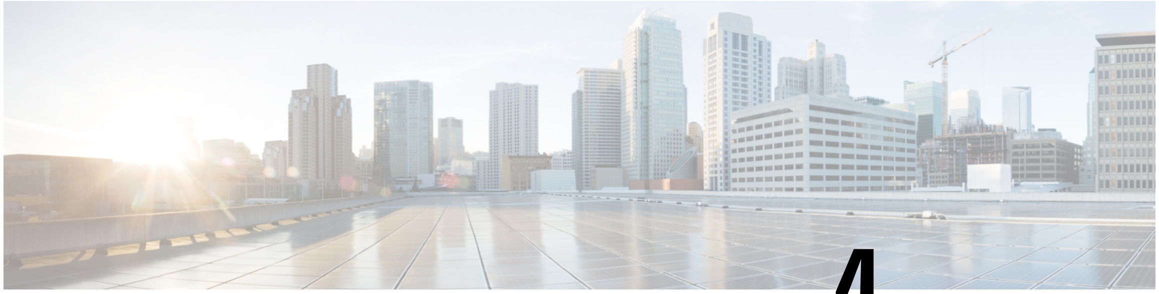
WLJ8102S_Rendering_64	Capture the Console logs in Lync Server under WIRELESS page	To verify console logs are captured or not	Failed	CSCvr29632
WLJ8102S_Rendering_65	Capture the Console logs in Country under WIRELESS page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_66	Capture the Console logs in Timers under WIRELESS page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_67	Capture the Console logs in Net flow under WIRELESS page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_68	Capture the Console logs in QoS under WIRELESS page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_69	Capture the Console logs in AAA under SECURITY page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_70	Capture the Console logs in Local EAP under SECURITY page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_71	Capture the Console logs in Advanced EAP under SECURITY page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_72	Capture the Console logs in Priority Order under SECURITY page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_73	Capture the Console logs in Certificate under SECURITY page	To verify console logs are captured or not	Passed	

WLJ8102S_Rendering_74	Capture the Console logs in Access Control Lists under SECURITY page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_75	Capture the Console logs in Wireless Protection Policies under SECURITY page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_76	Capture the Console logs in Web Auth under SECURITY page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_77	Capture the Console logs in TrustSec under SECURITY page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_78	Capture the Console logs in Local Policies under SECURITY page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_79	Capture the Console logs in Umbrella under SECURITY page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_80	Capture the Console logs in Summary under MANAGEMENT page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_81	Capture the Console logs in SNMP under MANAGEMENT page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_82	Capture the Console logs in HTTP-HTTPS under MANAGEMENT page	To verify console logs are captured or not	Passed	

WLJ8102S_Rendering_83	Capture the Console logs in IPSEC under MANAGEMENT page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_84	Capture the Console logs in Telnet-SSH under MANAGEMENT page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_85	Capture the Console logs in Serial Port under MANAGEMENT page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_86	Capture the Console logs in Local Management Users under MANAGEMENT page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_87	Capture the Console logs in User Sessions under MANAGEMENT page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_88	Capture the Console logs in Logs under MANAGEMENT page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_89	Capture the Console logs in Mgmt Via Wireless under MANAGEMENT page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_90	Capture the Console logs in Cloud Services under MANAGEMENT page	To verify console logs are captured or not	Passed	

WLJ8102S_Rendering_91	Capture the Console logs in Software Activation under MANAGEMENT page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_92	Capture the Console logs in Tech Support under MANAGEMENT page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_93	Capture the Console logs in Download File under COMMANDS page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_94	Capture the Console logs in Upload File under COMMANDS page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_95	Capture the Console logs in Reboot under COMMANDS page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_96	Capture the Console logs in Restart under COMMANDS page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_97	Capture the Console logs in Config Boot under COMMANDS page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_98	Capture the Console logs in Scheduled Reboot under COMMANDS page	To verify console logs are captured or not	Passed	

WLJ8102S_Rendering_99	Capture the Console logs in Reset to Factory Default under COMMANDS page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_100	Capture the Console logs in Set Time under COMMANDS page	To verify console logs are captured or not	Passed	
WLJ8102S_Rendering_101	Capture the Console logs in Login Banner under COMMANDS page	To verify console logs are captured or not	Passed	



CHAPTER 4

Regression Features - Test Summary

IOS-XE

Assurance - Sensor Test Configuration

Logical ID	Title	Description	Status	Defect ID
WLJ1612S_Reg_12	Adding the eWLC in DNAC	Provisioning the controller in DNAC	Passed	
WLJ1612S_Reg_13	Performing Network Test in Sensor - Driven Test	Verifying the IP Addressing, DNS, Host Reachability & RADIUS Tests in Sensor - Driven Test	Passed	
WLJ1612S_Reg_14	Capturing the Network Test from Wireless Sensor Dashboard	Mentoring the IP Addressing, DNS, Host Reachability & RADIUS Tests in Wireless Sensor Dashboard	Passed	
WLJ1612S_Reg_15	Performing Performance Test in Sensor - Driven Test	Verifying the Speed Test & ISPLA Test in Sensor - Driven Test	Passed	
WLJ1612S_Reg_16	Capturing the Performance Test from Wireless Sensor Dashboard	Monitoring the Speed Test & ISPLA Test in Wireless Sensor Dashboard	Passed	

WLJ1612S_Reg_17	Performing Application Test in Sensor - Driven Test	Verifying the Email Test, Web Test & File Transfer Test in Sensor - Driven Test	Passed	
WLJ1612S_Reg_18	Capturing the Application Test from Wireless Sensor Dashboard	Monitoring the Email Test, Web Test & File Transfer Test in Wireless Sensor Dashboard	Passed	
WLJ1612S_Reg_19	Performing Scheduling Onboarding Packet Capture Test	Checking whether the Scheduling Onboarding Packet capture is done as per the schedule or not	Passed	
WLJ1612S_Reg_20	Capturing Configured APs using Auto-Capture Settings	Testing whether the user able to capture or not the Configured APs using Auto-Capture Settings	Passed	

Assurance - Sensor Client On-Boarding Failures & Times – WebAuth

Logical ID	Title	Description	Status	Defect ID
WLJ1612S_Reg_01	Adding the controller in DNAC	Provisioning the controller in DNAC	Passed	
WLJ1612S_Reg_02	Upgrading eWLC from DNAC	Verifying whether the user is able to upgrade the controller or not from DNAC	Passed	
WLJ1612S_Reg_03	Checking the Performance of APs in DNAC	Verifying whether the Performance of APs are monitored correctly as per in the controller or not in DNAC	Passed	
WLJ1612S_Reg_04	Verifying how many wireless devices are added in DNAC	Checking whether how many wireless devices are added in DNAC and they are monitored properly or not	Passed	

WLJ1612S_Reg_05	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	
WLJ1612S_Reg_06	Checking the Client connectivity status in DNAC	Verifying whether the Client status are monitored correctly as per in the controller or not in DNAC	Passed	
WLJ1612S_Reg_07	Checking the Client Onboarding Times in DNAC	Verifying whether the Client Onboarding Times are monitored correctly as per in the controller or not in DNAC	Passed	
WLJ1612S_Reg_08	Checking the Client Count per SSID in DNAC	Verifying whether the Client Count per SSID are monitored correctly as per in the controller or not in DNAC	Passed	
WLJ1612S_Reg_09	Checking the Client Count per Band in DNAC	Verifying whether the Client Count per Band are monitored correctly as per in the controller or not in DNAC	Passed	
WLJ1612S_Reg_10	Checking the Client RSSI & SNR values in DNAC	Verifying whether the RSSI & SNR are monitored correctly as per in the controller or not in DNAC	Passed	
WLJ1612S_Reg_11	Checking the throughput & Packet loss details for the wireless devices	Verifying the Usage of Bytes, Average throughput & Packet loss details for the wireless devices	Passed	

N + 1 Rolling AP Upgrade for full Controller Image Upgrade

Logical ID	Title	Description	Status	Defect ID

WLJ1612S_Reg_53	Upgrade the eWLC image from eWLC rolling AP upgrade using Device.	To check whether the eWLC is upgraded using Device from eWLC	Passed	
WLJ1612S_Reg_54	Upgrade the eWLC image from eWLC rolling AP upgrade using FTP.	To check whether the eWLC is upgraded using FTP from eWLC	Passed	
WLJ1612S_Reg_55	Upgrade the eWLC image from eWLC rolling AP upgrade using TFTP.	To check whether the eWLC is upgraded using TFTP from eWLC	Passed	
WLJ1612S_Reg_56	Upgrade the eWLC image from eWLC rolling AP upgrade using SFTP.	To check whether the eWLC is upgraded using SFTP from eWLC	Passed	
WLJ1612S_Reg_57	Upgrade the wrong file name into the eWLC	To verify whether the error message will display when trying to upgrade wrong file into the eWLC.	Passed	
WLJ1612S_Reg_58	Upgrading the software image in a eWLC	To check whether the software image is upgraded in Primary eWLC	Passed	
WLJ1612S_Reg_59	Upgrading the software image into a group of AP	To check whether the software image is upgraded in group of AP	Passed	
WLJ1612S_Reg_60	Upgrading the software image into existing group of AP	To check whether the software image is upgraded into existing group of AP	Passed	
WLJ1612S_Reg_61	Reboot trigger to eWLC from PI after upgrade the software image in eWLC	To check whether WLC is reloaded when triggering from PI after upgrade the software image in controller.	Passed	
WLJ1612S_Reg_62	Moving AP's back to primary eWLC from PI.	To verify whether the AP's are move back into primary eWLC	Passed	

WLJ1612S_Reg_63	Adding the AP in AP upgrade group	To verify whether the AP added into AP upgrade group	Passed	
EWLCJ1612S_Reg_523	Upgrade the eWLC image from eWLC rolling AP upgrade using Device.	To check whether the eWLC is upgraded using Device from eWLC	Passed	
EWLCJ1612S_Reg_524	Upgrade the eWLC image from eWLC rolling AP upgrade using FTP.	To check whether the eWLC is upgraded using FTP from eWLC	Passed	
EWLCJ1612S_Reg_525	Upgrade the eWLC image from eWLC rolling AP upgrade using TFTP.	To check whether the eWLC is upgraded using TFTP from eWLC	Passed	
EWLCJ1612S_Reg_526	Upgrade the eWLC image from eWLC rolling AP upgrade using SFTP.	To check whether the eWLC is upgraded using SFTP from eWLC	Passed	
EWLCJ1612S_Reg_527	Upgrade the wrong file name into the eWLC	To verify whether the error message will display when trying to upgrade wrong file into the eWLC.	Passed	
EWLCJ1612S_Reg_528	Upgrading the software image in a eWLC	To check whether the software image is upgraded in Primary eWLC	Passed	
EWLCJ1612S_Reg_529	Upgrading the software image into a group of AP	To check whether the software image is upgraded in group of AP	Passed	
EWLCJ1612S_Reg_530	Upgrading the software image into existing group of AP	To check whether the software image is upgraded into existing group of AP	Passed	
EWLCJ1612S_Reg_531	Reboot trigger to eWLC from PI after upgrade the software image in eWLC	To check whether WLC is reloaded when triggering from PI after upgrade the software image in controller.	Passed	

EWLCJ1612S_Reg_532	Moving AP's back to primary eWLC from PI.	To verify whether the AP's are move back into primary eWLC	Passed	
EWLCJ1612S_Reg_533	Adding the AP in AP upgrade group	To verify whether the AP added into AP upgrade group	Passed	

Static Anchor WGB

Logical ID	Title	Description	Status	Defect ID
WLJ1612S_Reg_387	Configuring the LWAPP AP to autonomous AP	To change the LWAPP AP to autonomous A{ and check if the AP is converted	Passed	
WLJ1612S_Reg_388	Configuring the Autonomous AP as the WGB	To configure the autonomous AP as WGB and check if the AP changes as WGB.	Passed	
WLJ1612S_Reg_389	Configuring WGB in eWLC	To verify WGB configuration is successful or not in eWLC	Passed	
WLJ1612S_Reg_390	Associating the WGB on open authentication with IOS bridge AP	To associate the WGB on open authentication with IOS bridge and check if the WGB associates with the open WLAN or not.	Passed	
WLJ1612S_Reg_391	Associating the WGB on WPA 2 with PSK with IOS bridge AP	To associate the WGB on WPA 2 PSK security with IOS bridge AP and check if the WGB associates with the WLAN or not.	Passed	

WLJ1612S_Reg_392	Associating the WGB on WPA 2 with 802.1x with IOS bridge 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	
WLJ1612S_Reg_393	Associating the WGB on open authentication with COS fkex+bridge AP	To associate the WGB on open authentication with COS flex+bridge AP and check if the WGB associates with the open WLAN or not.	Passed	
WLJ1612S_Reg_394	Associating the WGB on WPA 2 with PSK with COS flex+bridge AP	To associate the WGB on WPA 2 PSK security with COS flex+bridge AP and check if the WGB associates with the WLAN or not.	Passed	
WLJ1612S_Reg_395	Associating the WGB on WPA 2 with 802.1x with COS flex+bridge AP	To associate the WGB on WPA 2 802.1x security with COS flex+bridge AP and check if the WGB associates with the WLAN or not.	Passed	
WLJ1612S_Reg_396	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	
WLJ1612S_Reg_397	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	

WLJ1612S_Reg_398	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	
WLJ1612S_Reg_399	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	
WLJ1612S_Reg_400	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	
WLJ1612S_Reg_401	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	
WLJ1612S_Reg_402	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	
WLJ1612S_Reg_403	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	
WLJ1612S_Reg_404	Associating the WGB on open security with local authentication	To check WGB client association with OPEN security and local authentication	Passed	
WLJ1612S_Reg_405	Checking Reassociation happens for WGB clients after session timeout	To verify reassociation for WGB clients after session timeout	Passed	

WLJ1612S_Reg_406	Performing local switching for WGB clients with IOS AP	To verify local switching traffic for client with IOS AP	Passed	

Lobby Ambassador

Logical ID	Title	Description	Status	Defect ID
WLJ1612S_Reg_94	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	
WLJ1612S_Reg_95	Create 3 lobby users and try to login GUI with all 3 lobby users with different brewers.	To verify the user able to login GUI with the all 3 lobby user credentials with different brewers.	Passed	
WLJ1612S_Reg_96	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	
WLJ1612S_Reg_97	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	
WLJ1612S_Reg_98	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	
WLJ1612S_Reg_99	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	
WLJ1612S_Reg_100	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	
WLJ1612S_Reg_101	Create and verify the lobby user in CLI	To verify the User able to login with Lobby credentials	Passed	

EWLCJ1612S_Reg_599	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	
EWLCJ1612S_Reg_600	Create 3 lobby users and try to login GUI with all 3 lobby users with different browers.	To verify the user able to login GUI with the all 3 lobby user credentials with different browers.	Passed	
EWLCJ1612S_Reg_601	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	
EWLCJ1612S_Reg_602	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	
EWLCJ1612S_Reg_603	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	
EWLCJ1612S_Reg_604	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	
EWLCJ1612S_Reg_605	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	
EWLCJ1612S_Reg_606	Create and verify the lobby user in CLI	To verify the User able to login with Lobby credentials	Passed	

Support for AP4800

Logical ID	Title	Description	Status	Defect ID

WLJ1612S_Reg_228	Association of 4800 AP with 3504/5520/8540 eWLC	To associate 4800 AP to eWLC with latest image and check if the AP gets associated or not	Passed	
WLJ1612S_Reg_229	Associating 4800 AP with different country code as with eWLC	To associate 4800 AP with different country code and check if the AP does not get joined to eWLC	Passed	
WLJ1612S_Reg_230	Configuring AP with duplicate IP	To configure AP with a duplicate IP address and check if the AP shows error message and AP does not join the eWLC	Passed	
WLJ1612S_Reg_231	Rebooting the 4800 AP	To check if the AP gets Rebooted or not and check if the AP joins the controller again.	Passed	
WLJ1612S_Reg_232	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	
WLJ1612S_Reg_233	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	
WLJ1612S_Reg_234	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	
WLJ1612S_Reg_235	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	

WLJ1612S_Reg_236	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	
WLJ1612S_Reg_237	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	
WLJ1612S_Reg_238	AP failover priority with critical	To check AP failover priority with critical and check if the AP gets connected to the next controller .	Passed	
WLJ1612S_Reg_239	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	
WLJ1612S_Reg_240	Moving AP from 3504 controller to 5520 through High availability	To check if the AP moves from 3504 eWLC to 5520 eWLC through high availability.	Passed	
WLJ1612S_Reg_241	Reassociation of client to the AP after reboot	To verify if the client gets reassociated to the to the AP .	Passed	
WLJ1612S_Reg_242	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	
WLJ1612S_Reg_243	Performing Intra controller roaming of Windows J OS client	To check whether intra controller roaming of windows clients works properly or not in eWLC	Passed	

WLJ1612S_Reg_244	Performing Intra controller roaming of Android client	To check whether intra controller roaming of Android clients works properly or not	Passed	
WLJ1612S_Reg_245	Performing Intra controller roaming of IOS client	To check whether intra controller roaming of IOS clients works properly or not in eWLC	Passed	
WLJ1612S_Reg_246	Performing Intra controller roaming of Mac OS client	To check whether intra controller roaming of MacOS clients works properly or not	Passed	
WLJ1612S_Reg_247	Performing Inter controller roaming of Windows J OS client	To check whether inter controller roaming of windows clients works properly or not	Passed	
WLJ1612S_Reg_248	Performing Inter controller roaming of Android client	To check whether inter controller roaming of Android clients works properly or not	Passed	
WLJ1612S_Reg_249	Performing Inter controller roaming of IOS client	To check whether inter controller roaming of IOS clients works properly or not	Passed	
WLJ1612S_Reg_250	Performing Inter controller roaming of Mac OS client	To check whether inter controller roaming of Mac OS clients works properly or not	Passed	
WLJ1612S_Reg_251	Change AP mode from local to FlexConnect in 4800 AP.	To change the mode of AP from local mode to FlexConnect mode and check if the AP does not reboot.	Passed	
WLJ1612S_Reg_252	Changing the AP from FlexConnect to Local mode and check if the AP reboot	To check if the AP reboots when AP mode is changed from FlexConnect to Local mode .	Passed	

WLJ1612S_Reg_253	Checking FlexConnect Local Switching and Local Auth works properly	To check if FlexConnect Local Switching and Local Auth works in 4800 AP and check if the clients gets locally authenticated and switched locally	Passed	
WLJ1612S_Reg_254	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	
WLJ1612S_Reg_255	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	
WLJ1612S_Reg_256	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	
WLJ1612S_Reg_257	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	

Intelligent Capture for 1850 AP

Logical ID	Title	Description	Status	Defect ID
WLJ1612S_IC_01	Configuring Intelligent Capture parameter details on 1800 AP	To configure Intelligent capture parameters in 1800 Aps	Passed	

WLJ1612S_IC_02	Check Configuration after the AP reboot	To Configure Intelligent capture parameters in different Aps 1800 and check if the configuration remains same after the AP reboot.	Passed	
WLJ1612S_IC_03	Packet capture of client when the client is connected to 1800 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	
WLJ1612S_IC_04	Packet capture of client when the client is connected to 1800 AP with 5 GHz	To capture the Packet of the client when the client is connected to AP with radio as 5 GHz	Passed	
WLJ1612S_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 1800 AP with security as OPEN	Passed	
WLJ1612S_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 1800 AP with security as WPA 2 PSK	Passed	
WLJ1612S_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 1800 AP with security as WPA 2 802.1x	Passed	
WLJ1612S_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 1800 AP with security as Static WEP	Passed	

WLJ1612S_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	
WLJ1612S_IC_10	Verify 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	
WLJ1612S_IC_11	Verify 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	
WLJ1612S_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	
WLJ1612S_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	
WLJ1612S_IC_14	Capturing Packet of Windows client when the client connected to 1800 AP	To capture packet when the Window client is connected to the 1800 AP	Passed	
WLJ1612S_IC_15	Capturing Packet of Android client when the client connected to 1800 AP	To capture packet when the Android client is connected to the 1800 AP	Passed	

WLJ1612S_IC_16	Capturing Packet of Mac OS client when the client connected to 1800 AP	To capture packet when the Mac OS client is connected to the 1800 AP	Passed	
WLJ1612S_IC_17	Capturing Packet of IOS client when the client connected to 1800 AP	To capture packet when the IOS client is connected to the 1800 AP	Passed	

802.1x on Wave 2 AP (EAP -TLS, EAP-PEAP)

Logical ID	Title	Description	Status	Defect ID
WLJ1612S_Reg_433	Enabling dot1x auth for AP and joining AP to eWLC	To check whether AP joins eWLC or not after dot1x authentication from Switch/ISE	Passed	
WLJ1612S_Reg_434	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	
WLJ1612S_Reg_435	Joining COS AP to eWLC through Dot1x+PEAP authentication	To check whether COS AP joins eWLC or not after dot1x authentication from Switch/ISE via EAP method PEAP	Passed	
WLJ1612S_Reg_436	Joining iOS AP to eWLC through Dot1x+EAP TLS authentication	To check whether iOS AP joins eWLC or not after dot1x authentication from Switch/ISE via EAP method TLS	Passed	
WLJ1612S_Reg_437	Trying to join AP's through Dot1x authentication with LSC provisioning	To check whether AP's joins eWLC or not through LSC provisioning & dot1x authentication	Passed	

WLJ1612S_Reg_438	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	
WLJ1612S_Reg_439	Disabling dot1x support in Switch and trying to associate AP via Dot1x authentication to eWLC	To check whether AP joins eWLC or not even dot1x is disabled in switch	Passed	
WLJ1612S_Reg_440	Enabling dot1x auth for AP in 3850 Switch	Configuring the 3850 Switch for Dot1x authentication by mapping the identity profiles to a port.	Passed	
WLJ1612S_Reg_441	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 eWLC UI via TFTP	Passed	
WLJ1612S_Reg_442	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	
WLJ1612S_Reg_443	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	
WLJ1612S_Reg_444	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	

Passpoint R2 Flex Mode

Logical ID	Title	Description	Status	Defect ID
WLJ1612S_Reg_120	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	Failed	CSCvp90962
WLJ1612S_Reg_121	Enabling the Internet Access WLAN and connecting client	To verify whether Internet Access mode is enabled or not	Passed	
WLJ1612S_Reg_122	Configuring the Network type from one to another	To verify whether client connecting or not with network type changes from one to other	Passed	
WLJ1612S_Reg_123	Configuring the Network Authentication	To verify whether Client is connecting after Network Authentication or not	Passed	
WLJ1612S_Reg_124	Checking with IPv4 type details	To verify whether Client connecting or not after IPv4 type changes from one to another	Passed	
WLJ1612S_Reg_125	Creating OUI with Duplicate name	To verify whether OUI is creating with duplicate name or not	Passed	
WLJ1612S_Reg_126	Configuring the NAI-realm and EAP-methods.	To verify whether client will connect with NAI-realm credentials or not	Passed	
WLJ1612S_Reg_127	Adding cellular network information with duplicate name	To verify whether Cellular network information added successfully	Passed	
WLJ1612S_Reg_128	Configuring the OSU SSID	To verify whether OSU SSID applying or not	Passed	

WLJ1612S_Reg_129	Configuring the OSU Provider information	To verify whether OSU Provider information applying or not	Passed	
WLJ1612S_Reg_130	Configure the WAN metrics.	To verify whether WAN statues is varying or not	Passed	
WLJ1612S_Reg_131	Varying Port configurations	To verify whether Port configurations can vary after client connect	Passed	
WLJ1612S_Reg_132	Downgrading the AP after Hotspot configurations	To verify whether Client connected or not after downgrade with Hotspot	Passed	
WLJ1612S_Reg_133	Upgrading the AP after Hotspot configurations	To verify whether all hotspot details are showing properly or not	Passed	
WLJ1612S_Reg_134	Changing the AP modes after Client connect to Hotspot	To verify whether client will connect or not after modes changes in AP	Passed	
WLJ1612S_Reg_135	Configure the Venue name and URL.	To verify whether venue name or URL applying or not.	Passed	
WLJ1612S_Reg_136	Configure the Domain name.	To verify whether Domain name applying or not.	Passed	
WLJ1612S_Reg_137	Checking the Roaming after roaming-oi configurations	To verify whether client will roam between hotspots or not	Passed	
WLJ1612S_Reg_138	Configure the Operating class	To verify whether operating class configured or not.	Passed	
EWLCJ1612S_Reg_547	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	

EWLCJ1612S_Reg_548	Enabling the Internet Access WLAN and connecting client	To verify whether Internet Access mode is enabled or not	Passed	
EWLCJ1612S_Reg_549	Configuring the Network type from one to another	To verify whether client connecting or not with network type changes from one to other	Passed	
EWLCJ1612S_Reg_550	Configuring the Network Authentication	To verify whether Client is connecting after Network Authentication or not	Passed	
EWLCJ1612S_Reg_551	Checking with IPv4 type details	To verify whether Client connecting or not after IPv4 type changes from one to another	Passed	
EWLCJ1612S_Reg_552	Creating OUI with Duplicatate name	To verify whether OUI is creating with duplicate name or not	Passed	
EWLCJ1612S_Reg_553	Configuring the NAI-relam and Eap-methods.	To verify whether client willl connect with NAI-relam credentials or not	Passed	
EWLCJ1612S_Reg_554	Adding cellular network information with duplicate name	To verify whether Cellular network information added successfully	Passed	
EWLCJ1612S_Reg_555	Configuring the OSU SSID	To verify whether OSU SSID applying or not	Passed	
EWLCJ1612S_Reg_556	Configuring the OSU Provider information	To verify whether OSU Provider information applying or not	Passed	
EWLCJ1612S_Reg_557	Configure the WAN metrics.	To verify whether WAN satues is varying or not	Passed	
EWLCJ1612S_Reg_558	Varying Port configurations	To verify whether Port configurations can vary after client connect	Passed	

EWLCJ1612S_Reg_559	Downgrading the AP after Hotspot configurations	To verfiy whetherClient connected or not after downgrade with Hotspot	Passed	
EWLCJ1612S_Reg_560	Upgrading the AP after Hotspot configurations	To verify whether all hotspot details are showing properly or not	Passed	
EWLCJ1612S_Reg_561	Changing the AP modes after Client connect to Hotspot	To verify whether client will connect or not afyter modes changes in AP	Passed	
EWLCJ1612S_Reg_562	Configure the Venue name and URL.	To verify whether venue name or Url applying or not.	Passed	
EWLCJ1612S_Reg_563	Configure the Domain name.	To verify whether Domain name applying or not.	Passed	
EWLCJ1612S_Reg_564	Checking the Roaming after roaming-oi configurations	To verify whether client will roam between hotspots or not	Passed	
EWLCJ1612S_Reg_565	Configure the Operating class	To verify whether operating class configured or not.	Passed	

eWLC Config

Logical ID	Title	Description	Detail:Procedure	Detail:Pass/Fail Criteria
WLJ1612S_config_02	Rogue AP rules after creating shows empty	To check whether the rogue AP rules after creating shows empty or not	Passed	
WLJ1612S_config_03	Check if Sensor mode support is there for 9115	To check whether the sensor mode is shown in 9115 AP	Passed	
WLJ1612S_config_04	Checking the regulatory domain for 1815AP after changed country code	To verify whether regulatory domain showing correct or nor after changed country code	Failed	CSCvq39044

WLJ1612S_config_05	Check the Configuration of WLAN with PMF-PSK security	To Verify the Configuration of WLAN with PMF-PSK security	Failed	CSCvq39055
WLJ1612S_config_06	Check the Configuration of OSEN with PSK security in CLI	To verify the Configurations of OSEN with PSK security in CLI.	Failed	CSCvr51021
WLJ1612S_config_07	Verify th Configuration of WLAN with Static WEP security	To Verify the configuration of WLAN with Static WEP security	Passed	
WLJ1612S_config_08	Check the Configurations of Policy Map-Local Policy	To verify the Configuration of Policy Map-Local Policy	Failed	CSCvp78775
WLJ1612S_config_09	Check the Configuration of WLAN with FT+PSK security	To verify the configurations of WLAN with FT+PSK security.	Passed	
WLJ1612S_config_11	Check the Configuration of WPA3 and OWE support in GUI	To check the Configuration of WPA3 and OWE support in GUI.	Passed	
WLJ1612SII_config_2	Bridge mode not reflecting when APC9115AXI-D mode changed from flex to Bridge in eWLC UI	To check whether Bridge mode is not reflecting while the changing APC9115AXI-D from flex to Bridge in eWLC UI	Failed	CSCvr14732
WLJ1612SII_config_4	Accounting Identity list name has no restriction in eWLC CLI	To check whether the accounting identity list name is accepting maximum 31 Characters or not	Failed	CSCvr31441

Passive Client ARP Unicast

Logical ID	Title	Description	Status	Defect ID
WLJ1612S_Reg_166	Passive Clients is sent to all AP’s as unicast packet	To verify whether ARP Unicast packets send to all AP's or not	Passed	

WLJ1612S_Reg_167	Enabling the Passive client data in 2500/5520/8510/8540 controllers	To verify whether Passive client or sending the Unicast data from AP to client or not	Passed	
WLJ1612S_Reg_168	Checking the ARP Packet with Multicast-multicast enable	To verify whether ARP packet is sending or not whether Multicast mode enabled	Passed	
WLJ1612S_Reg_169	Checking the ARP packet when Multicast-unicast enable	To verify whether Packed is sending or not whether Multicast-unicast enable	Passed	
WLJ1612S_Reg_170	Connecting with two WLAN with different client ARP	To verify whether WLAN will support with two different ARP methods in same Interface	Passed	
WLJ1612S_Reg_171	ARP unicast verification when AP's are in AP group	To verify whether ARP unicast enabling and accessing fine or not at the time of AP's are in same AP group	Passed	
WLJ1612S_Reg_172	Checking with ARP unicast behavior when feature is disabled and passive client is enabled	To verify whether Client accessing or not whenever we have disable the feature	Passed	
WLJ1612S_Reg_173	Testing with non-Cisco WGB with wired clients	To verify whether non-cisco WGB with wired clients will connect or not	Passed	
WLJ1612S_Reg_174	Rebooting the AP after Client ARP unicast enable	To verify whether WLAN showing the information correctly after reboot also	Passed	
WLJ1612S_Reg_175	Checking after Upgrade/Downgrade	To verify whether Client is connecting or not after Upgrade/Downgrade	Passed	

WLJ1612S_Reg_176	Debugging the ARP client data	To verify whether ARP details are showing properly or not	Passed	
WLJ1612S_Reg_177	Verifying Maximum packets per second	To verify whether the Maximum packets per second the AP will send	Passed	
EWLCJ1612S_Reg_468	Passive Clients is sent to all AP’s as unicast packet	To verify whether ARP Unicast packets send to all AP's or not	Passed	
EWLCJ1612S_Reg_469	Enabling the Passive client data in 2500/5520/8510/8540 controllers	To verify whether Passive client or sending the Unicast data from AP to client or not	Passed	
EWLCJ1612S_Reg_470	Cheking the ARP Packet with Multicast-multicast enable	To verify whether ARP packet is sending or not whether Multicast mode enabled	Passed	
EWLCJ1612S_Reg_471	Cheking the ARP packet when Multicast-unicast enable	To verify whether Packed is sending or not whether Multicast-unicast enable	Passed	
EWLCJ1612S_Reg_472	Connecting with two WLAN with different client ARP	To verify whether WLAN will support with two different ARP methods in same Interface	Passed	
EWLCJ1612S_Reg_473	ARP unicast verification when AP's are in AP group	To verify whether ARP unicast enabling and accessing fine or not at the time of AP's are in same AP group	Passed	
EWLCJ1612S_Reg_474	Checking with ARP unicast behavior when feature is disabled and passive client is enabled	To verify whether Client accessing or not whenever we have disable the feature	Passed	

EWLCJ1612S_Reg_475	Testing with non-Cisco WGB with wired clients	To verify whether non-cisco WGB with wired clients will connect or not	Passed	
EWLCJ1612S_Reg_476	Rebootinthe AP after Client ARP unicast enable	To verify whether WLAN showing the information correctly after reboot also	Passed	
EWLCJ1612S_Reg_477	Checking after Upgrade/Downgrade	To verify whether Client is connecting or not after Upgrade/Downgrade	Passed	
EWLCJ1612S_Reg_478	Debuging the ARPclient data	To verify whether ARP details are showing properly or not	Passed	
EWLCJ1612S_Reg_479	Veryfying Maximum packets per second	To verify whether the Maximum packets per second the AP will send	Passed	

Split Tunneling Support

Logical ID	Title	Description	Status	Defect ID
WLJ1612S_Reg_75	Verifying permit rule of split tunnel ACL with Windows client.	To check whether traffic is routing or not when Windows client is connected to ACL enabled WLAN	Passed	
WLJ1612S_Reg_76	Verifying deny rule of split tunnel ACL with Windows client.	To check whether traffic is blocked or not when Windows client is connected to ACL enabled WLAN	Passed	
WLJ1612S_Reg_77	Verifying permit rule of split tunnel ACL with MAC/iOS client.	To check whether traffic is routing or not when MAC/iOS client is connected to ACL enabled WLAN	Passed	
WLJ1612S_Reg_78	Verifying deny rule of split tunnel ACL with MAC/iOS client.	To check whether traffic is blocked or not when Windows client is connected to ACL enabled WLAN	Passed	

WLJ1612S_Reg_79	Verifying permit rule of split tunnel ACL with Android client.	To check whether traffic is routing or not when Android client is connected to ACL enabled WLAN	Passed	
WLJ1612S_Reg_80	Verifying deny rule of split tunnel ACL with Android client.	To check whether traffic is blocked or not when Android client is connected to ACL enabled WLAN	Passed	
WLJ1612S_Reg_81	Verifying permit rule of split tunnel ACL with Windows/ Android/ MAC/ iOS clients at AP level	To check whether traffic is routing or not when Windows/ Android/ MAC/ iOS clients are connected to ACL enabled WLAN	Passed	
WLJ1612S_Reg_82	Verifying deny rule of split tunnel ACL with Windows/Android/MAC/ iOS clients at AP level	To check whether traffic is blocked or not when Windows/Android/MAC/ iOS clients are connected to ACL enabled WLAN	Passed	
WLJ1612S_Reg_83	Verifying split tunnel ACL configuration at Flexgroup level through WLC UI	To verify whether split tunnel ACL are configured or not through WLC UI	Passed	
WLJ1612S_Reg_84	Verifying split tunnel ACL configuration at AP level through WLC UI	To verify whether local split tunnel ACL can be applied to AP level or not from WLC UI	Passed	
WLJ1612S_Reg_85	Verifying split tunnel ACL configuration through WLC CLI	To verify whether local split tunnel ACL are applied or not from WLC UI	Passed	
EWLCJ1612S_Reg_500	Verifying permit rule of split tunnel ACL with Windows client.	To check whether traffic is routing or not when Windows client is connected to ACL enabled WLAN	Passed	
EWLCJ1612S_Reg_501	Verifying deny rule of split tunnel ACL with Windows client.	To check whether traffic is blocked or not when Windows client is connected to ACL enabled WLAN	Passed	

EWLCJ1612S_Reg_502	Verifying permit rule of split tunnel ACL with MAC/iOS client.	To check whether traffic is routing or not when MAC/iOS client is connected to ACL enabled WLAN	Passed	
EWLCJ1612S_Reg_503	Verifying deny rule of split tunnel ACL with MAC/iOS client.	To check whether traffic is blocked or not when Windows client is connected to ACL enabled WLAN	Passed	
EWLCJ1612S_Reg_504	Verifying permit rule of split tunnel ACL with Android client.	To check whether traffic is routing or not when Android client is connected to ACL enabled WLAN	Passed	
EWLCJ1612S_Reg_505	Verifying deny rule of split tunnel ACL with Android client.	To check whether traffic is blocked or not when Android client is connected to ACL enabled WLAN	Passed	
EWLCJ1612S_Reg_506	Verifying permit rule of split tunnel ACL with Windows/Android/MAC/iOS clients at AP level	To check whether traffic is routing or not when Windows/Android/MAC/iOS clients are connected to ACL enabled WLAN	Passed	
EWLCJ1612S_Reg_507	Verifying deny rule of split tunnel ACL with Windows/Android/MAC/iOS clients at AP level	To check whether traffic is blocked or not when Windows/Android/MAC/iOS clients are connected to ACL enabled WLAN	Passed	
EWLCJ1612S_Reg_508	Verifying split tunnel ACL configuration at flexgroup level through WLC UI	To verify whether split tunnel ACL are configured or not through WLC UI	Passed	
EWLCJ1612S_Reg_509	Verifying split tunnel ACL configuration at AP level through WLC UI	To verify whether local split tunnel ACL can be applied to AP level or not from WLC UI	Passed	
EWLCJ1612S_Reg_510	Verifying split tunnel ACL configuration through WLC CLI	To verify whether local split tunnel ACL are applied or not from WLC UI	Passed	

MAB Bypass Support

Logical ID	Title	Description	Status	Defect ID
WLJ1612S_Reg_319	Associating different OS client with MAB	Check whether different OS client is able connect or not with MAB	Passed	
WLJ1612S_Reg_320	Verifying the MAC filtering enabled status through CLI	To check whether MAC Filtering enabled details showing properly or not on CLI	Passed	
WLJ1612S_Reg_321	Client reassociate with macfiltering enabled through external radius server.	Verifying the client is reassociated or not with macfilter enabled through external RADIUS server	Passed	
WLJ1612S_Reg_322	Verifying JSSID client reassociation with MAC filtering enabled on WLAN with external radius server.	Verifying the JSSID client is reassociated or not with MAC filter enabled through external RADIUS server	Passed	
WLJ1612S_Reg_323	Configuring specific mac address allowed on WLAN by using AAA-attribute list.	Verifying the specific mac address allowed on WLAN by using AAA-attribute list	Passed	
WLJ1612S_Reg_324	Configure a named authorization list via AAA config on WLAN.	Verifying the named authorization list is configured, the authorization list is mapped on WLAN and client is join/disconnect/rejoin.	Passed	
WLJ1612S_Reg_325	Verifying the JSSID client maximum retries failed	To check whether JSSID client is moved/excluded or not after maximum retries failed	Passed	
WLJ1612S_Reg_326	Verifying client is reauthenticated or not after session timeout	Checking after session timeout client is reauthenticated or not	Passed	

WLJ1612S_Reg_327	Checking the JSSID client is reauthenticated or not after session expired	To check whether JSSID client is reauthenticated or not after client session expired	Passed	
WLJ1612S_Reg_328	Verifying the JSSID client status on monitor page	Checking the JSSID client details on monitor page	Passed	
EWLCJ1612S_Reg_581	Associating different OS client with MAB	Check whether different os client is able connect or not with MAB	Passed	
EWLCJ1612S_Reg_582	Verifying the MAC filtering enabled status through CLI	To check whether MAC Filtering enabled details showing properly or not on CLI	Passed	
EWLCJ1612S_Reg_583	Client reassociate with mac filtering enabled through external radius server.	Verifying the client is reassociated or not with with MAC filter enabled through external RADIUS server	Passed	
EWLCJ1612S_Reg_584	Verifying JSSID client reassociation with MAC filtering enabled on WLAN with external radius server.	Verifying the JSSID client is reassociated or not with with MAC filter enabled through external RADIUS server	Passed	
EWLCJ1612S_Reg_585	Configuring specifc mac address allowed on wlan by using AAA-attribute list.	Verifying the specific mac address allowed on wlan by using AAA-attribute list	Passed	
EWLCJ1612S_Reg_586	Configure a named authorization list via aaa config on wlan.	Verifying the named authorization list is configured, the authorization list is mapped on wlan and client is join/disconnect/rejoin.	Passed	
EWLCJ1612S_Reg_587	Verifying the JSSID client maximum retries failed	To check whether JSSID client is moved/excluded or not after maximum retries failed	Passed	

EWLCJ1612S_Reg_588	Verifying client is reauthenticated or not after session timeout	Checking after session timeout client is reauthenticated or not	Passed	
EWLCJ1612S_Reg_589	Checking the JSSID client is reauthenticated or not after session expired	To check whether JSSID client is reauthenticated or not after client session expired	Passed	
EWLCJ1612S_Reg_590	Verifying the JSSID client status on monitor page	Checking the JSSID client details on monitor page	Passed	

Selective Re-anchor

Logical ID	Title	Description	Status	Defect ID
WLJ1612S_Reg_381	Checking the Windows Client connectivity after enabling Selective reanchor in WLAN	To verify whether windows jOS client is connecting properly or not	Passed	
WLJ1612S_Reg_382	Checking the android Client connectivity after enabling Selective reanchor in WLAN	To verify whether android client is connecting properly or not	Passed	
WLJ1612S_Reg_383	Checking the IOS Client connectivity after enabling Selective reanchor in WLAN	To verify whether IOS client is connecting properly or not	Passed	
WLJ1612S_Reg_384	Roaming the client between 2 controllers	To verify whether client roaming successfully between two controllers	Passed	
WLJ1612S_Reg_385	Reboot the Controller after Re-anchor enabling	To verify whether Configurations are showing same or different after controller reboot	Passed	

WLJ1612S_Reg_386	Downgrade/upgrade the controller with Re-anchor enable	To verify whether Downgrade/upgrade the controller with Re-anchor enable	Passed	
EWLCJ1612S_Reg_517	Checking the Windows Client connectivity after enabling Selective reanchor in WLAN	To verify whether windows jos client is connecting properly or not	Passed	
EWLCJ1612S_Reg_518	Checking the android Client connectivity after enabling Selective reanchor in WLAN	To verify whether android client is connecting properly or not	Passed	
EWLCJ1612S_Reg_519	Checking the IOS Client connectivity after enabling Selective reanchor in WLAN	To verify whether IOS client is connecting properly or not	Passed	
EWLCJ1612S_Reg_520	Roaming the client between 2 controllers	To verify whether client roaming successfully between two controllers	Passed	
EWLCJ1612S_Reg_521	Reboot the Controller after Re-anchor enabling	To verify whether Configurations are showing same or different after controller reboot	Passed	
EWLCJ1612S_Reg_522	Downgrade/upgrade the controller with Re-anchor enable	To verify whether Downgrade/upgrade the controller with Re-anchor enable	Passed	

WGB Support for COS AP

Logical ID	Title	Description	Status	Defect ID
WLJ1612S_Reg_423	Associating the WGB on open authentication with AP on local mode	To associate the WGB on open authentication when AP in local mode and check if the WGB associates with the open WLAN or not.	Passed	

WLJ1612S_Reg_424	Associating the WGB on WPA 2 with PSK with AP on local mode	To associate the WGB on WPA 2 PSK security when AP in local mode and check if the WGB associates with the WLAN or not.	Passed	
WLJ1612S_Reg_425	Associating the WGB on WPA 2 with 802.1x with AP on local mode	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	
WLJ1612S_Reg_426	Associating the WGB on WPA 2 CCKM with AP on local mode	To associate the WGB on WPA 2 CCKM security when AP in local mode and check if the WGB associates with the WLAN or not.	Passed	
WLJ1612S_Reg_427	Associating the WGB on open authentication with AP on Flex mode	To associate the WGB on open authentication when AP in Flex mode and check if the WGB associates with the open WLAN or not.	Passed	
WLJ1612S_Reg_428	Associating the WGB on WPA 2 with PSK with AP on Flex mode	To associate the WGB on WPA 2 PSK security when AP in local mode and check if the WGB associates with the WLAN or not.	Passed	
WLJ1612S_Reg_429	Associating the WGB on WPA 2 with 802.1x with AP on Flex mode	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	

WLJ1612S_Reg_430	Associating the WGB on WPA 2 CCKM with AP on Flex mode	To associate the WGB on WPA 2 CCKM security when AP in local mode and check if the WGB associates with the WLAN or not.	Passed	
WLJ1612S_Reg_431	Checking of WGB roaming from one AP to another AP in local mode	To check the roaming of WGB from one AP to another AP when the AP is in local mode .	Passed	
WLJ1612S_Reg_432	Checking of WGB roaming from one AP to another AP in flex mode	To check the roaming of WGB from one AP to another AP when APs are in flex mode	Passed	
EWLCJ1612S_Reg_480	Configuring the lwapp ap to autonomous AP	To change the lwapp apto autonomous ap and check if the AP is converted	Passed	
EWLCJ1612S_Reg_481	Configuring the Autonomous AP as the WGB	To configure the autonomous AP as WGB and check if the AP changes as WGB.	Passed	
EWLCJ1612S_Reg_482	Configuring WGB in eWLC	To verify WGB configuration is successful or not in eWLC	Passed	
EWLCJ1612S_Reg_483	Associating the WGB on open authentication with IOS bridge AP	To associate the WGB on open authentication with IOS bridge and check if the WGB associates with the open WLAN or not.	Passed	
EWLCJ1612S_Reg_484	Associating the WGB on WPA 2 with PSK with IOS bridge AP	To associate the WGB on WPA 2 PSK security with IOS bridge AP and check if the WGB associates with the WLAN or not.	Passed	

EWLCJ1612S_Reg_485	Associating the WGB on WPA 2 with 802.1x with IOS bridge 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	
EWLCJ1612S_Reg_486	Associating the WGB on open authentication with COS fkex+bridge AP	To associate the WGB on open authentication with COS flex+bridge AP and check if the WGB associates with the open WLAN or not.	Passed	
EWLCJ1612S_Reg_487	Associating the WGB on WPA 2 with PSK with COS flex+bridge AP	To associate the WGB on WPA 2 PSK security with COS flex+bridge AP and check if the WGB associates with the WLAN or not.	Passed	
EWLCJ1612S_Reg_488	Associating the WGB on WPA 2 with 802.1x with COS flex+bridge AP	To associate the WGB on WPA 2 802.1x security with COS flex+bridge AP and check if the WGB associates with the WLAN or not.	Passed	
EWLCJ1612S_Reg_489	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	
EWLCJ1612S_Reg_490	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	

EWLCJ1612S_Reg_491	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	
EWLCJ1612S_Reg_492	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	
EWLCJ1612S_Reg_493	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	
EWLCJ1612S_Reg_494	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	
EWLCJ1612S_Reg_495	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	
EWLCJ1612S_Reg_496	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	
EWLCJ1612S_Reg_497	Associating the WGB on open security with local authentication	To check WGB client association with OPEN security and local authentication	Passed	
EWLCJ1612S_Reg_498	Checking Reassociation happens for WGB clients after session timeout	To verify reassociation for WGB clients afte session timeout	Passed	

EWLCJ1612S_Reg_499	Performing local switching for WGB clients with IOS AP	To verify local switching traffic for client with IOS AP	Passed	

Domain Based URL ACL

Logical ID	Title	Description	Status	Defect ID
WLJ1612S_Reg_178	Check if the Dummy Domain address is accepted in the URL ACL.	To Verify if the Invalid domain names are accepting or not	Passed	
WLJ1612S_Reg_179	Create new URL ACL , Add new URL on ACL on 5520 eWLC	To verify that new ACL created , rule added or not using UI	Passed	
WLJ1612S_Reg_180	Add new URL domain on created URL ACL	To verify that new URL domain (www.cisco.com / www.yahoo.com) added or not	Passed	
WLJ1612S_Reg_181	Configure URL ACL as blacklist on WLAN and connect one Window client , open URL that configured in ACL	To verify that URL is blocking that configured in URL-ACL profile and showing hit count in UI of WLC	Passed	
WLJ1612S_Reg_182	Configure URL ACL on interface using CLI and connect iOS client	To verify that URL ACL configured on interface or not and iOS client connectivity with URL blocked	Passed	
WLJ1612S_Reg_183	Delete URL ACL rule after applied	To verify that URL ACL rule delete successfully or not	Passed	
WLJ1612S_Reg_184	Modified rule of URL ACL and connect Android client	To verify that rule action modified or not and Android client connectivity	Passed	
WLJ1612S_Reg_185	Clear counter of URL ACL profile after open URL in client web browser	To verify that counter is clear or not of URL ACL profile	Passed	

WLJ1612S_Reg_186	Show URL ACL status on WLAN using CLI	To verify that URL ACL status showing configured on WLAN	Passed	

Location Analytics

Logical ID	Title	Description	Status	Defect ID
WLJ1612S_Reg_86	Adding access points to Floor map	To verify whether client devices are displayed in the floor map or not	Passed	
WLJ1612S_Reg_87	Checking windows Client Location is displaying in Floor map	To verify whether windows client devices are displayed in the floor map or not	Passed	
WLJ1612S_Reg_88	Checking Android Client Location is displaying in Floor map	To verify whether android client devices are displayed in the floor map or not	Passed	
WLJ1612S_Reg_89	Performing filter operation for connected client by MAC address/IP/SSID	To verify whether client device can be searched by specifying its MAC address/IP/SSID or not	Passed	
WLJ1612S_Reg_90	Interferers in Floor map	To verify whether interferers are displayed in the floor map or not	Passed	
WLJ1612S_Reg_91	Checking Rogue Devices are displaying in Floor map	To verify whether rogues are displayed in the floor map or not	Passed	
WLJ1612S_Reg_92	Client movement history playback	To verify whether client's movement history is shown or not	Passed	
WLJ1612S_Reg_93	Creating New Report for building and floor	To verify whether new report can be created or not	Passed	

EWLCJ1612S_Reg_591	Adding access points to Floor map	To verify whether client devices are displayed in the floor map or not	Passed	
EWLCJ1612S_Reg_592	Checking windows Client Location is displaying in Floor map	To verify whether windows client devices are displayed in the floor map or not	Passed	
EWLCJ1612S_Reg_593	Checking Android Client Location is displaying in Floor map	To verify whether android client devices are displayed in the floor map or not	Passed	
EWLCJ1612S_Reg_594	Performing filter operation for connected client by MAC address/IP/SSID	To verify whether client device can be searched by specifying its MAC address/IP/SSID or not	Passed	
EWLCJ1612S_Reg_595	Interferers in Floor map	To verify whether interferers are displayed in the floor map or not	Passed	
EWLCJ1612S_Reg_596	Checking Rogue Devices are displaying in Floor map	To verify whether rogues are displayed in the floor map or not	Passed	
EWLCJ1612S_Reg_597	Client movement history playback	To verify whether client's movement history is shown or not	Passed	
EWLCJ1612S_Reg_598	Creating New Report for building and floor	To verify whether new report can be created or not	Passed	

EoGRE Tunnel Priority / Fallback

Logical ID	Title	Description	Status	Defect ID

WLJ1612S_Reg_187	Associating Android clients to a local switching enabled WLAN with Tunnel profile mapped	To check whether Android clients gets associated or not to 2800/3800 AP's with local switching enabled WLAN with EoGRE tunnel mapped in it	Passed	
WLJ1612S_Reg_188	Associating IOS clients to a local switching enabled WLAN with Tunnel profile mapped	To check whether IOS clients gets associated or not to 2800/3800 AP's with local switching enabled WLAN with EoGRE tunnel mapped in it	Passed	
WLJ1612S_Reg_189	Associating Windows clients to a local switching enabled WLAN with Tunnel profile mapped	To check whether windows clients gets associated or not to 2800/3800 AP's with local switching enabled WLAN with EoGRE tunnel mapped in it	Passed	
WLJ1612S_Reg_190	Associating Apple MacBook clients to a local switching enabled WLAN with Tunnel profile mapped	To check whether Apple MacBook clients gets associated or not to 2800/3800 AP's with local switching enabled WLAN with EoGRE tunnel mapped in it	Passed	
WLJ1612S_Reg_191	Checking the tunnel gateway fallback works properly for Android clients	To check whether Android clients fallback to secondary tunnel or not when primary tunnel gateway goes down	Passed	
WLJ1612S_Reg_192	Checking the tunnel gateway fallback works properly for IOS clients	To check whether IOS clients fallback to secondary tunnel or not when primary tunnel gateway goes down	Passed	

WLJ1612S_Reg_193	Checking the tunnel gateway fallback works properly for Windows clients	To check whether Windows clients fallback to secondary tunnel or not when primary tunnel gateway goes down	Passed	
WLJ1612S_Reg_194	Checking the tunnel gateway fallback works properly for Apple MacBook clients	To check whether Apple MacBook clients fallback to secondary tunnel or not when primary tunnel gateway goes down	Passed	
WLJ1612S_Reg_195	Checking the tunnel configuration in HA eWLCs	To check whether config sync occurs or not for tunnel gateway/domain configuration between Active and Standby WLC's	Passed	
WLJ1612S_Reg_196	Creating a tunnel gateway with invalid ipv4 address	To check whether proper error message thrown or not while creating tunnel gateway with invalid ipv4 address	Passed	
WLJ1612S_Reg_197	Associating Client to a local switching enabled and dot1X security WLAN with Tunnel profile mapped in AP standalone mode	To check whether clients gets associated or not to 2800/3800 AP's with local switching enabled WLAN with EoGRE tunnel mapped in it in AP standalone mode	Passed	
WLJ1612S_Reg_198	Associating Client to a local switching enabled and open security WLAN with Tunnel profile mapped in AP standalone mode	To check whether clients gets associated or not to 2800/3800 AP's with local switching enabled WLAN with EoGRE tunnel mapped in it in AP standalone mode	Passed	

Facebook Wi-Fi

Logical ID	Title	Description	Status	Defect ID
WLJ1612S_Reg_293	Redirection to Facebook Page	To verify redirection to Facebook page for logging in is successful or not	Passed	
WLJ1612S_Reg_294	Restricting free internet access for unauthenticated Windows client	To verify denial of internet access for unauthenticated Windows users is successful or not	Passed	
WLJ1612S_Reg_295	Http Redirection for Continuing Browsing in Android Phone	To Verify Redirection to the Http page initially requested by the Android user is successful or not	Passed	
WLJ1612S_Reg_296	Https Redirection for Continuing Browsing in Windows Laptop	To Verify Redirection to the Https page initially requested by the Windows Laptop user is successful or not	Passed	
WLJ1612S_Reg_297	Show Logs tab	To Verify successful download of each individual log file listed in the show logs tab	Passed	
WLJ1612S_Reg_298	User data statistics	To verify whether the user's data statistics are displayed correctly or not	Passed	
WLJ1612S_Reg_299	KNOWN Users	To verify whether authenticated users are listed in the user data tab or not	Passed	
WLJ1612S_Reg_300	UNKNOWN Users	To verify whether users not authenticated are listed in the user data tab or not	Passed	

WLJ1612S_Reg_301	IN-AUTH Users	To verify whether users attempting to get authenticated are listed in the user data tab or not	Passed	

HA WLC Auth/Authz

Logical ID	Title	Description	Status	Defect ID
WLJ1612S_Reg_281	Allowing the user for complete access to WLC network via TACACS and connecting a client to it.	To check whether user can able to read-write access the primary controller of WLC network or not via TACACS	Passed	
WLJ1612S_Reg_282	Providing the user for monitoring access to the Primary Controller of WLC via TACACS	To check whether user can able to have monitoring access read-only or not to WLC via TACACS and check if any configuration changes can be made or not.	Passed	
WLJ1612S_Reg_283	Providing the user for lobby admin access to the Primary WLC via TACACS	To check whether user can able to have lobby admin access or not to Primary WLC via TACACS	Passed	
WLJ1612S_Reg_284	Allowing the user for complete access to Secondary WLC after Bringing the Primary WLC down via TACACS and connecting a JOS client to it.	To check whether user can able to read-write access the Secondary controller of WLC network after the primary controller goes down via TACACS or not and connecting a JOS Client to the Secondary WLC.	Passed	

WLJ1612S_Reg_285	Allowing the user for complete access to Secondary WLC after Bringing the Primary WLC down via TACACS and connecting a Window client to it.	To check whether user can able to read-write access the Secondary controller of WLC network after the primary controller goes down via TACACS or not and connecting a Window Client to the Secondary WLC.	Passed	
WLJ1612S_Reg_286	Allowing the user for complete access to Secondary WLC after Bringing the Primary WLC down via TACACS and connecting a IOS client to it.	To check whether user can able to read-write access the Secondary controller of WLC network after the primary controller goes down via TACACS or not and connecting a IOS Client to the Secondary WLC.	Passed	
WLJ1612S_Reg_287	Allowing the user for complete access to Secondary WLC after Bringing the Primary WLC down via TACACS and connecting a Mac OS client to it.	To check whether user can able to read-write access the Secondary controller of WLC network after the primary controller goes down via TACACS or not and connecting a Mac OS Client to the Secondary WLC.	Passed	
WLJ1612S_Reg_288	Providing the user for monitoring access to the Secondary Controller via TACACS if the primary controller goes down.	To check whether user can able to have monitoring access read-only or not to Secondary WLC via TACACS if Primary Controller link is down and check if any configuration changes can be made or not.	Passed	

WLJ1612S_Reg_289	Providing the user for lobby admin access to the Secondary WLC via TACACS when the link of the Primary WLC goes down.	To check whether user can able to have lobby admin access or not with Secondary WLC via TACACS when the link of the Primary WLC goes down.	Passed	
WLJ1612S_Reg_290	Providing the user for specific page access like Wireless page or Controller page to the Primary WLC via TACACS	To check whether the user is able to access Wireless page or controller page or not	Passed	
WLJ1612S_Reg_291	Providing the user to access only WLAN page and checking access availability for other pages in the primary controller	To check whether the user is able access only WLAN page and checking whether other pages are in read-only mode or not	Passed	
WLJ1612S_Reg_292	Bring down the primary WLC and down and provide the user to access only the WLAN page	To check whether the user is able access only WLAN page or not in secondary WLC while primary WLC is down	Passed	
EWLCJ1612S_Reg_613	Allowing the user for complete access to WLC network via TACACS and connecting a client to it.	To check whether user can able to read-write access the primary controller of WLC network or not via TACACS	Passed	
EWLCJ1612S_Reg_614	Providing the user for monitoring access to the Primary Controller of WLC via TACACS	To check whether user can able to have monitoring access read-only or not to WLC via TACACS and check if any configuration changes can be made or not.	Passed	
EWLCJ1612S_Reg_615	Providing the user for lobby admin access to the Primary WLC via TACACS	To check whether user can able to have lobby admin access or not to Primary WLC via TACACS	Passed	

EWLCJ1612S_Reg_616	Allowing the user for complete access to Secondary WLC after Bringing the Primary WLC down via TACACS and connecting a JOS client to it.	To check whether user can able to read-write access the Secondary controller of WLC network after the primary controller goes down via TACACS or not and connecting a JOS Client to the Secondary WLC.	Passed	
EWLCJ1612S_Reg_617	Allowing the user for complete access to Secondary WLC after Bringing the Primary WLC down via TACACS and connecting a Window client to it.	To check whether user can able to read-write access the Secondary controller of WLC network after the primary controller goes down via TACACS or not and connecting a Window Client to the Secondary WLC.	Passed	
EWLCJ1612S_Reg_618	Allowing the user for complete access to Secondary WLC after Bringing the Primary WLC down via TACACS and connecting a IOS client to it.	To check whether user can able to read-write access the Secondary controller of WLC network after the primary controller goes down via TACACS or not and connecting a IOS Client to the Secondary WLC.	Passed	
EWLCJ1612S_Reg_619	Allowing the user for complete access to Secondary WLC after Bringing the Primary WLC down via TACACS and connecting a Mac OS client to it.	To check whether user can able to read-write access the Secondary controller of WLC network after the primary controller goes down via TACACS or not and connecting a Mac OS Client to the Secondary WLC.	Passed	

EWLCJ1612S_Reg_620	Providing the user for monitoring access to the Secondary Controller via TACACS if the primary controller goes down.	To check whether user can able to have monitoring access read-only or not to Secondary WLC via TACACS if Primary Controller link is down and check if any configuration changes can be made or not.	Passed	
EWLCJ1612S_Reg_621	Providing the user for lobby admin access to the Secondary WLC via TACACS when the link of the Primary WLC goes down.	To check whether user can able to have lobby admin access or not with Secondary WLC via TACACS when the link of the Primary WLC goes down.	Passed	
EWLCJ1612S_Reg_622	Providing the user for specific page access like Wireless page or Controller page to the Primary WLC via TACACS	To check whether the user is able to access Wireless page or controller page or not	Passed	
EWLCJ1612S_Reg_623	Providing the user to access only WLAN page and checking access availability for other pages in the primary controller	To check whether the user is able access only WLAN page and checking whether other pages are in read-only mode or not	Passed	
EWLCJ1612S_Reg_624	Bring down the primary WLC and down and provide the the user to access only the WLAN page	To check whether the user is able access only WLAN page or not in secondary WLC while primary WLC is down	Failed	CSCvr31335

Client Auth Failures(AAA Failures/WLC Failures)

Logical ID	Title	Description	Status	Defect ID

WLJ1612S_Reg_346	Configure maximum allowed clients per AP radio	To configure maximum allowed clients per AP radio and check if the number of clients given alone gets connected or not	Passed	
WLJ1612S_Reg_347	Applying access control list to the WLAN and check if the ACL rule works to deny the client .	To check whether the ACL applied to WLAN works and check if the client get denied or not.	Passed	
WLJ1612S_Reg_348	Configuring maximum allowed clients for the WLAN and check if the specified clients alone gets connected	To connect a specified number of clients to a specific WLAN and check if client more than the specified value does not authenticated or not	Passed	
WLJ1612S_Reg_349	Checking client moving to sleeping client after timeout	To verify whether client moving to sleeping client after timeout	Passed	
WLJ1612S_Reg_350	Creating a local policy adding device type as Apple and Sleeping client Timeout and check if client move into sleeping client after timeout.	To create a local policy with device type as Apple and configuring Sleeping Client Timeout and check the sleeping timeout	Passed	
WLJ1612S_Reg_351	Creating a local policy adding device type as android and Sleeping Client Timeout and check if client move into sleeping client after Timeout.	To create a local policy with device type as android and configuring Sleeping Client Timeout and check the sleeping timeout	Passed	
WLJ1612S_Reg_352	Creating a local policy adding device type as Windows and Sleeping Client Timeout and check if client move into sleeping client after Timeout.	To create a local policy with device type as Windows and configuring Sleeping Client Timeout and check the sleeping timeout	Passed	

WLJ1612S_Reg_353	Configuring Session timeout for WLAN and check if the client re-auth when the timer gets expired.	To Enable and configure session timeout for WLAN and check if the session timeout interval works fine or not	Passed	
WLJ1612S_Reg_354	Creating a DHCP scope and check if the IP address given in the scope is given to client.	To Configure DHCP scope and check if the IP address is given to the client and check if the IP address allocated is shown in the DHCP Allocates leases.	Passed	
WLJ1612S_Reg_355	Checking the client status if the security of the WLAN changes when a client connected to WLAN .	To Check the status of the client if the security of the WLAN changes when the client is connected to the WLAN.	Passed	

CMX Support

Logical ID	Title	Description	Status	Defect ID
WLJ1612S_Reg_258	Adding Cisco WLC to CMX	To add a Cisco WLC to CMX and check if the WLC gets added to the CMX with the WLC status showing	Passed	
WLJ1612S_Reg_259	Importing maps from prime infrastructure	To import maps from prime infrastructure and check if the maps gets imported to the cmx .	Passed	
WLJ1612S_Reg_260	Importing the maps with 2 to 3 Access points from PI to CMX	To import the maps from prime infra to CMX with 2 to 3 access point and check if the access point details are shown correctly including clients connected .	Passed	

WLJ1612S_Reg_261	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	
WLJ1612S_Reg_262	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	
WLJ1612S_Reg_263	Searching the client by MAC address	To check whether client device can be searched by specifying its MAC address or not	Passed	
WLJ1612S_Reg_264	Searching the client using its IP address	To check whether client device can be searched by specifying its IP address or not	Passed	
WLJ1612S_Reg_265	Searching client using its SSID	To verify whether client device can be searched by specifying the SSID or not	Passed	
WLJ1612S_Reg_266	Check the number of clients visiting the building and floor in hourly basic and daily basic	To check the number of client visiting the building or floor on hourly and daily basic	Passed	
WLJ1612S_Reg_267	Checking the number of new and repeat visitors to the building or floor.	To check the number of new and repeat clients to the building or floor .	Passed	

Limit clients per WLAN/Radio

Logical ID	Title	Description	Status	Defect ID

WLJ1612S_Reg_149	Configuring maximum Allowed Clients Per AP Radio with radio policy as 2.4 GHz and connecting client with different security policy.	To configure maximum allowed client Per AP radio with radio policy as 2.4GHz and connecting a client.	Passed	
WLJ1612S_Reg_150	Configuring maximum Allowed Clients Per AP Radio with radio policy as 5 GHz and connecting client with different security policy.	To configure maximum allowed client Per AP radio with radio policy as 5 GHz and connecting a client.	Passed	
WLJ1612S_Reg_151	Configuring maximum Allowed Clients Per AP Radio with radio policy as 2.4 GHz and connecting client to different AP's.	To connect client to different AP's configuring maximum allowed client per AP radio and check if the configured client alone gets authenticated.	Passed	
WLJ1612S_Reg_152	Configuring maximum Allowed Clients Per AP Radio with radio policy as 5 GHz and connecting client to different AP's.	To connect client to different AP's configuring maximum allowed client per AP radio and check if the configured client alone gets authenticated.	Passed	
WLJ1612S_Reg_153	Configuring maximum allowed client Per AP radio with radio policy as 2.4 GHz with central switching WLAN	To configure maximum allowed client Per AP radio as 2.4 GHZ with central switching and connecting a clients to it.	Passed	
WLJ1612S_Reg_154	Configuring maximum allowed client Per AP radio with radio policy as 2.4 GHz with local switching WLAN	To configure maximum allowed client Per AP radio as 2.4 GHZ with Local switching and connecting a clients to it.	Passed	

WLJ1612S_Reg_155	Configuring maximum allowed client Per AP radio with radio policy as 2.4 GHz with local switching and local authentication	To configure maximum allowed client Per AP radio as 2.4 GHZ with local switching and local authentication and connecting a clients to it.	Passed	
WLJ1612S_Reg_156	Configuring maximum allowed client Per AP radio with radio policy as 5 GHz with central switching WLAN	To configure maximum allowed client Per AP radio as 5 GHZ with central switching and connecting a clients to it.	Passed	
WLJ1612S_Reg_157	Configuring maximum allowed client Per AP radio as 5 GHz with local switching WLAN	To configure maximum allowed client Per AP radio as 5 GHZ with Local switching and connecting a clients to it.	Passed	
WLJ1612S_Reg_158	Configuring maximum allowed client Per AP radio as 5 GHz with local switching and local authentication	To configure maximum allowed client Per AP radio as 5 GHZ with local switching and local authentication and connecting a clients to it.	Passed	
WLJ1612S_Reg_159	Configuring maximum allowed client Per AP radio as 2.4 GHz and try connecting 5 GHZ client.	To configuring maximum allowed client Per AP radio as 2.4 GHz and try connecting 5 GHZ client . check if only 2.4 GHz clients gets connected and 5 GHz client does not get connected.	Passed	

WLJ1612S_Reg_160	Configuring maximum allowed client Per AP radio as 5 GHz and try connecting 2.4 GHZ client.	To configuring maximum allowed client Per AP radio as 5 GHz and try connecting 5 GHZ client . check if only 2.4 GHz clients gets connected and 2.4 GHz client does not get connected.	Passed	
WLJ1612S_Reg_161	Deleting one already existing client in 2.4 GHz when max limit reached and try connecting new client .	To delete one existing client in 2.4 GHz when the client limit is reached to maximum and try connecting a new client and check if the clients gets connected to it .	Passed	
WLJ1612S_Reg_162	Deleting one already existing client in 5 GHz when max limit reached and try connecting new client .	To delete one existing client in 5 GHz when the client limit is reached to maximum and try connecting a new client and check if the clients gets connected to it .	Passed	
WLJ1612S_Reg_163	Trying AP failover priority when clients connected to a AP .	To try AP failover priority when clients connected and the HA WLC has the same WLAN with radio as 2.4 GHz .The WLAN is configured with maximum allowed client Per AP	Passed	
WLJ1612S_Reg_164	Intra roaming of clients configuring maximum allowed client Per AP radio	To try intra roaming of clients on the same WLC in a WLAN configured with maximum allowed client Per AP radio and check if the client roam from one AP to another AP.	Passed	

WLJ1612S_Reg_165	Inter roaming of clients configuring maximum allowed client Per AP radio	To try inter roaming of clients configuring maximum allowed client per AP radio and check if only the configured limit of clients alone gets connected.	Passed	

Ethernet VLAN tag on AP

Logical ID	Title	Description	Status	Defect ID
WLJ1612S_Reg_102	Providing the VLAN tag to the 2800 AP from eWLC CLI.	To Verify the VLAN tag status of the 2800 AP after reboot and join back to the eWLC.	Passed	
WLJ1612S_Reg_103	Unassign the VLAN tag to the 2800 AP from eWLC CLI.	To Verify the VLAN tag status of the 2800 AP after reboot and join back to the eWLC.	Passed	
WLJ1612S_Reg_104	Providing the VLAN tag to the 3800 AP from eWLC CLI.	To Verify the VLAN tag status of the 3800 AP after reboot and join back to the eWLC.	Passed	
WLJ1612S_Reg_105	Unassign the VLAN tag to the 3800 AP from eWLC CLI.	To Verify the VLAN tag status of the 3800 AP after reboot and join back to the eWLC.	Passed	
WLJ1612S_Reg_106	Providing the VLAN tag to the 2700 AP from eWLC CLI.	To Verify the VLAN tag status of the 2700 AP after reboot and join back to the eWLC.	Passed	
WLJ1612S_Reg_107	Unassign the VLAN tag to the 2700 AP from eWLC CLI.	To Verify the VLAN tag status of the 2700 AP after reboot and join back to the eWLC.	Passed	

WLJ1612S_Reg_108	Providing the VLAN tag to the 702W AP from eWLC CLI.	To Verify the VLAN tag status of the 702W AP after reboot and join back to the eWLC.	Passed	
WLJ1612S_Reg_109	Unassign the VLAN tag to the 702W AP from eWLC CLI.	To Verify the VLAN tag status of the 702W AP after reboot and join back to the eWLC.	Passed	
WLJ1612S_Reg_110	Providing the VLAN tag to the ClickOS/IOS AP from eWLC CLI and connect the Android Client.	To Verify the VLAN tag status of the ClickOS/IOS AP after reboot and join back to the eWLC and Verify the Android client connectivity.	Passed	
WLJ1612S_Reg_111	Providing the VLAN tag to the ClickOS/IOS AP from eWLC CLI and connect the Windows Client.	To Verify the VLAN tag status of the ClickOS/IOS AP after reboot and join back to the eWLC and Verify the Windows client connectivity.	Passed	
WLJ1612S_Reg_112	Providing the VLAN tag to the ClickOS/IOS AP from eWLC CLI and connect the IOS Client.	To Verify the VLAN tag status of the ClickOS/IOS AP after reboot and join back to the eWLC and Verify the IOS client connectivity.	Passed	
WLJ1612S_Reg_113	Providing the VLAN tag to the ClickOS/IOS AP from eWLC CLI and connect the Anyconnect Client.	To Verify the VLAN tag status of the ClickOS/IOS AP after reboot and join back to the eWLC and Verify the Anyconnect client connectivity.	Passed	
WLJ1612S_Reg_114	Providing the VLAN tag to the Group of AP's from eWLC CLI.	To Verify the VLAN tag status of the Group of AP's after reboot and join back to the eWLC.	Passed	

WLJ1612S_Reg_115	Unassign the VLAN tag to the Group of AP's from eWLC CLI.	To Verify the VLAN tag status of the Group of AP's after reboot and join back to the eWLC.	Passed	
WLJ1612S_Reg_116	Providing the VLAN tag to the ClickOS/IOS AP from eWLC CLI and change the mode of the AP to Monitor from local.	To Verify the VLAN tag status of the ClickOS/IOS AP after changing the mode of the AP to monitor from local.	Passed	
WLJ1612S_Reg_117	Providing the VLAN tag to the ClickOS/IOS AP from eWLC CLI and change the mode of the AP to Bridge from Local.	To Verify the VLAN tag status of the ClickOS/IOS AP after changing the mode of the AP to Bridge from local.	Passed	
WLJ1612S_Reg_118	Providing the VLAN tag to the ClickOS/IOS AP from eWLC CLI and change the mode of the AP to sniffer from Local.	To Verify the VLAN tag status of the ClickOS/IOS AP after changing the mode of the AP to sniffer from local.	Passed	
WLJ1612S_Reg_119	Check the VLAN tag is overriding or not	To verify whether the VLAN tag is overriding or not after assigning to the particular AP and group of APs.	Passed	
EWLCJ1612S_Reg_636	Providing the VLAN tag to the 2800 AP from eWLC CLI.	To Verify the VLAN tag status of the 2800 AP after reboot and join back to the eWLC.	Passed	
EWLCJ1612S_Reg_637	Unassign the VLAN tag to the 2800 AP from eWLC CLI.	To Verify the VLAN tag status of the 2800 AP after reboot and join back to the eWLC.	Passed	
EWLCJ1612S_Reg_638	Providing the VLAN tag to the 3800 AP from eWLC CLI.	To Verify the VLAN tag status of the 3800 AP after reboot and join back to the eWLC.	Passed	

EWLCJ1612S_Reg_639	Unassign the VLAN tag to the 3800 AP from eWLC CLI.	To Verify the VLAN tag status of the 3800 AP after reboot and join back to the eWLC.	Passed	
EWLCJ1612S_Reg_640	Providing the VLAN tag to the 2700 AP from eWLC CLI.	To Verify the VLAN tag status of the 2700 AP after reboot and join back to the eWLC.	Passed	
EWLCJ1612S_Reg_641	Unassign the VLAN tag to the 2700 AP from eWLC CLI.	To Verify the VLAN tag status of the 2700 AP after reboot and join back to the eWLC.	Passed	
EWLCJ1612S_Reg_642	Providing the VLAN tag to the 702W AP from eWLC CLI.	To Verify the VLAN tag status of the 702W AP after reboot and join back to the eWLC.	Passed	
EWLCJ1612S_Reg_643	Unassign the VLAN tag to the 702W AP from eWLC CLI.	To Verify the VLAN tag status of the 702W AP after reboot and join back to the eWLC.	Passed	
EWLCJ1612S_Reg_644	Providing the VLAN tag to the ClickOS/IOS AP from eWLC CLI and connect the Android Client.	To Verify the VLAN tag status of the ClickOS/IOS AP after reboot and join back to the eWLC and Verify the Android client connectivity.	Passed	
EWLCJ1612S_Reg_645	Providing the VLAN tag to the ClickOS/IOS AP from eWLC CLI and connect the Windows Client.	To Verify the VLAN tag status of the ClickOS/IOS AP after reboot and join back to the eWLC and Verify the Windows client connectivity.	Passed	

EWLCJ1612S_Reg_646	Providing the VLAN tag to the ClickOS/IOS AP from eWLC CLI and connect the IOS Client.	To Verify the VLAN tag status of the ClickOS/IOS AP after reboot and join back to the eWLC and Verify the IOS client connectivity.	Passed	
EWLCJ1612S_Reg_647	Providing the VLAN tag to the ClickOS/IOS AP from eWLC CLI and connect the anyconnect Client.	To Verify the VLAN tag status of the ClickOS/IOS AP after reboot and join back to the eWLC and Verify the anyconnect client connectivity.	Passed	
EWLCJ1612S_Reg_648	Providing the VLAN tag to the Group of AP's from eWLC CLI.	To Verify the VLAN tag status of the Group of AP's after reboot and join back to the eWLC.	Passed	
EWLCJ1612S_Reg_649	Unassign the VLAN tag to the Group of AP's from eWLC CLI.	To Verify the VLAN tag status of the Group of AP's after reboot and join back to the eWLC.	Passed	
EWLCJ1612S_Reg_650	Providing the VLAN tag to the ClickOS/IOS AP from eWLC CLI and change the mode of the AP to Monitor from local.	To Verify the VLAN tag status of the ClickOS/IOS AP after changing the mode of the AP to monitor from local.	Passed	
EWLCJ1612S_Reg_651	Providing the VLAN tag to the ClickOS/IOS AP from eWLC CLI and change the mode of the AP to Bridge from Local.	To Verify the VLAN tag status of the ClickOS/IOS AP after changing the mode of the AP to Bridge from local.	Passed	
EWLCJ1612S_Reg_652	Providing the VLAN tag to the ClickOS/IOS AP from eWLC CLI and change the mode of the AP to sniffer from Local.	To Verify the VLAN tag status of the ClickOS/IOS AP after changing the mode of the AP to sniffer from local.	Passed	

EWLCJ1612S_Reg_653	Check the VLAN tag is overriding or not	To verify whether the VLAN tag is overriding or not after assigning to the particular Ap and group of AP's.	Passed	

Aging Cases

Logical ID	Title	Description	Status	Defect ID
WLJ1612S_Reg_218	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	
WLJ1612S_Reg_219	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	
WLJ1612S_Reg_220	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	
WLJ1612S_Reg_221	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	
WLJ1612S_Reg_222	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	

WLJ1612S_Reg_223	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	
WLJ1612S_Reg_224	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	
WLJ1612S_Reg_225	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	
WLJ1612S_Reg_226	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	
WLJ1612S_Reg_227	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	

1815 RLAN Features

Logical ID	Title	Description	Status	Defect ID

WLJ1612S_Reg_356	Checking the client connectivity to RLAN configured with Open security and macfiltering	To verify whether client is connecting to RLAN with open security and macfiltering	Passed	
WLJ1612S_Reg_357	Enabling the 802.1x security and MAC filtering to RLAN	To create a RLAN with 802.1x security and MAC filtering connecting a windows client to the RLAN and check if the client gets connected to the RLAN port in the AP or not	Passed	
WLJ1612S_Reg_358	Configuring RLAN with open security and connect three wired clients (windows,MAC and JOS)	To verify whether three wired clients gets connected with open security	Failed	CSCvp98647
WLJ1612S_Reg_359	Configuring RLAN with open+macfilter security and connect three wired clients (windows,MAC and JOS)	To verify whether three wired clients gets connected with open+macfilter security	Passed	
WLJ1612S_Reg_360	Configuring RLAN with 802.1X security and connect three wired clients (windows,MAC and JOS)	To verify whether three wired clients gets connected with 802.1X security	Passed	
WLJ1612S_Reg_361	Configuring RLAN with 802.1X+macfilter security and connect three wired clients (windows,MAC and JOS)	To verify whether three wired clients gets connected with 802.1X+macfilter security	Passed	
WLJ1612S_Reg_362	Connecting the client to the RLAN configuring with 802.1x security and host mode as single Host	To verify whether a windows client connecting to the RLAN with 802.1x security and host mode as single Host	Passed	

WLJ1612S_Reg_363	Configuring RLAN with 802.1x security and host mode as multi host and connect the client	To verify whether a client connecting to RLAN with 802.1x security and host mode as multi host	Passed	
WLJ1612S_Reg_364	Configuring RLAN with 802.1x security and host mode as multi domain and connect the client	To verify whether a client connecting to RLAN with 802.1x security and host mode as multi domain	Passed	
WLJ1612S_Reg_365	Checking the client connectivity to a RLAN with 802.1x security and AVC profile is applied	To create a RLAN with 802.1x security and applying AVC profile, connecting a windows client to the RLAN and check if the AVC profile gets applied to the client connecting to it or not.	Passed	
WLJ1612S_Reg_366	Checking the client connectivity with 802.1x security and host mode as single Host and violation mode as Replace	To verify whether client connecting to a RLAN with 802.1x security and host mode as single host along with violation mode as Replace	Passed	
WLJ1612S_Reg_367	Checking the client connectivity with 802.1x security and host mode as single Host and violation mode as Shutdown	To verify whether client connecting to a RLAN with 802.1x security and host mode as single host along with violation mode as Shutdown	Passed	
WLJ1612S_Reg_368	Checking the client connectivity with 802.1x security and host mode as single Host and violation mode as protect	To verify whether client connecting to a RLAN with 802.1x security and host mode as single host along with violation mode as Protect	Passed	

WLJ1612S_Reg_369	Checking the client connectivity to RLAN configured with 802.1x security and preauthentication enabled	To verify whether client connecting to a RLAN with 802.1x security and preauthentication enabling	Passed	
WLJ1612S_Reg_370	Rebooting the eWLC after connecting the client to RLAN	Checking whether RLAN configurations showing same or different after rebooting	Passed	
WLJ1612S_Reg_371	Downgrading the eWLC after configuring RLAN and connect the client	Checking whether RLAN configurations showing same or different after downgrading eWLC and also verifying client connectivity	Passed	
WLJ1612S_Reg_372	Upgrade the eWLC after configuring RLAN and connect the client	Checking whether RLAN configurations showing same or different after upgrading the eWLC and also verifying client connectivity	Passed	
WLJ1612S_Reg_373	uploading and downloading the config file and checking the RLAN configuration	To verify whether RLAN configurations showing same or different after uploading and downloading file to eWLC and also verifying client connectivity	Passed	

MIMO Coverage

Logical ID	Title	Description	Status	Defect ID

WLJ1612S_Reg_374	Enabling HT either in 802.11b/g/n or 802.11a/n/ac and checking the clients association & their throughput	To check whether clients data rates are getting at maximum output or not as configured in 802.11b/g/n or 802.11a/n/ac	Passed	
WLJ1612S_Reg_375	Enabling VHT alone in 802.11a/n/ac and checking the clients association & their throughput	To check whether clients data rates are getting at maximum output or not as per their spatial streams configured in 802.11a/n/ac	Passed	
WLJ1612S_Reg_376	Setting the channel width to 40MHz and checking the clients association	To check whether clients data rates are getting at maximum output or not as per their spatial streams configured in 802.11a/n/ac when it is configured with 40MHz	Passed	
WLJ1612S_Reg_377	Setting the channel width to 80MHz and checking the clients association	To check whether clients data rates are getting at maximum output or not as per their spatial streams configured in 802.11a/n/ac when it is configured with 80MHz	Passed	
WLJ1612S_Reg_378	Capturing the beacon packets and checking the HT & VHT parameters	To check whether HT & VHT parameters displays the configurations properly or not in beacon packets.	Passed	
WLJ1612S_Reg_379	Setting the channel width to best and checking the clients association	To check whether clients data rates are getting at maximum output or not as per their spatial streams configured in 802.11a/n/ac when it is configured with best	Passed	

WLJ1612S_Reg_380	Enabling clean air in both 5 GHZ and 2.4 GHZ and verify clean air in AP	To verify whether clean air configuration is applied in APs	Passed	
EWLCJ1612S_Reg_574	Enabling HT either in 802.11b/g/n or 802.11a/n/ac and checking the clients association & their throughput	To check whether clients data rates are getting at maximum output or not as configured in 802.11b/g/n or 802.11a/n/ac	Passed	
EWLCJ1612S_Reg_575	Enabling VHT alone in 802.11a/n/ac and checking the clients association & their throughput	To check whether clients data rates are getting at maximum output or not as per their spatial streams configured in 802.11a/n/ac	Passed	
EWLCJ1612S_Reg_576	Setting the channel width to 40MHz and checking the clients association	To check whether clients data rates are getting at maximum output or not as per their spatial streams configured in 802.11a/n/ac when it is configured with 40MHz	Passed	
EWLCJ1612S_Reg_577	Setting the channel width to 80MHz and checking the clients association	To check whether clients data rates are getting at maximum output or not as per their spatial streams configured in 802.11a/n/ac when it is configured with 80MHz	Passed	
EWLCJ1612S_Reg_578	Capturing the beacon packets and checking the HT & VHT parameters	To check whether HT & VHT parameters displays the configurations properly or not in beacon packets.	Passed	

EWLCJ1612S_Reg_579	Setting the channel width to best and checking the clients association	To check whether clients data rates are getting at maximum output or not as per their spatial streams configured in 802.11a/n/ac when it is configured with best	Passed	
EWLCJ1612S_Reg_580	Enabling clean air in both 5 GHZ and 2.4 GHz and verify clean air in AP	To verify whether clean air configuration is applied in Aps	Passed	

DHCP Option 82 - Google

Logical ID	Title	Description	Status	Defect ID
WLJ1612S_Reg_268	Connecting the android/IOS/MAC clients without enabling DHCP proxy	To verify whether android/IOS/MAC Clients are getting the internal DHCP IP address or not when DHCP Proxy is in disabled state	Passed	
WLJ1612S_Reg_269	Connecting the android/IOS/MAC clients after enable DHCP proxy	To verify whether android/IOS/MAC Clients are getting IP address or not when Proxy is in enable state	Passed	
WLJ1612S_Reg_270	Enable/disable the DHCP Proxy through CLI	To verify whether DHCP proxy server enable/disable through CLI or not	Passed	
WLJ1612S_Reg_271	Configuring the DHCP Option 82 Remote Id field format with AP-MAC	To verify whether DHCP option 82 with AP-MAC is sending the client association/disassociation requests or not	Passed	
WLJ1612S_Reg_272	Configuring the DHCP Option 82 Remote Id field format with AP-MAC-SSID	To verify whether DHCP option 82 with AP-MAC-SSID is sending the client association/disassociation requests or not	Passed	

WLJ1612S_Reg_273	Configuring the DHCP Option 82 Remote Id field format with AP-ETHMAC	To verify whether DHCP option 82 with AP-ETHMAC is sending the client association/disassociation requests or not	Passed	
WLJ1612S_Reg_274	Configuring the DHCP Option 82 Remote Id field format with AP-Name-SSID	To verify whether DHCP option 82 with AP-Name-SSID is sending the client association/disassociation requests or not	Passed	
WLJ1612S_Reg_275	Configuring the DHCP Option 82 Remote Id field format with Flex-Group-Name	To verify whether DHCP option 82 with Flex-Group-Name is sending the client association/disassociation requests or not	Passed	
WLJ1612S_Reg_276	Configuring the DHCP Option 82 Remote Id field format with AP-Location	To verify whether DHCP option 82 with AP-Location is sending the client association/disassociation requests or not	Passed	
WLJ1612S_Reg_277	Configuring the DHCP Option 82 Remote Id field format with AP-MAC-VLAN-ID	To verify whether DHCP option 82 with AP-MAC-VLAN-ID is sending the client association/disassociation requests or not	Passed	
WLJ1612S_Reg_278	Configuring the DHCP Option 82 Remote Id field format with AP-NAME-VLAN-ID	To verify whether DHCP option 82 with AP-NAME-VLAN-ID is sending the client association/disassociation requests or not	Passed	
WLJ1612S_Reg_279	Configuring the DHCP Option 82 Remote Id field format with AP-ETHMAC-SSID	To verify whether DHCP option 82 with AP-ETHMAC-SSID is sending the client association/disassociation requests or not	Passed	
WLJ1612S_Reg_280	Configuring the DHCP option 82 through PI	To verify whether DHCP option 82 is enabling through PI or not	Passed	

ATF on Mesh

Logical ID	Title	Description	Status	Defect ID
WLJ1612S_Reg_139	Config Mesh setup and apply config on Mesh Aps	To verify that Mesh setup configured and ATF applied on Mesh Aps	Passed	
WLJ1612S_Reg_140	Apply ATF Enforcement mode on MESH AP	To verify that ATF Enforcement mode applied on MESH AP or not	Passed	
WLJ1612S_Reg_141	Apply ATF policy on WLAN and connect Android client	To verify that policy applied on WLAN or not and client connected successfully	Passed	
WLJ1612S_Reg_142	Mac OS client connectivity with l2 security WLAN which having different Policy weight	To verify the client connectivity with two SSID having different weight.	Passed	
WLJ1612S_Reg_143	Mapping policy to the WLAN and connecting client to enforced mode ATF	To verify that ATF Enforcement mode applied on AP group or not	Passed	
WLJ1612S_Reg_144	Configuring mesh on AP and connecting client with ATF monitor mode using 2.5 GHZ	To Monitor client statistics with Mesh AP connect the client with 2.5 GHZ	Passed	
WLJ1612S_Reg_145	Configuring mesh on AP and connecting client with ATF monitor mode using 5 GHZ	To Monitor client statistics with Mesh AP connect the client with 5GhZ	Failed	CSCvq38803
WLJ1612S_Reg_146	Configuring mesh on AP and connecting client with ATF enforcement mode	To verify client statistics with mesh AP and connect the client with enforcement with 2.5 GhZ	Passed	

WLJ1612S_Reg_147	Attaching ATF Policies to Policy-Profile with 2.4 GHZ and 5 GHZ	To check whether user able to Attach ATF Policies to Policy-Profile or not	Passed	
WLJ1612S_Reg_148	Configure two ATF policies with different weights and map to different WLANs and connecting 2 clients	To verify clients capability, interference and other factors able to see After connected with different weights and map to different WLANs	Passed	
EWLCJ1612S_Reg_662	Config Mesh setup and apply config on Mesh Aps	To verify that Mesh setup configured and ATF applied on Mesh Aps	Passed	
EWLCJ1612S_Reg_663	Apply ATF Enforcement mode on MESH AP	To verify that ATF Enforcement mode applied on MESH AP or not	Passed	
EWLCJ1612S_Reg_664	Apply ATF policy on wlan and connect Android client	To verify that policy applied on WLAN or not and client connected succesfully	Passed	
EWLCJ1612S_Reg_665	Mac OS client connectivity with l2 security WLAN which having different Policy weight	To verify the client connectivity with two SSID having different weight.	Passed	
EWLCJ1612S_Reg_666	Mapping policy to the WLAN and connecting client to enforced mode ATF	To verify that ATF Enforcement mode applied on AP group or not	Passed	
EWLCJ1612S_Reg_667	Configuring mesh on AP and connecting client with ATF monitor mode using 2.5 ghz	To Monitor client statistics with Mesh AP connect the client with 2.5 GHZ	Passed	
EWLCJ1612S_Reg_668	Configuring mesh on AP and connecting client with ATF monitor mode using 5 ghz	To Monitor client statistics with Mesh AP connect the client with 5Ghz	Passed	

EWLCJ1612S_Reg_669	Configuring mesh on AP and connecting client with ATF enforcement mode	To verify client statistics with mesh AP and connect the client with enforcement with 2.5 Ghz	Passed	
EWLCJ1612S_Reg_670	Attaching ATF Policies to Policy-Profile with 2.4Ghz and 5Ghz	To check whether user able to Attach ATF Policies to Policy-Profile or not	Passed	
EWLCJ1612S_Reg_671	Configure two ATF policies with different weights and map to diffent WLANs and connecting 2 clinets	To verify clients capability, interference and other factors able to see ATFer connected with different weights and map to diffent WLANs	Passed	

TrustSec Enhancements

Logical ID	Title	Description	Status	Defect ID
WLJ1612S_Reg_302	Associating Android clients to TrustSec configured AP and checking the policy hit statistics in WLC UI	To verify the policy hit for Android client after TrustSec configured on AP	Passed	
WLJ1612S_Reg_303	Performing Inter controller roaming of Windows client in TrustSec enabled WLC's with Dot1x security.	To check whether inter controller roaming of windows clients works properly or not between WLC's with Dot1x security.	Passed	
WLJ1612S_Reg_304	Performing Inter controller roaming of Android client in TrustSec enabled WLC's with Dot1x security.	To check whether inter controller roaming of Android clients works properly or not between WLC's with Dot1x security.	Passed	

WLJ1612S_Reg_305	Performing Inter controller roaming of IOS client in TrustSec enabled WLC's with Dot1x security.	To check whether inter controller roaming of IOS clients works properly or not between WLC's with Dot1x security.	Passed	
WLJ1612S_Reg_306	Performing Inter controller roaming of MacOS client in TrustSec enabled WLC's with Dot1x security.	To check whether inter controller roaming of windows clients works properly or not between WLC's with Dot1x security.	Passed	
WLJ1612S_Reg_307	Performing Inter controller roaming of Windows client in TrustSec enabled WLC's with WPA2-dot1x security.	To check whether inter controller roaming of windows clients works properly or not between WLC's with WPA2-dot1xsecurity.	Passed	
WLJ1612S_Reg_308	Performing Inter controller roaming of Android client in TrustSec enabled WLC's with WPA2-dot1x security.	To check whether inter controller roaming of Android clients works properly or not between WLC's with WPA2-dot1x security.	Passed	
WLJ1612S_Reg_309	Performing Inter controller roaming of IOS client in TrustSec enabled WLC's with WPA2-dot1x security.	To check whether inter controller roaming of IOS clients works properly or not between WLC's with WPA2-dot1x security.	Passed	
WLJ1612S_Reg_310	Performing Inter controller roaming of MacOS client in TrustSec enabled WLC's with WPA2-dot1x security.	To check whether inter controller roaming of MacOS clients works properly or not between WLC's with WPA2-dot1x security.	Passed	

WLJ1612S_Reg_311	Enabling CTS override in 2800/3800 AP's which is joined in 5520 WLC UI/CLI	To check that CTS override is enabled or not for 2800/3800 AP's	Failed	CSCvq21727
WLJ1612S_Reg_312	Checking the TrustSec configuration sync in HA WLC's	To check that TrustSec configuration sync or not in HA WLC's	Passed	

Flex Video Stream

Logical ID	Title	Description	Status	Defect ID
WLJ1612S_Reg_64	MC2UC traffic to local-switching client	To verify that the local-switching client subscribed to video streaming receives MC2UC traffic	Passed	
WLJ1612S_Reg_65	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	
WLJ1612S_Reg_66	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	
WLJ1612S_Reg_67	Multiple LS clients in same VLAN, same WLAN, receiving MC2UC traffic	To verify whether the multiple local-switching clients receives MC2UC traffic when subscribed to videostream	Passed	
WLJ1612S_Reg_68	Client disassociates when receiving MC2UC traffic	To verify whether AP stops sending traffic when client disassociates	Passed	

WLJ1612S_Reg_69	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	
WLJ1612S_Reg_70	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	
WLJ1612S_Reg_71	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	
WLJ1612S_Reg_72	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	
WLJ1612S_Reg_73	Videostream config sync for LS WLAN in HA setup	To verify whether the videostreaming config for LS WLAN has been synced between the Active and Standby in HA setup	Passed	
WLJ1612S_Reg_74	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	
EWLCJ1612S_Reg_625	MC2UC traffic to local-switching client	To verify that the local-switching client subscribed to videostreaming receives MC2UC traffic	Passed	

EWLCJ1612S_Reg_626	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	
EWLCJ1612S_Reg_627	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	
EWLCJ1612S_Reg_628	Multiple LS clients in same vlan, same wlan, receiving MC2UC traffic	To verify whether the multiple local-switching clients receives MC2UC traffic when subscribed to videostream	Passed	
EWLCJ1612S_Reg_629	Client disassociates when receiving MC2UC traffic	To verify whether AP stops sending traffic when client disassociates	Passed	
EWLCJ1612S_Reg_630	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	
EWLCJ1612S_Reg_631	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	
EWLCJ1612S_Reg_632	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	

EWLCJ1612S_Reg_633	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	
EWLCJ1612S_Reg_634	Videstream config sync for LS WLAN in HA setup	To verify whether the videostreaming config for LS WLAN has been synced between the Active and Standby in HA setup	Passed	
EWLCJ1612S_Reg_635	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	

Hyperlocation Module supports for AP 37XX

Logical ID	Title	Description	Status	Defect ID
WLJ1612S_Reg_212	Importing maps to CMX through Japanese PI	To check whether the maps can be imported in CMX from PI	Passed	
WLJ1612S_Reg_213	Sync the eWLC in to CMX	To check whether the eWLC and CMX gets synced up	Passed	
WLJ1612S_Reg_214	Tracking the Window, iPhone client devices in CMX	To check the tracking of Window ,iPhone devices using CMX	Passed	
WLJ1612S_Reg_215	Android, iOS Client Locate in CMX	To verify the Location of the clients	Passed	
WLJ1612S_Reg_216	Location Accuracy Test in CMX of Window client	To verify the location accuracy of the clients	Passed	
WLJ1612S_Reg_217	History of client location(Client Playback)	To verify the client location history	Passed	

EWLCJ1612S_Reg_607	Importing maps to CMX through Japanese PI	To check whether the maps can be imported in CMX from PI	Passed	
EWLCJ1612S_Reg_608	Sync the eWLC in to CMX	To check whether the eWLC and CMX gets synced up	Passed	
EWLCJ1612S_Reg_609	Tracking the Window,iPhone client devices in CMX	To check the tracking of Window ,iphone devices using CMX	Passed	
EWLCJ1612S_Reg_610	Android,iOS Client Locate in CMX	To verify the Location of the clients	Passed	
EWLCJ1612S_Reg_611	Location Accuracy Test in CMX of Window client	To verify the location accuracy of the clients	Passed	
EWLCJ1612S_Reg_612	History of client location(Client Playback)	To verify the client location history	Passed	

Dot1x and Web-Auth

Logical ID	Title	Description	Status	Defect ID
WLJ1612S_Reg_415	Authentication of Android client with Security WPA2+Dot1x and Web-Auth	Checking for the Authentication of the client when connected to a WLAN in which WPA2+Dot1x and Web-Auth is enabled	Passed	
WLJ1612S_Reg_416	Authentication of Windows client with Security WPA2+Dot1x and Web-Auth	Checking for the Authentication of the Windows client when connected to a WLAN in which WPA2+Dot1x and Web-Auth is enabled	Passed	

WLJ1612S_Reg_417	Authentication of JOS client with Security WPA2+Dot1x and consent	Checking for the Authentication of the JOS client when connected to a WLAN in which WPA2+Dot1x and consent is enabled	Passed	
WLJ1612S_Reg_418	Authentication of IOS client with Security WPA2+Dot1x and consent	Checking for the Authentication of the IOS client when connected to a WLAN in which WPA2+Dot1x and consent is enabled	Passed	
WLJ1612S_Reg_419	Authenticating of client with Security WPA2+Dot1x and web consent	Checking for the Authentication of the client when connected to a WLAN in which WPA2+Dot1x and web consent is enabled	Passed	
WLJ1612S_Reg_420	Authentication of client with Security WPA3+Dot1x and Web-Auth	Checking for the Authentication of the client when connected to a WLAN in which WPA3+Dot1x and Web-Auth is enabled	Passed	
WLJ1612S_Reg_421	Authentication of JOS client with Security WPA3+Dot1x and consent	Checking for the Authentication of the JOS client when connected to a WLAN in which WPA3+Dot1x and consent is enabled	Passed	
WLJ1612S_Reg_422	Authenticating of client with Security WPA3+Dot1x and web consent	Checking for the Authentication of the client when connected to a WLAN in which WPA3+Dot1x and web consent is enabled	Passed	

EWLCJ1612S_Reg_654	Authentication of Android client with Security WPA2+Dot1x and Web-Auth	Checking for the Authentication of the client when connected to a WLAN in which WPA2+Dot1x and Web-Auth is enabled	Passed	
EWLCJ1612S_Reg_655	Authentication of Windows client with Security WPA2+Dot1x and Web-Auth	Checking for the Authentication of the Windows client when connected to a WLAN in which WPA2+Dot1x and Web-Auth is enabled	Passed	
EWLCJ1612S_Reg_656	Authentication of JOS client with Security WPA2+Dot1x and consent	Checking for the Authentication of the JOS client when connected to a WLAN in which WPA2+Dot1x and consent is enabled	Passed	
EWLCJ1612S_Reg_657	Authentication of IOS client with Security WPA2+Dot1x and consent	Checking for the Authentication of the IOS client when connected to a WLAN in which WPA2+Dot1x and consent is enabled	Passed	
EWLCJ1612S_Reg_658	Authenticating of client with Security WPA2+Dot1x and web consent	Checking for the Authentication of the client when connected to a WLAN in which WPA2+Dot1x and web consent is enabled	Passed	
EWLCJ1612S_Reg_659	Authentication of client with Security WPA3+Dot1x and Web-Auth	Checking for the Authentication of the client when connected to a WLAN in which WPA3+Dot1x and Web-Auth is enabled	Passed	

EWLCJ1612S_Reg_660	Authentication of JOS client with Security WPA3+Dot1x and consent	Checking for the Authentication of the JOS client when connected to a WLAN in which WPA3+Dot1x and consent is enabled	Passed	
EWLCJ1612S_Reg_661	Authenticating of client with Security WPA3+Dot1x and web consent	Checking for the Authentication of the client when connected to a WLAN in which WPA3+Dot1x and web consent is enabled	Passed	

Network Assurance

Logical ID	Title	Description	Status	Defect ID
WLJ1612S_Reg_407	Creating the SSID and connecting the sensor mode AP	Verify that user is able to connect the sensor mode AP as a client	Passed	
WLJ1612S_Reg_408	Radius server up/down event data to Network Assurance	Verify that Radius server up/down event data is sending to Network Assurance server or not	Passed	
WLJ1612S_Reg_409	Verify that JSON data is sending out from eWLC	Checking that JSON data is sending out from eWLC to NA server or not	Passed	
WLJ1612S_Reg_410	eWLC allowing XOR radio as sensor even when WSA is disabled	Checking that user is able to use XOR radio as a sensor while WSA disabled	Passed	
WLJ1612S_Reg_411	Verify that eWLC sends nearest AP neighbors data to NA server correctly or not	Checking that eWLC sends nearest C308AP neighbors data to NA server correctly or not+C318	Passed	

WLJ1612S_Reg_412	Verify that WLAN changes are reflecting in client event reason type for retries or not	Checking that WLAN changes are reflecting in NA server or not	Passed	
WLJ1612S_Reg_413	Verify that WSA server URL config is syncing to standby eWLC or not	Checking that WSA config syncing with standby in HA mode	Passed	
WLJ1612S_Reg_414	Verifying that mac filtering working properly for sensor mode AP debug	Checking that mac-filtering working properly for sensor mode AP debug or not	Passed	
EWLCJ1612S_Reg_517	Checking the Windows Client connectivity after enabling Selective reanchor in WLAN	To verify whether windows jos client is connecting properly or not	Passed	
EWLCJ1612S_Reg_518	Checking the android Client connectivity after enabling Selective reanchor in WLAN	To verify whether android client is connecting properly or not	Passed	
EWLCJ1612S_Reg_519	Checking the IOS Client connectivity after enabling Selective reanchor in WLAN	To verify whether IOS client is connecting properly or not	Passed	
EWLCJ1612S_Reg_520	Roaming the client between 2 controllers	To verify whether client roaming successfully between two controllers	Passed	
EWLCJ1612S_Reg_521	Reboot the Controller after Re-anchor enabling	To verify whether Configurations are showing same or different after controller reboot	Passed	
EWLCJ1612S_Reg_522	Downgrade/upgrade the controller with Re-anchor enable	To verify whether Downgrade/upgrade the controller with Re-anchor enable	Passed	

Reboot APs by Groups

Logical ID	Title	Description	Status	Defect ID
WLJ1612S_Reg_199	Creating a site tag in eWLC UI	To create a site tag in eWLC UI and check if the site tag is created or not.	Passed	
WLJ1612S_Reg_200	Creating a site tag in eWLC CLI	To create a site tag in eWLC CLI and check if the site tag is created or not.	Passed	
WLJ1612S_Reg_201	Mapping a AP profile to the site tag using eWLC UI	To map a AP profile to the site tag and check if the AP profile is mapped to site tag or not.	Passed	
WLJ1612S_Reg_202	Mapping a Site to AP in eWLC UI	To map a AP profile to the site tag and check if the AP profile is mapped to site tag or not.	Passed	
WLJ1612S_Reg_203	Adding one COS AP to site and rebooting the AP	To add one COS AP to site and applying the site reboot command and check if the AP gets rebooted	Passed	
WLJ1612S_Reg_204	Adding 3 COS AP to site and rebooting the AP	To add 3 COS AP to site and applying the site reboot command and check if all the AP gets rebooted and joins the eWLC again	Passed	
WLJ1612S_Reg_205	Adding COS AP to site and rebooting the AP with different AP modes	To add COS AP to site and applying the site reboot command and check if the AP gets rebooted in all modes or not	Passed	

WLJ1612S_Reg_206	Adding one IOS AP to the site and rebooting the AP through AP site reset command	To add one IOS to the site creates and giving the AP reboot command through CLI to check if the AP gets rebooted or not.	Passed	
WLJ1612S_Reg_207	Adding 3 IOS AP to site and rebooting the AP	To add 3 IOS AP to site and applying the site reboot command and check if all the AP gets rebooted and joins the eWLC again	Passed	
WLJ1612S_Reg_208	Adding IOS AP to site and rebooting the AP with different AP modes	To add IOS AP to site and applying the site reboot command and check if the AP gets rebooted in all modes or not	Passed	
WLJ1612S_Reg_209	Adding 1810 AP to site and rebooting the AP with different AP modes	To add 1810 AP to site and applying the site reboot command and check if the AP gets rebooted in all modes or not	Passed	
WLJ1612S_Reg_210	Trying to reboot the AP with a non existing site name	To give the reboot command using site name with a non existing site name and check if the AP is rebooting or not .	Passed	
WLJ1612S_Reg_211	Trying to reboot the AP which is already rebooting using site reboot command	To reboot the AP using AP site reboot command which is already being rebooted .	Passed	
EWLCJ1612S_Reg_534	Creating a site tag in eWLC UI	To create a site tag in eWLC UI and check if the site tag is created or not.	Passed	
EWLCJ1612S_Reg_535	Creating a site tag in eWLC CLI	To create a site tag in eWLC CLI and check if the site tag is created or not.	Passed	

EWLCJ1612S_Reg_536	Mapping a AP profile to the site tag using eWLC UI	To map a AP profile to the site tag and check if the AP profile is mapped to site tag or not.	Passed	
EWLCJ1612S_Reg_537	Mapping a Site to AP in eWLC UI	To map a AP profile to the site tag and check if the AP profile is mapped to site tag or not.	Passed	
EWLCJ1612S_Reg_538	Adding one COS AP to site and rebooting the AP	To add one COS AP to site and applying the site reboot command and check if the AP gets reeboted	Passed	
EWLCJ1612S_Reg_539	Adding 3 COS AP to site and rebooting the AP	To add 3 COS AP to site and applying the site reboot command and check if all the AP gets reeboted and joins the eWLC again	Passed	
EWLCJ1612S_Reg_540	Adding COS AP to site and rebooting the AP with different AP modes	To add COS AP to site and applying the site reboot command and check if the AP gets rebooted in all modes or not	Passed	CSCvr63038
EWLCJ1612S_Reg_541	Adding one IOS AP to the site and rebooting the AP through AP site reset command	To add one IOS to the site creates and giving the AP reboot command through CLI to check if the AP gets rebooted or not.	Passed	
EWLCJ1612S_Reg_542	Adding 3 IOS AP to site and rebooting the AP	To add 3 IOS AP to site and applying the site reboot command and check if all the AP gets reeboted and joins the eWLC again	Passed	

EWLCJ1612S_Reg_543	Adding IOS AP to site and rebooting the AP with different AP modes	To add IOS AP to site and applying the site reboot command and check if the AP gets rebooted in all modes or not	Passed	
EWLCJ1612S_Reg_544	Adding 1810 AP to site and rebooting the AP with different AP modes	To add 1810 AP to site and applying the site reboot command and check if the AP gets rebooted in all modes or not	Passed	
EWLCJ1612S_Reg_545	Trying to reboot the AP with a non existing site name	To give the reboot comand using site name with a non existing site name and check if the AP is rebooting or not .	Passed	
EWLCJ1612S_Reg_546	Trying to reboot the AP which is already rebooting using site reboot command	To reboot the AP using AP site reboot command which is already being rebooted .	Passed	

SFTP Support

Logical ID	Title	Description	Status	Defect ID
WLJ1612S_Reg_313	eWLC Software updating via SFTP server	Verifying eWLC software updating or not via SFTP server	Passed	
WLJ1612S_Reg_314	Invalid eWLC Software updating via SFTP server	Verifying eWLC software updating or not via SFTP server	Passed	
WLJ1612S_Reg_315	eWLC .bin Software updating via SFTP server	Checking the eWLC .bin software updating or not via SFTP server	Passed	
WLJ1612S_Reg_316	eWLC .SSH Software updating via SFTP server	Checking the eWLC .bin software updating or not via SFTP server	Passed	

WLJ1612S_Reg_317	eWLC Software updating through Invalid SFTP IP	To check whether software is upgrading or not through Invalid SFTP IP	Passed	
WLJ1612S_Reg_318	eWLC Software updating through Invalid SFTP user name/password	Verifying eWLC software is upgrading or not through Invalid SFTP user name/password	Passed	
EWLCJ1612S_Reg_511	eWLC Software updating via SFTP server	Verifying eWLC software updating or not via SFTP server	Passed	
EWLCJ1612S_Reg_512	Invalid eWLC Software updating via SFTP server	Verifying eWLC software updating or not via SFTP server	Passed	
EWLCJ1612S_Reg_513	eWLC .bin Software updating via SFTP server	Checking the eWLC .bin software updating or not via SFTP server	Passed	
EWLCJ1612S_Reg_514	eWLC .SSH Software updating via SFTP server	Checking the eWLC .bin software updating or not via SFTP server	Passed	
EWLCJ1612S_Reg_515	eWLC Software updating through Invalid SFTP IP	To check whether software is upgrading or not through Invalid SFTP IP	Passed	
EWLCJ1612S_Reg_516	eWLC Software updating through Invalid SFTP user name/password	Verifying eWLC software is upgrading or not through Invalid SFTP user name/password	Passed	

New WLC 9800 support

Logical ID	Title	Description	Status	Defect ID
WLJ1612S_Reg_21	Configuring WLC9800 in Day0 mode with wired client	To verify the Day0 configuration of WLC3504 through wired client.	Passed	

WLJ1612S_Reg_22	Configuring WLC9800 in Day0 mode by connecting wireless client.	To verify the Day0 configuration of WLC3504 through wireless client.	Passed	
WLJ1612S_Reg_23	Checking AP joining to WLC	To verify the Aps are joining the WLC without any issues.	Passed	
WLJ1612S_Reg_24	Performing Ping test for Client connected to Day0 SSID	Verifying Ping test for client connected to Day0 SSID	Passed	
WLJ1612S_Reg_25	Connecting windows client with L2 security Open.	To verify the windows client connectivity with L2 Security Open.	Passed	
WLJ1612S_Reg_26	Connecting IOS client with L2 security Static WEP.	To verify the IOS client connectivity with L2 Security WEP.	Passed	
WLJ1612S_Reg_27	Connecting MACOs client with L2 Security - WPA/WPA2 + PSK	To verify the MACOs client connectivity with L2 Security WPA/WPA2 + PSK	Passed	
WLJ1612S_Reg_28	Connecting client with L2 Security - WPA/WPA2 + dot1x	To verify the client connectivity with L2 security WPA/WPA2+dot1x	Passed	
WLJ1612S_Reg_29	Connecting client with L2 Security CKIP	To verify the client connectivity with L2 security CKIP	Passed	
WLJ1612S_Reg_30	Connecting client with L3 security - WebAuth Internal	To verify the client connectivity with L3 security internal web authentication.	Passed	
WLJ1612S_Reg_31	Upgrading the WLC9800 to the latest build.	To verify the upgrading of WLC9800 to the latest build without any issues.	Passed	
WLJ1612S_Reg_32	Downgrading the WLC9800 to the previous version.	To verify the Downgrading of WLC9800 to the previous version without any issues.	Passed	

WLJ1612S_Reg_33	Upload/download config file from WLC.	To verify the config retain on upload/download the config file.	Passed	
WLJ1612S_Reg_34	Configuring HA between two CT9800	To verify the HA pair setup between the WLC9800.	Passed	
WLJ1612S_Reg_35	Checking AP SSO behavior when active WLC in down.	To verify the AP SSO when active WLC is down.	Passed	
WLJ1612S_Reg_36	Performing Intra-controller roaming for Android clients in WLC 3504	To check whether intra-controller roaming is successful or not for Android clients in WLC 3504	Passed	
WLJ1612S_Reg_37	Performing Intra-controller roaming for IOS clients in WLC 3504	To check whether intra-controller roaming is successful or not for IOS clients in WLC 3504	Passed	
WLJ1612S_Reg_38	Performing Intra-controller roaming for MAC OS clients in WLC 3504	To check whether intra-controller roaming is successful or not for MAC OS clients in WLC 3504	Passed	
WLJ1612S_Reg_39	Performing Intra-controller roaming for Windows JOS clients in WLC 3504	To check whether intra-controller roaming is successful or not for Windows JOS clients in WLC 3504	Passed	
WLJ1612S_Reg_40	Checking client connection when local switching is enabled	To verify client is connecting properly or not when local switching is enabled	Passed	
WLJ1612S_Reg_41	Performing client connecting with local authentication and local switching	To verify client is connecting properly when local authentication and local switching are enabled	Passed	

WLJ1612S_Reg_42	Verifying WLC 9800 is able to add in PI	To verify WLC 9800 is able to add in PI or not	Passed	
WLJ1612S_Reg_43	Changing AP mode from PI	To verify AP mode is able to change from PI or not	Passed	
WLJ1612S_Reg_44	Deploying template from PI	To verify template is deploying successfully or not	Passed	
WLJ1612S_Reg_45	Undeploying template from PI	To verify template is undeploying from PI or not	Passed	
WLJ1612S_Reg_46	Performing Day0 from PI	To verify WLC9800 is coming to day0 or not from PI	Passed	
WLJ1612S_Reg_47	Associating Android clients to a local switching enabled WLAN with Tunnel profile mapped	To check whether Android clients gets associated or not to 2800/3800 AP's with local switching enabled WLAN with EoGRE tunnel mapped in it	Passed	
WLJ1612S_Reg_48	Associating windows clients to TrustSec configured AP and checking the policy hit statistics in WLC UI	To verify the policy hit for Windows client after TrustSec configured on AP	Passed	
WLJ1612S_Reg_49	Configure URL ACL with permit action on the controller and connect the windows client	To verify whether clients get connected and redirect to permit URL	Passed	
WLJ1612S_Reg_50	Configure AVC profile and connect the clients	To verify whether clients get connected and AVC is applied	Passed	
WLJ1612S_Reg_51	Checking client connection when security type changed	To verify client is disconnecting or not when security type is changed	Passed	
WLJ1612S_Reg_52	Checking client connectivity when AP placed in AP group	To verify client connection when AP placed in AP group	Passed	

EWLCJ1612S_Reg_672	Configuring WLC9800 in Day0 mode with wired client	To verify the Day0 configuration of WLC3504 through wired client.	Passed	
EWLCJ1612S_Reg_673	Configuring WLC9800 in Day0 mode by connecting wireless client.	To verify the Day0 configuration of WLC3504 through wireless client.	Passed	
EWLCJ1612S_Reg_674	Checking AP joining to WLC	To verify the Aps are joining the WLC without any issues.	Passed	
EWLCJ1612S_Reg_675	Performing Ping test for Client connected to Day0 SSID	Verfying Ping test for client connected to Day0 SSID	Passed	
EWLCJ1612S_Reg_676	Connecting windows client with L2 security Open.	To verify the windows client connectivity with L2 Security Open.	Passed	
EWLCJ1612S_Reg_677	Connecting IOS client with L2 security Static WEP.	To verify the IOS client connectivity with L2 Security WEP.	Passed	
EWLCJ1612S_Reg_678	Connecting MACOs client with L2 Security - WPA/WPA2 + PSK	To verify the MACOs client connectivity with L2 Security WPA/WPA2 + PSK	Passed	
EWLCJ1612S_Reg_679	Connecting client with L2 Security - WPA/WPA2 + dot1x	To verify the client connectivity with L2 security WPA/WPA2+dot1x	Passed	
EWLCJ1612S_Reg_680	Connecting client with L2 Security CKIP	To verify the client connectivity with L2 security CKIP	Passed	
EWLCJ1612S_Reg_681	Connecting client with L3 security - WebAuth Internal	To verify the client connectivity with L3 security internal web authentication.	Passed	
EWLCJ1612S_Reg_682	Upgrading the WLC9800 to the latest build.	To verify the upgrading of WLC9800 to the latest build without any issues.	Passed	

EWLCJ1612S_Reg_683	Downgrading the WLC9800 to the previous version.	To verify the Downgrading of WLC9800 to the previous version without any issues.	Passed	
EWLCJ1612S_Reg_684	Upload/download config file from WLC.	To verify the config retain on upload/download the config file.	Passed	
EWLCJ1612S_Reg_685	Configuring HA between two CT9800	To verify the HA pair setup between the WLC9800.	Passed	
EWLCJ1612S_Reg_686	Checking AP SSO behavior when active WLC in down.	To verify the AP SSO when active WLC is down.	Passed	
EWLCJ1612S_Reg_687	Performing Intra-controller roaming for Android clients in WLC 3504	To check whether intra-controller roaming is successful or not for Android clients in WLC 3504	Passed	
EWLCJ1612S_Reg_688	Performing Intra-controller roaming for IOS clients in WLC 3504	To check whether intra-controller roaming is successful or not for IOS clients in WLC 3504	Passed	
EWLCJ1612S_Reg_689	Performing Intra-controller roaming for MAC OS clients in WLC 3504	To check whether intra-controller roaming is successful or not for MAC OS clients in WLC 3504	Passed	
EWLCJ1612S_Reg_690	Performing Intra-controller roaming for Windows JOS clients in WLC 3504	To check whether intra-controller roaming is successful or not for Windows JOS clients in WLC 3504	Passed	
EWLCJ1612S_Reg_691	Checking client connection when local switching is enabled	To verify client is connecting properly or not when local switching is enabled	Passed	

EWLCJ1612S_Reg_692	Performing client connecting with local authentication and local switching	To verify client is connecting properly when local authentication and local switching are enabled	Passed	
EWLCJ1612S_Reg_693	Verfying WLC 9800 is able to add in PI	To verify wlc 9800 is able to add in PI or not	Passed	
EWLCJ1612S_Reg_694	Changing AP mode from PI	To verify AP mode is able to change from PI or not	Passed	
EWLCJ1612S_Reg_695	Deploying template from PI	To verify template is deploying successfully or not	Passed	
EWLCJ1612S_Reg_696	Undeplying template from PI	To verify template is undeploying from PI or not	Passed	
EWLCJ1612S_Reg_697	Performing Day0 from PI	To verify WLC9800 is coming to day0 or not from PI	Passed	
EWLCJ1612S_Reg_698	Associating Android clients to a local switching enabled WLAN with Tunnel profile mapped	To check whether Android clients gets associated or not to 2800/3800 AP's with local switching enabled WLAN with EoGRE tunnel mapped in it	Passed	
EWLCJ1612S_Reg_699	Associating windows clients to TrustSec configured AP and checking the policy hit statistics in WLC UI	To verify the policy hit for Windows client after Trustsec configured on AP	Passed	
EWLCJ1612S_Reg_700	Configure URL ACL with permit action on the controller and connect the windows client	To verify whether clients get connected and redirect to permit URL	Passed	
EWLCJ1612S_Reg_701	Configure AVC profile and connect the clients	To verify whether clients get connected and AVC is applied	Passed	

EWLCJ1612S_Reg_702	Checking client connection when security type changed	To verify client is disconneting or not when security type is changed	Passed	
EWLCJ1612S_Reg_703	Checking client connectivity when AP placed in AP group	To verify client connection when AP placed in AP group	Passed	

CME

Captive Portal with Email address and Web Consent

Logical ID	Title	Description	Status	Defect ID
MEJ810S_Reg_271	Configuring the Email address in Internal /External splash page and associating different types clients to a W LAN	To check whether JOS client gets associated successfully or not to a W LAN in which captive portal enabled as Internal splash page with m AP ping username as Email address	Passed	
MEJ810S_Reg_272	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	
MEJ810S_Reg_273	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	

MEJ810S_Reg_274	Making all clients as blacklist and checking the association of the clients to a W LAN	To check whether blacklisted clients associating or not to a WLAN in which captive portal enabled with access type as Email address.	Passed	
MEJ810S_Reg_275	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	

TLS Tunnel

Logical ID	Title	Description	Status	Defect ID
MEJ810S_Reg_71	Associating Windows JOS Client with WPA2-dot1x using ISE server in cloud via TLS Tunnel	To verify whether Windows JOS client associated successfully or not with WPA2-dot1x via ISE server configured in cloud	Passed	
MEJ810S_Reg_72	Associating iOS Client with WPA2-dot1x using ISE server in cloud via TLS Tunnel	To verify whether APPLE iOS client associated successfully or not with WPA2-dot1x via ISE server configured in cloud	Passed	
MEJ810S_Reg_73	Associating MAC OS Client with WPA2-dot1x using ISE server in cloud via TLS Tunnel	To verify whether MAC OS client associated successfully or not with WPA2-dot1x via ISE server configured in cloud	Passed	

MEJ810S_Reg_74	Associating Android Client with WPA2-dot1x using ISE server in cloud via TLS Tunnel	To verify whether Android client associated successfully or not with WPA2-dot1x via ISE server configured in cloud	Passed	
MEJ810S_Reg_75	Allowing the user for complete access to CME network via TACACS (ISE server configured in cloud)	To check whether user can able to read-write access the complete CME network or not via TACACS (ISE server configured in cloud)	Passed	
MEJ810S_Reg_76	Associating all OS clients to CME with Security MAC filtering via Cloud ISE server	To check whether all OS clients associated successfully or not to CME with Mac filtering via Cloud ISE server	Passed	
MEJ810S_Reg_77	Setting up the tunnel configurations in CME	To check whether tunnel status get UP or not after configuring in CME	Passed	
MEJ810S_Reg_78	Checking the ME association with PI after establishing TLS tunnel	To check whether ME is getting synchronized or not with PI	Passed	
MEJ810S_Reg_79	Checking the TLS Tunnel configurations after export/import the config file via TFTP	To check whether TLS Tunnel configurations gets retained or not while export/import the config file via TFTP	Passed	
MEJ810S_Reg_80	Checking the RADIUS server's reachability from CME	To check whether cloud RADIUS server is reachable or not from CME using Ping functionality/username in troubleshooting tools page	Passed	

TACACS

Logical ID	Title	Description	Status	Defect ID
MEJ810S_Reg_191	Allowing the user for complete access to CME network via TACACS	To check whether user can able to read-write access the complete CME network or not via TACACS	Passed	
MEJ810S_Reg_192	Providing the user for lobby admin access to the CME via TACACS	To check whether user can able to have lobby admin access or not to CME via TACACS	Passed	
MEJ810S_Reg_193	Providing the user for monitoring access to the CME via TACACS	To check whether user can able to have monitoring access (which is read-only) or not to CME via TACACS	Passed	
MEJ810S_Reg_194	Trying to login CME via TACACS with invalid credentials	To check whether user can able to login or not in CME via TACACS with invalid credentials	Passed	
MEJ810S_Reg_195	Verifying the auth server TACACS through CME CLI	To check whether auth server added or not to the TACACS from CME CLI.	Passed	
MEJ810S_Reg_196	Providing the user for selected access to the CME via TACACS	To check whether user can able to have access with the selected checkbox's like "WLAN " and "Controller" checkboxes.	Passed	
MEJ810S_Reg_197	Providing the user for selected access to the CME via TACACS	To check whether user can able to have access with the selected checkbox's like "Wireless" and "Security" checkboxes.	Passed	

MEJ810S_Reg_198	Providing the user for selected access to the CME via TACACS	To check whether user can able to have access with the selected checkbox's like "Command" and "Management" checkboxes.	Passed	
MEJ810S_Reg_199	Providing the user for selected access to the CME via TACACS	To check whether user can able to have access with the selected checkbox's like" WLAN, Controller,Wireless,Security,Command and "Management" checkboxes.	Passed	
MEJ810S_Reg_200	Trying to login CME network via TACACS with Invalid credentials.	To verify whether user can able to login or not in CME via TACACS with invalid credentials	Passed	

Client Auth Failures(AAA Failures/WLC Failures)

Logical ID	Title	Description	Status	Defect ID
MEJ810S_Reg_289	Client connectivity with WPA2 personal security with Wrong credentials .	To verify if the client connects to W LAN with WPA2 personal security or not with the Wrong credentials.	Passed	
MEJ810S_Reg_290	Configuring Client Idle timeout/Session timeout for a particular W LAN and check if the timeout works properly.	To configure Client ideal Timeout/Session timeout and check if the timeout for the client works .	Passed	
MEJ810S_Reg_291	Configuring Maximum no. of client connections to be accepted for a particular W LAN .	To configure maximum number of clients to a particular W LAN and check if only the configured number of clients gets connected to the W LAN	Passed	

MEJ810S_Reg_292	Configuring Maximum 802.1x session initiation per AP at a time	To configure Maximum 802.1x session per AP and connecting a client to it and check if the only the particular clients with 802.1x auth gets connected.	Passed	
MEJ810S_Reg_293	Connecting a client with WPA2 enterprises security with incorrect credentials and debugging the client for errors .	To provide wrong credentials for the client and check if the clients gets connected or not.	Passed	
MEJ810S_Reg_294	Connecting a JOS/Android/MAC Client with WPA2 enterprises security and debugging the client for errors .	To verify that JOS/Android/MAC client connect successfully with WPA2 enterprises or not	Passed	
MEJ810S_Reg_295	Connecting 2 different Android Client with WPA2 enterprises security and debugging the client for errors and performing the PING test	To verify that 2 different Android clients connected and pinging each other with different WPA2 enterprises or not	Passed	
MEJ810S_Reg_296	Connecting a Client with WPA2 enterprises with Local Authentication (AP) and debugging the client for errors .	To verify that client connect successfully to W LAN with WPA2 enterprises and Local Authentication or not	Passed	
MEJ810S_Reg_297	Client connectivity with WPA2 personal security with Mac Filtering	To Connect a client with WPA2 personal with MAC filtering enabled and Whitelisting the clients MAC address.	Passed	

MEJ810S_Reg_298	Client connectivity with WPA2 personal security with Mac Filtering with Black list	To Connect a client with WPA2 personal with MAC filtering enabled and Black listing the clients MAC address.	Passed	
MEJ810S_Reg_299	Connecting a client through Guest with Internal Splash page Network through AAA server.	To Connect a client to a Guest Network using a AAA server and check if the client gets connected to it	Passed	
MEJ810S_Reg_300	Connecting a client through Guest with External Splash page Network through AAA server.	To Connect a client to a Guest Network using a AAA server and check if the client gets connected to it	Passed	

SNMP trap Reciver

Logical ID	Title	Description	Status	Defect ID
MEJ810S_Reg_65	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 G UI	Passed	
MEJ810S_Reg_66	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 G UI	Passed	
MEJ810S_Reg_67	Checking the validation of SNMP trap receiver information.	To check whether the SNMP trap receiver is received the information or not.	Passed	
MEJ810S_Reg_68	Verifying the severity filtering for SNMP trap receiver information.	To verify the severity filtering for SNMP trap receiver information.	Passed	

MEJ810S_Reg_69	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	
MEJ810S_Reg_70	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	

Master AP Failover Issues

Logical ID	Title	Description	Status	Defect ID
MEJ810S_Reg_536	Changing the next preferred ME capable AP to Controller from UI	To verify whether Next preferred Master AP can changing the ME or not by using the UI	Passed	
MEJ810S_Reg_537	Changing the next preferred ME capable AP to Controller from CLI	To verify whether Next preferred Master AP can changing the ME or not by using the CLI	Passed	
MEJ810S_Reg_538	Making the More than 5 AP s to ME capable	To verify whether more than 5 AP s are changing the state to ME c AP able or not	Passed	
MEJ810S_Reg_539	Deleting the Master Prepared AP from CLI	To verify whether Master preferred AP is deleting from CLI or not	Passed	
MEJ810S_Reg_540	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	
MEJ810S_Reg_541	Assigning the Global AP Configurations	To verify whether Global AP Configurations authenticate to the AP or not	Passed	

Hotspot 2.0

Logical ID	Title	Description	Status	Defect ID
MEJ810S_Reg_201	Configuring WLAN with WPA, 802.1x authentication policy in ME 1852/1832 AP	Verifying that user is able to configure WLAN with WPA, 802.1x authentication policy or not	Passed	
MEJ810S_Reg_202	Connecting IOS client via hotspot 2.0	Verifying that user is able to connect IOS client via hotspot 2.0 or not	Passed	
MEJ810S_Reg_203	Verifying that client is connecting automatically without asking credentials even when client come under coverage area of W LAN	To check whether the client comes under coverage area or not without asking credentials	Passed	
MEJ810S_Reg_204	Verifying that hotspot 2.0 config same after uploading the exported config file	To check hotspot 2.0 config same after uploading the exported config file	Passed	
MEJ810S_Reg_205	Try to disable WPA on Hotspot enabled WLAN	Verifying that user is able to disable WPA on Hotspot enabled WLAN or not	Passed	
MEJ810S_Reg_206	Trying to config Passpoint on guset-LAN	Verifying that user is able to config Passpoint on guest-LAN or not	Passed	
MEJ810S_Reg_207	Verifying that user is able to edit or delete the 802.11u and HS 2.0 parameter via CLI and G UI or not	Checking that user is able to edit or delete the 802.11u and HS 2.0 parameter via CLI and GUI or not	Passed	
MEJ810S_Reg_208	Try to enable hotspot on open/Guest network	Verifying that user is able to enable hotspot on open network or not	Passed	

MEJ810S_Reg_209	Validating the client using WAN and client Downlink Load by enabling Hotspot 2.0	Verifying the client using WAN Downlink Load by enabling Hotspot 2.0	Passed	
MEJ810S_Reg_210	Validating the client using WAN and client Uplink Load by enabling Hotspot 2.0	Verifying the client using WAN Uplink Load by enabling Hotspot 2.0	Passed	
MEJ810S_Reg_211	Assigning the venue group and venue type for the specific AP on 802.11u	Providing the venue group and venue type for the specific AP on 802.11u	Passed	

Mac filtering (for L2 security)

Logical ID	Title	Description	Status	Defect ID
MEJ810S_Reg_56	Adding Windows (7,10) Client mac address in CME and checking the connection of Clients in 1800 Series ME	To add the windows Client mac address in mac filtering in CME and checking whether Clients gets associated or not successfully in 1800 Series ME	Passed	
MEJ810S_Reg_57	Uploading the empty CSV file in ME UI	To check whether an b LAN k CSV file could be uploaded in ME UI	Passed	
MEJ810S_Reg_58	Importing the .CSV file with modifications in ME	To check whether .CSV file gets imported or not after importing the updated file with some changes in it	Passed	
MEJ810S_Reg_59	Connecting the Client with WLAN security mac filtering + WPA personal	To Connect the Client with WLAN security mac filtering + WPA personal	Passed	
MEJ810S_Reg_60	Connecting the Client with WLAN security mac filtering + WPA enterprise	To Connect the Client with WLAN security mac filtering + WPA enterprise	Passed	

MEJ810S_Reg_61	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	
MEJ810S_Reg_62	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	
MEJ810S_Reg_63	Connecting the client after client identity account expired in ISE	To Connect the Client after client identity account expired in ISE	Passed	
MEJ810S_Reg_64	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	

Intra/Inter WLC Roaming Failures(Ping Pong Issues)

Logical ID	Title	Description	Status	Defect ID
MEJ810S_Reg_14	Intra Controller Roaming with Open Security	To verify whether Client is Roaming with Open Security or not between APs	Passed	
MEJ810S_Reg_15	Intra Controller Roaming with WPA2 Security	To verify whether Client is Roaming with WPA2 Security or not between APs	Passed	
MEJ810S_Reg_16	Intra Controller Roaming with WPA Enterprise + Radius server Security	To verify whether Client is Roaming with WPA Enterprise + RadiOS Security or not between APs	Passed	

MEJ810S_Reg_17	Intra Controller Roaming with WPA Enterprise + AP Security	To verify whether Client is Roaming with WPA Enterprise + AP Security or not between APs	Passed	
MEJ810S_Reg_18	Intra Controller Roaming with WPA2+Mac-filtering	To verify whether Client is Roaming with WPA2+ Mac-filtering security or not between APs	Passed	
MEJ810S_Reg_19	Intra Controller Roaming with Guest Network+Mac-filtering	To verify whether Client is Roaming with Guest Network+Mac-filtering security or not between AP s	Passed	
MEJ810S_Reg_20	Intra Controller Roaming with Guest Network in Internal splash page+Local user account	To verify whether Client is Roaming in Guest Network with Internal splash page+Local user account or not	Passed	
MEJ810S_Reg_21	Intra Controller Roaming with Guest Network in Internal splash page+Web consent	To verify whether Client is Roaming in Guest Network with Internal splash page+Web consent	Passed	
MEJ810S_Reg_22	Intra Controller Roaming with Guest Network in Internal splash page+Email address	To verify whether Client is Roaming in Guest Network with Internal splash page+Email address	Passed	
MEJ810S_Reg_23	Intra Controller Roaming with Guest Network in Internal splash page+Radius server	To verify whether Client is Roaming in Guest Network with Internal splash page+Radius server	Passed	
MEJ810S_Reg_24	Intra Controller Roaming with Guest Network in Internal splash page+WPA2 personal	To verify whether Client is Roaming in Guest Network with Internal splash page+WPA2 personal	Passed	

MEJ810S_Reg_25	Intra Controller Roaming with Guest Network in CMX Connect	To verify whether Client is Roaming in Guest Network with CMX Connect or not	Passed	
MEJ810S_Reg_26	Intra Controller Roaming with Guest Network in External splash page+Local user account	To verify whether Client is Roaming in Guest Network with External splash page+Local user account	Passed	
MEJ810S_Reg_27	Intra Controller Roaming with Guest Network in External splash page+Web consent	To verify whether Client is Roaming in Guest Network with External splash page+Web consent	Passed	
MEJ810S_Reg_28	Intra Controller Roaming with Guest Network in External splash page+Email address	To verify whether Client is Roaming in Guest Network with External splash page+Email address	Passed	
MEJ810S_Reg_29	Intra Controller Roaming with Guest Network in External splash page+Radius server	To verify whether Client is Roaming in Guest Network with External splash page+Radius server	Passed	
MEJ810S_Reg_30	Intra Controller Roaming with Guest Network in External splash page+WPA personal	To verify whether Client is Roaming in Guest Network with External splash page+WPA2 personal	Passed	

NAT

Logical ID	Title	Description	Status	Defect ID
MEJ810S_Reg_522	Configuring the Central-NAT configuration at DHCP Scope level	To verify whether Central-NAT Configuration AP plied successfully or not	Passed	
MEJ810S_Reg_523	Associating the DHCP Scope to W LAN	To verify whether DHCP Scope is associate the W LAN or not	Passed	

MEJ810S_Reg_524	Peer-to-peer blocking the configuration on DHCP through CLI	To verify whether Peer-to-peer blocking AP plied successfully or not	Passed	
MEJ810S_Reg_525	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	
MEJ810S_Reg_526	Configuring the NAT functionality in radio 5GHZ band AP	To verify whether NATing working or not in 5 GHZ radio band	Passed	
MEJ810S_Reg_527	Checking Client performance in Monitoring page after client connect	To verify whether Client performance is showing or not in monitoring page	Passed	
MEJ810S_Reg_528	Checking the Connection and event log after client connect	To verify whether Connection showing properly or not	Passed	
MEJ810S_Reg_529	Checking the NAT configuration with invalid DHCP parameters	To verify whether NAT configured for invalid DHCP scope	Passed	

Application visibility control

Logical ID	Title	Description	Status	Defect ID
MEJ810S_Reg_212	Drop/mark the different types of social application for the connected clients to the created AVC profile	To confirm whether the particular Facebook application is been dropped/marked	Passed	
MEJ810S_Reg_213	Gmail application and Drop/mark action to the created AVC for JSSID MAC OS	Verifying the Gmail application is dropped/marked or not after created JSSID client connecting	Passed	

MEJ810S_Reg_214	Mark the Gmail application for the MAC OS to the created AVC profile by specifying Custom value	To check for the Gmail application DSCP values can be changed or not	Passed	
MEJ810S_Reg_215	Configuring the custom value for Gmail application with JSSID MAC OS	verify whether custom value is assigned or not for Gmail application	Passed	
MEJ810S_Reg_216	Drop/mark the cisco-jabber-im application for the MAC OS to the created AVC profile	To confirm whether the particular cisco-jabber-im application is been dropped/marked	Passed	
MEJ810S_Reg_217	Drop/Mark the APPLE -iOS-updates for the MAC OS clients to the created AVC profile	To confirm whether the particular APPLE-iOS-updates AP plication is been dropped/Marked.	Passed	
MEJ810S_Reg_218	APPLE -iOS-updates application with Drop/mark action for JSSID to the created AVC	Verify whether Drop/Mark action is configured or not for APPLE -iOS-updates application	Passed	
MEJ810S_Reg_219	configure the custom value with mark action for APPLE-services with JSSID	Verify whether customer value is configured or not for APPLE-services	Passed	
MEJ810S_Reg_220	configure the Drop/mark action for amazon-instant-video application to the created AVC profile	To confirm whether the particular amazon-instant-video application is been dropped/marked	Passed	
MEJ810S_Reg_221	Drop/mark the amazon-instant-video application for JSSID to the created AVC profile	Validating the amazon-instant-video application is dropped/marked or not after connecting JSSID with different OS clients	Passed	

MEJ810S_Reg_222	Drop/mark the google-services application for JSSID to the created AVC profile	Validating the google-services application is dropped/marked or not after connecting JSSID with different OS clients	Passed	
MEJ810S_Reg_223	Drop/mark the Instagram application for JSSID to the created AVC profile	Validating the Instagram application is dropped/marked or not after connecting JSSID with different OS clients	Passed	
MEJ810S_Reg_224	Configure the Drop/mark action for monster-com application to the created AVC profile	To confirm whether the particular monster-com application is been dropped/marked	Passed	
MEJ810S_Reg_225	Drop/mark the monster-com application for JSSID to the created AVC profile	Validating the monster-com application is dropped/marked or not after connecting JSSID with different OS clients	Passed	
MEJ810S_Reg_226	Drop/mark theny-daily-news application for JSSID to the created AVC profile	Validating the ny-daily-news appilication is droped/marked or not after connecting JSSID with different OS clients	Passed	

Internal DHCP Server

Logical ID	Title	Description	Status	Defect ID
MEJ810S_Reg_330	M AP ping a Internal DHCP pool to WLAN and verifying Windows Client IP Address and v LAN id	To verify whether a window client get IP address and v LAN id from a specified DHCP pool or not	Passed	

MEJ810S_Reg_331	M AP ping a Internal DHCP pool to WLAN and verifying Android Client IP Address and v LAN id	To verify whether a Android client get IP address and v LAN id from a specified DHCP pool or not	Passed	
MEJ810S_Reg_332	M AP ping 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	
MEJ810S_Reg_333	M AP ping a Internal DHCP pool to W LAN 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	
MEJ810S_Reg_334	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	

DNS Based ACL Rules

Logical ID	Title	Description	Status	Defect ID
MEJ810S_Reg_128	Create URL ACL rule with guest network WLAN	To verify that URL ACL created with guest network	Passed	
MEJ810S_Reg_129	Configure guest network with captive portal Internal Splash Page - local user account and checking URL ACL rule by connecting Window JOS client	To verify that Window client connect successfully with guest network with captive portal Internal Splash Page , Access type local user account and URL ACL rule deny	Passed	

MEJ810S_Reg_130	Configure guest network with captive portal Internal Splash Page-Radius server and checking URL ACL rule by connecting Window JOS client	To verify that Window client connect successfully with guest network with captive portal Internal Splash Page , Access type radius server and URL ACL rule Permit	Passed	
MEJ810S_Reg_131	Configure guest network with captive portal Internal Splash Page-Radius server and checking URL ACL rule by connecting iOS client	To verify that iOS client connect successfully with guest network with captive portal Internal Splash Page , Access type radius server and URL ACL rule deny	Passed	
MEJ810S_Reg_132	Configure guest network with captive portal Internal Splash Page-local user account and checking URL ACL rule by connecting iOS client	To verify that iOS client connect successfully with guest network with captive portal Internal Splash Page , Access type local user account and URL ACL rule deny	Passed	
MEJ810S_Reg_133	Configure guest network with captive portal Internal Splash Page-WPA2 personal and checking URL ACL rule with permit by connecting Android client	To verify that Android client connect successfully with guest network with captive portal Internal Splash Page , Access type WPA2 Per and URL ACL rule deny	Passed	
MEJ810S_Reg_134	Configure guest network with captive portal External Splash page-local user account and checking URL ACL rule by connecting Window client	To verify that Window client connect successfully with guest network with captive portal External Splash Page , Access type local user account and URL ACL rule deny	Passed	

MEJ810S_Reg_135	Configure guest network with captive portal External Splash page-local user account and checking permit URL ACL rule by connecting Android client	To verify that Android client connect successfully with guest network with captive portal External Splash Page , Access type local user account and URL ACL rule Permit	Passed	
MEJ810S_Reg_136	Configure guest network with captive portal External Splash page-Radius sever and checking deny URL ACL rule by connecting iOS client	To verify that iOS client connect successfully with guest network with captive portal External Splash Page , Access type radius Server and URL ACL rule deny	Passed	
MEJ810S_Reg_137	Configure guest network with captive portal CMX Connect and checking deny URL ACL rule by connecting Android client	To verify that Android client connect successfully with guest network with captive portal CMX Connect and URL ACL rule deny	Passed	
MEJ810S_Reg_138	Configure guest network with captive portal CMX Connect and checking Permit URL ACL rule by connecting iOS client	To verify that iOS client connect successfully with guest network with captive portal CMX Connect and URL ACL rule Permit	Passed	
MEJ810S_Reg_139	Configure guest network with captive portal Internal Splash Page-WPA Personal Mac Filtering enabled and checking URL ACL rule by connecting Window JOS client	To verify that Window JOS client connect successfully with guest network with captive portal Internal Splash Page-WPA Personal Mac Filtering enabled and URL ACL rule Permit	Passed	

CME Crashes

Logical ID	Title	Description	Status	Defect ID
MEJ810S_Reg_01	Creating the DHCP scope form CLI with invalid IP address	To verify whether DHCP scope is created or not with invalid IP address form CLI	Passed	
MEJ810S_Reg_02	Changing the DHCP scope default gateway from Network to Mobility Express	To verify whether DHCP scope default gateway changing from Network to Mobility Express or not	Passed	
MEJ810S_Reg_03	Changing the RRM details after client connected to WLAN	To verify whether DHCP going to Crash or not after changing the RRM details	Passed	
MEJ810S_Reg_04	Enabling/Disabling the Central NAT	To verify whether Central NAT enabling/Disabling without any issues or not	Passed	
MEJ810S_Reg_05	Creating more than 10 DHCP scopes and assign to different WLANs	To verify whether more than 10 DHCP scopes are created and assigned to WLAN without any issues or not	Passed	
MEJ810S_Reg_06	Assigning the DHCP scope to W LAN with Mobility Express	To verify whether DHCP scope assigned to the W LAN or not with mobility capable DHCP	Passed	
MEJ810S_Reg_07	Clearing the Controller Configurations	To verify whether Controller Configurations are clearing or not	Passed	
MEJ810S_Reg_08	Export/Import the Controller Configurations	To verify whether Controller Configurations are Exporting/Importing or not	Passed	

MEJ810S_Reg_09	Migrate the Cisco Mobility express deployment	To verify whether AP can be migrating to new controller or not	Passed	
MEJ810S_Reg_10	Downloading the support bundle from Controller	To verify whether Support bundle downloading successfully or not	Passed	
MEJ810S_Reg_11	Invalid DNS server IP address configuration	To verify whether DNS IP address field accepting the Invalid IP address or not	Passed	
MEJ810S_Reg_12	Checking the Radius/ping response	To verify whether Radius/ping response is Applying successfully or not	Passed	
MEJ810S_Reg_13	Performing the all tests	To verify whether all tests are performing or not	Passed	

Rogue AP

Logical ID	Title	Description	Status	Defect ID
MEJ810S_Reg_170	Configuring the rogue AP rule in CME via CLI	To verify that user is able to configure the rogue AP rule in CME via CLI or not	Passed	
MEJ810S_Reg_171	Enabling/disabling rogue detection on CME CLI	To verify that user is able to enable/disable rogue detection on CME or not	Passed	
MEJ810S_Reg_172	Classifying the rogue Client on CME after Client connect	To verify that user is able to classify rogue Client on CME or not	Passed	
MEJ810S_Reg_173	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	

MEJ810S_Reg_174	Verifying the special character names rogue devices	To verifying that special character names rogue devices are appearing under rogue AP or not	Passed	
MEJ810S_Reg_175	After appearing the rogue AP in CME , Updating the their class	To verifying that user is able to update the rogue APs class or not	Passed	
MEJ810S_Reg_176	Manual mitigation of rogue device	Verify that user is able to manually mitigate the rogue AP or not	Passed	
MEJ810S_Reg_177	Auto mitigation of rogue device	Verify that user is able to auto mitigate the rogue AP or not	Passed	
MEJ810S_Reg_178	Classifying the rogue Adhoc on CME	Verify that user is able to classify rogue Adhoc on CME or not	Passed	
MEJ810S_Reg_179	Deleting the specific rogue AP or all rogue from CME	Verify that user is able to delete the rogue specific rogue AP or all rogue AP from CME or not	Passed	

Access Control List

Logical ID	Title	Description	Status	Defect ID
MEJ810S_Reg_227	Creating the ACL name with Duplicate name	To verify whether ACL name is created with existing name or not	Passed	
MEJ810S_Reg_228	Applying the ACL rule with Ingress and egress values	To verify whether ingress and Egress rule is applied to ACL or not	Passed	
MEJ810S_Reg_229	Creating the ACL rule for Specified source address with Permit/Deny action	To verify whether ACL rule is applied to the specified source address with Permit/Deny action or not	Passed	

MEJ810S_Reg_230	Creating the ACL rule for Specified destination address with Permit/Deny action	To verify whether ACL rule is applied to the specified destination address with Permit/Deny action or not	Passed	
MEJ810S_Reg_231	Creating ACL rule with specific Protocol for Permit rule	To verify whether ACL rule with specific Protocol for Permit rule is applied successfully or not	Passed	
MEJ810S_Reg_232	Creating ACL rule with specific DSCP for Deny rule	To verify whether ACL rule is creating with specific DSCP for Deny rule or not	Passed	
MEJ810S_Reg_233	Creating ACL rule with specific DSCP for Permit rule	To verify whether ACL rule is creating with specific DSCP for Permit rule or not	Passed	
MEJ810S_Reg_234	Creating the ACL name with special characters through CLI	To verify whether ACL name is creating with special characters or not	Passed	
MEJ810S_Reg_235	Adding the action to the ACL rule through CLI	To verify whether ACL action is AP plied successfully or not through CLI	Passed	
MEJ810S_Reg_236	Changing the Protocol from one to another	To verify whether Protocols are changing from one to another or not	Passed	
MEJ810S_Reg_237	AP plying the ACL rule with Protocol TCP/UDP enabled in source	To verify whether ACL rule with protocol TCP/UDP is AP plying at the source filed or not	Passed	
MEJ810S_Reg_238	AP plying the ACL rule with Protocol TCP/UDP enabled in destination	To verify whether ACL rule with protocol TCP/UDP is AP plying at the Destination filed or not	Passed	

CMX 10.5 Support

Logical ID	Title	Description	Status	Defect ID
MEJ810S_Reg_160	Adding Cisco CME to CMX	To add a Cisco CME to CMX and check if the CME gets added to the CMX with the CME status showing	Passed	
MEJ810S_Reg_161	Importing maps from prime infrastructure	To import maps from prime infrastructure and check if the m APs gets imported to the cmx .	Passed	
MEJ810S_Reg_162	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	
MEJ810S_Reg_163	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	
MEJ810S_Reg_164	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	
MEJ810S_Reg_165	Using MAC address the Client devices are searched	To check whether Client device can be searched by specifying its MAC address or not	Passed	
MEJ810S_Reg_166	Using IP address the Client devices are searched	To check whether Client device can be searched by specifying its IP address or not	Passed	

MEJ810S_Reg_167	Using SSID the Client devices are searched	To verify whether Client device can be searched by specifying the SSID or not	Passed	
MEJ810S_Reg_168	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	
MEJ810S_Reg_169	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
MEJ810S_Reg_301	Transferring the data via HTTP between IOS client with fast lane enabled AP p	Transferring the traffic between two IOS client with fast lane coverage	Passed	
MEJ810S_Reg_302	Validate the application library scenarios by adding applications in the Ixchariot	To validate the application in the Ixchariot library and check the output of each library	Passed	
MEJ810S_Reg_303	Transferring the data via UDP and measure the throughput between Windows and IOS client with fast LAN e enabled W LAN	Verify that user is able to transfer the data via UDP and measure the throughput between IOS and non IOS client with fast LAN e enabled W LAN	Passed	
MEJ810S_Reg_304	Measuring the throughput of TCP packets between client	To measure throughput of TCP packet transfer between client	Passed	

MEJ810S_Reg_305	Connecting the IOS and Android/Windows/Mac client with flexconnect mode AP and performe UDP perfomance test	Testing the UDP performance between different client that associated with flexconnect mode AP	Passed	
MEJ810S_Reg_306	Connecting the client with flexconnect mode AP and perform the measure the TCP performance	Testing the TCP performance between different client that associated with flexconnect mode AP	Passed	
MEJ810S_Reg_307	Connecting the IOS client with fast lane coverage W LAN and test the FaceTime AP p throughput	Measure the performance of FaceTime AP with fast lane coverage	Passed	
MEJ810S_Reg_308	Connecting a client and stream a video file and check the performance of the client using IXchariot	To stream a video from the client and check if the streaming occurs without any lag in performance using the IX chariot	Passed	
MEJ810S_Reg_309	Connecting a client continuously to the same WLAN by disconnecting and connecting	To connect the same client to the same WLAN by connecting and disconnecting continuously and check the behavior .	Passed	
MEJ810S_Reg_310	Throughput test using the 5 GHz radio using Ixchariot for 2 to 3 hours	To test the throughput of the 5 GHz radio using Ixchariot for a period of 2 to 3 hours	Passed	
MEJ810S_Reg_311	Throughput test using the 2.4 GHz radio using Ixchariot for 2 to 3 hours	To test the throughput of the 2.4 GHz radio using Ixchariot for a period of 2 to 3 hours	Passed	

MEJ810S_Reg_312	Configuring session timeout for the client and monitoring the client activity	To configure the session timeout for the clients and monitoring the client activity .	Passed	
MEJ810S_Reg_313	Checking the RSSI values after client connect to the W LAN near to AP	To verify whether RSSI values are showing properly or not after client connected to the W LAN	Passed	
MEJ810S_Reg_314	Checking the RSSI values after client connect to the W LAN with certain range	To verify whether Client is showing the proper RSSI details or not	Passed	
MEJ810S_Reg_315	Performing the PING test after client connect	To verify whether PING test is performing or not after client connect	Passed	
MEJ810S_Reg_316	Capturing the TCP Packets after Client connected to W LAN	To verify whether TCP Packets are transferring or not after client connect	Passed	
MEJ810S_Reg_317	Capturing the UDP Packets after client connect to W LAN	To verify whether UDP packets are transferring or not	Passed	
MEJ810S_Reg_318	Performing the FTP operation after client connected to W LAN	To verify whether FTP operation is performing or not	Passed	

AP 4800 support

Logical ID	Title	Description	Status	Defect ID
MEJ810S_Reg_450	Making the 4800 AP as ME controller	To verify whether 4800 AP is coming as ME controller or not	Passed	
MEJ810S_Reg_451	Checking MC2UC traffic when clients connected with different securities in 4800 ME	Verifying MC2UC traffic for clients connected with different securities in 4800 ME	Passed	

MEJ810S_Reg_452	Checking mDNS services are applied to MacOS and IOS with W LAN WPA2 personal security in 4800 ME	Verifying mDNS services are applied to MacOS and IOS with WPA2 personal security	Passed	
MEJ810S_Reg_453	Checking the Roaming between APs	To verify whether Roaming successfully happening or not in 4800 ME	Passed	
MEJ810S_Reg_454	Creating W LAN with Guest security and connecting clients	To verify whether client is connecting with Guest security or not	Passed	
MEJ810S_Reg_455	Creating the W LAN with WPA2 Enterprise	To verify whether client is able to connect W LAN with enterprise or not	Passed	
MEJ810S_Reg_456	Downgrading the 4800 ME controller with old image using http/TFTP/ftp	To verify whether 4800 ME Controller downgrading with old version or not	Passed	
MEJ810S_Reg_457	Updating the 4800 ME Controller with latest image using http/TFTP/ftp	To verify whether 4800 ME Controller upgrading with latest version or not	Passed	
MEJ810S_Reg_458	Rebooting the 4800 ME controller and checking the configurations	To check whether 4800 ME controller configuration are showing proper or not after reboot	Passed	
MEJ810S_Reg_459	Disabling the 802.11 radiOS and checking the SSID broadcasting or not	To verify whether SSID are broadcasting or not after 802.11 radiOS are in disable state	Passed	
MEJ810S_Reg_460	Configuring the 4800 AP dot1x credentials	To verify whether 4800 AP dot.1x credentials are AP plying successfully or not	Passed	

MEJ810S_Reg_461	Performing the Master AP failover with 4800 AP	To verify whether 4800 AP coming as ME controller or not after master failover	Passed	
MEJ810S_Reg_462	Joining the 4800 CAPWAP AP to ME as external AP	To verify whether 4800 AP joining to ME controller as external AP or not	Passed	
MEJ810S_Reg_463	Changing the 4800 External AP between different AP groups	To verify whether 4800 External AP changing groups without reboot or not	Passed	
MEJ810S_Reg_464	Changing the 4800 Internal AP between different AP groups	To verify whether 4800 Internal AP changing groups without reboot or not	Passed	
MEJ810S_Reg_465	Performing the master failover in read-only access	To verify whether Master AP failover happening in read-only access or not	Passed	
MEJ810S_Reg_466	Interchanging the 4800 ME AP image and check the details	To verify whether Image inter change happening or not	Passed	
MEJ810S_Reg_467	Performing the 4800 ME AP LED blink	To verify whether 4800 ME AP LED is blinking or not	Passed	
MEJ810S_Reg_468	Performing PING and Radius test	To verify whether PING and Radius test passed successfully or not	Passed	
MEJ810S_Reg_469	Login to the 4800 ME with different users	To verify whether User is able to login successfully with different users or nor	Passed	
MEJ810S_Reg_470	Restrict/grant the access to ME controller using HTTP/HTTPS/SSH/TELNET	To verify whether user is able to restrict the access or not	Passed	

MEJ810S_Reg_471	Checking the AP plication details after connect the clients to AVC	To verify whether accessed AP plications details showing properly or not in monitor page	Passed	
MEJ810S_Reg_472	Enabling more than 2 next preferred controllers	To verify whether more than 2 AP are possible to make as next preferred AP s	Passed	
MEJ810S_Reg_473	Configuring the Mac address of client in white list	To verify whether White list configured MAC address are accessing successfully or not	Passed	
MEJ810S_Reg_474	Configuring the Mac address of client in black list	To verify whether Black list configured MAC address are not accessing successfully or not	Passed	
MEJ810S_Reg_475	Assigning the IP address to Internal/External AP using Static/DHCP	To verify whether possible to assign the IP address to Internal/External AP using static/DHCP	Passed	
MEJ810S_Reg_476	Assigning the IP address to ME controller using Static/DHCP	To verify whether possible to assign the IP address to ME controller using static/DHCP	Passed	
MEJ810S_Reg_477	Configuring the AP default location details with Japanese/English LAN gauge	To verify whether AP location details are possible to add with Japanese/English	Passed	
MEJ810S_Reg_478	Assigning the internal DHCP to W LAN	To verify whether client is getting the valid IP address from Internal DHCP or not	Passed	

MEJ810S_Reg_479	Enabling the Schedule details in W LAN with Cisco any connect	To verify whether schedule details are enabling successfully or not with cisco any connect	Passed	
MEJ810S_Reg_480	Enabling the SSH to AP	To verify whether AP SSH details are changing successfully or not	Passed	
MEJ810S_Reg_481	Verifying ME backup image version after upgrade/downgrade	To check whether the backup image version showing properly or not after upgrade/downgrade	Passed	
MEJ810S_Reg_482	Monitoring the client details in 4800 ME controller	To check whether clients are able to show on the monitoring page or not.	Passed	
MEJ810S_Reg_483	Creating the W LAN with English/Japanese LAN gauge	To check whether the WLAN with Japanese/English character is creating or not	Passed	
MEJ810S_Reg_484	Associating the different client to SSID with Invalid credentials	To check whether different clients connecting to SSID with invalid credentials or not	Passed	
MEJ810S_Reg_485	Checking disabled SSID is broadcasting or not	To verify whether disabled WLAN is broadcasting or not	Passed	
MEJ810S_Reg_486	Configuring CME name with Japanese character	To check whether the CME name is possible configure with Japanese or not	Passed	
MEJ810S_Reg_487	Connecting the client with invalid credentials as W LAN created with mac filtering +WPA personal	To verify whether client is connecting with invalid credentials as W LAN created with mac filtering +WPA personal	Passed	

MEJ810S_Reg_488	Creating the NTP server with invalid IP and syncing the time	To check whether NTP server with invalid IP adding successfully or not on CME	Passed	
MEJ810S_Reg_489	Searching the AP and client	To check whether AP and client search details are showing proper or not	Passed	
MEJ810S_Reg_490	Clearing controller configuration	To check whether configuration can be cleared or not from CME G UI	Passed	
MEJ810S_Reg_491	Integrating the CMX setup with 4800 ME controller	To check whether CMX can be integrated or not in CME G UI	Passed	
MEJ810S_Reg_492	Creating invalid SNMP communities and traps	To check whether able to create invalid SNMP communities and traps or not through CLI	Passed	
MEJ810S_Reg_493	Exporting configuration file to controller through CLI/ UI	To check whether configuration file can be exported or not to the controller in CME CLI/ UI	Passed	
MEJ810S_Reg_494	Importing configuration file from controller through CLI/ UI	To check whether configuration file can be imported or not from the controller UI /CLI	Passed	
MEJ810S_Reg_495	Verifying that AVC rule that are applied on a deleted WLAN is applying automatically on same name WLAN or not	To check whether AVC rule that are applied on a deleted WLAN is applying automatically on same name WLAN or not	Passed	

MEJ810S_Reg_496	Verifying that AVC rule of first WLAN automatically AP plying on second WLAN also with second AVC profile name or not	To check whether AVC rule of first WLAN automatically AP plying on second WLAN also with second AVC profile name or not	Passed	
MEJ810S_Reg_497	Verifying the clients status in Monitor dashboard in ME GUI page	To check whether able to connect the different client in CME and shown properly in Monitor Dashboard page.	Passed	
MEJ810S_Reg_498	Monitoring multiple client mac address in CME and checking the clients status in Monitoring page	To check whether able to connect the multiple clients mac address in mac filtering and checking the clients status are shown properly or not in Monitoring page.	Passed	
MEJ810S_Reg_499	Converting a 4800 ME AP into a CAPWAP AP	To check whether able to convert the ME AP into a CAPWAP AP	Passed	
MEJ810S_Reg_500	Joining the external AP if Internal AP name is configured with Japanese characters	To check whether External AP able to join ME Controller name with Japanese or not	Passed	
MEJ810S_Reg_501	Configuring the System time manually/time zone based	To verify whether TIME configured successful with manual or time zone base	Passed	
MEJ810S_Reg_502	Adding the 4800 ME controller in PI	To verify whether 4800 ME controller adding successfully to PI or not	Passed	
MEJ810S_Reg_503	Configuring the 4800 ME details from PI	To verify whether 4800 ME controller details possible to configure from PI or not	Passed	

MEJ810S_Reg_504	Monitoring the 4800 ME details in PI	To verify whether 4800 ME details are showing properly in PI or not	Passed	
MEJ810S_Reg_505	Joining the multiple external APs with same name to 4800 ME	To verify whether multiple external APs joining with same name to 4800 ME or not	Passed	

Passpoint Maintenance Support

Logical ID	Title	Description	Status	Defect ID
MEJ810S_Reg_626	Enabling 802.11u in W LAN with 802.1x security	To verify whether 802.11u enabling in W LAN with 802.1x security or not	Passed	
MEJ810S_Reg_627	Deploying Pass point certificate to device from APPLE configuration and connecting Client	To verify whether it is possible to deploy pass point certificate to client from APPLE configuration or not	Passed	
MEJ810S_Reg_628	Configuring Hotspot details from CLI	To verify whether it is possible to configure Hotspot from CLI or not	Passed	
MEJ810S_Reg_629	Connecting Client to hotspot enabled W LAN after initial connection	To verify whether clients connecting to W LAN automatically whenever Client come to coverage zone	Passed	
MEJ810S_Reg_630	Checking Hotspot details after import and export configuration file	To verify whether Hotspot details showing properly or not after import and export configuration file	Passed	
MEJ810S_Reg_631	Disabling Hotspot details when Client connected to W LAN	Verifying that user is able to disable WPA on Hotspot enabled W LAN or not	Passed	

MEJ810S_Reg_632	Trying to change the W LAN security when Hotspot is in enable state	Verifying whether W LAN security is possible to change when Hotspot is in enable state	Passed	
MEJ810S_Reg_633	Deleting Radius server, When Radius server attached to hot spot enabled W LAN	To verify whether possible to delete radius server when it is attached to Hotspot enabled W LAN	Passed	
MEJ810S_Reg_634	Enabling 802.11u and Hotspot in W LAN with Open security	To verify whether possible to enable 802.11u and Hotspot in W LAN with Open security or not	Passed	
MEJ810S_Reg_635	Enabling 802.11u and Hotspot in W LAN with WPA security	To verify whether possible to enable 802.11u and Hotspot in W LAN with WPA security or not	Passed	
MEJ810S_Reg_636	Enabling 802.11u and Hotspot in W LAN with Central web authentication security	To verify whether possible to enable 802.11u and Hotspot in Central web authentication with WPA security or not	Passed	
MEJ810S_Reg_637	Upgrading ME and checking Hotspot details	To verify whether Hotspot details are showing proper after Upgrade	Passed	
MEJ810S_Reg_638	Downgrading ME and checking Hotspot details	To verify whether Hotspot details are showing proper after Downgrade	Passed	
MEJ810S_Reg_639	Changing Security from dot1x to WPA when Hotspot enabled	To verify whether W LAN security changing from dot1x to WPA when Hotspot is in enable state or not	Passed	
MEJ810S_Reg_640	Configuring Roam O UI value with duplicate name	To verify whether Roam O UI value possible to configure with Duplicate or not	Passed	

MEJ810S_Reg_641	Checking the Client Downlink and Uplink data transfer	To verify whether Client WAN Downlink and Uplink values are transferring successfully or not	Passed	
MEJ810S_Reg_642	Assigning the venue group and venue type for the specific AP on 802.11u	To verify whether Venue type and venue group details are showing proper or not	Passed	
MEJ810S_Reg_643	Configuring 802.11u details with Invalid details	To verify whether 802.11u details are possible to configure with invalid or not	Passed	

Efficient AP join

Logical ID	Title	Description	Status	Defect ID
MEJ810S_Reg_584	Enable efficient join with slave and master AP 2800 of same model	To verify whether slave AP downloading image from master AP	Passed	
MEJ810S_Reg_585	Enable efficient join with slave and master AP 2800/1542 of different model using TFTP	To verify whether slave AP downloading image from TFTP	Passed	
MEJ810S_Reg_586	Perform client connectivity after enabling efficient join for same model and same version	To verify whether client gets connected after enabling efficient join and joining as C AP W AP	Passed	
MEJ810S_Reg_587	Perform client connectivity after enabling efficient join for same model with different version using TFTP	To verify whether client gets connected after enabling efficient join and joining as ME C AP ABLE	Passed	
MEJ810S_Reg_588	Join 4 AP 's to controller and check pre downloading status for efficient join	To verify whether predownloading status is showing proper for efficient join	Passed	

MEJ810S_Reg_589	Removal of AP bundle for particular AP and perform TFTP	To verify whether TFTP aborted successfully after removal of AP bundle	Passed	
MEJ810S_Reg_590	Perform efficient join for same model of 1542 AP	To verify whether efficient AP join enabled and image downloaded from master AP	Passed	
MEJ810S_Reg_591	Perform efficient join for different model of 1542/1850 AP using TFTP	To verify whether efficient AP join enabled and image downloaded from TFTP	Passed	
MEJ810S_Reg_592	Enable efficient join with slave and master AP 1850/1542 of different model and same version using TFTP	To verify whether slave AP downloading image from TFTP and joining as ME C AP ABLE	Passed	
MEJ810S_Reg_593	Enable efficient join with slave and master AP 2800/1815 of different model and different version using TFTP	To verify whether slave AP downloading image from TFTP and joining as ME C AP ABLE	Passed	
MEJ810S_Reg_594	Disable efficient join with slave and master AP 1850 of same model using TFTP	To verify whether slave AP downloading image from TFTP	Passed	
MEJ810S_Reg_595	Disable efficient join with slave and master AP 1850/2800 of different model using TFTP	To verify whether slave AP downloading image from TFTP	Passed	
MEJ810S_Reg_596	Perform efficient join for different model of 1542/3800 AP using SFTP	To verify whether slave AP downloading image from SFTP	Passed	

MEJ810S_Reg_597	Enable efficient join with slave and master AP 1542/1850 of different model through CLI using SFTP	To verify whether efficient AP join enabled and image downloaded from SFTP	Passed	
MEJ810S_Reg_598	Perform efficient join for different model and same version of 1815/3800 AP using SFTP	To verify whether slave AP downloading image from SFTP and joining as ME C AP ABLE	Passed	
MEJ810S_Reg_599	Disable efficient join with slave and master AP 3800 of same model using SFTP	To verify whether slave AP downloading image from SFTP	Passed	
MEJ810S_Reg_600	Disable efficient join with slave and master AP 3800/1850 of different model using SFTP	To verify whether slave AP downloading image from SFTP	Passed	

CWA (Central Web Authentication)

Logical ID	Title	Description	Status	Defect ID
MEJ810S_Reg_102	Creating a CWA along with ACL Configuration in CME UI	To check Whether CWA along with ACL Configuration in CME UI created or not	Passed	
MEJ810S_Reg_103	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	
MEJ810S_Reg_104	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	

MEJ810S_Reg_105	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	
MEJ810S_Reg_106	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	
MEJ810S_Reg_107	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	
MEJ810S_Reg_108	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 AP plication is dropped or not	Passed	
MEJ810S_Reg_109	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	
MEJ810S_Reg_110	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	
MEJ810S_Reg_111	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	

MEJ810S_Reg_112	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	
MEJ810S_Reg_113	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	
MEJ810S_Reg_114	Validate whether CME is switch between configured Radius servers	To verify whether AAA authentication is occurring when one radius server goes down	Passed	
MEJ810S_Reg_115	Reboot the Controller after CWA enabling	To verify whether Configurations are showing same or different after controller reboot	Passed	
MEJ810S_Reg_116	Creating a CWA along with ACL Configuration through CLI	To verify whether ACL rule is created or not through CLI	Passed	
MEJ810S_Reg_117	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	
MEJ810S_Reg_118	Exporting/Importing configuration of CWA	To verify whether export and import is done successfully	Passed	

Intelligent Capture

Logical ID	Title	Description	Status	Defect ID
MEJ810S_Reg_568	Packet capture for Android client using Intelligent Capture option in AP group	To verify the packet capture for Android client using Intelligent Capture in AP group	Passed	

MEJ810S_Reg_569	Packet capture for Windows JOS client using Intelligent Capture option in AP group	To verify the packet capture for Windows client using Intelligent Capture in AP group	Passed	
MEJ810S_Reg_570	Packet capture for IOS client using Intelligent Capture option in AP group	To verify the packet capture for IOS client using Intelligent Capture in AP group	Passed	
MEJ810S_Reg_571	Packet capture for Mac OS client using Intelligent Capture option in AP group	To verify the packet capture for MAC OS client using Intelligent Capture in AP group	Passed	
MEJ810S_Reg_572	Packet capture of client when the client is connected to 3800 AP with 2.4 GHz	To capture the Packet of the client when the client is connected to 3800 AP with radio as 2.4 GHz in ME	Passed	
MEJ810S_Reg_573	Packet capture of client when the client is connected to 2800 AP with 5 GHz	To capture the Packet of the client when the client is connected to 2800 AP with radio as 5 GHz in ME	Passed	
MEJ810S_Reg_574	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 ME	Passed	
MEJ810S_Reg_575	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 ME	Passed	
MEJ810S_Reg_576	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 ME	Passed	

MEJ810S_Reg_577	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 4800 AP with security as captive portal-web consent	Passed	
MEJ810S_Reg_578	Packet capture for Anyconnect client using Intelligent Capture option in AP group page	To verify the packet capture for Anyconnect client using Intelligent Capture in AP group page	Passed	
MEJ810S_Reg_579	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	
MEJ810S_Reg_580	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	
MEJ810S_Reg_581	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	
MEJ810S_Reg_582	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	
MEJ810S_Reg_583	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	

DNA-C Support for ME

Logical ID	Title	Description	Status	Defect ID
MEJ810S_Reg_140	Adding the ME in DNA-C via inventory method	Verify that user is able to add ME in DNA-C via inventory method or not	Passed	

MEJ810S_Reg_141	Exporting the CSV file of CME from DNA-C using Credential export type	To check whether the exported CSV file using Credential export type has correct information of CME	Passed	
MEJ810S_Reg_142	Adding CME to DNAC by Importing CSV file using Credential export type	To check whether the user is able to add CME device in DNA-C by importing CSV file exported using Credential export type	Passed	
MEJ810S_Reg_143	Exporting the CSV file of CME from DNA-C using data export type	To check whether the exported CSV file using data export type has correct information of CME	Passed	
MEJ810S_Reg_144	Adding CME to DNAC by Importing CSV file using data export type	To check whether user is able to import the CSV file or not	Passed	
MEJ810S_Reg_145	Creating WLAN through Enterprise Wireless with different level of security type and with advanced security types like MAC Filtering & Fast Transition	Checking whether SSID is created or not with the selected security type	Passed	
MEJ810S_Reg_146	Creating Guest Wireless for adding ISE or any other External Authentication	Verifying whether user can add ISE or another External authentic an in Guest Wireless network	Passed	
MEJ810S_Reg_147	Creating Wireless Interface and Wireless Radio Frequency Profile	To check whether Wireless interface are created or not and modifying radio frequency to our requirements.	Passed	

MEJ810S_Reg_148	Creating Sensor SSID with WPA2 Enterprise, WPA2 Personal, Open with anyone of the security type	Checking whether Sensor SSID is created or not with the selected security type	Passed	
MEJ810S_Reg_149	Adding CMX in DNA-C	To check whether the user is able to add CMX in DNA-C or not	Passed	
MEJ810S_Reg_150	Provisioning ME via DNA-C	Verify that user is able to add ME in DNA-C via provisioning method or not	Passed	
MEJ810S_Reg_151	Importing maps from DNA-C	To import m APs from DNA-C and check if the m APs gets imported to the cmx .	Passed	
MEJ810S_Reg_152	Adding Access Points from CME to the imported maps from DNA-C to CMX	To check whether the imported Access Points are shown correctly in CMX or not	Passed	
MEJ810S_Reg_153	Checking the Client details by connecting to the Access Points	Connecting the Client to the Access Points and checking the connectivity	Passed	
MEJ810S_Reg_154	Discovering CME device IP in DNA-C	To check whether the added CME device IP is discovered in DNA-C or not	Passed	
MEJ810S_Reg_155	Updating the credentials, in CME and checking the same in DNA-C	Verifying whether the updated credentials are reflected in DNA-C or not	Passed	
MEJ810S_Reg_156	Updating the management IP in CME and checking the same in DNA-C	Connecting the Client to the Access Points and checking the connectivity	Passed	

MEJ810S_Reg_157	Resync CME in DNA-C after updating the management IP and check the resync interval	Verifying whether CME resyncs with DNA-C successfully or not after updating management IP	Passed	
MEJ810S_Reg_158	Using Launch Command Runner we can execute the CLI commands for selected device from the inventory	Verifying whether CLI commands are executed successfully or not for selected the device from the inventory	Passed	
MEJ810S_Reg_159	Upgrading CME OS image from DNA-C	Upgrading the OS image for CME through DNA-C and checking whether CME is upgraded or not from CME G UI .	Passed	

Authentication Survivability Support

Logical ID	Title	Description	Status	Defect ID
MEJ810S_Reg_601	Creating WLAN with Radius server and connecting client	To verify whether Client is connecting to WLAN with Radius server or not	Passed	
MEJ810S_Reg_602	Guest WLAN with Radius survivability	To verify whether Client able to connect Guest WLAN with Radius survivability o not	Failed	CSCvq40887,CSCvq45042
MEJ810S_Reg_603	Captive network enabled WLAN with Radius survivability	To verify whether Client able to connect captive network enabled WLAN with Radius survivability or not	Passed	
MEJ810S_Reg_604	MAC filter enabled WLAN with Radius survivability	To verify whether Client able to connect MAC filter enabled WLAN with Radius survivability or not	Passed	

MEJ810S_Reg_605	Guest+MAC enabled WLAN with Radius survivability	To verify whether Client able to connect Guest+MAC enabled WLAN with Radius survivability or not	Passed	
MEJ810S_Reg_606	Guest+Capative+MAC enabled W LAN with Radius survivability	To verify whether Client able to connect Guest+Capative+MAC enabled W LAN with Radius survivability or not	Passed	
MEJ810S_Reg_607	ACL configured WLAN with Radius survivability	To verify whether ACL rules are AP plying to WLAN with Radius survivability or not	Passed	
MEJ810S_Reg_608	AVC configured WLAN with Radius survivability	To verify whether AVC rules are AP plying to WLAN with Radius survivability or not	Passed	
MEJ810S_Reg_609	Assigning DHCP Radius survivability enabled WLAN	To verify whether Client is getting the IP address from DHCP pool or not with Radius survivability	Passed	
MEJ810S_Reg_610	Enabling Hotspot on WLAN with Radius survivability	To verify whether Client is connecting to Hotspot enabled WLAN with Radius survivability or not	Passed	
MEJ810S_Reg_611	Checking Client details in Auth cards page	To verify whether Clients are able to connect Radius survivability and showing same in Auth cards or not	Passed	
MEJ810S_Reg_612	Check Authorization details in ISE	To verify whether Client details are showing proper in ISE or not	Passed	

MEJ810S_Reg_613	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	
MEJ810S_Reg_614	Upgrading ME and checking Radius survivability details	To verify whether Radius survivability details showing or not after image downgrade	Passed	
MEJ810S_Reg_615	Downgrading ME and checking Radius survivability details	To verify whether Radius survivability details showing or not after image Downgrade	Passed	
MEJ810S_Reg_616	Checking Radius survivability details after import & export configurations	To verify whether Radius survivability details are showing proper or not after import &export	Passed	
MEJ810S_Reg_617	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	
MEJ810S_Reg_618	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	
MEJ810S_Reg_619	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	
MEJ810S_Reg_620	Configuring client Cache time to minimum and checking details	To verify whether Client are able to disconnect after minimum time expired or not	Passed	
MEJ810S_Reg_621	Configuring client Cache time to Maximum and checking details	To verify whether Client are able to disconnect after maximum time expired or not	Passed	

MEJ810S_Reg_622	Enabling Radius profiling & BYOD on W LAN with Radius survivability	To verify whether Client is able to connect or not when Radius profiling enabled	Passed	
MEJ810S_Reg_623	Scheduling W LAN with Radius survivability	To verify whether W LAN able to schedule with Radius survivability or not	Passed	
MEJ810S_Reg_624	Configuring Radius survivability with R LAN support	To verify whether R LAN is possible to configure with Radius survivability or not	Passed	
MEJ810S_Reg_625	Enabling Radius survivability without AAA override	To verify whether Radius survivability enabling without AAA override or not	Passed	

Optimized Roaming

Logical ID	Title	Description	Status	Defect ID
MEJ810S_Reg_335	Configuring optimized roaming with 2.4 GHz band & default interval and roam Android client	To verify that optimized roaming with 2.4 GHz band & default interval gets configured or not and check association of Android client	Passed	
MEJ810S_Reg_336	Configuring optimized roaming with 2.4 GHz band & customized interval ,1 MBPS Thresholds and roam Android client	To verify that optimized roaming with 2.4 GHz band & customized interval ,1 MBPS Thresholds gets configured or not and check association of Android client	Passed	

MEJ810S_Reg_337	Configuring optimized roaming with 5 GHz band & customized interval and roam Android client	To verify that optimized roaming with 5 GHz band &customized interval configured and check association of Android client	Passed	
MEJ810S_Reg_338	Configuring optimized roaming with 5 GHz band & default interval , 6 MBPS Threshold and roam Android client	To verify that optimized roaming with 5 GHz band &default interval , 6 MBPS Threshold configured and check association of Android client	Passed	
MEJ810S_Reg_339	Configuring optimized roaming with 2.4 GHz band & default interval ,5.5 MBPS Threshold and roam iOS client	To verify that optimized roaming with 2.4 GHz band &default interval ,5.5 MBPS Threshold configured successfully and check association of iOS client	Passed	
MEJ810S_Reg_340	Configuring optimized roaming with 2.4 GHz band & customized interval(5 Sec) ,9 MBPS Threshold and roam iOS client	To verify that optimized roaming with 2.4 GHz band &customized interval(5 Sec) ,9 MBPS Threshold configured and check association of iOS client	Passed	
MEJ810S_Reg_341	Configuring optimized roaming with 5 GHz band & customized interval(40 Sec) 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	

MEJ810S_Reg_342	Configuring optimized roaming with 5 GHz band & default interval , 12 MBPS Threshold and roam iOS client	To verify that optimized roaming with 5 GHz band & default interval , 12 MBPS Threshold configured successfully and check association of iOS client	Passed	
MEJ810S_Reg_343	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	
MEJ810S_Reg_344	Moving the Android client from 4800 ME AP after enable optimized roaming	To verify that client got disassociated when signal is poor while moving from 4800 AP	Passed	
MEJ810S_Reg_345	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	
MEJ810S_Reg_346	Moving the Android client from 2700 AP after enable optimized roaming in ME	To verify that client got disassociated when signal is poor while moving from 2700 AP	Passed	
MEJ810S_Reg_347	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	
MEJ810S_Reg_348	Configuring optimized roaming in ME 1815 with 2.4 GHz band & default interval ,5.5 MBPS Threshold and roam iOS client	To verify that optimized roaming in ME 1815 with 2.4 GHz band & default interval ,5.5 MBPS Threshold configured successfully and check association of iOS client	Passed	

MEJ810S_Reg_349	Configuring optimized roaming in ME 2800 with 2.4 GHz band & default interval ,5.5 MBPS Threshold and roam iOS client	To verify that optimized roaming in ME 2800 with 2.4 GHz band & default interval ,5.5 MBPS Threshold configured successfully and check association of iOS client	Passed	
MEJ810S_Reg_350	Connect iOS client from where SSID signal is week	To verify that iOS client connecting or not from where SSID signal is week	Passed	
MEJ810S_Reg_351	Configuring the 802.11a optimized roaming in CLI and roam Android client	To verify that optimized roaming with 802.11a gets configured or not and check association of Android client	Passed	
MEJ810S_Reg_352	Configuring the 802.11b optimized roaming in CLI and roam iOS client	To verify that optimized roaming with 802.11b gets configured or not and check association of iOS client	Passed	
MEJ810S_Reg_353	Restarting the ME Controller after optimized roaming configuration	To verify that optimization roaming configuration remain same after reboot	Passed	
MEJ810S_Reg_354	Importing/exporting configuration file after optimized roaming configuring	To verify that optimization roaming configuration remain same after import and export configuration file	Passed	

1815 RLAN Features

Logical ID	Title	Description	Status	Defect ID

MEJ810S_Reg_542	Configure RLAN with Open security and connect the wired clients	To verify whether RLAN clients is connected with Open security	Passed	
MEJ810S_Reg_543	Configure RLAN with Open+mac filter having type as whitelist and connect the wired clients	To verify whether RLAN clients is connected with open+macfilter having type as whitelist	Passed	
MEJ810S_Reg_544	Configure RLAN with Open+mac filter having type as blacklist and connect the wired clients	To verify whether RLAN clients gets disconnected with open+macfilter having type as blacklist	Passed	
MEJ810S_Reg_545	Changing whitelist to blacklist in RLAN and connect the wired clients	To verify whether wired clients gets disconnected when changing from whitelist to blacklist	Passed	
MEJ810S_Reg_546	Configure RLAN with open security and connect three wired clients (windows,MAC and JOS)	To verify whether three wired clients gets connected with open security	Passed	
MEJ810S_Reg_547	Configure RLAN with open+macfilter security and connect three wired clients (windows,MAC and JOS)	To verify whether three wired clients gets connected with open+macfilter security	Passed	
MEJ810S_Reg_548	Configure RLAN with 802.1X security and connect three wired clients (windows,MAC and JOS)	To verify whether three wired clients gets connected with 802.1X security	Passed	
MEJ810S_Reg_549	Configure RLAN with 802.1X+macfilter security and connect three wired clients (windows,MAC and JOS)	To verify whether three wired clients gets connected with 802.1X+macfilter security	Passed	

MEJ810S_Reg_550	Enable 2 ports in RLAN and connect three wired clients	To verify whether only two wired clients gets connect successfully	Passed	
MEJ810S_Reg_551	Configure DHCP pool and connect the wired clients	To verify whether wired client getting IP from DHCP pool successfully	Passed	
MEJ810S_Reg_552	Configure 802.1X RLAN with host mode as single host and connect the wired clients	To verify whether wired clients gets connected with single host in RLAN	Passed	
MEJ810S_Reg_553	Configure 802.1X RLAN with host mode as multi host and connect the wired clients	To verify whether wired clients gets connected with multi host in RLAN	Passed	
MEJ810S_Reg_554	Configure 802.1X RLAN with authentication server as AP and connect the wired clients	To verify whether wired clients gets connected with authentication server as AP in R LAN	Passed	
MEJ810S_Reg_555	Configure 802.1X R LAN with authentication server as external Radius and connect the wired clients	To verify whether wired clients gets connected with authentication server as external radius in R LAN	Passed	
MEJ810S_Reg_556	Enable MAB with 802.1X using authentication server as AP and connect the wired clients	To verify whether wired clients gets connected with MAB using authentication server as AP in R LAN	Passed	
MEJ810S_Reg_557	Enable MAB with 802.1X using authentication server as External Radius and connect the wired clients	To verify whether wired clients gets connected with MAB using authentication server as external radius in R LAN	Passed	
MEJ810S_Reg_558	Enable AAA override and connect the wired client with 802.1x security .	To verify whether AAA override the RLAN and connect the wired client	Passed	

MEJ810S_Reg_559	Create a RLAN with Guest network having different access type and connect the wired client	To verify whether wired clients gets connected with guest network	Passed	
MEJ810S_Reg_560	Create a RLAN with Guest+macfilter network having different access type and connect the wired client	To verify whether wired clients gets connected with guest+macfilter	Passed	
MEJ810S_Reg_561	Configure AVC in RLAN and connect the wired client	To verify whether wired clients gets connected with AVC	Passed	
MEJ810S_Reg_562	Configure ACL in RLAN and connect the wired client	To verify whether wired clients gets connected with ACL and redirects successfully	Passed	
MEJ810S_Reg_563	Configure RLAN and reboot the controller	To verify whether RLAN configuration showing proper after rebooting	Passed	
MEJ810S_Reg_564	Configure RLAN and upgrade/downgrade the controller	To verify whether RLAN configuration showing proper after upgrading/downgrading	Passed	
MEJ810S_Reg_565	Configure R LAN in ME and edit from PI	To verify whether RLAN configuration is editing successfully from PI	Passed	
MEJ810S_Reg_566	Checking the configuration of RLAN in Read-only user	To verify whether any updation in RLAN display error message in Read-only	Passed	
MEJ810S_Reg_567	Export/Import RLAN configurations	To verify whether RLAN configurations importing and exporting successfully	Passed	

EOGRE Support on ME

Logical ID	Title	Description	Status	Defect ID
MEJ810S_Reg_389	Establishing the EoGRE tunnel and connecting the Windows client	To verify whether Windows client communicating with device through tunnel or not	Passed	
MEJ810S_Reg_390	Establishing the EoGRE tunnel and connecting the IOS client	To verify whether IOS client communicating with device through tunnel or not	Passed	
MEJ810S_Reg_391	Establishing the EoGRE tunnel and connecting the MAC client	To verify whether MAC client communicating with device through tunnel or not	Passed	
MEJ810S_Reg_392	Establishing the EoGRE tunnel and connecting the Japanese client	To verify whether Japanese client communicating with device through tunnel or not	Passed	
MEJ810S_Reg_393	Establishing the EoGRE tunnel and connecting the Android client	To verify whether Android client communicating with device through tunnel or not	Passed	
MEJ810S_Reg_394	Rebooting the AP and checking the EoGRE configurations	To verify whether after reboot EoGRE configurations are available or not	Passed	
MEJ810S_Reg_395	Upgrading the ME and checking the ME configuration	To verify whether after Image upgrade EoGRE details are showing properly or not	Passed	
MEJ810S_Reg_396	Copying the EoGRE rule details to other profile	To verify whether EoGRE rules are copying to the other profile or not	Passed	
MEJ810S_Reg_397	Modifying the EoGRE profile details	To verify whether EoGRE profile details are modifying or not	Passed	

Schedule WLAN Support

Logical ID	Title	Description	Status	Defect ID
MEJ810S_Reg_355	Schedule the WLAN with open security for enabled hours/days	To check whether SSID is broadcasting or not on enabled time	Passed	
MEJ810S_Reg_356	Schedule the WLAN with open security for disabled hours/days	To check whether SSID is stopped broadcasting or not on disabled time	Passed	
MEJ810S_Reg_357	Configure the schedule WLAN with WPA2 Personal security for enabled hours/days	Verify whether Scheduled WLAN is broadcasting or not on enabled time	Passed	
MEJ810S_Reg_358	Configure the schedule W LAN with WPA2 Personal security for disabled hours/days	Verify whether SSID is stopped broadcasting or not on disabled time	Passed	
MEJ810S_Reg_359	Configure the None option for scheduled W LAN	Verify whether Scheduled W LAN configuration get cleared or not after enabling the None option	Passed	
MEJ810S_Reg_360	Schedule the WLAN with WPA2 Enterprise for enabled hours/days	To check whether WLAN is broadcasting or not on Scheduled time	Passed	
MEJ810S_Reg_361	Schedule the WLAN with WPA2 Enterprise for disabled hours/days	To check whether WLAN is stopped broadcasting or not on Scheduled time	Passed	
MEJ810S_Reg_362	Configure the schedule WLAN with Internal Splash Page with WPA2 PSK for enabled hours/days/week	Verify the schedule WLAN is broadcasting or not on scheduled WLAN enabled hours	Passed	
MEJ810S_Reg_363	Configure the schedule WLAN with Internal Splash Page for disabled hours/days/week	Verifying whether SSID is stopped broadcasting or not on disabled time/hours	Passed	

MEJ810S_Reg_364	Configure the Schedule WLAN with CWA for enabled hours/days/week	To check whether SSID is broadcasting or not on enabled hours/days/time	Passed	
MEJ810S_Reg_365	Configure the Schedule W LAN with CWA for disabled hours/days/time	To check whether SSID is stopped broadcasting or not on disabled hours/days/time	Passed	
MEJ810S_Reg_366	Verify the Schedule WLAN with Authentication Server(AP) for enabled hours/days/time	Validate the SSID is broadcasting or not for enabled Scheduled WLAN	Passed	
MEJ810S_Reg_367	Verify the Schedule WLAN with Authentication Server(AP) for disabled hours/days/time	Validate the SSID is stopped broadcasting or not for disabled hours/time/days	Passed	
MEJ810S_Reg_368	Verifying the CMX connect with Schedule W LAN broadcasting for enabled hours/days/time	To check whether scheduled WLAN broadcasting and client is connecting successfully on enabled scheduled time/day	Passed	
MEJ810S_Reg_369	Verifying the CMX connect with Schedule W LAN broadcasting for disabled hours/days/time	To check whether scheduled W LAN is stopped broadcasting and client is disconnecting successfully for disabled time	Passed	
MEJ810S_Reg_370	Configuring the Schedule WLAN with Web Consent for enabled hours/days	Validate the scheduled WLAN is broadcasting or not on particular day/time	Passed	
MEJ810S_Reg_371	Configuring the Schedule WLAN with Web Consent for disabled hours/days/time	To check whether scheduled WLAN is stopped broadcasting on particular day/time	Passed	

MEJ810S_Reg_372	Configure the Local User Account with Scheduled WLAN for enabled hours	To check whether SSID is broadcasting and client is able to connect successfully via Local User Account	Passed	
MEJ810S_Reg_373	Configure the Local User Account with Scheduled WLAN for disabled hours	To check whether SSID is stopped broadcasting on particular time and client disconnect.	Passed	
MEJ810S_Reg_374	Configure the Scheduled WLAN with Internal Splash Page Email Address for enabled hours	Validate the Scheduled WLAN SSID is broadcasting successfully on particular time.	Passed	
MEJ810S_Reg_375	Configure the Internal Splash Page Email Address for Scheduled WLAN disabled hours	Validate the Scheduled WLAN SSID is stopped broadcasting successfully or not on particular time.	Passed	
MEJ810S_Reg_376	Configure the Schedule WLAN with external Splash page Local User Account for enabled hours	Validate scheduled WLAN is broadcasting on time and client is connecting successfully	Passed	
MEJ810S_Reg_377	Configure the Schedule WLAN with external Splash page Local User Account for disabled hours	Validate scheduled WLAN is stopped broadcasting on time and client is disconnecting successfully	Passed	
MEJ810S_Reg_378	Verifying the Schedule WLAN with External Splash Page Web Consent for enabled hours	To check whether the schedule WLAN is broadcasting or not on particular time	Passed	
MEJ810S_Reg_379	Verifying the Schedule WLAN with External Splash Page Web Consent for disabled hours	To check whether the schedule WLAN is stopped broadcasting on time	Passed	

MEJ810S_Reg_380	Configure the Schedule WLAN via cli with WPA security for enabled hours	To check whether SSID is broadcasting or not on time	Passed	
MEJ810S_Reg_381	Configure the Schedule WLAN via cli with WPA security for disabled hours	To check whether WLAN is stopped broadcasting or not on disabled time	Passed	
MEJ810S_Reg_382	Configure the Schedule WLAN as per system time for enabled hours	Verifying whether Schedule WLAN SSID is broadcasting or not as per system time	Passed	
MEJ810S_Reg_383	Change the SSID name of Scheduled W LAN for enabled hours	To check whether SSID is stopped broadcasting or not after changing the SSID Name for enabled hours	Passed	
MEJ810S_Reg_384	Verify the client connectivity if disabled hrs. have been changed to current system time	Verifying the client connectivity after changing the disabled hours of Scheduled WLAN	Passed	
MEJ810S_Reg_385	Verify the roaming client states of Scheduled WLAN for enabled hours	To check whether client is roaming or not from AP 1 to AP 2	Passed	
MEJ810S_Reg_386	Verifying the Scheduled WLAN configuration after importing and exporting the same config file for enabled hours	To check whether the Scheduled WLAN configuration importing/exporting same file or not for enabled hours	Passed	
MEJ810S_Reg_387	Verifying the client connectivity of scheduled W LAN if controller is made up during the enable time duration	To check whether SSID is broadcasting or not after WLC made-up	Passed	

MEJ810S_Reg_388	Verifying the scheduled WLAN status if controller is rebooted at the scheduled end time	To check whether SSID is stopped broadcasting or not after WLC reboot at end of scheduled time	Passed	

Maximum number of clients per WLAN/radio

Logical ID	Title	Description	Status	Defect ID
MEJ810S_Reg_530	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 checking if the number of client that is configured alone gets connected to the WLAN	Passed	
MEJ810S_Reg_531	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 W LAN	Passed	
MEJ810S_Reg_532	Configuring maximum Allowed Clients Per AP Radio in RF profile as 4 and in W LAN as 3 and connecting the client	To configure maximum allowed client Per AP radio in RF profile and also setting the same in W LAN and check which of the configured number of clients gets connected .	Passed	

MEJ810S_Reg_533	Creating WPA 2 Personal security W LAN with radio policy as 5 GHz and configuring Maximum Allowed Clients Per AP Radio	To configure maximum allowed client per AP radio setting the W LAN security with WPA 2 Personal and radio policy as 5 GHz and check if only the defined number of client alone connect to the W LAN .	Passed	
MEJ810S_Reg_534	Creating WPA 2 Enterprise security W LAN with radio policy as 5 GHz and configuring Maximum Allowed Clients Per AP Radio	To configure maximum allowed client per AP radio setting the W LAN security with WPA 2 Enterprise and radio policy as 5 GHz and check if only the defined number of client alone connect to the W LAN .	Passed	
MEJ810S_Reg_535	Creating WPA 2 Personal security W LAN with radio policy as 2.4 GHz and configuring Maximum Allowed Clients Per AP Radio	To create WPA 2 Personal security W LAN 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 W LAN .	Passed	

mDNS Support

Logical ID	Title	Description	Status	Defect ID
MEJ810S_Reg_398	Checking mDNS services are applied to MAC OS with W LAN open security	Verifying mDNS services are applied to Mac OS with open SSID	Passed	
MEJ810S_Reg_399	Checking mDNS services are applied to MacOS and IOS with W LAN WPA2 personal security	Verifying mDNS services are applied to MacOS and IOS with WPA2 personal security	Passed	

MEJ810S_Reg_400	Checking mDNS services are applied to APPLE TV and IOS with W LAN WPA2 Enterprise security and authentication server as radius	Verifying mDNS services are applied to APPLE TV and IOS with WPA2 Enterprise security and radius as authentication server	Passed	
MEJ810S_Reg_401	Checking mDNS services are applied to APPLE Devices with W LAN WPA2 Enterprise security and authentication server as AP	Verifying mDNS services are applied to APPLE TV and IOS with WPA2 Enterprise security and AP as authentication server	Passed	
MEJ810S_Reg_402	Checking mDNS services are applied to APPLE Devices with security Internal Splash and Radius as access type	Verifying mDNS services are applied to APPLE Devices with security Internal Splash and Radius as access type	Passed	
MEJ810S_Reg_403	Checking mDNS services are applied to APPLE Devices with security Internal Splash and WPA2 Personal as access type	Verifying mDNS services are applied to APPLE Devices with security Internal Splash and WPA2 Personal as access type	Passed	
MEJ810S_Reg_404	Checking mDNS services are applied to MacOS and IOS with WLAN CWA security	Verifying mDNS services are applied to MacOS and IOS with CWA security	Passed	
MEJ810S_Reg_405	Checking mDNS services are applied to APPLE Devices with Fast Lane enabled	Verifying mDNS services are applied to APPLE Devices with fast Lane enabled	Passed	
MEJ810S_Reg_406	Performing client communication between two clients connected two different vLAN	Checking client communication between two clients connected to different vLAN	Passed	

MEJ810S_Reg_407	Performing client communication between two clients connected two different vLAN with NAT enabled	Checking client communication between two clients connected to different vLAN with NAT enabled	Passed	
MEJ810S_Reg_408	Performing roaming operation when mDNS is applied	Checking roaming when mDNS is applied	Passed	
MEJ810S_Reg_409	Exporting config file after upgrading ME	Checking mDNS config after exporting config file	Passed	
MEJ810S_Reg_410	Creating mDNS profile by adding required services	Verifying mDNS profile is creating with required services	Passed	
MEJ810S_Reg_411	Enabling mDNS Snooping and mDNS Policy from UI	Verifying mDNS snooping and mDNS Policy is enabling	Passed	
MEJ810S_Reg_412	Disabling mDNS Snooping and mDNS Policy from CLI	Verifying mDNS snooping and mDNS Policy is disabling from CLI	Passed	
MEJ810S_Reg_413	Checking mDNS services are applied to Android and Chromecast with W LAN open security	Verifying DNS services are applied to Android and Chromecast with open SSID	Passed	
MEJ810S_Reg_414	Checking mDNS services are applied to android and Chromecast with W LAN WPA2 personal security	Verifying mDNS services are applied to Android and Chromecast with WPA2 personal security	Passed	
MEJ810S_Reg_415	Checking mDNS services are applied to Android and Chromecast with W LAN WPA2 Enterprise security and authentication server as radius	Verifying mDNS services are applied to Android and Chromecast with WPA2 Enterprise security and radius as authentication server	Passed	

MEJ810S_Reg_416	Checking mDNS services are applied to Android and Chromecast with W LAN WPA2 Enterprise security and authentication server as AP	Verifying mDNS services are applied to Android and Chromecast with WPA2 Enterprise security and AP as authentication server	Passed	
MEJ810S_Reg_417	Checking mDNS services are applied to Android and Chromecast with security Internal Splash and Radius as access type	Verifying mDNS services are applied to APPLE Devices with security Internal Splash and Radius as access type	Passed	
MEJ810S_Reg_418	Checking mDNS services are applied to android and Chromecast with security Internal Splash and WPA2 Personal as access type	Verifying mDNS services are applied to Android and Chromecast with security Internal Splash and WPA2 Personal as access type	Passed	

Open DNS

Logical ID	Title	Description	Status	Defect ID
MEJ810S_Reg_187	Configuring Open DNS in DHCP pool and associating Windows JOS clients to a WLAN in CME	To check whether Windows JOS clients gets associated or not to a WLAN in which DHCP pool with Open DNS configured is mapped	Passed	
MEJ810S_Reg_188	Configuring Open DNS in DHCP pool and associating Mac OS clients to a WLAN in CME	To check whether Mac OS clients gets associated or not to a WLAN in which DHCP pool with Open DNS configured is mapped	Passed	

MEJ810S_Reg_189	Configuring Open DNS in DHCP pool and associating APPLE iOS clients to a WLAN in CME	To check whether APPLE iOS clients gets associated or not to a WLAN in which DHCP pool with Open DNS configured is mapped	Passed	
MEJ810S_Reg_190	Configuring Open DNS in DHCP pool and associating Android clients to a WLAN in CME	To check whether Android clients gets associated or not to a WLAN in which DHCP pool with Open DNS configured is mapped	Passed	

ME GUI - MC2UC (Videostreaming)

Logical ID	Title	Description	Status	Defect ID
MEJ810S_Reg_419	Checking MC2UC traffic when clients connected with open security	Verifying MC2UC traffic for clients connected with open security	Passed	
MEJ810S_Reg_420	Checking MC2UC traffic when clients connected with WPA2 Personal security	Verifying MC2UC traffic for clients connected with WPA2 Personal security	Passed	
MEJ810S_Reg_421	Checking MC2UC traffic when clients connected with WPA2 Enterprise security with Radius as authentication server	Verifying MC2UC traffic for clients connected with WPA2 Enterprise security with radius as authentication server	Passed	
MEJ810S_Reg_422	Checking MC2UC traffic when clients connected with WPA2 Enterprise security with AP as authentication server	Verifying MC2UC traffic for clients connected with WPA2 Enterprise security with AP as authentication server	Passed	
MEJ810S_Reg_423	Checking MC2UC traffic when clients switches between AP radiOS	Verifying MC2UC traffic for clients when it roams between AP radiOS	Passed	

MEJ810S_Reg_424	Performing Intra controller roaming for client and checking MC2UC traffic	Verifying MC2UC traffic for clients when it roams between APs	Passed	
MEJ810S_Reg_425	Verifying Multicast-direct is enabling from CLI globally	To verify whether multicast-direct is enabling from CLI globally	Passed	
MEJ810S_Reg_426	Checking MC2UC traffic when clients connected with QOS Platinum	Verifying MC2UC traffic for clients connected with QOS Platinum	Passed	
MEJ810S_Reg_427	Checking MC2UC traffic while blocking RTP server	Verifying MC2UC traffic while blocking RTP server	Passed	
MEJ810S_Reg_428	Checking MC2UC traffic when AP changed to different group	Verifying MC2UC traffic when AP changed to different group	Passed	
MEJ810S_Reg_429	Checking MC2UC traffic after updating MAC address profile	Verifying MC2UC traffic after updating MAC address profile	Passed	
MEJ810S_Reg_430	Checking MC2UC traffic for client using different DHCP pool	Verifying MC2UC traffic for client using different DHCP pool	Passed	
MEJ810S_Reg_431	Checking MC2UC traffic for client with NAT enabled	Verifying MC2UC traffic for client with NAT enabled	Passed	
MEJ810S_Reg_432	Checking MC2UC traffic for client when applying AVC with RTP application drop	Verifying MC2UC traffic for client when applying AVC with RTP application drop	Passed	
MEJ810S_Reg_433	Checking MC2UC traffic for client when applying AVC with RTP-video application drop	Verifying MC2UC traffic for client when applying AVC with RTP-video application drop	Passed	
MEJ810S_Reg_434	Checking MC2UC traffic for client when applying AVC with RTP-audio application drop	Verifying MC2UC traffic for client when applying AVC with RTP-audio application drop	Passed	

MEJ810S_Reg_435	Creating media stream with Valid data	Verifying media stream is created with valid data	Passed	
MEJ810S_Reg_436	Creating media stream with duplicated data	Verifying media stream is created with duplicated data or not	Passed	
MEJ810S_Reg_437	Creating media stream parameters with valid data	Verifying media stream parameters are creating with valid data or not	Passed	
MEJ810S_Reg_438	Creating media stream parameters with invalid data	Verifying media stream parameters are creating with invalid data or not	Passed	
MEJ810S_Reg_439	Creating media stream with read-only user	Verifying media stream is able to create with read only user or not	Passed	

Syslogs

Logical ID	Title	Description	Status	Defect ID
MEJ810S_Reg_506	Enabling logging for Errors in CME	To check whether log can be generated or not for Error Message in CME GUI	Passed	
MEJ810S_Reg_507	Disabling logging for Errors in CME	To check whether logging for Errors disabled or not in CME	Passed	
MEJ810S_Reg_508	Enabling logging for Debugging in CME	To check whether log can be generated or not for Debug Message in CME GUI	Passed	
MEJ810S_Reg_509	Enabling logging server for Emergencies	To check whether log can be generated or not for Emergencies in CME GUI	Passed	

MEJ810S_Reg_510	Enabling logging for Alerts	To check whether log can be generated or not for alerts in CME GUI	Passed	
MEJ810S_Reg_511	Enabling logging for Warning	To check whether log can be generated or not for warning in CME GUI	Passed	
MEJ810S_Reg_512	Enabling logging for Critical	To check whether log can be generated or not for critical events in CME GUI	Passed	
MEJ810S_Reg_513	Enabling logging for Notification	To check whether log can be generated or not for notification in CME GUI	Passed	
MEJ810S_Reg_514	Enabling logging for Information message	To check whether log can be generated or not for Informational message in CME GUI	Passed	
MEJ810S_Reg_515	Checking the validation of syslog errors in PI	To check whether the syslog errors are displayed in PI	Passed	
MEJ810S_Reg_516	Checking the validation of syslog information in PI	To check whether the syslog information are displayed in PI	Passed	
MEJ810S_Reg_517	Checking the historic information about syslog in PI	To check whether the historic information about syslog in PI	Passed	
MEJ810S_Reg_518	Validating the syslog warning message in PI	To check whether the syslog warning message in PI	Passed	
MEJ810S_Reg_519	Validating the syslog notification in PI	To check whether syslog notification in PI	Passed	
MEJ810S_Reg_520	Verifying the severity filtering for syslog in PI	To verify the severity filtering for syslog in PI	Passed	

MEJ810S_Reg_521	Verifying the Device IP address filtering for syslog in PI	To verify the Device IP address filtering for syslog in PI	Passed	

SFTP Domain Name support

Logical ID	Title	Description	Status	Defect ID
MEJ810S_Reg_440	SFTP support with valid username from UI	To verify whether ME is updating the image with SFTP with valid username or not	Passed	
MEJ810S_Reg_441	SFTP support with Invalid username from UI	To verify whether ME is updating the image with SFTP with Invalid username or not	Passed	
MEJ810S_Reg_442	Performing the day0 configurations to AP with valid username	To verify whether AP is coming as ME controller with valid username or not	Passed	
MEJ810S_Reg_443	Performing the day0 configurations to AP with Invalid username	To verify whether AP is coming as ME controller with Invalid username or not	Passed	
MEJ810S_Reg_444	Initiating the SFTP image Upgrading with valid username from CLI	To verify whether AP is downloading the image from SFTP using valid name or not	Passed	
MEJ810S_Reg_445	Initiating the SFTP image Upgrading with Invalid username from CLI	To verify whether AP is downloading the image from SFTP using invalid name or not	Passed	
MEJ810S_Reg_446	Downgrading the image via SFTP username from UI	To verify whether ME image is downgrading via SFTP username or not from UI	Passed	

MEJ810S_Reg_447	Downgrading the image via SFTP username from CLI	To verify whether image is downgrading to the old version using SFTP username	Passed	
MEJ810S_Reg_448	Scheduling the SFTP transfer	To verify whether Schedule downloading happening or not	Passed	
MEJ810S_Reg_449	Aborting the Update and checking the error details	To verify whether after abort what the error message is showing	Passed	

Lobby Ambassador

Logical ID	Title	Description	Status	Defect ID
MEJ810S_Reg_239	Creating a Lobby Admin in CME GUI /CLI	To check whether lobby admin user is created or not in CME GUI /CLI	Passed	
MEJ810S_Reg_240	Creating /deleting a management guest User	To check whether a guest user can be added /deleted or not in CME guest management GUI	Passed	
MEJ810S_Reg_241	Deleting a management guest user	To check whether guest user can be deleted or not in CME GUI	Passed	
MEJ810S_Reg_242	Generating auto Password for management guest user	To check whether Password is generated or not for management guest user	Passed	
MEJ810S_Reg_243	Generating Password manually for management guest user	To check whether manually Password is generating or not for management guest user	Passed	
MEJ810S_Reg_244	Creating a guest user from admin local account	To check whether a guest user can be added or not from local account in CME GUI	Passed	

MEJ810S_Reg_245	Configuring Guest WLAN with default login Page	To check whether a default page can be configured or not for guest login	Passed	
MEJ810S_Reg_246	Configuring Guest WLAN with customized login Page	To check whether a customized page can be configured or not for guest login	Passed	

ME AP convert to CAPWAP via DHCP Option 43

Logical ID	Title	Description	Status	Defect ID
MEJ810S_Reg_319	Change the 1852 ME AP type to CAPWAP using DHCP 43	To change the AP type to CAPWAP using DHCP 43	Passed	
MEJ810S_Reg_320	Change the 2800 ME AP type to CAPWAP using DHCP 43	To change the AP type to CAPWAP using DHCP 43	Passed	
MEJ810S_Reg_321	Change the 1542 ME AP type to CAPWAP using DHCP 43	To change the AP type to CAPWAP using DHCP 43	Passed	
MEJ810S_Reg_322	Change the 1815i ME AP type to CAPWAP using DHCP 43	To change the AP type to CAPWAP using DHCP 43	Passed	
MEJ810S_Reg_323	Change the AP mode after converting in to CAPWAP	To change the AP mode after converting in to CAPWAP	Passed	
MEJ810S_Reg_324	Connect iOS client to C AP w AP converted AP from ME with WPA2-PSK security	To connect the iOS client to CAPWAP converted AP from ME with WPA2-PSK security	Passed	
MEJ810S_Reg_325	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	

MEJ810S_Reg_326	Config primary, secondary controller in AP and reload ME controller	To verify that ME changed to c AP w AP and send join request to controller that configured using DHCP option 43	Passed	
MEJ810S_Reg_327	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	
MEJ810S_Reg_328	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	
MEJ810S_Reg_329	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	

Mobexp

Logical ID	Title	Description	Status	Defect ID
MEJ810S_config_01	ME - WPA3 security not reflecting properly under WLAN Configuration in Prime	To check whether WPA3 Security reflecting properly under WLAN configuration	Failed	CSCvq37457
MEJ810S_Config_04	Not able to change the Security type from Enhanced Open to Personal WPA3	To check whether the security type change from enhanced open to personal WPA3	Failed	CSCvq39003

Import EAP certificates

Logical ID	Title	Description	Status	Defect ID

MEJ810S_Reg_247	Downloading the EAP device certificate through HTTP	To verify whether EAP device certificate is downloading or not through HTTP mode	Passed	
MEJ810S_Reg_248	downloading the EAP device certificate via SFTP	To verify whether EAP device certificate is downloading or not through SFTP	Passed	
MEJ810S_Reg_249	Downloading the EAP device certificate through FTP	To verify whether EAP device certificate is downloading or not through FTP mode	Passed	
MEJ810S_Reg_250	Downloading the EAP device certificate through TFTP	To verify whether EAP device certificate is downloading or not through TFTP mode	Passed	
MEJ810S_Reg_251	Downloading the EAP CA certificate through HTTP	To verify whether EAP CA certificate is downloading or not through HTTP mode	Passed	
MEJ810S_Reg_252	Downloading the EAP CA certificate through FTP	To verify whether EAP CA certificate is downloading or not through FTP mode	Passed	
MEJ810S_Reg_253	Downloading the EAP CA certificate through SFTP	To check whether EAP CA certificate is downloading or not through SFTP server	Passed	
MEJ810S_Reg_254	Downloading the EAP CA certificate through TFTP	To verify whether EAP CA certificate is downloading or not through TFTP mode	Passed	
MEJ810S_Reg_255	Downloading the NA SERV CA Certificate through HTTP	To verify whether NA SERV CA Certificate is downloading or not through HTTP mode	Passed	

MEJ810S_Reg_256	Downloading the NA SERV CA Certificate through FTP	To verify whether NA SERV CA Certificate is downloading or not through FTP mode	Passed	
MEJ810S_Reg_257	Downloading the NA SERV CA Certificate through SFTP	To check whether NA SERV CA Certificate is downloading or not through SFTP mode	Passed	
MEJ810S_Reg_258	Downloading the NA SERV CA Certificate through TFTP	To verify whether NA SERV CA Certificate is downloading or not through TFTP mode	Passed	
MEJ810S_Reg_259	Initiate the download with read-only mode	To verify whether image download initiating or not for read-only user or not	Passed	
MEJ810S_Reg_260	Trying to reset the system at the time of certificate download	To verify whether system resetting or not at the time of downloading the certificate	Passed	
MEJ810S_Reg_261	Initiating the certificates(EAP ,EAP CA,NA SEV) download through HTTP from CLI	To verify whether image is downloading or not from HTTP mode through CLI	Passed	
MEJ810S_Reg_262	Initiating the certificates(EAP ,EAP CA,NA SEV) download through FTP from CLI	To verify whether image is downloading or not from FTP mode through CLI	Passed	
MEJ810S_Reg_263	Initiating the certificates(EAP ,EAP CA,NA SEV) download through SFTP from CLI	To verify whether certificate is downloading or not from SFTP mode through CLI	Passed	
MEJ810S_Reg_264	Initiating the certificates(EAP ,EAP CA,NA SEV) download through TFTP from CLI	To verify whether image is downloading or not from TFTP mode through CLI	Passed	

MEJ810S_Reg_265	Initiating the download through read-only mode	To verify whether certificate are downloading or not read-only user	Passed	

No reboot of AP when AP joins AP group

Logical ID	Title	Description	Status	Defect ID
MEJ810S_Reg_42	Creating the AP group with Japanese LAN gauge and assigning the COS AP	To verify whether AP associating to the AP group or not	Passed	
MEJ810S_Reg_43	Moving the 1852/1832 COS AP between different Groups in CME(1800/2800/3800/1500)	To verify whether 1852/1832 COS AP changing the groups or not without reboot in 1800/2800/3800/1500 CME models	Passed	
MEJ810S_Reg_44	Moving the 1542/1562 COS AP between different AP Groups in CME(1800/2800/3800/1500)	To verify whether 1542/1562 COS AP moving between different groups or not without reboot in CME(1800/2800/3800/1500)	Passed	
MEJ810S_Reg_45	Moving the 2802I COS AP between different AP Groups in CME(1800/2800/3800/1500)	To verify whether 2802I2 COS AP moving between different groups or not without reboot in CME(1800/2800/3800/1500)	Passed	
MEJ810S_Reg_46	Moving the 3802I/3802E COS AP between different AP Groups in CME(1800/2800/3800/1500)	To verify whether 3802I/3802E COS AP moving between different groups or not without reboot in CME(1800/2800/3800/1500)	Passed	
MEJ810S_Reg_47	Moving the 1815I/1810 COS AP between different AP Groups in CME(1800/2800/3800/1500)	To verify whether 1815I/1810 COS AP moving between different groups or not without reboot in CME(1800/2800/3800/1500)	Passed	

MEJ810S_Reg_48	Changing the AP between groups at the time of software upgrade/downgrade	To verify whether it is possible to change the AP group or not at the time upgrading the image	Passed	
MEJ810S_Reg_49	Master/Next-preferred AP Changing between different groups at the time of software upgrade/downgrade	To verify whether after AP group change Master/Next-preferred AP downloading the image or not	Passed	
MEJ810S_Reg_50	Changing the AP between different AP group in read-only mode	To verify whether AP is Changing the Groups or not in read-only mode	Passed	
MEJ810S_Reg_51	Moving the 702/3700/2700 IOS AP between different AP Groups in CME(1800/2800/3800/1500)	To verify whether 702/3700/2700 COS AP moving between different groups or not without reboot in CME(1800/2800/3800/1500)	Passed	
MEJ810S_Reg_52	Assigning the default RF-Profile to AP group from PI	To verify whether default RF-Profile is AP plying to the AP -group or not	Passed	
MEJ810S_Reg_53	Assigning the user defined RF-Profile with 2.4/5 GHZ to AP group from PI	To verify whether user defined RF-profile with 2.4/5GHZ is applying to the AP -group or not	Passed	
MEJ810S_Reg_54	Changing the COS APs between different AP -groups from PI	To verify whether COS APs are changing successfully between AP groups without reboot or not	Passed	
MEJ810S_Reg_55	Changing the IOS APs between different AP -groups from PI	To verify whether IOS APs are changing successfully between AP groups without reboot or not	Passed	

Bidirectional rate limit per client

Logical ID	Title	Description	Status	Defect ID

MEJ810S_Reg_266	Configuring rate limit for per client for different types of client with WPA 2 Personal security with QOS as Silver	To configure rate limit for JOS client with open security and QOS as silver and check if the client gets the rate that is been configured or not.	Passed	
MEJ810S_Reg_267	Configuring rate limit for per client with QOS as Gold for different types of client with WPA 2 Enterprise security	To configure rate limit per client with QOS as Gold and connecting a JOS client with WPA 2 Enterprise security and check if the rate limit is AP plied or not.	Passed	
MEJ810S_Reg_268	Connecting a client to a WLAN configured with rate limit using two different AP	To configure rate limit for client and connecting a client to one AP and check the rate limit and making that AP down and connecting the client to other AP and check if the behavior of the client is same or not	Passed	
MEJ810S_Reg_269	Connecting a client to a WLAN configured with rate limit using one ME capable AP and Non Me capable AP in AP group	To Connecting a client to a WLAN configured with rate limit using one ME capable AP and Non Me capable AP in AP group	Passed	
MEJ810S_Reg_270	Creating a AVC rule for the W LAN for which rate limit is configured .	To configure lesser rate limit in WLAN and configuring higher rate limit in AVC and check if the rate limit for the client	Passed	

Capwap Image Conversion

Logical ID	Title	Description	Status	Defect ID

MEJ810S_Reg_31	Joining the AP image with less than other than ME and checking the details	To verify whether AP join to the CME and downloading the image or not	Passed	
MEJ810S_Reg_32	Joining the AP after Efficient join enable/Disable state	To verify whether AP is joining & downloading image from ME or not after efficient join enable state	Passed	
MEJ810S_Reg_33	COS AP with CAPWAP image joins to ME WLC with	To verify whether COS AP is joining to the ME with ME capable or not	Passed	
MEJ810S_Reg_34	IOSAP with CAPWAP image joins to ME WLC	To verify whether IOS AP is joining to the ME with AP & ME different version and not downloading the image	Passed	
MEJ810S_Reg_35	Upgrading the ME image and making the CAPWAPs to ME capable	To verify whether APs converting the ME capable or not after upgrade the ME image	Passed	
MEJ810S_Reg_36	Downgrading the ME image and making the CAPWAP APs to ME capable	To verify whether APs converting the ME capable or not after downgrade the ME image	Passed	
MEJ810S_Reg_37	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	
MEJ810S_Reg_38	Changing the ME time and trying to join the AP	To verify whether AP joining to the ME or not with AP and ME times are different	Passed	
MEJ810S_Reg_39	Performing the Master AP failover	To verify whether after Master AP failover, AP is again downloading the images or not	Passed	

MEJ810S_Reg_40	Interchanging the ME image	To verify whether after image interchange ME coming as changed version or not	Passed	
MEJ810S_Reg_41	Interchanging the AP image and making as ME Controller	To verify whether after AP interchange, AP is coming as changed image with ME capable controller or not	Passed	

AAA Override of VLAN Name / VLAN Name-id template

Logical ID	Title	Description	Status	Defect ID
MEJ810S_Reg_119	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 W LAN and check if the VLAN from AAA server is overridden to the client	Passed	
MEJ810S_Reg_120	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	

MEJ810S_Reg_121	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	
MEJ810S_Reg_122	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 V LAN from AAA server is overridden to the client	Passed	
MEJ810S_Reg_123	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	
MEJ810S_Reg_124	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 V LAN is overridden or not.	Passed	
MEJ810S_Reg_125	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	

MEJ810S_Reg_126	Connecting a MacOS client to the AAA override enabled WLAN with WPA 2 Enterprise security enabled with AAA overide .	To connect a Mac OS client to AAA override enabled WLAN with WPA 2 Enterprise security and check if the Native V LAN is overridden or not.	Passed	
MEJ810S_Reg_127	Connecting a client to the WLAN enabled with AAA override but the configuration of VLAN on AAA is not done.	To connect a client to the WLAN enabled with AAA override and the configuration of VLAN is not done in the AAA server.	Passed	

Software update using SFTP

Logical ID	Title	Description	Status	Defect ID
MEJ810S_Reg_90	ME AP 1815 Software updating via SFTP server	Verifying AP 1815 ME software updating or not via SFTP server	Passed	
MEJ810S_Reg_91	Invalid software updating via SFTP server for ME AP 1815	To check whether Invalid software updating or not via SFTP server	Passed	
MEJ810S_Reg_92	Software Schedule Update on ME AP 1830 via SFTP server	Validate the software Schedule Update on ME AP 1830 via SFTP server	Passed	
MEJ810S_Reg_93	Software Update on ME AP 1850 via SFTP server	Verifying AP 1850 ME software updating or not via SFTP server	Passed	
MEJ810S_Reg_94	Invalid software updating via SFTP server on ME AP 1850	Verifying whether Invalid software updating or not on ME AP 1850	Passed	
MEJ810S_Reg_95	Schedule the Software update on 1850 ME AP	Verifying on schedule time ME software is updating or not	Passed	

MEJ810S_Reg_96	Software updating via SFTP server on ME 2800 AP	To check whether software is updating or not via SFTP server on 2800 AP	Passed	
MEJ810S_Reg_97	Invalid software updating on ME 2800 AP via SFTP software	Verifying whether Invalid software updating or not on ME AP 2800	Passed	
MEJ810S_Reg_98	Software Update Schedule on ME AP 2800 via SFTP server	Validate the software Schedule Update on ME AP 2800 via SFTP server	Passed	
MEJ810S_Reg_99	Software updating via SFTP server on ME 3800 AP	To check whether software is updating or not via SFTP server on 3800 AP	Passed	
MEJ810S_Reg_100	Invalid software updating on ME 3800 AP via SFTP software	Verifying whether Invalid software updating or not on ME AP 3800	Passed	
MEJ810S_Reg_101	Software Update Schedule on ME AP 3800 via SFTP server	Validate the software Schedule Update on ME AP 3800 via SFTP server	Passed	

P2P Blocking

Logical ID	Title	Description	Status	Defect ID
MEJ810S_Reg_180	Connecting any two different OS Client to a open security WLAN enabling Peer to Peer Block	To connect two JOS Client to a open security WLAN enabling Peer to Peer Block and check if there is a traffic flow between two Clients or not	Passed	

MEJ810S_Reg_181	Connecting two different OS Client to a WPA 2 Personal security WLAN enabling Peer to Peer Block	To connect two JOS Client to a WPA 2 Personal security WLAN enabling Peer to Peer Block and check if there is a traffic flow between two Clients or not	Passed	
MEJ810S_Reg_182	Connecting two different OS Client to a WPA 2 Enterprise security WLAN enabling Peer to Peer Block	To connect two JOS Client to a WPA 2 Enterprise security WLAN enabling Peer to Peer Block and check if there is a traffic flow between two Clients or not	Passed	
MEJ810S_Reg_183	Connecting four different Client to a open security WLAN enabling Peer to Peer Block	To connect four different Client to a open security WLAN enabling Peer to Peer Block and check if there is a traffic flow between two Clients or not	Passed	
MEJ810S_Reg_184	Connecting four different Client to a WPA 2 Personal security WLAN enabling Peer to Peer Block	To connect four different Client to a WPA 2 Personal security WLAN enabling Peer to Peer Block and check if there is a traffic flow between two Clients or not	Passed	
MEJ810S_Reg_185	Connecting four different Client to a WPA 2 Enterprise security W LAN enabling Peer to Peer Block	To connect four different Client to a WPA 2 Enterprise security WLAN enabling Peer to Peer Block and check if there is a traffic flow between two Clients or not	Passed	

MEJ810S_Reg_186	Connecting two Windows Client to W LAN enabling Peer to Peer Block and trying WebEx meeting between Client	To connect two Windows Client to W LAN enabling Peer to Peer Block and trying WebEx meeting between Client	Passed	

802.1x support for EAP-TLS & PEAP

Logical ID	Title	Description	Status	Defect ID
MEJ810S_Reg_276	Enabling dot1x auth for AP and joining AP to ME WLC	To check whether AP joins ME or not after dot1x authentication from Switch/ISE	Passed	
MEJ810S_Reg_277	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	
MEJ810S_Reg_278	Joining COS AP to ME through Dot1x+PE AP authentication	To check whether COS AP joins ME or not after dot1x authentication from Switch/ISE via E AP method PE AP	Passed	
MEJ810S_Reg_279	Joining iOS AP to ME through Dot1x+E AP TLS authentication	To check whether iOS AP joins ME or not after dot1x authentication from Switch/ISE via E AP method TLS	Passed	
MEJ810S_Reg_280	Trying to join APs through Dot1x authentication with LSC provisioning	To check whether APs joins ME or not through LSC provisioning & dot1x authentication	Passed	
MEJ810S_Reg_281	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	

MEJ810S_Reg_282	Disabling dot1x support in Switch and trying to associate AP via Dot1x authentication to ME WLC	To check whether AP joins ME or not even dot1x is disabled in switch	Passed	
MEJ810S_Reg_283	Enabling dot1x auth for AP in 3850 Switch	Configuring the 3850 Switch for Dot1x authentication by m AP ping the identity profiles to a port.	Passed	
MEJ810S_Reg_284	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 ME UI via TFTP	Passed	
MEJ810S_Reg_285	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	
MEJ810S_Reg_286	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	
MEJ810S_Reg_287	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	
MEJ810S_Reg_288	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 ME UI	Passed	

Dynamic OUI update

Logical ID	Title	Description	Status	Defect ID
MEJ810S_Reg_81	OUI file uploading via TFTP server In ME UI	To check whether OUI file is uploading or not via TFTP server	Passed	
MEJ810S_Reg_82	OUI file uploading via TFTP server In ME CLI	Validate the OUI file is uploading or not in ME CLI	Passed	
MEJ810S_Reg_83	Uploading the invalid OUI file through via TFTP server	Verify Invalid OUI file is uploading or not via TFTP sever	Passed	
MEJ810S_Reg_84	OUI file uploading via HTTP server in ME UI	To check whether OUI file is uploading via HTTP server or not in ME UI	Passed	
MEJ810S_Reg_85	OUI file uploading via HTTP server in ME CLI	validate via http server OUI file is uploading or not in ME CLI	Passed	
MEJ810S_Reg_86	Invalid OUI File uploading via HTTP sever	Validate Invalid OUI file is uploading or not via HTTP server	Passed	
MEJ810S_Reg_87	Uploading the OUI file via FTP server in ME UI	To check whether OUI file is uploading or not	Passed	
MEJ810S_Reg_88	Uploading the OUI file via FTP server in ME CLI	Validate the OUI file is uploading via ftp server in ME CLI	Passed	
MEJ810S_Reg_89	Invalid OUI File uploading via FTP sever	To check whether Invalid OUI file is uploading or not via FTP server	Passed	

WLC AireOS

Assurance - Sensor test Configuration - 11b, 11ac, # of spatial stream, certain 802.11 protocol

Logical ID	Title	Description	Status	Defect ID
WLJ810S_Reg_54	Adding the controller in DNAC	Provisioning the controller in DNAC	Passed	
WLJ810S_Reg_55	Performing Network Test in Sensor - Driven Test	Verifying the IP Addressing, DNS, Host Reachability & RADIUS Tests in Sensor - Driven Test	Passed	
WLJ810S_Reg_56	Capturing the Network Test from Wireless Sensor Dashboard	Monitoring the IP Addressing, DNS, Host Reachability & RADIUS Tests in Wireless Sensor Dashboard	Passed	
WLJ810S_Reg_57	Performing Performance Test in Sensor - Driven Test	Verifying the Speed Test & ISPLA Test in Sensor - Driven Test	Passed	
WLJ810S_Reg_58	Capturing the Performance Test from Wireless Sensor Dashboard	Monitoring the Speed Test & ISPLA Test in Wireless Sensor Dashboard	Passed	
WLJ810S_Reg_59	Performing Application Test in Sensor - Driven Test	Verifying the Email Test, Web Test & File Transfer Test in Sensor - Driven Test	Passed	
WLJ810S_Reg_60	Capturing the Application Test from Wireless Sensor Dashboard	Monitoring the Email Test, Web Test & File Transfer Test in Wireless Sensor Dashboard	Passed	
WLJ810S_Reg_61	Performing Scheduling Onboarding Packet Capture Test	Checking whether the Scheduling Onboarding Packet capture is done as per the schedule or not	Passed	

WLJ810S_Reg_62	Capturing Configured APs using Auto-Capture Settings	Testing whether the user able to capture or not the Configured APs using Auto-Capture Settings	Passed	
WLJ8102S_Reg_25	Adding the controller in DNAC	Provisioning the controller in DNAC	Passed	
WLJ8102S_Reg_26	Performing Network Test in Sensor - Driven Test	Verifying the IP Addressing, DNS, Host Reachability & RADIUS Tests in Sensor - Driven Test	Passed	
WLJ8102S_Reg_27	Capturing the Network Test from Wireless Sensor Dashboard	Montoring the IP Addressing, DNS, Host Reachability & RADIUS Tests in Wireless Sensor Dashboard	Passed	
WLJ8102S_Reg_28	Performing Performance Test in Sensor - Driven Test	Verifying the Speed Test & ISPLA Test in Sensor - Driven Test	Passed	
WLJ8102S_Reg_29	Capturing the Performance Test from Wireless Sensor Dashboard	Monitoring the Speed Test & ISPLA Test in Wireless Sensor Dashboard	Passed	
WLJ8102S_Reg_30	Performing Application Test in Sensor - Driven Test	Verifying the Email Test, Web Test & File Transfer Test in Sensor - Driven Test	Passed	
WLJ8102S_Reg_31	Capturing the Application Test from Wireless Sensor Dashboard	Monitoring the Email Test, Web Test & File Transfer Test in Wireless Sensor Dashboard	Passed	
WLJ8102S_Reg_32	Performing Scheduling Onboarding Packet Capture Test	Checking whether the Scheduling Onboarding Packet capture is done as per the schedule or not	Passed	

WLJ8102S_Reg_33	Capturing Configured APs using Auto-Capture Settings	Testing whether the user able to capture or not the Configured APs using Auto-Capture Settings	Passed	

Assurance - Sensor Client On-Boarding Failures & Times – WebAuth

Logical ID	Title	Description	Status	Defect ID
WLJ810S_Reg_27	Adding the controller in DNAC	Provisioning the controller in DNAC	Passed	
WLJ810S_Reg_28	Upgrading WLC from DNAC	Verifying whether the user is able to upgrade the controller or not from DNAC	Passed	
WLJ810S_Reg_29	Checking the Performance of APs in DNAC	Verifying whether the Performance of APs are monitored correctly as per in the controller or not in DNAC	Passed	
WLJ810S_Reg_30	Verifying how many wireless devices are added in DNAC	Checking whether how many wireless devices are added in DNAC and they are monitored properly or not	Passed	
WLJ810S_Reg_31	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	
WLJ810S_Reg_32	Checking the Client connectivity status in DNAC	Verifying whether the Client status are monitored correctly as per in the controller or not in DNAC	Passed	

WLJ810S_Reg_33	Checking the Client Onboarding Times in DNAC	Verifying whether the Client Onboarding Times are monitored correctly as per in the controller or not in DNAC	Passed	
WLJ810S_Reg_34	Checking the Client Count per SSID in DNAC	Verifying whether the Client Count per SSID are monitored correctly as per in the controller or not in DNAC	Passed	
WLJ810S_Reg_35	Checking the Client Count per Band in DNAC	Verifying whether the Client Count per Band are monitored correctly as per in the controller or not in DNAC	Passed	
WLJ810S_Reg_36	Checking the Client RSSI & SNR values in DNAC	Verifying whether the RSSI & SNR are monitored correctly as per in the controller or not in DNAC	Passed	
WLJ810S_Reg_37	Checking the throughput & Packet loss details for the wireless devices	Verifying the Usage of Bytes, Average throughput & Packet loss details for the wireless devices	Passed	
WLJ8102S_Reg_01	Adding the controller in DNAC	Provisioning the controller in DNAC	Passed	
WLJ8102S_Reg_02	Upgrading WLC from DNAC	Verifying whether the user is able to upgrade the controller or not from DNAC	Passed	
WLJ8102S_Reg_03	Checking the Performance of APs in DNAC	Verifying whether the Performance of APs are monitored correctly as per in the controller or not in DNAC	Passed	

WLJ8102S_Reg_04	Verifying how many wireless devices are added in DNAC	Checking whether how many wireless devices are added in DNAC and they are monitored properly or not	Passed	
WLJ8102S_Reg_05	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	
WLJ8102S_Reg_06	Checking the Client connectivity status in DNAC	Verifying whether the Client status are monitored correctly as per in the controller or not in DNAC	Passed	
WLJ8102S_Reg_07	Checking the Client Onboarding Times in DNAC	Verifying whether the Client Onboarding Times are monitored correctly as per in the controller or not in DNAC	Passed	
WLJ8102S_Reg_08	Checking the Client Count per SSID in DNAC	Verifying whether the Client Count per SSID are monitored correctly as per in the controller or not in DNAC	Passed	
WLJ8102S_Reg_09	Checking the Client Count per Band in DNAC	Verifying whether the Client Count per Band are monitored correctly as per in the controller or not in DNAC	Passed	
WLJ8102S_Reg_10	Checking the Client RSSI & SNR values in DNAC	Verifying whether the RSSI & SNR are monitored correctly as per in the controller or not in DNAC	Passed	

WLJ8102S_Reg_11	Checking the throughput & Packet loss details for the wireless devices	Verifying the Usage of Bytes, Average throughput & Packet loss details for the wireless devices	Passed	

LAG support in Flexconnect

Logical ID	Title	Description	Status	Defect ID
WLJ810S_Reg_01	Verify the LAG after changing AP mode from Local to Flex	Checking the LAG mode after changing the AP mode from local to Flex	Passed	
WLJ810S_Reg_02	Verify LAG can be enabled when AP in Flex mode	To check whether LAG is enabled or not when AP in Flex mode	Passed	
WLJ810S_Reg_03	Verify the traffic load balance via inner CAPWAP 4-tuple hashing with traffic streams on AP in Flex mode	Checking the traffic load balance via inner CAPWAP 4-tuple hashing with traffic strams when AP on Flex mode	Passed	
WLJ810S_Reg_04	Join the AP to WLC using only the 2nd port in Ether Channel Active mode & external power source	To check whether AP is joined or not using only 2nd port in Ether Channel Active mode & with external power source	Passed	
WLJ810S_Reg_05	Verifying the LAG bring up workflow on switch/WLC/AP	To check whether wireless client is connected or not after LAG bringup	Passed	
WLJ810S_Reg_06	Enable global LAG with a lag capable ap joined on default-ap-profile	Verifying the global LAG is enabled or not after LAG capable ap joined on default-ap-profile	Passed	
WLJ810S_Reg_07	Enable global lag with a lag incapable ap joined on default-ap-profile	To check whether Ap disconnects and joins back when global LAG mode enabled on controller	Passed	

WLJ810S_Reg_08	Enable per ap profile lag with a lag capable ap joined on default-ap-profile	Verify the AP reboots and joins back with global lag and ap lag enabled	Passed	
WLJ810S_Reg_09	Disable lag on lag capable ap and reconnect it with both global lag and per ap-profile lag enabled on controller	To check whether AP reboots and joins with LAG enabled or not	Passed	
WLJ810S_Reg_10	Join lag enabled ap with both global lag and per ap-profile lag enabled on controller	To check whether AP reboots or not while joining to controller	Passed	
WLJ810S_Reg_11	Join the lag enabled ap with both global lag and per ap-profile lag enabled, now disable global lag	To check whether AP reboots and joins back with lag disabled or not	Passed	
WLJ810S_Reg_12	Verify the lag enabled ap with global lag enabled, per-ap profile lag enabled	Verify AP joined back with disable LAG mode or not after per-ap profile lag disabled	Passed	
WLJ810S_Reg_13	Verify the TX counters on both AP ports	To check whether TX counter increased or not on both AP port	Passed	
WLJ8102S_Reg_12	Verify the LAG after changing AP mode from Local to Flex	Checking the LAG mode after changing the AP mode from local to Flex	Passed	
WLJ8102S_Reg_13	Verify LAG can be enabled when AP in Flex mode	To check whether LAG is enabled or not when AP in Flex mode	Passed	
WLJ8102S_Reg_14	Verify the traffic load balance via inner CAPWAP 4-tuple hashing with traffic streams on AP in Flex mode	Checking the traffic load balance via inner CAPWAP 4-tuple hashing with traffic strams when AP on Flex mode	Passed	

WLJ8102S_Reg_15	Join the AP to WLC using only the 2nd port in EtherChannel Active mode & external power source	To check whether AP is joined or not using only 2nd port in EtherChannel Active mode & with external power source	Passed	
WLJ8102S_Reg_16	Verifying the LAG bring up workflow on switch/WLC/AP	To check whether wireless client is connected or not after LAG bringup	Passed	
WLJ8102S_Reg_17	Enable global LAG with a lag capable ap joined on default-ap-profile	Verifying the global LAG is enabled or not after LAG capable ap joined on default-ap-profile	Passed	
WLJ8102S_Reg_18	Enable global lag with a lag incapable ap joined on default-ap-profile	To check whether Ap disconnects and joins back when global LAG mode enabled on controller	Passed	
WLJ8102S_Reg_19	Enable per ap profile lag with a lag capable ap joined on default-ap-profile	Verify the AP reboots and joins back with global lag and ap lag enabled	Passed	
WLJ8102S_Reg_20	Disable lag on lag capable ap and reconnect it with both global lag and per ap-profile lag enabled on controller	To check whether AP reboots and joins with LAG enabled or not	Passed	
WLJ8102S_Reg_21	Join lag enabled ap with both global lag and per ap-profile lag enabled on controller	To check whether AP reboots or not while joining to controller	Passed	
WLJ8102S_Reg_22	Join the lag enabled ap with both global lag and per ap-profile lag enabled, now disable global lag	To check whether AP reboots and joins back with lag disabled or not	Passed	

WLJ8102S_Reg_23	Verify the lag enabled ap with global lag enabled, per-ap profile lag enabled	Verify AP joined back with disable LAG mode or not after per-ap profile lag disabled	Passed	
WLJ8102S_Reg_24	Verify the Tx counters on both AP ports	To check whether Tx counter increased or not on both AP port	Passed	

Intelligent Capture using AP 2800/3800/4800

Logical ID	Title	Description	Status	Defect ID
WLJ810S_Reg_74	Configuring Intelligent Capture parameter details on 2800/3800/4800 AP	To configure Intelligent capture parameters in different Aps 2800/3800/4800	Passed	
WLJ810S_Reg_75	Check Configuration after the AP reboot	To Configure Intelligent capture parameters in different Aps 2800/3800/4800 and check if the configuration remains same after the AP reboot.	Passed	
WLJ810S_Reg_76	Configure Intelligent Capture parameters on WLC CLI	To configure Intelligent Capture parameters on WLC CLI and check if all the parameters can be configured using CLI or not	Passed	
WLJ810S_Reg_77	Packet capture of client when the client is connected to 2800/3800/4800 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	
WLJ810S_Reg_78	Packet capture of client when the client is connected to 2800/3800/4800 AP with 5 GHz	To capture the Packet of the client when the client is connected to AP with radio as 5 GHz	Passed	

WLJ810S_Reg_79	Capturing of Packet of the client when the client is connected with open security.	To capture packet when the client is connected to the 2800/3800/4800 AP with security as OPEN	Passed	
WLJ810S_Reg_80	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 2800/3800/4800 AP with security as WPA 2 PSK	Passed	
WLJ810S_Reg_81	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 2800/3800/4800 AP with security as WPA 2 802.1x	Passed	
WLJ810S_Reg_82	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 2800/3800/4800 AP with security as Static WEP	Passed	
WLJ810S_Reg_83	Verifying the packet capture happen 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	
WLJ810S_Reg_84	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	

WLJ810S_Reg_85	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	
WLJ810S_Reg_86	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	
WLJ810S_Reg_87	Performing Inter controller roaming of client and capturing the packet .	To check whether inter controller roaming of Android clients works properly or not	Passed	
WLJ810S_Reg_88	Configuring WLAN session timeout and capturing the packet.	To configure WLAN session timeout and check if the packet capture shows deauth and re association packets or not.	Passed	
WLJ810S_Reg_89	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	
WLJ810S_Reg_90	Packet capture using the AP group with 2800 AP	To capture the packet using the Intelligent packet capture option in AP Group with 2800 AP	Passed	
WLJ810S_Reg_91	Packet capture using the AP group with 3800 AP	To capture the packet using the Intelligent packet capture option in AP Group with 3800 AP	Passed	

WLJ810S_Reg_92	Packet capture using the AP group with 4800 AP	To capture the packet using the Intelligent packet capture option in AP Group with 4800 AP	Passed	
WLJ810S_Reg_93	Packet Capture using AP group without a AP in it	To Check if packet capture occurs or not if no AP is in the AP group.	Passed	
WLJ810S_Reg_94	Packet capture using the AP group with different security	To capture packet when the client is connected to the 2800/3800/4800 AP with different security	Passed	
WLJ810S_Reg_95	Packet capture using roaming scenario in AP group using different Aps	To capture the Packet by using different AP in AP group and check if the client roams between different Aps	Passed	
WLJ810S_Reg_96	Packet Capture for Android client using intelligent capture option in AP group.	To verify the packet capture for Android client using Intelligent capture in AP Group.	Passed	
WLJ810S_Reg_97	Packet Capture for Windows client using intelligent capture option in AP group.	To verify the packet capture for Windows client using Intelligent capture in AP Group.	Passed	
WLJ810S_Reg_98	Packet Capture for IOS client using intelligent capture option in AP group.	To verify the packet capture for IOS client using Intelligent capture in AP Group.	Passed	
WLJ810S_Reg_99	Packet Capture for Mac OS client using intelligent capture option in AP group.	To verify the packet capture for Mac OS client using Intelligent capture in AP Group.	Passed	

WLJ8102S_Reg_58	Configuring Intelligent Capture parameter details on 2800/3800/4800 AP	To configure Intelligent capture parameters in different Aps 2800/3800/4800	Failed	CSCvr82264
WLJ8102S_Reg_59	Check Configuration after the AP reboot	To Configure Intelligent capture parameters in different Aps 2800/3800/4800 and check if the configuration remains same after the AP reboot.	Passed	
WLJ8102S_Reg_60	Configure Intelligent Capture parameters on WLC CLI	To configure Intelligent Capture parameters on WLC CLI and check if all the parameters can be configured using CLI or not	Passed	
WLJ8102S_Reg_61	Packet capture of client when the client is connected to 2800/3800/4800 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	
WLJ8102S_Reg_62	Packet capture of client when the client is connected to 2800/3800/4800 AP with 5 GHz	To capture the Packet of the client when the client is connected to AP with radio as 5 GHz	Passed	
WLJ8102S_Reg_63	Capturing of Packet of the client when the client is connected with open security.	To capture packet when the client is connected to the 2800/3800/4800 AP with security as OPEN	Passed	
WLJ8102S_Reg_64	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 2800/3800/4800 AP with security as WPA 2 PSK	Passed	

WLJ8102S_Reg_65	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 2800/3800/4800 AP with security as WPA 2 802.1x	Passed	
WLJ8102S_Reg_66	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 2800/3800/4800 AP with security as Static WEP	Passed	
WLJ8102S_Reg_67	Verifying the packet caputure happen 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	
WLJ8102S_Reg_68	Verify 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	
WLJ8102S_Reg_69	Verify 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	
WLJ8102S_Reg_70	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	

WLJ8102S_Reg_71	Performing Inter controller roaming of client and capturing the packet .	To check whether inter controller roaming of Android clients works properly or not	Passed	
WLJ8102S_Reg_72	Configuring WLAN session timeout and capturing the packet.	To configure WLAN session timeout and check if the packet capture shows deauth and re association packets or not.	Passed	
WLJ8102S_Reg_73	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	
WLJ8102S_Reg_74	Packet capture using the AP group with 2800 AP	To capture the packet using the Intelligent packet capture option in AP Group with 2800 AP	Passed	
WLJ8102S_Reg_75	Packet capture using the AP group with 3800 AP	To capture the packet using the Intelligent packet capture option in AP Group with 3800 AP	Passed	
WLJ8102S_Reg_76	Packet capture using the AP group with 4800 AP	To capture the packet using the Intelligent packet capture option in AP Group with 4800 AP	Passed	
WLJ8102S_Reg_77	Packet Capture using AP group without a AP in it	To Check if packet capture occurs or not if no AP is in the AP group.	Passed	
WLJ8102S_Reg_78	Packet capture using the AP group with different security	To capture packet when the client is connected to the 2800/3800/4800 AP with different security	Passed	

WLJ8102S_Reg_79	Packet capture using roaming scenario in AP group using different Aps	To capture the Packet by using different AP in AP group and check if the client roams between different Aps	Passed	
WLJ8102S_Reg_80	Packet Capture for Android client using intellingent capture option in AP group.	To verify the packet capture for Android client using Intelligent capture in AP Group.	Passed	
WLJ8102S_Reg_81	Packet Capture for Windows client using intellingent capture option in AP group.	To verify the packet capture for Windows client using Intelligent capture in AP Group.	Passed	
WLJ8102S_Reg_82	Packet Capture for IOS client using intellingent capture option in AP group.	To verify the packet capture for IOS client using Intelligent capture in AP Group.	Passed	
WLJ8102S_Reg_83	Packet Capture for Mac OS client using intellingent capture option in AP group.	To verify the packet capture for Mac OS client using Intelligent capture in AP Group.	Passed	

Workgroup Bridge

Logical ID	Title	Description	Status	Defect ID
WLJ810S_Reg_115	Configuring the lwapp ap to autonomous AP	To change the lwapp apto autonomous ap and check if the AP is converted	Passed	
WLJ810S_Reg_116	Configuring the Autonomous AP as the WGB	To configure the autonomous AP as WGB and check if the AP changes as WGB.	Passed	

WLJ810S_Reg_117	Associating the WGB on open authentication with AP on local mode	To associate the WGB on open authentication when AP in local mode and check if the WGB associates with the open WLAN or not.	Passed	
WLJ810S_Reg_118	Associating the WGB on WPA 2 with PSK with AP on local mode	To associate the WGB on WPA 2 PSK security when AP in local mode and check if the WGB associates with the WLAN or not.	Passed	
WLJ810S_Reg_119	Associating the WGB on WPA 2 with 802.1x with AP on local mode	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	
WLJ810S_Reg_120	Associating the WGB on WPA 2 CCKM with AP on local mode	To associate the WGB on WPA 2 CCKM security when AP in local mode and check if the WGB associates with the WLAN or not.	Passed	
WLJ810S_Reg_121	Associating the WGB on open authentication with AP on Flex mode	To associate the WGB on open authentication when AP in Flex mode and check if the WGB associates with the open WLAN or not.	Passed	
WLJ810S_Reg_122	Associating the WGB on WPA 2 with PSK with AP on Flex mode	To associate the WGB on WPA 2 PSK security when AP in local mode and check if the WGB associates with the WLAN or not.	Passed	

WLJ810S_Reg_123	Associating the WGB on WPA 2 with 802.1x with AP on Flex mode	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	
WLJ810S_Reg_124	Associating the WGB on WPA 2 CCKM with AP on Flex mode	To associate the WGB on WPA 2 CCKM security when AP in local mode and check if the WGB associates with the WLAN or not.	Passed	
WLJ810S_Reg_125	Checking of WGB roaming from one AP to another AP in local mode	To check the roaming of WGB from one AP to another AP when the AP is in local mode .	Passed	
WLJ810S_Reg_126	Checking of WGB roaming from one AP to another AP in flex mode	To check the roaming of WGB from one AP to another AP when Aps arein flex mode	Passed	
WLJ8102S_Reg_84	Configuring the lwapp ap to autonomous AP	To change the lwapp apto autonomous ap and check if the AP is converted	Passed	
WLJ8102S_Reg_85	Configuring the Autonomous AP as the WGB	To configure the autonomous AP as WGB and check if the AP changes as WGB.	Passed	
WLJ8102S_Reg_86	Associating the WGB on open authentication with AP on local mode	To associate the WGB on open authentication when AP in local mode and check if the WGB associates with the open WLAN or not.	Passed	

WLJ8102S_Reg_87	Associating the WGB on WPA 2 with PSK with AP on local mode	To associate the WGB on WPA 2 PSK security when AP in local mode and check if the WGB associates with the WLAN or not.	Passed	
WLJ8102S_Reg_88	Associating the WGB on WPA 2 with 802.1x with AP on local mode	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	
WLJ8102S_Reg_89	Associating the WGB on WPA 2 CCKM with AP on local mode	To associate the WGB on WPA 2 CCKM security when AP in local mode and check if the WGB associates with the WLAN or not.	Passed	
WLJ8102S_Reg_90	Associating the WGB on open authentication with AP on Flex mode	To associate the WGB on open authentication when AP in Flex mode and check if the WGB associates with the open WLAN or not.	Passed	
WLJ8102S_Reg_91	Associating the WGB on WPA 2 with PSK with AP on Flex mode	To associate the WGB on WPA 2 PSK security when AP in local mode and check if the WGB associates with the WLAN or not.	Passed	
WLJ8102S_Reg_92	Associating the WGB on WPA 2 with 802.1x with AP on Flex mode	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	

WLJ8102S_Reg_93	Associating the WGB on WPA 2 CCKM with AP on Flex mode	To associate the WGB on WPA 2 CCKM security when AP in local mode and check if the WGB associates with the WLAN or not.	Passed	
WLJ8102S_Reg_94	Checking of WGB roaming from one AP to another AP in local mode	To check the roaming of WGB from one AP to another AP when the AP is in local mode .	Passed	
WLJ8102S_Reg_95	Checking of WGB roaming from one AP to another AP in flex mode	To check the roaming of WGB from one AP to another AP when Aps arein flex mode	Passed	

Passpoint

Logical ID	Title	Description	Status	Defect ID
WLJ810S_Reg_150	Enabling the 802.11u mode on WLAN with WPA	To verify whether 802.11u mode enabled or not on WLAN	Passed	
WLJ810S_Reg_151	Enabling the Internet Access WLAN and connecting a client	To verify whether Internet Access mode is enabled or not	Passed	
WLJ810S_Reg_152	Configuring the Network type	To verify whether client connecting or not with network type changes from one to other	Passed	
WLJ810S_Reg_153	Configuring the Network Authentication	To verify whether Client is connecting after Network Authentication or not	Passed	
WLJ810S_Reg_154	Checking with IPv4 type details	To verify whether Client connecting or not after IPv4 type changes from one to another	Passed	

WLJ810S_Reg_155	Creating OUI with Duplicatate name	To verify whether OUI is creating with duplicate name or not	Passed	
WLJ810S_Reg_156	Checking the Roaming after Relam configurations	To verify whether client will roam between hotspots or not	Passed	
WLJ810S_Reg_157	Adding cellular network information with duplicate name	To verify whether Cellular network information added successfully	Passed	
WLJ810S_Reg_158	Configuring domain and OSU ID	To verify whether domain and OSU id are applying or not	Passed	
WLJ810S_Reg_159	WAN link selection after cliect connection	To verify whether WAN statues is varying or not	Passed	
WLJ810S_Reg_160	Configure the OSU and Operator name	To verify whether OSU and Operator selection applied successfully or not	Passed	
WLJ810S_Reg_161	Varying Port configurations	To verify whether Port configurations can vary after client connect	Passed	
WLJ810S_Reg_162	Downgrading the AP after Hotspot configurations	To verify whether Client connected or not after downgrade with Hotspot	Passed	
WLJ810S_Reg_163	Upgrading the AP after Hotspot configurations	To verify whether all hotspot details are showing properly or not	Passed	
WLJ810S_Reg_164	Changing the AP modes after Client connect to Hotspot	To verify whether client will connect or not after modes changes in AP	Passed	
WLJ810S_Reg_165	Disable the Internet access check the connectivity	To verify whether Internet is accessing the client or not at the time of internet access disable	Passed	

WLJ810S_Reg_166	Checking the Hotspot details through CLI	To verify whether Hotspot details showing properly or not	Passed	
WLJ810S_Reg_167	Debugging the Hotspot details	To verify the Hotspot details with debug command	Passed	
WLJ810S_Reg_168	Installing cred.conf file in Client devices for EAP-SIM method	Verifying that user is able to Install cred.conf file in Client devices for EAP-SIM or not	Passed	
WLJ810S_Reg_169	Installing CA certificate on Client device for EAP-TLS/TTLS	Verifying that user is able to Install CA certificate on Client device for EAP-TLS/TTLS or not	Passed	
WLJ810S_Reg_170	Assigning the Venue Group to access points	To verify whether Hotspot enabled access point will comes under venue group or not	Passed	

Passive Client ARP Unicast

Logical ID	Title	Description	Status	Defect ID
WLJ810S_Reg_171	Passive Clients is sent to all AP’s as unicast packet	To verify whether ARP Unicast packets send to all AP's or not	Passed	
WLJ810S_Reg_172	Enabling the Passive client data in 2500/5520/8510/8540 controllers	To verify whether Passive client or sending the Unicast data from AP to client or not	Passed	
WLJ810S_Reg_173	Checking the ARP Packet with Multicast-multicast enable	To verify whether ARP packet is sending or not whether Multicast mode enabled	Passed	

WLJ810S_Reg_174	Checking the ARP packet when Multicast-unicast enable	To verify whether Packed is sending or not whether Multicast-unicast enable	Passed	
WLJ810S_Reg_175	Connecting with two WLAN with different client ARP	To verify whether WLAN will support with two different ARP methods in same Interface	Passed	
WLJ810S_Reg_176	ARP unicast verification when AP's are in AP group	To verify whether ARP unicast enabling and accessing fine or not at the time of AP's are in same AP group	Passed	
WLJ810S_Reg_177	Checking with ARP unicast behaviour when feature is disabled and passive client is enabled	To verify whether Client accessing or not whenever we have disable the feature	Passed	
WLJ810S_Reg_178	Testing with non-Cisco WGB with wired clients	To verify whether non-cisco WGB with wired clients will connect or not	Passed	
WLJ810S_Reg_179	Rebootinthe AP after Client ARP unicast enable	To verify whether WLAN showing the information correctly after reboot also	Passed	
WLJ810S_Reg_180	Checking after Upgrade/Downgrade	To verify whether Client is connecting or not after Upgrade/Downgrade	Passed	
WLJ810S_Reg_181	Debugging the ARPclient data	To verify whether ARP details are showing properly or not	Passed	
WLJ810S_Reg_182	Verifying Maximum packets per second	To verify whether the Maximum packets per second the AP will send	Passed	

WLJ8102S_Reg_140	Passive Clients is sent to all AP’s as unicast packet	To verify whether ARP Unicast packets send to all AP's or not	Passed	
WLJ8102S_Reg_141	Enabling the Passive client data in 2500/5520/8510/8540 controllers	To verify whether Passive client or sending the Unicast data from AP to client or not	Passed	
WLJ8102S_Reg_142	Cheking the ARP Packet with Multicast-multicast enable	To verify whether ARP packet is sending or not whether Multicast mode enabled	Passed	
WLJ8102S_Reg_143	Cheking the ARP packet when Multicast-unicast enable	To verify whether Packed is sending or not whether Multicast-unicast enable	Passed	
WLJ8102S_Reg_144	Connecting with two WLAN with different client ARP	To verify whether WLAN will support with two different ARP methods in same Interface	Passed	
WLJ8102S_Reg_145	ARP unicast verification when AP's are in AP group	To verify whether ARP unicast enabling and accessing fine or not at the time of AP's are in same AP group	Passed	
WLJ8102S_Reg_146	Checking with ARP unicast behavior when feature is disabled and passive client is enabled	To verify whether Client accessing or not whenever we have disable the feature	Passed	
WLJ8102S_Reg_147	Testing with non-Cisco WGB with wired clients	To verify whether non-cisco WGB with wired clients will connect or not	Passed	
WLJ8102S_Reg_148	Rebootinthe AP after Client ARP unicast enable	To verify whether WLAN showing the information correctly after reboot also	Passed	

WLJ8102S_Reg_149	Checking after Upgrade/Downgrade	To verify whether Client is connecting or not after Upgrade/Downgrade	Passed	
WLJ8102S_Reg_150	Debuging the ARPclient data	To verify whether ARP details are showing properly or not	Passed	
WLJ8102S_Reg_151	Veryfying Maximum packets per second	To verify whether the Maximum packets per second the AP will send	Passed	

Selective Re-anchor

Logical ID	Title	Description	Status	Defect ID
WLJ810S_Reg_183	Reboot the Controller after Re-anchor enabling	To verify whether Configurations are showing same or different after controller reboot	Passed	
WLJ810S_Reg_184	Downgrade/upgrade the controller with Re-anchor enable	To verify whether Downgrade/upgrade the controller with Re-anchor enable	Passed	
WLJ810S_Reg_185	Checking the Windows JOS Client connectivity after enabling Selective reanchor in WLAN	To verify whether windows jos client is connecting properly or not	Passed	
WLJ810S_Reg_186	Checking the android Client connectivity after enabling Selective reanchor in WLAN	To verify whether android client is connecting properly or not	Passed	
WLJ810S_Reg_187	Checking the IOS Client connectivity after enabling Selective reanchor in WLAN	To verify whether IOS client is connecting properly or not	Passed	
WLJ810S_Reg_188	Roaming the client between 2 controllers	To verify whether client roaming successfully between two controllers	Passed	

WLJ810S_Reg_189	Checking FT roaming for the client	To verify FT roaming for the client using FT protocols	Passed	
WLJ8102S_Reg_152	Reboot the Controller after Re-anchor enabling	To verify whether Configurations are showing same or different after controller reboot	Passed	
WLJ8102S_Reg_153	Downgrade/upgrade the controller with Re-anchor enable	To verify whether Downgrade/upgrade the controller with Re-anchor enable	Passed	
WLJ8102S_Reg_154	Checking the Windows JOS Client connectivity after enabling Selective reanchor in WLAN	To verify whether windows jos client is connecting properly or not	Passed	
WLJ8102S_Reg_155	Checking the android Client connectivity after enabling Selective reanchor in WLAN	To verify whether android client is connecting properly or not	Passed	
WLJ8102S_Reg_156	Checking the IOS Client connectivity after enabling Selective reanchor in WLAN	To verify whether IOS client is connecting properly or not	Passed	
WLJ8102S_Reg_157	Roaming the client between 2 controllers	To verify whether client roaming successfully between two controllers	Passed	
WLJ8102S_Reg_158	Checking FT roaming for the client	To verify FT roaming for the client using FT protocols	Passed	

802.1x on Wave 2 AP (EAP -TLS, EAP-PEAP)

Logical ID	Title	Description	Status	Defect ID
WLJ810S_Reg_127	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	

WLJ810S_Reg_128	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	
WLJ810S_Reg_129	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	
WLJ810S_Reg_130	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	
WLJ810S_Reg_131	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	
WLJ810S_Reg_132	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	
WLJ810S_Reg_133	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	
WLJ810S_Reg_134	Enabling dot1x auth for AP in 3850 Switch	Configuring the 3850 Switch for Dot1x authentication by mapping the identity profiles to a port.	Passed	

WLJ810S_Reg_135	Checking the configuration of 802.1x authentication parameters after export/import the confit file	To check whether 802.1x auth parameters restores or not after export/import the confit file in WLC UI via TFTP	Passed	
WLJ810S_Reg_136	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	
WLJ810S_Reg_137	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	
WLJ810S_Reg_138	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	
WLJ810S_Reg_139	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	
WLJ8102S_Reg_96	Enabling dot1x auth for AP and ioining AP to WLC	To check whether AP joins WLC or not after dot1x authentication from Switch/ISE	Passed	
WLJ8102S_Reg_97	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	

WLJ8102S_Reg_98	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	
WLJ8102S_Reg_99	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	
WLJ8102S_Reg_100	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	
WLJ8102S_Reg_101	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	
WLJ8102S_Reg_102	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	
WLJ8102S_Reg_103	Enabling dot1x auth for AP in 3850 Switch	Configuring the 3850 Switch for Dot1x authentication by mapping the identity profiles to a port.	Passed	
WLJ8102S_Reg_104	Checking the configuration of 802.1x authentication paramaters after export/import the config file	To check whether 802.1x auth parameters restores or not after export/import the config file in WLC UI via TFTP	Passed	

WLJ8102S_Reg_105	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	
WLJ8102S_Reg_106	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	
WLJ8102S_Reg_107	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	
WLJ8102S_Reg_108	Trying to configure of 802.1x authentication paramaters via Read-only User	To check whether Read only user can be able to configure or not the 802.1x auth parameters in WLC UI	Passed	

SR Cases

Logical ID	Title	Description	Status	Defect ID
WLJ810S_SR_01	Configuring sleeping client with external web authentication and connect the windows clients	To verify whether client doesn't authenticate after sleeping clients	Passed	
WLJ810S_SR_02	Overriding external web authentication in web auth and WLAN and connect window clients	To verify whether WLAN web type overrides global web auth successfully	Passed	
WLJ810S_SR_03	Configure external web type globally and internal web type in WLAN and connect the clients	To verify whether client redirects to internal login page successfully	Passed	

WLJ810S_SR_04	Checking SGT ACL's applied to windows client	To verify whether SGT ACL's applied to client successfully	Passed	
WLJ810S_SR_05	Checking SGT ACL's applied from AP to windows client	To verify whether SGT ACL's applied from AP to client successfully	Passed	
WLJ810S_SR_06	Overriding SGT ACL's globally and from AP to windows client	To verify whether SGT ACL'S override successfully	Passed	
WLJ810S_SR_07	Checking speed for client in 5520 controller when LAG is enabled	Verifying client speed is same or not for client in 5520 controller when LAG is enabled	Passed	
WLJ810S_SR_08	Checking speed for client HA controller when LAG is enabled	Verifying client speed is same or not for client in HA controller when LAG is enabled	Passed	
WLJ810S_SR_09	Checking speed of wireless client while uploading/downloading the file	Verifying wireless client speed while uploading or downloading the file	Passed	
WLJ810S_SR_10	Checking the " apple_device_map.xml " file in 8540 WLC after clear the config	To verify that file present in WLC after clear config in the WLC and no error present message while booting	Passed	
WLJ810S_SR_11	Checking the file empty error after reload the ME	To verify that file empty error not there after reload ME	Passed	
WLJ810S_SR_12	Connect Android client with ISR AP where wlan enabled with Local Auth , local Switching	To check the Android client not getting de-auth while AP moved from connected to standalone mode	Passed	

WLJ810S_SR_13	Check iOS clients connectivity when ISR AP move from connected ->standalone->connected mode	To checks the iOS client not getting de-auth while AP moved from connected to standalone mode and new iOS client getting connect when AP came back in connected state	Passed	
WLJ810S_SR_14	Verifying the clients details in CMX for different clients keeping the client idel for some time .	To verify different client details in CMX keeping the client ideal for some time and check the details of the client	Passed	
WLJ810S_SR_15	Verifying the clients details in CMX for different clients connected to different AP.	To verify different client details in CMX keeping the client ideal for some time and check the details of the client	Passed	
WLJ810S_SR_16	Verify the AP status in WLC and DNAC	Checking the AP status are same or not in both the WLC & DNAC	Passed	
WLJ810S_SR_17	Verify the AP status on stand-by controller and in DNAC	Checking the AP status in stand-by controller matches with the AP status in DNAC or not	Passed	
WLJ810S_SR_18	Checking client is connecting to secondary radius after radius fallback	To verify client is connecting to secondary radius server after radius fallback	Passed	
WLJ810S_SR_19	Checking WLC is able to probe only the radius server which is down	To verify WLC is sending probe request to only the radius server which is down	Passed	
WLJ810S_SR_20	Checking client is connecting to primary radius after recover	To verify client is connecting to primary radius server or not after recovery	Passed	

WLJ810S_SR_21	Checking the client connectivity when the primary controller goes down and secondary controller act as active	To check whether there is no failover in client connectivity when primary controller goes down	Passed	
WLJ810S_SR_22	Setting Rx Sop threshold value in 2800 AP	Checking whether we are able to set the values for Rx Sop threshold for 2800 AP or not	Passed	
WLJ810S_SR_23	Setting Rx Sop threshold value in 4800 ME	Checking whether we are able to set the values for Rx Sop threshold for 4800 ME or not	Passed	
WLJ810S_SR_24	Executing CLI commands for rf-profile coverage exception level and checking the same UI	Verifying the rf-profile coverage exception level CLI commands and checking whether it is configured successfully or not in WLC UI	Passed	
WLJ810S_SR_25	Executing CLI commands for rf-profile coverage data and checking the same UI	Verifying the rf-profile coverage data CLI commands and checking whether it is configured successfully or not in WLC UI	Passed	
WLJ810S_SR_26	Executing CLI commands for rf-profile coverage voice and checking the same UI	Verifying the rf-profile coverage voice CLI commands and checking whether it is configured successfully or not in WLC UI	Passed	
WLJ810S_SR_27	Executing CLI commands for rf-profile coverage level and checking the same UI	Verifying the rf-profile coverage level CLI commands and checking whether it is configured successfully or not in WLC UI	Passed	

WLJ810S_SR_28	Pushing interactive CLI template for disabling / enabling 802.11a network from PI to the controller	Verifying the interactive CLI commands for disabling / enabling 802.11a network are pushed successfully from PI to the controller or not	Passed	
WLJ810S_SR_29	Pushing interactive CLI template for creating a WLAN from PI to the controller	Verifying the interactive CLI commands for creating a WLAN are pushed successfully from PI to the controller or not	Passed	
WLJ810S_SR_30	Pushing interactive CLI template for disabling / enabling a WLAN from PI to the controller	Verifying the interactive CLI commands for disabling / enabling a WLAN are pushed successfully from PI to the controller or not	Passed	
WLJ810S_SR_31	Pushing multiple interactive CLI commands for upgrading the controller from PI to the controller	Verifying whether multiple interactive commands for upgrading the controller from PI is successfully excited or not	Passed	
WLJ810S_SR_32	Uploading config file to ftp/tftp server from WLC	To verify whether config files are uploading to ftp/tftp servers with out any issues	Passed	
WLJ810S_SR_33	downloading config files from ftp/tftp servers to WLC	To verify whether config files are downloading to WLC from ftp/tftp servers with out any issues	Passed	

WLJ810S_SR_34	downloading empty/missing config files from ftp/tftp server to WLC	To verify whether empty/missing config files config files are downloading to WLC from ftp/tftp servers or not	Passed	
WLJ810S_SR_35	Configuring rogue rule as malicious and connecting client	To verify whether rogue client details showing as malicious AP after connected client	Passed	
WLJ810S_SR_36	Configuring rogue rule as friendly and connecting client	To verify whether rogue client details showing as friendly AP after connected client	Passed	
WLJ810S_SR_37	Configuring rogue rule as custom and connecting client	To verify whether rogue client details showing as custom AP after connected client	Passed	
WLJ810S_SR_38	Adding a WLC to PI and checking WLC configuration, synced details in PI after upgrade	To Check added device configuration details in PI after upgrading	Passed	
WLJ810S_SR_39	Adding a WLC to PI and checking WLC configuration ,synced details in PI after downgrade	To Check added device configuration details in PI after downgrade	Passed	
WLJ810S_SR_40	Adding a WLC to PI and reboot PI after delete the device	To verify whether added and synced WLC are able to deleted in PI after rebooting PI	Passed	
WLJ810S_SR_41	Validating the Local switching WLAN's by moving the AP one Controller to another.	To verify the Local switching WLAN's by moving the AP from one WLC to another WLC	Passed	
WLJ810S_SR_42	Validating the Local switching WLAN's in HA failover condition.	To verify the Local switching WLAN's by making down the Primary WLC.	Passed	

WLJ810S_SR_43	Verifying the AP logs by changing the AP mode.	To verify the AP logs after joining into Secondary controller.	Passed	
WLJ810S_SR_44	Validating the AP logs	To verify the AP logs after joining into Secondary controller.	Passed	
WLJ810S_SR_45	Verifying the AP logs by configuring the MTU	To verify the AP logs after joining into Secondary controller.	Passed	
WLJ810S_SR_46	Verifying the AP logs by connecting the Client.	To verify the AP logs after joining into Secondary controller.	Passed	
WLJ810S_SR_47	Configure the rouge AP rules and dot11 radio parameters.	To verify whether the Rouge AP rules and dot11 radio parameters are applying to AP.	Passed	
WLJ810S_SR_48	Configure the rouge AP rules and dot11 radio parameters.	To verify whether the Rouge AP rules and dot11 radio parameters are applying to AP.	Passed	
WLJ810S_SR_49	Verify the SNMP trape logs after Adding the Controller to CMX	To verify whether SNMP requests are generating after adding the Controller in to CMX.	Passed	
WLJ810S_SR_50	Check the SNMP trape logs after Adding the Upgraded Controller to CMX	To Check whether SNMP requests are generating after adding the Upgraded Controller in to CMX.	Passed	
WLJ810S_SR_51	Verify the AP mode after moving the WLC1 to WLC2	To check whether AP mode is changed or not after moving to WLC1 to WLC2	Passed	

WLJ810S_SR_52	Move the flex Connect AP from WLC1 user flexgroup to WLC2 default flexgroup	Checking the AP is moved or not from WLC1 user flexgroup to WLC2 default flexgroup	Passed	
WLJ810S_SR_53	Enable the SSH for AP1810	Verify the SSH mode status after moving to 5520WLC to 3504WLC	Passed	
WLJ810S_SR_54	Checking the SSH mode in 600 OEAP	To check whether SSH AP specific enabled/disabled after OEAP enabled	Passed	
WLJ810S_SR_55	Configuring beacon interval to 500 ms and checking the association request/response after editing security type with iOS AP's	To verify that association request/response is proper after configure beacon interval 500 ms and edit security type	Passed	
WLJ810S_SR_56	Check the Association Req/Rasp after set the beacon interval in 1000ms for COS Aps	To verify that association request/response is accepting both client & AP after set the beacon interval in 1000ms	Passed	
WLJ810S_SR_57	Checking the wireless client RSSI/SNR value in PI/MSE MAP	To check whether the wireless client RSSI/SNR value is proper ot not in PI/MSE MAP	Passed	
WLJ810S_SR_58	Checking the direct console response from MSE	Verify the direct console response when installed CMX to MSE physical	Passed	
WLJ810S_SR_59	Checking the association of IP phones when AP moves to Standalone mode	To check whether IP phones gets associated successfully or not to AP when it moves to Standalone from Connected	Passed	

WLJ810S_SR_60	Enabling WPA GTK-randomize State in a WLAN and checking Client association with WPA2 PSK	To check whether clients getting associated successfully or not after enabling WPA GTK-randomize State in a WLAN with WPA2-PSK	Passed	
WLJ810S_SR_61	Enabling WPA GTK-randomize State in a WLAN and checking Client association with WPA2 802.1x	To check whether clients getting associated successfully or not after enabling WPA GTK-randomize State in a WLAN with WPA2-802.1x	Passed	
WLJ810S_SR_62	Performing Inter roaming with enabling WPA GTK-randomize state in a WLAN	To check whether clients getting associated successfully or not during inter-roaming with GTK-randomize state enabled	Passed	
WLJ810S_SR_63	Checking the association of clients after AP high availability	To check whether clients stays connected or not after AP got moved to secondary when primary WLC goes down	Passed	
WLJ810S_SR_64	Checking the clients sync in HA after deleting & adding the client in Secondary WLC	To check whether clients in sync or not after deleting & adding the client in Secondary WLC	Passed	
WLJ810S_SR_65	Verifying the trap logs during channel change in XOR radio	To check whether trap logs is shown properly or not during channel change in XOR radio	Passed	
WLJ8102S_SR_01	Checking the client AID in Intra roaming with AP flexmode and localswitching	To check the client association id in intra roaming condition with AP flex and localswitching	Passed	

WLJ8102S_SR_02	Checking the Association Id for different OS clients with 2.4/5 GHZ	To check the Association Id for different OS clients with 2.4/5GHZ	Passed	
WLJ8102S_SR_03	Verify the client Association Id by configuring the max allowed client per AP radio	To verify the client Association Id by configuring the max allowed client per AP radio	Passed	
WLJ8102S_SR_04	Checking the client AID in Standby controller	To check the client AID by making the HA sync to standby controller	Passed	
WLJ8102S_SR_05	Configuring WLC9800 in Day0 mode with NTP server	To verify the Day0 configuration of WLC9800 with NTP server.	Passed	
WLJ8102S_SR_06	Configuring WLC9800 in Day0 mode wrong NTP server.	To verify the Day0 configuration of WLC9800 with wrong NTP server.	Passed	
WLJ8102S_SR_07	Configuring WLC9800 in Day0 mode with wrong interface	To verify the Day0 configuration of WLC9800 with wrong interface.	Passed	
WLJ8102S_SR_08	Verify the Client devices are reporting health.	To verify whether Client device are reporting healith or not.	Passed	
WLJ8102S_SR_09	Check the number of Client visits to the building and the floor and devices are reporting health.	To check the number of new Clients and repeated Clients to the building or floor	Passed	
WLJ8102S_SR_10	Verify the AP tcp-mss size after upgrading with the controller latest image.	To verify the AP tcp-mss size after upgrading with the controller latest image.	Passed	
WLJ8102S_SR_11	Verify the AP tcp-mss size after Downgrading the controller	To verify the AP tcp-mss size after downgrading the controller	Passed	

WLJ8102S_SR_12	Verify the AP tcp-mss size after upgrading with the controller latest image and configuration file.	To verify the AP tcp-mss size after upgrading with the controller latest image and configuration file.	Passed	
WLJ8102S_SR_13	Verify the RF-Profile parameters	To verify the RF-Profile parameters in show run-configurations	Passed	
WLJ8102S_SR_14	Verify the RF parameters after connecting the client to 802.11a	To verify the RF Parameters after connecting the client to 802.11a	Passed	
WLJ8102S_SR_15	Verify the RF parameters after connecting the client to 802.11b/g	To verify the RF Parameters after connecting the client to 802.11b/g	Passed	
WLJ8102S_SR_16	Checking the AP Crash issue while Changing the AP Mode	To verify whetherAP Crash issue occur while Changing the AP modes	Passed	
WLJ8102S_SR_17	Checking the AP Crash issue during HA failover	To check whether AP is getting crash or not during HA failover	Passed	
WLJ8102S_SR_18	Checking the AP Crash issue while Changing the AP group	To verify whether AP Crash issue occur while Changing the AP group	Passed	
WLJ8102S_SR_19	Checking the rendering issue while navigating to buildings > floors in Detect and locate tab.	To verify whether the rendering issue is not found while navigating to floors in latest chrome browser.	Passed	
WLJ8102S_SR_20	Checking the rendering issue while navigating to Report in Analytics tab.	To verify whether the rendering issue is not found while navigating to reports in latest chrome browser.	Passed	

WLJ8102S_SR_21	Checking the rendering issue while navigating to existing Report in Analytics tab.	To verify whether the rendering issue is not found while navigating to Existing report in latest chrome browser.	Passed	
WLJ8102S_SR_22	Checking the rendering issue while navigating to existing Report in Analytics tab.	To verify whether the rendering issue is not found while navigating toexisting report in latest chrome browser.	Passed	
WLJ8102S_SR_23	Checking the rendering issue while navigating to Location in Connect tab.	To verify whether the rendering issue is not found while navigating to Location in Chrome browser.	Passed	
WLJ8102S_SR_24	Checking the 1810 AP's SSH connection status after changing connected->Standalone->connected mode	To verify the SSH connection working for 1810 AP after changing Standalone to connected mode	Passed	
WLJ8102S_SR_25	Checking the 4800 AP's SSH connection status after download/upload config file	To verify that SSH connection working for 4800 AP after download/upload config file	Passed	
WLJ8102S_SR_26	Checking the logging trace info configuration in GUI	To verify whether the logging trace info is configured on GUI or not	Passed	
WLJ8102S_SR_27	Checking the Messagelog configuration by disabling the traceinfo command.	To verify there is any change while disabling the traceinfo option.	Passed	
WLJ8102S_SR_28	Checking the logs during the upload and download configuration.	To verify the process of uploading and downloading the configuration file.	Passed	

WLJ8102S_SR_29	Associate the 2.4ghz multiple clients to the created WLAN	Verify the 2.4ghz multiple clients connected or not for AP 4800	Passed	
WLJ8102S_SR_30	Verify the 3800AP beacons for 2.4/5ghz radio	To check whether beacon is brodcasting or not for 2.4/5ghz radio on AP3800	Passed	
WLJ8102S_SR_31	Checking the AP/Radio health while Upgrading/ downgrading controller	Verify the Radio/AP health after controller upgrading/ downgrading	Passed	
WLJ8102S_SR_32	Associating the VPN client to the created WLAN	To check whether VPN client is associated or not	Passed	
WLJ8102S_SR_33	Verifying the ARP caching statistics on AP3800 after roam the client	To check whether ARP caching performed or not after "arp-caching disable"	Passed	
WLJ8102S_SR_34	Verify the client connectivity in standalone mode AP to connected mode	Check whether the client is associated or not after AP come back to connected mode	Passed	
WLJ8102S_SR_35	Associate the multiple clients to the flexconnect group WLAN	Verify the clients connectivity in flexConnect group WLAN	Passed	
WLJ8102S_SR_36	Create the flexConnect group on 5520 HA setup	To check whether flexConnect group is created or not on HA setup	Passed	
WLJ8102S_SR_37	Verifying the enhanced client session ID on both controller and prime side	To check whether enhanced client session ID count matched or not on both controller and Prime	Passed	
WLJ8102S_SR_38	Checking the client count on both controller and PI Map	Verify the client count is matched or not both controller and PI Map	Passed	

WLJ8102S_SR_39	Verifying the AP specific vlan after moving WLC1 to WLC2	To check whether AP is moved from WLC1 to WLC2 or not with valid VLAN	Passed	
WLJ8102S_SR_40	Checking the Radios, Regulatory Domains and Country Code configuration of AP	Verify the Radios, Regulatory Domains and Country Code after moving from WLC1 to WLC2	Passed	
WLJ8102S_SR_41	Associate the client with PEAP method and check reassociation happens or not.	To check whether client is associated or not with PEAP method	Passed	
WLJ8102S_SR_42	Configure sleeping client using 2800 AP with LEAP method to check reassociation happenes or not.	To check whether client is associated or not with LEAP method while client configured as Sleeping client and check if reassociation of clients happens or not.	Passed	
WLJ8102S_SR_43	Perform Roaming between 3800 and 4800 AP with EAP-FAST method	To check whether client roamed or not with FAST method	Passed	
WLJ8102S_SR_44	Associate the client using 4800 AP with EAP-TLS method and local authentication.	To check whether client is associated or not with EAP-TLS and Local authentication	Passed	
WLJ8102S_SR_45	Associate the client using cos AP with PEAP method configured in ISE server.	To check whether client is connected or not with cos AP using PEAP configure in external server.	Passed	
WLJ8102S_SR_46	Checking device details after restoring the backup configuration	To verify whether user able to take backup from device and restore to device without any issues	Passed	

WLJ8102S_SR_47	Uploading the backup configuration from device with FTP/TFTP/SFTP	To verify whether user able to take backup from device using FTP/TFTP/SFTP	Passed	
WLJ8102S_SR_48	Modifiying or erasing the backup configuration and dowloading to device	To verify whether eWLC downloading the Modified configuration file to controller or not	Passed	
WLJ8102S_SR_49	Connecting client and checking AID value for client while doing FT roming with Aps in Local/flex	To verify whether clients getting AID value after the FT roaming or not	Passed	
WLJ8102S_SR_50	Doing inter roaming and checking the AID values for the roamed client	To verify whether clients getting AID value after the inter roaming or not	Passed	
WLJ8102S_SR_51	Verifying the AID and SNR ,RSS values after client roamed with intra roaming	To verify whether clients getting AID value ,SNR,RSS after doing intra roaming or not	Passed	
WLJ8102S_SR_52	Upgrading CMX device with latest image using localfile option	To verify whether user able to upgrade CMX with latest image using localfile option or not	Passed	
WLJ8102S_SR_53	Upgrading CMX device with latest image using remote location option (https,FTP,TFTP)	To verify whether user able to upgrade CMX with remote location option (htpps ,FTP) or not	Passed	
WLJ8102S_SR_54	Testing Radius fallback when primary server recovers and become responsive	To verify whether radius fallback working when server recovers and become responsive	Passed	
WLJ8102S_SR_55	Changing fallback mode as "off" and testing Radius fallback when primary server recovers and become responsive	To verify whether radius fallback working when fallback mode is off	Passed	

WLJ8102S_SR_56	Checking WLC probe messages when server in down state	To verify whether WLC sending probe messages when server is down	Passed	
WLJ8102S_SR_57	Verifying the AP general config in stand by controller after HA failover	To Verify the AP general config in stand by controller after HA failover	Passed	
WLJ8102S_SR_58	Verifying the AP general config in stand by controller after failover with a client connected to it.	To Verify the AP general config in stand by controller after failover with a client connected to it.	Passed	
WLJ8102S_SR_59	Configuring HA pair in 5520 enabling telnet after Masterfail over and upgrade the image through Ftp server from CLI.	To verify whether the HA pair is up and image is upgraded successfully by using cli command	Passed	
WLJ8102S_SR_60	Configuring HA Setup check the iOS client connectivity after master failover and upgrading the image through TFTP server	To verify the iOS client connectivity after masterfailover and image upgrade through TFTP Server	Passed	
WLJ8102S_SR_61	Configuring HA Setup check the Android client connectivity after master failover and upgrading the image through TFTP server	To verify the Android client connectivity after masterfailover and image upgrade through TFTP Server	Passed	
WLJ8102S_SR_62	Installing CMX license and adding Cisco WLC to CMX	Checking the WLC gets added to the CMX	Passed	
WLJ8102S_SR_63	Installing CMX license and Importing maps from prime infrastructure	To import maps from prime infrastructure and check if the maps gets imported to the cmx .	Passed	
WLJ8102S_SR_64	Checking multicast traffic when clients connected with Dot1x security	Verfying Multicast traffic for clients connected with Dot1x security	Passed	

WLJ8102S_SR_65	Checking Multicast traffic when clients switches between AP radios	Verfying Multicast traffic for clients when it roams between AP radios	Passed	
WLJ8102S_SR_66	Performing Intra roaming for client and checking Multicast traffic	Verfying client Multicast traffic with Intra roaming	Passed	
WLJ8102S_SR_67	Checking the AP crash issue while upgrade/downgrade the latest software image	To verify whether AP crashes occur or not while upgrade/downgrade the latest software image	Passed	
WLJ8102S_SR_68	Checking the AP Crash issue while Changing the AP radios	To verify whetherAP Crash issue occur while Changing the AP radios	Passed	
WLJ8102S_SR_69	Verify the all joined APs-predownloaded primary image	To verify whether the AP-Pre downloading primary images or not.	Passed	
WLJ8102S_SR_70	Verify AP predownloaded primary image in particular AP(4800) with 3504 WLC	To check whether the AP-Pre download with primary images is successfull or not.	Passed	
WLJ8102S_SR_71	Verify AP predownloaded primary image using TFTP server	To check whether the AP-Pre download with primary images is successfull or not using TFTP mode transfer	Passed	
WLJ8102S_SR_72	Upgarding Flexconnect mode AP	Checking the Pre-downloading for AP 4800	Passed	
WLJ8102S_SR_73	Upgrading Flexconnect mode AP via CLI	Checking the Pre-downloading for AP	Passed	

WLJ8102S_SR_74	Verify AP predownloaded primary image in eWLC	To check whether the AP-Pre download with primary images is successfull or not.	Passed	

Config Wireless

Logical ID	Title	Description	Status	Defect ID
WLJ810S_config_02	1562 AP got crashed After upgrading WLC	To check whether,after upgrading WLC 1562 AP got crashed or not	Failed	CSCvp98478
WLJ810S_config_03	lex bridge mode(AP-C9115AXI-D) should be removed from PI side	To check whether the AP modes are changing or not in PI	Failed	CSCvq25783
WLJ810S_config_06	Configuring NTP server with max&min poll intervals	To verify whether user able to config NTP server with poll intervals or not	Passed	
WLJ810S_config_07	Checking the controller crash log while upgrading spamReceiveTask	To verify the controller crash logs while upgrading	Passed	
WLJ810S_config_10	Checking the logs for 9115AX AP while joining to the WLC	To check whether any error messages are getting in AP console or not	Failed	CSCvq24204
WLJ810S_config_13	Verifying split tunnel ACL configuration at flexgroup level through WLC CLI	To verify whether split tunnel ACL can be configured at flex group level or not through WLC CLI	Passed	
MEJ810S_config_01	ME - WPA3 security not reflecting properly under WLAN Configuration in Prime	To check whether WPA3 Security reflecting properly under WLAN configuration	Failed	CSCvq37457

MEJ810S_Config_04	Not able to change the Security type from Enhanced Open to Personal WPA3	To check whether the security type change from enhanced open to personal WPA3	Passed	
WLJ1612S_config_02	Rogue AP rules after creating shows empty	To check whether the rogue AP rules after creating shows empty or not	Passed	
WLJ1612S_config_03	Check if Sensor mode support is there for 9115	To check whether the sensor mode is shown in 9115 AP	Failed	CSCvq35277
WLJ1612S_config_04	Checking the regulatory domain for 1815AP after changed country code	To verify whether regulatory domain showing correct or nor after changed country code	Failed	CSCvq39044
WLJ1612S_config_05	Check the Configuration of WLAN with PMF-PSK security	To Verify the Configuration of WLAN with PMF-PSK security	Failed	CSCvq39055
WLJ1612S_config_06	Check the Configuration of OSEN with PSK security in CLI	To verify the Configurations of OSEN with PSK security in CLI.	Passed	
WLJ1612S_config_07	Verify th Configuration of WLAN with Static WEP security	To Verify the configuration of WLAN with Static WEP security	Passed	
WLJ1612S_config_08	Check the Configurations of Policy Map-Local Policy	To verify the Configuration of Policy Map-Local Policy	Passed	
WLJ8102s_config_01	Not able to configure the Radius NAC after configuring the Tunneling profile.	To check whether the Radius NAC is configured or not after configuring Tunneling Profile	Failed	CSCvr60426

MAB Bypass Support

Logical ID	Title	Description	Status	Defect ID

WLJ810S_Reg_140	Associating different OS client with MAB	Check whether different os client is able connect or not with MAB	Passed	
WLJ810S_Reg_141	Verifying the MAC filtering enabled status through CLI	To check whether MAC Filtering enabled details showing properly or not on CLI	Passed	
WLJ810S_Reg_142	Client reassociate with mac filtering enabled through external radius server.	Verifying the client is associated or not with with MAC filter enabled through external RADIUS server	Passed	
WLJ810S_Reg_143	Verifying JSSID client association with MAC filtering enabled on WLAN with external radius server.	Verifying the JSSID client is associated or not with with MAC filter enabled through external RADIUS server	Passed	
WLJ810S_Reg_144	Configuring specific mac address allowed on wlan by using AAA-attribute list.	Verifying the specific mac address allowed on wlan by using AAA-attribute list	Passed	
WLJ810S_Reg_145	Configure a named authorization list via aaa confit on wlan.	Verifying the named authorization list is configured, the authorization list is mapped on wlan and client is join/disconnect/re-join.	Passed	
WLJ810S_Reg_146	Verifying the JSSID client maximum retries failed	To check whether JSSID client is moved/excluded or not after maximum retries failed	Passed	
WLJ810S_Reg_147	Verifying client is reauthenticated or not after session timeout	Checking after session timeout client is reauthenticated or not	Passed	

WLJ810S_Reg_148	Checking the JSSID client is reauthenticated or not after session expired	To check whether JSSID client is reauthenticated or not after client session expired	Passed	
WLJ810S_Reg_149	Verifying the JSSID client status on monitor page	Checking the JSSID client details on monitor page	Passed	
WLJ8102S_Reg_109	Associating different OS client with MAB	Check whether different os client is able connect or not with MAB	Passed	
WLJ8102S_Reg_110	Verifying the MAC filtering enabled status through CLI	To check whether MAC Filtering enabled details showing properly or not on CLI	Passed	
WLJ8102S_Reg_111	Client reassociate with mac filtering enabled through external radius server.	Verifying the client is reassociated or not with with MAC filter enabled through external RADIUS server	Passed	
WLJ8102S_Reg_112	Verifying JSSID client reassociation with MAC filtering enabled on WLAN with external radius server.	Verifying the JSSID client is reassociated or not with with MAC filter enabled through external RADIUS server	Passed	
WLJ8102S_Reg_113	Configuring specifc mac address allowed on wlan by using AAA-attribute list.	Verifying the specific mac address allowed on wlan by using AAA-attribute list	Passed	
WLJ8102S_Reg_114	Configure a named authorization list via aaa config on wlan.	Verifying the named authorization list is configured, the authorization list is mapped on wlan and client is join/disconnect/rejoin.	Passed	
WLJ8102S_Reg_115	Verifying the JSSID client maximum retries failed	To check whether JSSID client is moved/excluded or not after maximum retries failed	Passed	

WLJ8102S_Reg_116	Verifying client is reauthenticated or not after session timeout	Checking after session timeout client is reauthenticated or not	Passed	
WLJ8102S_Reg_117	Checking the JSSID client is reauthenticated or not after session expired	To check whether JSSID client is reauthenticated or not after client session expired	Passed	
WLJ8102S_Reg_118	Verifying the JSSID client status on monitor page	Checking the JSSID client details on monitor page	Passed	

Dot1x and WEB-Auth Support

Logical ID	Title	Description	Status	Defect ID
WLJ810S_Reg_205	Authentication of Android client with Security Dot1x and Web-Auth	Checking for the Authentication of the client when connected to a WLAN in which Dot1x and Web-Auth is enabled	Passed	
WLJ810S_Reg_206	Authentication of window 10 client with Security Dot1x and Web-Auth	Checking for the Authentication of the client when connected to a WLAN in which Dot1x and Web-Auth is enabled	Passed	
WLJ810S_Reg_207	Authentication of Win 7 laptop with Security Dot1x and Web-Auth	Checking for the Authentication of the clients when connected to a WLAN in which Static WEP and Web-Auth is enabled. \u0007	Passed	

WLJ810S_Reg_208	Authentication of Android client with Security Static WEP+DOT1X and Web-Auth	Checking for the Authentication of the client when connected to a WLAN in which Static WEP+Dot1x and Web-Auth is enabled. \u0007	Passed	
WLJ810S_Reg_209	Authentication of Window 10 client with Security Static WEP+DOT1X and Web-Auth	Checking for the Authentication of the client when connected to a WLAN in which Static WEP+Dot1x and Web-Auth is enabled. \u0007	Passed	
WLJ810S_Reg_210	Authentication of client(Apple Mac Book) with Security Static WEP+DOT1X and Web-Auth	Checking for the Authentication of the client when connected to a WLAN in which Static WEP+Dot1x and Web-Auth is enabled. \u0007	Passed	
WLJ810S_Reg_211	Authentication of client(Apple Mac Book) with Security Dot1x and Web-Auth	Checking for the Authentication of the client when connected to a WLAN in which Dot1x and Web-Auth is enabled. \u0007	Passed	
WLJ810S_Reg_212	Authentication of clients(Apple Mac Book &Win 7) with Security Dot1x and Web-Auth(Same SSID) .	Checking for the Authentication of the clients when connected to a WLAN in which Dot1x and Web-Auth is enabled. \u0007	Passed	
WLJ810S_Reg_213	Authentication of clients(Apple Mac Book &Win 10) with Security Dot1x and Web-Auth(Same SSID)	Checking for the Authentication of the clients when connected to a WLAN in which Dot1x and Web-Auth is enabled. \u0007	Passed	

WLJ810S_Reg_214	Authentication of clients(Apple Mac Book &Win 7) with Security Static WEP+Dot1x and Web-Authoring ISE	Checking for the Authentication of the clients when connected to a WLAN in which Static WEP+Dot1x and Web-Auth is enabled. \u0007	Passed	
WLJ810S_Reg_215	Authentication of clients(Apple Mac Book & Win 10) with Security Static WEP+Dot1x and Web-Authoring ISE	Checking for the Authentication of the clients when connected to a WLAN in which Static WEP+Dot1x and Web-Auth is enabled. \u0007	Passed	
WLJ810S_Reg_216	Authentication of clients(Apple Mac Book & Win 7) with Security Static WEP+Dot1x and Web-Authoring ISE	Checking for the Authentication of the clients when connected to a WLAN in which Static WEP+Dot1x and Web-Auth is enabled. \u0007	Passed	
WLJ810S_Reg_217	Authentication of clients(Apple Mac Book & Win 10) with Security Dot1x using ISE and WebAuth	Checking for the Authentication of the clients when connected to a WLAN in which Dot1x and Web-Auth is enabled. \u0007	Passed	
WLJ810S_Reg_218	Authentication of clients(Apple Mac Book & Win 7) with Security Dot1x using ISE and WebAuth	Checking for the Authentication of the clients when connected to a WLAN in which Dot1x and Web-Auth is enabled. \u0007	Passed	
WLJ810S_Reg_219	Authentication of clients(Apple Mac Book & Win 10) with Security Dot1x using ISE and WebAuth	Checking for the Authentication of the clients when connected to a WLAN in which Dot1x and Web-Auth is enabled. \u0007	Passed	

WLJ8102S_Reg_163	Authentication of Android client with Security Dot1x and Web-Auth	Checking for the Authentication of the client when connected to a WLAN in which Dot1x and Web-Auth is enabled	Passed	
WLJ8102S_Reg_164	Authentication of window 10 client with Security Dot1x and Web-Auth	Checking for the Authentication of the client when connected to a WLAN in which Dot1x and Web-Auth is enabled	Passed	
WLJ8102S_Reg_165	Authentication of Win 7 laptop with Security Dot1x and Web-Auth	Checking for the Authentication of the clients when connected to a WLAN in which Static WEP and Web-Auth is enabled. \u0007	Passed	
WLJ8102S_Reg_166	Authentication of Android client with Security Static WEP+DOT1X and Web-Auth	Checking for the Authentication of the client when connected to a WLAN in which Static WEP+Dot1x and Web-Auth is enabled. \u0007	Passed	
WLJ8102S_Reg_167	Authentication of Window 10 client with Security Static WEP+DOT1X and Web-Auth	Checking for the Authentication of the client when connected to a WLAN in which Static WEP+Dot1x and Web-Auth is enabled. \u0007	Passed	
WLJ8102S_Reg_168	Authentication of client(Apple Mac Book) with Security Static WEP+DOT1X and Web-Auth	Checking for the Authentication of the client when connected to a WLAN in which Static WEP+Dot1x and Web-Auth is enabled. \u0007	Passed	

WLJ8102S_Reg_169	Authentication of client(Apple Mac Book) with Security Dot1x and Web-Auth	Checking for the Authentication of the client when connected to a WLAN in which Dot1x and Web-Auth is enabled. \u0007	Passed	
WLJ8102S_Reg_170	Authentication of clients(Apple Mac Book &Win 7) with Security Dot1x and Web-Auth(Same SSID) .	Checking for the Authentication of the clients when connected to a WLAN in which Dot1x and Web-Auth is enabled. \u0007	Passed	
WLJ8102S_Reg_171	Authentication of clients(Apple Mac Book &Win 10) with Security Dot1x and Web-Auth(Same SSID)	Checking for the Authentication of the clients when connected to a WLAN in which Dot1x and Web-Auth is enabled. \u0007	Passed	
WLJ8102S_Reg_172	Authentication of clients(Apple Mac Book &Win 7) with Security Static WEP+Dot1x and Web-Authusing ISE	Checking for the Authentication of the clients when connected to a WLAN in which Static WEP+Dot1x and Web-Auth is enabled. \u0007	Passed	
WLJ8102S_Reg_173	Authentication of clients(Apple Mac Book & Win 10) with Security Static WEP+Dot1x and Web-Authusing ISE	Checking for the Authentication of the clients when connected to a WLAN in which Static WEP+Dot1x and Web-Auth is enabled. \u0007	Passed	
WLJ8102S_Reg_174	Authentication of clients(Apple Mac Book & Win 7) with Security Static WEP+Dot1x and Web-Authusing ISE	Checking for the Authentication of the clients when connected to a WLAN in which Static WEP+Dot1x and Web-Auth is enabled. \u0007	Passed	

WLJ8102S_Reg_175	Authentication of clients(Apple Mac Book & Win 10) with Security Dot1x using ISE and WebAuth	Checking for the Authentication of the clients when connected to a WLAN in which Dot1x and Web-Auth is enabled. \u0007	Passed	
WLJ8102S_Reg_176	Authentication of clients(Apple Mac Book & Win 7) with Security Dot1x using ISE and WebAuth	Checking for the Authentication of the clients when connected to a WLAN in which Dot1x and Web-Auth is enabled. \u0007	Passed	
WLJ8102S_Reg_177	Authentication of clients(Apple Mac Book & Win 10) with Security Dot1x using ISE and WebAuth	Checking for the Authentication of the clients when connected to a WLAN in which Dot1x and Web-Auth is enabled. \u0007	Passed	

Multiple RADIUS Server Per SSID

Logical ID	Title	Description	Status	Defect ID
WLJ810S_Reg_201	Performing Dot1x authentication over flexconnectAP with RADIUS servers configured(Secondary)	To verify whether Dot1x authentication can be performed successfully to the clients associated via the secondary RADIUS server over the flex connect connection with the Vlan mapped \u0007	Passed	

WLJ810S_Reg_202	Performing Dot1x authentication over flexconnectAP with RADIUS servers configured(Primary failover)	To verify whether Dot1x authentication can be performed successfully to the clients associated via the secondary RADIUS server over the flex connect connection with the Vlan mapped \u0007	Passed	
WLJ810S_Reg_203	Performing Dot1x authentication over Flex Connect AP with RADIUS servers configured(Primary)	To verify whether Dot1x authentication can be performed successfully to the clients associated via the Primary RADIUS server over the Flex AP connection with the Vlan mapped \u0007	Passed	
WLJ810S_Reg_204	Performing Dot1x authentication over Flex Connect AP with RADIUS servers configured(Secondary)	To verify whether Dot1x authentication can be performed successfully to the clients associated via the secondary RADIUS server over the Flex AP connection with the Vlan mapped \u0007	Passed	
WLJ8102S_Reg_159	Performing Dot1x authentication over flexconnectAP with RADIUS servers configured(Secondary)	To verify whether Dot1x authentication can be performed successfully to the clients associated via the secondary RADIUS server over the flexconnect connection with the Vlan mapped \u0007	Passed	

WLJ8102S_Reg_160	Performing Dot1x authentication over flexconnectAP with RADIUS servers configured(Primary failover)	To verify whether Dot1x authentication can be performed successfully to the clients associated via the secondary RADIUS server over the flexconnect connection with the Vlan mapped \u0007	Passed	
WLJ8102S_Reg_161	Performing Dot1x authentication over FlexConnect AP with RADIUS servers configured(Primary)	To verify whether Dot1x authentication can be performed successfully to the clients associated via the Primary RADIUS server over the Flex AP connection with the Vlan mapped \u0007	Passed	
WLJ8102S_Reg_162	Performing Dot1x authentication over FlexConnect AP with RADIUS servers configured(Secondary)	To verify whether Dot1x authentication can be performed successfully to the clients associated via the secondary RADIUS server over the Flex AP connection with the Vlan mapped \u0007	Passed	

Hyperlocation Module supports for AP 3702

Logical ID	Title	Description	Status	Defect ID
WLJ810S_Reg_238	Importing maps to CMX through Japanese PI	To check whether the maps can be imported in CMX from PI	Passed	
WLJ810S_Reg_239	Sync the WLC in to CMX	To check whether the WLC and CMX gets synced up	Passed	

WLJ810S_Reg_240	Tracking the Window, iPhone client devices in CMX	To check the tracking of Window ,iPhone devices using CMX	Failed	CSCvq31738
WLJ810S_Reg_241	Android, iOS Client Locate in CMX	To verify the Location of the clients	Passed	
WLJ810S_Reg_242	Location Accuracy Test in CMX of Window client	To verify the location accuracy of the clients	Passed	
WLJ810S_Reg_243	History of client location(Client Playback)	To verify the client location history	Passed	
WLJ8102S_Reg_196	Importing maps to CMX through Japanese PI	To check whether the maps can be imported in CMX from PI	Passed	
WLJ8102S_Reg_197	Sync the WLC in to CMX	To check whether the WLC and CMX gets synced up	Passed	
WLJ8102S_Reg_198	Tracking the Window,iPhone client devices in CMX	To check the tracking of Window ,iphone devices using CMX	Passed	
WLJ8102S_Reg_199	Android,iOS Client Locate in CMX	To verify the Location of the clients	Passed	
WLJ8102S_Reg_200	Location Accuracy Test in CMX of Window client	To verify the location accuracy of the clients	Passed	
WLJ8102S_Reg_201	History of client location(Client Playback)	To verify the client location history	Passed	

Internal DHCP Server

Logical ID	Title	Description	Status	Defect ID
WLJ810S_Reg_303	Assigning the Internal DHCP server to WLAN	To verify whether Internal DHCP server assigned successfully to WLAN or not	Passed	

WLJ810S_Reg_304	Disabling the DHCP Proxy server	To verify whether without DHCP proxy server enable client will get IP address or not	Passed	
WLJ810S_Reg_305	Configuring the DHCP option 82 with binary format	To verify whether DHCP option 82 configured client is showing binary format or not	Passed	
WLJ810S_Reg_306	Configuring the DHCP option 82 with asci format	To verify whether DHCP option 82 configured client is showing ASCII format or not	Passed	
WLJ810S_Reg_307	DHCP option 82 with Remote Id field all formats	To verify whether all formats details are showing or not at the time of debug	Passed	
WLJ810S_Reg_308	Configuring the DHCP with maximum & minimum timeout	To verify whether DHCP maximum & minimum values are configured successfully	Passed	
WLJ810S_Reg_309	Assigning the invalid Internal DHCP server to WLAN	To verify whether internal Internal DHCP server assigned successfully to WLAN or not	Passed	
WLJ8102S_Reg_236	Assigning the Internal DHCP server to WLAN	To verify whether Internal DHCP server assigend successfully to WLAN or not	Passed	
WLJ8102S_Reg_237	Disabling the DHCP Proxy server	To verify whether without DHCP proxy server enable client will get IP address or not	Passed	
WLJ8102S_Reg_238	Configuring the DHCP option 82 with binary format	To verify whether DHCP option 82 configured client is showing binary format or not	Passed	

WLJ8102S_Reg_239	Configuring the DHCP option 82 with ascii format	To verify whether DHCP option 82 configured client is showing ASCII format or not	Passed	
WLJ8102S_Reg_240	DHCP option 82 with Remote Id field all formats	To verify whether all formats details are showing or not at the time of debug	Passed	
WLJ8102S_Reg_241	Configuring the DHCP with maximum & minimum timeout	To verify whether DHCP maximum & minimum values are configured successfully	Passed	
WLJ8102S_Reg_242	Assigning the invalid Internal DHCP server to WLAN	To verify whether internal Internal DHCP server assigend successfully to WLAN or not	Passed	

MFP support

Logical ID	Title	Description	Status	Defect ID
WLJ810S_Reg_399	Checking if IMIC IE value in MFP is appended in 3800 AP	To check if the IMIC IE value in MFP is appended in 3800 AP or not after enabling MFP globally.	Passed	
WLJ810S_Reg_400	Checking if IMIC IE value in MFP is appended in 2800 AP	To check if the IMIC IE value in MFP is appended in 2800 AP or not after enabling MFP globally.	Passed	
WLJ810S_Reg_401	Connecting a CCXv5 Window client to a 3800 AP with MFP option as Required .	To connect a window CCxv5 client to a 3800 AP with MFP option as required and check the IMIC IE value in MFP .	Passed	

WLJ810S_Reg_402	Connecting a Mac OS CCXv5 client to a 3800 AP with MFP option as Required .	To connect a Mac OS CCxv5 client to a 3800 AP with MFP option as required and check the IMIC IE value in MFP .	Passed	
WLJ810S_Reg_403	Connecting a CCXv5 Window client to a 2800 AP with MFP option as Required .	To connect a window CCxv5 client to a 2800 AP with MFP option as required and check the IMIC IE value in MFP .	Passed	
WLJ810S_Reg_404	Connecting a Mac OS CCXv5 client to a 2800 AP with MFP option as Required .	To connect a Mac OS CCxv5 client to a 2800 AP with MFP option as required and check the IMIC IE value in MFP .	Passed	
WLJ810S_Reg_405	Pushing MFP configuration from PI and connecting a client .	To connect a client to the 2800 AP where the template is pushed from PI and check if the IMIC IE value is appended or not.	Passed	
WLJ810S_Reg_406	Exporting and Importing configuration of MFP	To exporting and importing configuration of MFP and check if the configuration remains the same after import and export.	Passed	
WLJ8102S_Reg_286	Checking if IMIC IE value in MFP is appended in 3800 AP	To check if the IMIC IE value in MFP is appeneded in 3800 AP or not after enabling MFP globally.	Passed	
WLJ8102S_Reg_287	Checking if IMIC IE value in MFP is appended in 2800 AP	To check if the IMIC IE value in MFP is appeneded in 2800 AP or not after enabling MFP globally.	Passed	

WLJ8102S_Reg_288	Connecting a CCXv5 Window client to a 3800 AP with MFP option as Required .	To connect a window CCxv5 client to a 3800 AP with MFP option as required and check the IMIC IE value in MFP .	Passed	
WLJ8102S_Reg_289	Connecting a Mac OS CCXv5 client to a 3800 AP with MFP option as Required .	To connect a Mac OS CCxv5 client to a 3800 AP with MFP option as required and check the IMIC IE value in MFP .	Passed	
WLJ8102S_Reg_290	Connecting a CCXv5 Window client to a 2800 AP with MFP option as Required .	To connect a window CCxv5 client to a 2800 AP with MFP option as required and check the IMIC IE value in MFP .	Passed	
WLJ8102S_Reg_291	Connecting a Mac OS CCXv5 client to a 2800 AP with MFP option as Required .	To connect a Mac OS CCxv5 client to a 2800 AP with MFP option as required and check the IMIC IE value in MFP .	Passed	
WLJ8102S_Reg_292	Pushing MFP configuration from PI and connecting a client .	To connect a client to the 2800 AP where the template is pushed from PI and check if the IMIC IE value is appened or not.	Passed	
WLJ8102S_Reg_293	Exporting and Importing configuration of MFP	To exporting and importing configuration of MFP and check if the configuration remains the same after import and export.	Passed	

DHCP Option 82 - Support

Logical ID	Title	Description	Status	Defect ID

WLJ810S_Reg_322	Connecting the android/IOS/MAC clients without enabling DHCP proxy	To verify whether android/IOS/MAC Clients are getting the internal DHCP IP address or not when DHCP Proxy is in disabled state	Passed	
WLJ810S_Reg_323	Connecting the android/IOS/MAC clients after enable DHCP proxy	To verify whether android/IOS/MAC Clients are getting IP address or not when Proxy is in enable state	Passed	
WLJ810S_Reg_324	Enable/disable the DHCP Proxy through CLI	To verify whether DHCP proxy server enable/disable through CLI or not	Passed	
WLJ810S_Reg_325	Configuring the DHCP Option 82 Remote Id field format with AP-MAC	To verify whether DHCP option 82 with AP-MAC is sending the client association/disassociation requests or not	Passed	
WLJ810S_Reg_326	Configuring the DHCP Option 82 Remote Id field format with AP-MAC-SSID	To verify whether DHCP option 82 with AP-MAC-SSID is sending the client association/disassociation requests or not	Passed	
WLJ810S_Reg_327	Configuring the DHCP Option 82 Remote Id field format with AP-ETHMAC	To verify whether DHCP option 82 with AP-ETHMAC is sending the client association/disassociation requests or not	Passed	
WLJ810S_Reg_328	Configuring the DHCP Option 82 Remote Id field format with AP-Name-SSID	To verify whether DHCP option 82 with AP-Name-SSID is sending the client association/disassociation requests or not	Passed	
WLJ810S_Reg_329	Configuring the DHCP Option 82 Remote Id field format with Flex-Group-Name	To verify whether DHCP option 82 with Flex-Group-Name is sending the client association/disassociation requests or not	Passed	

WLJ810S_Reg_330	Configuring the DHCP Option 82 Remote Id field format with AP-Location	To verify whether DHCP option 82 with AP-Location is sending the client association/disassociation requests or not	Passed	
WLJ810S_Reg_331	Configuring the DHCP Option 82 Remote Id field format with AP-MAC-VLAN-ID	To verify whether DHCP option 82 with AP-MAC-VLAN-ID is sending the client association/disassociation requests or not	Passed	
WLJ810S_Reg_332	Configuring the DHCP Option 82 Remote Id field format with AP-NAME-VLAN-ID	To verify whether DHCP option 82 with AP-NAME-VLAN-ID is sending the client association/disassociation requests or not	Passed	
WLJ810S_Reg_333	Configuring the DHCP Option 82 Remote Id field format with AP-ETHMAC-SSID	To verify whether DHCP option 82 with AP-ETHMAC-SSID is sending the client association/disassociation requests or not	Passed	
WLJ810S_Reg_334	Configuring the DHCP option 82 through PI	To verify whether DHCP option 82 is enabling through PI or not	Passed	
WLJ8102S_Reg_255	Connecting the android/IOS/MAC clients without enabling DHCP proxy	To verify whether android/IOS/MAC Clients are getting the internal DHCP IP address or not when DHCP Proxy is in disabled state	Passed	
WLJ8102S_Reg_256	Connecting the android/IOS/MAC clients after enable DHCP proxy	To verify whether android/IOS/MAC Clients are getting IP address or not when Proxy is in enable state	Passed	
WLJ8102S_Reg_257	Enable/disable the DHCP Proxy through CLI	To verify whether DHCP proxy server enable/disable through CLI or not	Passed	

WLJ8102S_Reg_258	Configuring the DHCP Option 82 Remote Id field format with AP-MAC	To verify whether DHCP option 82 with AP-MAC is sending the client aSSOciation/disaSSOciation requests or not	Passed	
WLJ8102S_Reg_259	Configuring the DHCP Option 82 Remote Id field format with AP-MAC-SSID	To verify whether DHCP option 82 with AP-MAC-SSID is sending the client aSSOciation/disaSSOciation requests or not	Passed	
WLJ8102S_Reg_260	Configuring the DHCP Option 82 Remote Id field format with AP-ETHMAC	To verify whether DHCP option 82 with AP-ETHMAC is sending the client aSSOciation/disaSSOciation requests or not	Passed	
WLJ8102S_Reg_261	Configuring the DHCP Option 82 Remote Id field format with AP-Name-SSID	To verify whether DHCP option 82 with AP-Name-SSID is sending the client aSSOciation/disaSSOciation requests or not	Passed	
WLJ8102S_Reg_262	Configuring the DHCP Option 82 Remote Id field format with Flex-Group-Name	To verify whether DHCP option 82 with Flex-Group-Name is sending the client aSSOciation/disaSSOciation requests or not	Passed	
WLJ8102S_Reg_263	Configuring the DHCP Option 82 Remote Id field format with AP-Location	To verify whether DHCP option 82 with AP-Location is sending the client aSSOciation/disaSSOciation requests or not	Passed	
WLJ8102S_Reg_264	Configuring the DHCP Option 82 Remote Id field format with AP-MAC-VLAN-ID	To verify whether DHCP option 82 with AP-MAC-VLAN-ID is sending the client aSSOciation/disaSSOciation requests or not	Passed	

WLJ8102S_Reg_265	Configuring the DHCP Option 82 Remote Id field format with AP-NAME-VLAN-ID	To verify whether DHCP option 82 with AP-NAME-VLAN-ID is sending the client aSSOciation/disaSSOciation requests or not	Passed	
WLJ8102S_Reg_266	Configuring the DHCP Option 82 Remote Id field format with AP-ETHMAC-SSID	To verify whether DHCP option 82 with AP-ETHMAC-SSID is sending the client aSSOciation/disaSSOciation requests or not	Passed	
WLJ8102S_Reg_267	Configuring the DHCP option 82 through PI	To verify whether DHCP option 82 is enabling through PI or not	Passed	

Client Auth Failures(AAA Failures/WLC Failures)

Logical ID	Title	Description	Status	Defect ID
WLJ810S_Reg_335	Configure maximum allowed clients per AP radio	To configure maximum allowed clients per AP radio and check if the number of clients given alone gets connected or not	Passed	
WLJ810S_Reg_336	Applying access control list to the WLAN and check if the ACL rule works to deny the client .	To check whether the ACL applied to WLAN works and check if the client get denied or not.	Passed	
WLJ810S_Reg_337	Configuring maximum allowed clients for the WLAN and check if the specified clients alone gets connected	To connect a specified number of clients to a specific WLAN and check if client more than the specified value does not authenticated or not	Passed	

WLJ810S_Reg_338	Creating a local policy adding device type as Android and Sleeping client Timeout and check if client move into sleeping client after Timeout.	To create a local policy with device type as Android and configuring Sleeping Client Timeout and check if the sleeping timeout	Passed	
WLJ810S_Reg_339	Creating a local policy adding device type as Apple and Sleeping client Timeout and check if client move into sleeping client after timeout.	To create a local policy with device type as Apple and configuring Sleeping Client Timeout and check the sleeping timeout	Passed	
WLJ810S_Reg_340	Creating a local policy adding device type as Windows and Sleeping Client Timeout and check if client move into sleeping client after Timeout.	To create a local policy with device type as Windows and configuring Sleeping Client Timeout and check the sleeping timeout	Passed	
WLJ810S_Reg_341	Configuring Identity Request Timeout and Identity Request Retries .	To configure Identity Request Timeout and Identity Request Retries and check if the request is send to client to the limited number of times within the limited time or not.	Passed	
WLJ810S_Reg_342	Configuring Session timeout for WLAN and check if the client re-auth when the timer gets expired.	To Enable and configure session timeout for WLAN and check if the session timeout interval works fine or not	Passed	

WLJ810S_Reg_343	Creating a DHCP scope and check if the IP address given in the scope is given to client.	To Configure DHCP scope and check if the Ip address is given to the client and check if the ip address allocated is shown in the DHCP Allocates leases.	Passed	
WLJ810S_Reg_344	Checking the client status if the security of the WLAN changes when a client connected to WLAN .	To Check the status of the client if the security of the WLAN changes when the client is connected to the WLAN.	Passed	
WLJ8102S_Reg_268	Configure maximum allowed clients per AP radio	To configure maximum allowed clients per AP radio and check if the number of clients given alone gets connected or not	Passed	
WLJ8102S_Reg_269	Applying access control list to the WLAN and check if the ACL rule works to deny the client .	To check whether the ACL apllied to WLAN works and check if the client get denied or not.	Passed	
WLJ8102S_Reg_270	Configuring maxium allowed clients for the WLAN and check if the specified clients alone gets connected	To connect a specified number of clients to a specific WLAN and check if client more than the specified value does not authenticated or not	Passed	
WLJ8102S_Reg_271	Creating a local policy adding device type as Android and Sleeping client Timeout and check if client move into sleeping client after Timeout.	To create a local policy with device type as Android and configuring Sleeping Client Timeout and check if the sleeping timeout	Passed	

WLJ8102S_Reg_272	Creating a local policy adding device type as Apple and Sleeping client Timeout and check if client move into sleeping client after timeout.	To create a local policy with device type as Apple and configuring Sleeping Client Timeout and check the sleeping timeout	Passed	
WLJ8102S_Reg_273	Creating a local policy adding device type as Windows and Sleeping Client Timeout and check if client move into sleeping client after Timeout.	To create a local policy with device type as Windows and configuring Sleeping Client Timeout and check the sleeping timeout	Passed	
WLJ8102S_Reg_274	Configuring Identity Request Timeout and Identity Request Retries .	To configure Identity Request Timeout and Identity Request Retries and check if the request is send to client to the limited number of times within the limeted time or not.	Passed	
WLJ8102S_Reg_275	Configuring Session timeout for WLAN and check if the client re-auth when the timer gets expired.	To Enable and configure session timeout for WLAN and check if the session timeout interval works fine or not	Passed	
WLJ8102S_Reg_276	Creating a DHCP scope and check if the IP address given in the scope is given to client.	To Configure DHCP scope and check if the Ip address is given to the client and check if the ip address allocated is shown in the DHCP Allocates leases.	Passed	
WLJ8102S_Reg_277	Checking the client status if the security of the WLAN changes when a client connected to WLAN .	To Check the status of the client if the security of the WLAN changes when the client is connected to the WLAN.	Passed	

MIMO Coverage

Logical ID	Title	Description	Status	Defect ID
WLJ810S_Reg_345	Enabling HT either in in 802.11b/g/n or 802.11a/n/ac and checking the clients association & their throughput	To check whether clients data rates are getting at maximum output or not as configured in 802.11b/g/n or 802.11a/n/ac	Passed	
WLJ810S_Reg_346	Enabling VHT alone in 802.11a/n/ac and checking the clients association & their throughput	To check whether clients data rates are getting at maximum output or not as per their spatial streams configured in 802.11a/n/ac	Passed	
WLJ810S_Reg_347	Setting the channel width to 40MHz/80MHz and checking the clients association	To check whether clients data rates are getting at maximum output or not as per their spatial streams configured in 802.11a/n/ac when it is configured with 40MHz	Passed	
WLJ810S_Reg_348	Capturing the beacon packets and checking the HT & VHT parameters	To check whether HT & VHT parameters displays the configurations properly or not in beacon packets.	Passed	
WLJ810S_Reg_349	Setting the AP channel to extended UNII-2 channels and checking the clients association	To check whether clients associated successfully or not to AP when AP configured in UNII-2 channels	Passed	
WLJ810S_Reg_350	Setting the channel width to best and checking the clients association	To check whether clients data rates are getting at maximum output or not as per their spatial streams configured in 802.11a/n/ac when it is configured with best channel width	Passed	

WLJ810S_Reg_351	Setting the AP channel to India extended channels and checking the clients association	To check whether clients associated successfully or not to AP when AP configured in India extended channels	Passed	
WLJ810S_Reg_352	Setting the maximum allowed clients range in 802.11a global parameters	To check whether more numbers of clients allowed or not than the range set in 802.11a global parameters	Passed	
WLJ8102S_Reg_278	Enabling HT either in in 802.11b/g/n or 802.11a/n/ac and checking the clients association & their throughput	To check whether clients data rates are getting at maximum output or not as configured in 802.11b/g/n or 802.11a/n/ac	Passed	
WLJ8102S_Reg_279	Enabling VHT alone in 802.11a/n/ac and checking the clients association & their throughput	To check whether clients data rates are getting at maximum output or not as per their spatial streams configured in 802.11a/n/ac	Passed	
WLJ8102S_Reg_280	Setting the channel width to 40MHz/80MHz and checking the clients association	To check whether clients data rates are getting at maximum output or not as per their spatial streams configured in 802.11a/n/ac when it is configured with 40MHz	Passed	
WLJ8102S_Reg_281	Capturing the beacon packets and checking the HT & VHT parameters	To check whether HT & VHT parameters displays the configurations properly or not in beacon packets.	Passed	
WLJ8102S_Reg_282	Setting the AP channel to extended UNII-2 channels and checking the clients association	To check whether clients associated successfully or not to AP when AP configured in UNII-2 channels	Passed	

WLJ8102S_Reg_283	Setting the channel width to best and checking the clients association	To check whether clients data rates are getting at maximum output or not as per their spatial streams configured in 802.11a/n/ac when it is configured with best channel width	Passed	
WLJ8102S_Reg_284	Setting the AP channel to India extended channels and checking the clients association	To check whether clients associated successfully or not to AP when AP configured in India extended channels	Passed	
WLJ8102S_Reg_285	Setting the maximum allowed clients range in 802.11a global parameters	To check whether more numbers of clients allowed or not than the range set in 802.11a global parameters	Passed	

CMX Support

Logical ID	Title	Description	Status	Defect ID
WLJ810S_Reg_407	Adding Cisco WLC to CMX	To add a Cisco WLC to CMX and check if the WLC gets added to the CMX with the WLC status showing	Passed	
WLJ810S_Reg_408	Importing maps from prime infrastructure	To import maps from prime infrastructure and check if the maps gets imported to the cmx .	Passed	
WLJ810S_Reg_409	Importing the maps with 2 to 3 Access points from PI to CMX	To import the maps from prime infra to CMX with 2 to 3 access point and check if the access point details are shown correctly including clients connected .	Passed	

WLJ810S_Reg_410	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	
WLJ810S_Reg_411	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	
WLJ810S_Reg_412	Searching the client by MAC address	To check whether client device can be searched by specifying its MAC address or not	Passed	
WLJ810S_Reg_413	Searching the client using its IP address	To check whether client device can be searched by specifying its IP address or not	Passed	
WLJ810S_Reg_414	Searching client using its SSID	To verify whether client device can be searched by specifying the SSID or not	Passed	
WLJ810S_Reg_415	Check the number of clients visting the building and floor in hourly basic and daily basic	To check the the number of client visiting the building or floor on hourly and daily basic	Passed	
WLJ810S_Reg_416	Checking the number of new and repeat visitors to the building or floor.	To check the number of new and repeat clients to the building or floor .	Passed	
WLJ8102S_Reg_294	Adding Cisco WLC to CMX	To add a Cisco WLC to CMX and check if the WLC gets added to the CMX with the WLC status showing	Passed	

WLJ8102S_Reg_295	Importing maps from prime infrastructure	To import maps from prime infrastructure and check if the maps gets imported to the cmx .	Passed	
WLJ8102S_Reg_296	Importing the maps with 2 to 3 Access points from PI to CMX	To import the maps from prime infra to CMX with 2 to 3 access point and check if the access point details are shown correctly including clients connected .	Passed	
WLJ8102S_Reg_297	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	
WLJ8102S_Reg_298	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	
WLJ8102S_Reg_299	Searching the client by MAC address	To check whether client device can be searched by specifying its MAC address or not	Passed	
WLJ8102S_Reg_300	Searching the client using its IP address	To check whether client device can be searched by specifying its IP address or not	Passed	
WLJ8102S_Reg_301	Searching client using its SSID	To verify whether client device can be searched by specifying the SSID or not	Passed	

WLJ8102S_Reg_302	Check the number of clients visting the building and floor in hourly basic and daily basic	To check the the number of client visiting the building or floor on hourly and daily basic	Passed	
WLJ8102S_Reg_303	Checking the number of new and repeat visitors to the building or floor.	To check the number of new and repeat clients to the building or floor .	Passed	

HA WLC Auth/Authz

Logical ID	Title	Description	Status	Defect ID
WLJ810S_Reg_310	Allowing the user for complete access to WLC network via TACACS and connecting a client to it.	To check whether user can able to read-write access the primary controller of WLC network or not via TACACS	Passed	
WLJ810S_Reg_311	Providing the user for monitoring access to the Primary Controller of WLC via TACACS	To check whether user can able to have monitoring access read-only or not to WLC via TACACS and check if any configuration changes can be made or not.	Passed	
WLJ810S_Reg_312	Providing the user for lobby admin access to the Primary WLC via TACACS	To check whether user can able to have lobby admin access or not to Primary WLC via TACACS	Passed	
WLJ810S_Reg_313	Allowing the user for complete access to Secondary WLC after Bringing the Primary WLC down via TACACS and connecting a JOS client to it.	To check whether user can able to read-write access the Secondary controller of WLC network after the primary controller goes down via TACACS or not and connecting a JOS Client to the Secondary WLC.	Passed	

WLJ810S_Reg_314	Allowing the user for complete access to Secondary WLC after Bringing the Primary WLC down via TACACS and connecting a Window client to it.	To check whether user can able to read-write access the Secondary controller of WLC network after the primary controller goes down via TACACS or not and connecting a Window Client to the Secondary WLC.	Passed	
WLJ810S_Reg_315	Allowing the user for complete access to Secondary WLC after Bringing the Primary WLC down via TACACS and connecting a IOS client to it.	To check whether user can able to read-write access the Secondary controller of WLC network after the primary controller goes down via TACACS or not and connecting a IOS Client to the Secondary WLC.	Passed	
WLJ810S_Reg_316	Allowing the user for complete access to Secondary WLC after Bringing the Primary WLC down via TACACS and connecting a Mac OS client to it.	To check whether user can able to read-write access the Secondary controller of WLC network after the primary controller goes down via TACACS or not and connecting a Mac OS Client to the Secondary WLC.	Passed	
WLJ810S_Reg_317	Providing the user for monitoring access to the Secondary Controller via TACACS if the primary controller goes down.	To check whether user can able to have monitoring access read-only or not to Secondary WLC via TACACS if Primary Controller link is down and check if any configuration changes can be made or not.	Passed	

WLJ810S_Reg_318	Providing the user for lobby admin access to the Secondary WLC via TACACS when the link of the Primary WLC goes down.	To check whether user can able to have lobby admin access or not with Secondary WLC via TACACS when the link of the Primary WLC goes down.	Passed	
WLJ810S_Reg_319	Providing the user for specific page access like Wireless page or Controller page to the Primary WLC via TACACS	To check whether the user is able to access Wireless page or controller page or not	Passed	
WLJ810S_Reg_320	Providing the user to access only WLAN page and checking access availability for other pages in the primary controller	To check whether the user is able access only WLAN page and checking whether other pages are in read-only mode or not	Passed	
WLJ810S_Reg_321	Bring down the primary WLC and down and provide the the user to access only the WLAN page	To check whether the user is able access only WLAN page or not in secondary WLC while primary WLC is down	Passed	
WLJ8102S_Reg_243	Allowing the user for complete access to WLC network via TACACS and connecting a client to it.	To check whether user can able to read-write access the primary controller of WLC network or not via TACACS	Passed	
WLJ8102S_Reg_244	Providing the user for monitoring access to the Primary Controller of WLC via TACACS	To check whether user can able to have monitoring access read-only or not to WLC via TACACS and check if any configuration changes can be made or not.	Passed	
WLJ8102S_Reg_245	Providing the user for lobby admin access to the Primary WLC via TACACS	To check whether user can able to have lobby admin access or not to Primary WLC via TACACS	Passed	

WLJ8102S_Reg_246	Allowing the user for complete access to Secondary WLC after Bringing the Primary WLC down via TACACS and connecting a JOS client to it.	To check whether user can able to read-write access the Secondary controller of WLC network after the primary controller goes down via TACACS or not and connecting a JOS Client to the Secondary WLC.	Passed	
WLJ8102S_Reg_247	Allowing the user for complete access to Secondary WLC after Bringing the Primary WLC down via TACACS and connecting a Window client to it.	To check whether user can able to read-write access the Secondary controller of WLC network after the primary controller goes down via TACACS or not and connecting a Window Client to the Secondary WLC.	Passed	
WLJ8102S_Reg_248	Allowing the user for complete access to Secondary WLC after Bringing the Primary WLC down via TACACS and connecting a IOS client to it.	To check whether user can able to read-write access the Secondary controller of WLC network after the primary controller goes down via TACACS or not and connecting a IOS Client to the Secondary WLC.	Passed	
WLJ8102S_Reg_249	Allowing the user for complete access to Secondary WLC after Bringing the Primary WLC down via TACACS and connecting a Mac OS client to it.	To check whether user can able to read-write access the Secondary controller of WLC network after the primary controller goes down via TACACS or not and connecting a Mac OS Client to the Secondary WLC.	Passed	

WLJ8102S_Reg_250	Providing the user for monitoring access to the Secondary Controller via TACACS if the primary controller goes down.	To check whether user can able to have monitoring access read-only or not to Secondary WLC via TACACS if Primary Controller link is down and check if any configuration changes can be made or not.	Passed	
WLJ8102S_Reg_251	Providing the user for lobby admin access to the Secondary WLC via TACACS when the link of the Primary WLC goes down.	To check whether user can able to have lobby admin access or not with Secondary WLC via TACACS when the link of the Primary WLC goes down.	Passed	
WLJ8102S_Reg_252	Providing the user for specific page access like Wireless page or Controller page to the Primary WLC via TACACS	To check whether the user is able to access Wireless page or controller page or not	Passed	
WLJ8102S_Reg_253	Providing the user to access only WLAN page and checking access availability for other pages in the primary controller	To check whether the user is able access only WLAN page and checking whether other pages are in read-only mode or not	Passed	
WLJ8102S_Reg_254	Bring down the primary WLC and down and provide the the user to access only the WLAN page	To check whether the user is able access only WLAN page or not in secondary WLC while primary WLC is down	Passed	

Autonomous AP

Logical ID	Title	Description	Status	Defect ID
WLJ810S_Reg_220	Association of a client with no security	To check whether clients gets associated or not with Open security.	Passed	

WLJ810S_Reg_221	Client association with WEP security	To check whether clients gets associated or not with WEP security.	Passed	
WLJ810S_Reg_222	Client association with WPA2+PSK	To check whether clients gets associated or with WPA2+PSK security.	Passed	
WLJ810S_Reg_223	Client association with 802.11x	To check whether clients gets associated or not Autonomous AP with 802.11x security.	Passed	
WLJ810S_Reg_224	Verifying the traffic flow between two wireless clients	To check whether 2 wireless clients are generating traffic flow or not	Passed	
WLJ810S_Reg_225	Checking the Trap logs for connected wireless client	To check whether Trap Logs is generating or not for connected wireless client	Passed	
WLJ8102S_Reg_178	Association of a client with no security	To check whether clients gets associated or not with Open security.	Passed	
WLJ8102S_Reg_179	Client association with WEP security	To check whether clients gets associated or not with WEP security.	Passed	
WLJ8102S_Reg_180	Client association with WPA2+PSK	To check whether clients gets associated or with WPA2+PSK security.	Passed	
WLJ8102S_Reg_181	Client association with 802.11x	To check whether clients gets associated or not Autonomous AP with 802.11x security.	Failed	CSCvr82264

WLJ8102S_Reg_182	Verifying the traffic flow between two wireless clients	To check whether 2 wireless clients are genrating traffic flow or not	Passed	
WLJ8102S_Reg_183	Checking the Trap logs for connected wireless client	To check whether Trap Logs is generating or not for connected wireless client	Passed	

Aging Cases

Logical ID	Title	Description	Status	Defect ID
WLJ810S_Reg_427	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	
WLJ810S_Reg_428	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	
WLJ810S_Reg_429	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	
WLJ810S_Reg_430	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	

WLJ810S_Reg_431	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	
WLJ810S_Reg_432	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	
WLJ810S_Reg_433	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	
WLJ810S_Reg_434	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	
WLJ810S_Reg_435	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	
WLJ810S_Reg_436	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	

WLJ8102S_Reg_304	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	
WLJ8102S_Reg_305	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	
WLJ8102S_Reg_306	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	
WLJ8102S_Reg_307	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	
WLJ8102S_Reg_308	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	
WLJ8102S_Reg_309	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	

WLJ8102S_Reg_310	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	
WLJ8102S_Reg_311	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	
WLJ8102S_Reg_312	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	
WLJ8102S_Reg_313	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	

iPSK in Local Switching

Logical ID	Title	Description	Status	Defect ID
WLJ810S_Reg_437	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	

WLJ810S_Reg_438	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	
WLJ810S_Reg_439	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	
WLJ810S_Reg_440	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	
WLJ810S_Reg_441	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	
WLJ810S_Reg_442	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	

WLJ810S_Reg_443	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	
WLJ810S_Reg_444	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	
WLJ810S_Reg_445	Verifying clients roaming with same iPSK tag	To verify whether the client is roaming from one Ap to another Ap.	Passed	
WLJ810S_Reg_446	Verifying clients roaming with different iPSK tag	To verify whether the client is roaming from one Ap to another Ap.	Passed	
WLJ8102S_Reg_314	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	
WLJ8102S_Reg_315	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	

WLJ8102S_Reg_316	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	
WLJ8102S_Reg_317	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	
WLJ8102S_Reg_318	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	
WLJ8102S_Reg_319	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	
WLJ8102S_Reg_320	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	

WLJ8102S_Reg_321	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	
WLJ8102S_Reg_322	Verifying clients roaming with same iPSK tag	To verify whether the client is roaming from one Ap to another Ap.	Passed	
WLJ8102S_Reg_323	Verifying clients roaming with different iPSK tag	To verify whether the client is roaming from one Ap to another Ap.	Passed	

TrustSec Enhancements

Logical ID	Title	Description	Status	Defect ID
WLJ810S_Reg_275	Associating Android clients to TrustSec configured AP and checking the policy hit statistics in WLC UI	To verify the policy hit for Android client after Trustsec configured on AP	Passed	
WLJ810S_Reg_276	Performing Inter controller roaming of Windows client in TrustSec enabled WLC's with Dot1x security.	To check whether inter controller roaming of windows clients works properly or not between WLC's with Dot1x security.	Passed	
WLJ810S_Reg_277	Performing Inter controller roaming of Android client in TrustSec enabled WLC's with Dot1x security.	To check whether inter controller roaming of Android clients works properly or not between WLC's with Dot1x security.	Passed	

WLJ810S_Reg_278	Performing Inter controller roaming of IOS client in TrustSec enabled WLC's with Dot1x security.	To check whether inter controller roaming of IOS clients works properly or not between WLC's with Dot1x security.	Passed	
WLJ810S_Reg_279	Performing Inter controller roaming of MacOS client in TrustSec enabled WLC's with Dot1x security.	To check whether inter controller roaming of windows clients works properly or not between WLC's with Dot1x security.	Passed	
WLJ810S_Reg_280	Performing Inter controller roaming of Windows client in TrustSec enabled WLC's with WPA2-dot1x security.	To check whether inter controller roaming of windows clients works properly or not between WLC's with WPA2-dot1xsecurity.	Passed	
WLJ810S_Reg_281	Performing Inter controller roaming of Android client in TrustSec enabled WLC's with WPA2-dot1x security.	To check whether inter controller roaming of Android clients works properly or not between WLC's with WPA2-dot1x security.	Passed	
WLJ810S_Reg_282	Performing Inter controller roaming of IOS client in TrustSec enabled WLC's with WPA2-dot1x security.	To check whether inter controller roaming of IOS clients works properly or not between WLC's with WPA2-dot1x security.	Passed	
WLJ810S_Reg_283	Performing Inter controller roaming of MacOS client in TrustSec enabled WLC's with WPA2-dot1x security.	To check whether inter controller roaming of MacOS clients works properly or not between WLC's with WPA2-dot1x security.	Passed	

WLJ810S_Reg_284	Enabling CTS override in 2800/3800 AP's which is joined in 5520 WLC UI/CLI	To check that CTS override is enabled or not for 2800/3800 AP's	Passed	
WLJ810S_Reg_285	Checking the trustsec configuration sync in HA WLC's	To check that trustsec configuration sync or not in HA WLC's	Passed	
WLJ8102S_Reg_225	Associating Android clients to TrustSec configured AP and checking the policy hit statistics in WLC UI	To verify the policy hit for Android client after Trustsec configured on AP	Passed	
WLJ8102S_Reg_226	Performing Inter controller roaming of Windows client in TrustSec enabled WLC's with Dot1x security.	To check whether inter controller roaming of windows clients works properly or not between WLC's with Dot1x security.	Passed	
WLJ8102S_Reg_227	Performing Inter controller roaming of Android client in TrustSec enabled WLC's with Dot1x security.	To check whether inter controller roaming of Android clients works properly or not between WLC's with Dot1x security.	Passed	
WLJ8102S_Reg_228	Performing Inter controller roaming of IOS client in TrustSec enabled WLC's with Dot1x security.	To check whether inter controller roaming of IOS clients works properly or not between WLC's with Dot1x security.	Passed	
WLJ8102S_Reg_229	Performing Inter controller roaming of MacOS client in TrustSec enabled WLC's with Dot1x security.	To check whether inter controller roaming of windows clients works properly or not between WLC's with Dot1x security.	Passed	

WLJ8102S_Reg_230	Performing Inter controller roaming of Windows client in TrustSec enabled WLC's with WPA2-dot1x security.	To check whether inter controller roaming of windows clients works properly or not between WLC's with WPA2-dot1xsecurity.	Passed	
WLJ8102S_Reg_231	Performing Inter controller roaming of Android client in TrustSec enabled WLC's with WPA2-dot1x security.	To check whether inter controller roaming of Android clients works properly or not between WLC's with WPA2-dot1x security.	Passed	
WLJ8102S_Reg_232	Performing Inter controller roaming of IOS client in TrustSec enabled WLC's with WPA2-dot1x security.	To check whether inter controller roaming of IOS clients works properly or not between WLC's with WPA2-dot1x security.	Passed	
WLJ8102S_Reg_233	Performing Inter controller roaming of MacOS client in TrustSec enabled WLC's with WPA2-dot1x security.	To check whether inter controller roaming of MacOS clients works properly or not between WLC's with WPA2-dot1x security.	Passed	
WLJ8102S_Reg_234	Enabling CTS override in 2800/3800 AP's which is joined in 5520 WLC UI/CLI	To check that CTS override is enabled or not for 2800/3800 AP's	Passed	
WLJ8102S_Reg_235	Checking the trustsec configuration sync in HA WLC's	To check that trustsec configuration sync or not in HA WLC's	Passed	

EoGRE Tunnel Priority / Fallback

Logical ID	Title	Description	Status	Defect ID

WLJ810S_Reg_261	Associating Android clients to a local switching enabled WLAN with Tunnel profile mapped	To check whether Android clients gets associated or not to 2800/3800 AP's with local switching enabled WLAN with EoGRE tunnel mapped in it	Failed	CSCvq56355
WLJ810S_Reg_262	Associating IOS clients to a local switching enabled WLAN with Tunnel profile mapped	To check whether IOS clients gets associated or not to 2800/3800 AP's with local switching enabled WLAN with EoGRE tunnel mapped in it	Passed	
WLJ810S_Reg_263	Associating Windows clients to a local switching enabled WLAN with Tunnel profile mapped	To check whether windows clients gets associated or not to 2800/3800 AP's with local switching enabled WLAN with EoGRE tunnel mapped in it	Passed	
WLJ810S_Reg_264	Associating Apple MacBook clients to a local switching enabled WLAN with Tunnel profile mapped	To check whether Apple MacBook clients gets associated or not to 2800/3800 AP's with local switching enabled WLAN with EoGRE tunnel mapped in it	Passed	
WLJ810S_Reg_265	Checking the tunnel gateway fallback works properly for Android clients	To check whether Android clients fallback to secondary tunnel or not when primary tunnel gateway goes down	Passed	
WLJ810S_Reg_266	Checking the tunnel gateway fallback works properly for IOS clients	To check whether IOS clients fallback to secondary tunnel or not when primary tunnel gateway goes down	Passed	

WLJ810S_Reg_267	Checking the tunnel gateway fallback works properly for Windows clients	To check whether Windows clients fallback to secondary tunnel or not when primary tunnel gateway goes down	Passed	
WLJ810S_Reg_268	Checking the tunnel gateway fallback works properly for Apple MacBook clients	To check whether Apple MacBook clients fallback to secondary tunnel or not when primary tunnel gateway goes down	Passed	
WLJ810S_Reg_269	Checking the tunnel configuration in HA WLCs	To check whether confit sync occurs or not for tunnel gateway/domain configuration between Active and Standby WLC's	Passed	
WLJ810S_Reg_270	Creating a tunnel gateway with invalid ipv4 address	To check whether proper error message thrown or not while creating tunnel gateway with invalid ipv4 address	Passed	
WLJ810S_Reg_271	Changing the role for created tunnel domain in WLC GUI/CLI	To check whether role can be changed or not for created tunnel domain via WLC GUI and CLI	Passed	
WLJ810S_Reg_272	Configuring the tunnel domain for WLC from PI	To check whether tunnel configurations can be done or not for WLC via PI and vice versa	Passed	
WLJ810S_Reg_273	Associating Client to a local switching enabled and dot1X security WLAN with Tunnel profile mapped in AP standalone mode	To check whether clients gets associated or not to 2800/3800 AP's with local switching enabled WLAN with EoGRE tunnel mapped in it in AP standalone mode	Passed	

WLJ810S_Reg_274	Associating Client to a local switching enabled and open security WLAN with Tunnel profile mapped in AP standalone mode	To check whether clients gets associated or not to 2800/3800 AP's with local switching enabled WLAN with EoGRE tunnel mapped in it in AP standalone mode	Passed	
WLJ8102S_Reg_211	Associating Android clients to a local switching enabled WLAN with Tunnel profile mapped	To check whether Android clients gets associated or not to 2800/3800 AP's with local switching enabled WLAN with EoGRE tunnel mapped in it	Passed	
WLJ8102S_Reg_212	Associating IOS clients to a local switching enabled WLAN with Tunnel profile mapped	To check whether IOS clients gets associated or not to 2800/3800 AP's with local switching enabled WLAN with EoGRE tunnel mapped in it	Passed	
WLJ8102S_Reg_213	Associating Windows clients to a local switching enabled WLAN with Tunnel profile mapped	To check whether windows clients gets associated or not to 2800/3800 AP's with local switching enabled WLAN with EoGRE tunnel mapped in it	Passed	
WLJ8102S_Reg_214	Associating Apple MacBook clients to a local switching enabled WLAN with Tunnel profile mapped	To check whether Apple MacBook clients gets associated or not to 2800/3800 AP's with local switching enabled WLAN with EoGRE tunnel mapped in it	Passed	

WLJ8102S_Reg_215	Checking the tunnel gateway fallback works properly for Android clients	To check whether Android clients fallback to secondary tunnel or not when primary tunnel gateway goes down	Passed	
WLJ8102S_Reg_216	Checking the tunnel gateway fallback works properly for IOS clients	To check whether IOS clients fallback to secondary tunnel or not when primary tunnel gateway goes down	Passed	
WLJ8102S_Reg_217	Checking the tunnel gateway fallback works properly for Windows clients	To check whether Windows clients fallback to secondary tunnel or not when primary tunnel gateway goes down	Passed	
WLJ8102S_Reg_218	Checking the tunnel gateway fallback works properly for Apple MacBook clients	To check whether Apple MacBook clients fallback to secondary tunnel or not when primary tunnel gateway goes down	Passed	
WLJ8102S_Reg_219	Checking the tunnel configuration in HA WLCs	To check whether config sync occurs or not for tunnel gateway/domain configuration between Active and Standby WLC's	Passed	
WLJ8102S_Reg_220	Creating a tunnel gateway with invalid ipv4 address	To check whether proper error message thrown or not while creating tunnel gateway with invalid ipv4 address	Passed	
WLJ8102S_Reg_221	Changing the role for created tunnel domain in WLC GUI/CLI	To check whether role can be changed or not for created tunnel domain via WLC GUI and CLI	Passed	

WLJ8102S_Reg_222	Configuring the tunnel domain for WLC from PI	To check whether tunnel configurations can be done or not for WLC via PI and vice versa	Passed	
WLJ8102S_Reg_223	Associating Client to a local switching enabled and dot1X security WLAN with Tunnel profile mapped in AP standalone mode	To check whether clients gets associated or not to 2800/3800 AP's with local switching enabled WLAN with EoGRE tunnel mapped in it in AP standalone mode	Passed	
WLJ8102S_Reg_224	Associating Client to a local switching enabled and open security WLAN with Tunnel profile mapped in AP standalone mode	To check whether clients gets associated or not to 2800/3800 AP's with local switching enabled WLAN with EoGRE tunnel mapped in it in AP standalone mode	Passed	

Domain Based URL ACL

Logical ID	Title	Description	Status	Defect ID
WLJ810S_Reg_244	Check if the Dummy Domain address is accepted in the URL ACL	To Verify if the Invalid domain names are accepting or not	Passed	
WLJ810S_Reg_245	Create new URL ACL , Add new URL on ACL on 5520 WLC	To verify that new ACL created , rule added or not using UI	Failed	CSCvq35980
WLJ810S_Reg_246	Add new URL domain on created url acl	To verify that new URL domain (www.cisco.com,www.yahoo.com) added or not	Passed	
WLJ810S_Reg_247	Configure URL ACL as blacklist on WLAN and connect one Window client , open URL that configured in acl	To verify that URL is blocking that configured in URL-ACL profile and showing hit count in UI of WLC	Passed	

WLJ810S_Reg_248	Configure URL ACL on interface using CLI and connect iOS client	To verify that URL ACL configured on interface or not and iOS client connectivity with URL blocked	Passed	
WLJ810S_Reg_249	Delete URL ACL rule after applied	To verify that URL ACL rule delete successfully or not	Passed	
WLJ810S_Reg_250	Modified rule of URL ACL and connect Android client	To verify that rule action modified or not and Android client connectivity	Passed	
WLJ810S_Reg_251	Clear counter of URL ACL profile after open url in client web browser	To verify that counter is clear or not of URL ACL profile	Passed	
WLJ810S_Reg_252	Show URL ACL status on WLAN using CLI	To verify that URL ACL status showing configured on WLAN	Passed	
WLJ8102S_Reg_202	Check if the Dummy Domain address is accepted in the URL ACL	To Verify if the Invalid doamin names are accepting or not	Passed	
WLJ8102S_Reg_203	Create new URL ACL , Add new URL on ACL on 5520 WLC	To verify that new ACL created , rule added or not using UI	Passed	
WLJ8102S_Reg_204	Add new URL domain on created url acl	To verify that new URL domain (www.cisco.com,www.yahoo.com) added or not	Passed	
WLJ8102S_Reg_205	Configure URL ACL as blacklist on WLAN and connect one Window client , open URL that configured in acl	To verify that URL is blocking that configured in URL-ACL profile and showing hit count in UI of WLC	Passed	
WLJ8102S_Reg_206	Configure URL ACL on interface using CLI and connect iOS client	To verify that URL ACL configured on interface or not and ioS client connectivity with URL blocked	Passed	

WLJ8102S_Reg_207	Delete URL ACL rule after applied	To verify that URL ACL rule delete succesfully or not	Passed	
WLJ8102S_Reg_208	Modified rule of URL ACL and connect Android client	To verify that rule action modified or not and Android client connectivity	Passed	
WLJ8102S_Reg_209	Clear counter of URL ACL profile after open url in client web browser	To verify that counter is clear or not of URL ACL profile	Passed	
WLJ8102S_Reg_210	Show URL ACL status on WLAN using CLI	To verify that URL ACL status showing configured on WLAN	Passed	

Flex Video streaming

Logical ID	Title	Description	Status	Defect ID
WLJ810S_Reg_226	MC2UC traffic to local-switching client	To verify that the local-switching client subscribed to video streaming receives MC2UC traffic	Failed	CSCvq52560
WLJ810S_Reg_227	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	
WLJ810S_Reg_228	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	
WLJ810S_Reg_229	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	

WLJ810S_Reg_230	Client disassociates when receiving MC2UC traffic	To verify whether AP stops sending traffic when client disassociates	Passed	
WLJ810S_Reg_231	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	
WLJ810S_Reg_232	LS client receiving MC2UC traffic roam between APs in the flex connect group	To verify the local-switching client receiving MC2UC traffic roaming between APs in the flex connect group	Passed	
WLJ810S_Reg_233	Flex LS client receiving MC2UC traffic when AP move from connected > SA > connected with same confit	To verify whether the LS client receives continuous MC2UC traffic when AP moves from connected > SA > connected with same confit	Passed	
WLJ810S_Reg_234	Flex LS client receiving MC2UC traffic when AP move from connected > SA > connected with different confit	To verify whether the LS client receives continuous MC2UC traffic when AP moves from connected > SA > connected with different confit	Passed	
WLJ810S_Reg_235	Flex AP reboot in connected mode when Flex LS client receiving MC2UC traffic	To verify whether client associates and receives MC2UC traffic when flex AP is rebooted in connected mode.	Passed	
WLJ810S_Reg_236	Vide stream confit sync for LS WLAN in HA setup	To verify whether the video streaming confit for LS WLAN has been synced between the Active and Standby in HA setup	Passed	

WLJ810S_Reg_237	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	
WLJ8102S_Reg_184	MC2UC traffic to local-switching client	To verify that the local-switching client subscribed to videostreaming receives MC2UC traffic	Passed	
WLJ8102S_Reg_185	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	
WLJ8102S_Reg_186	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	
WLJ8102S_Reg_187	Multiple LS clients in same vlan, same wlan, receiving MC2UC traffic	To verify whether the multiple local-switching clients receives MC2UC traffic when subscribed to videostream	Passed	
WLJ8102S_Reg_188	Client disassociates when receiving MC2UC traffic	To verify whether AP stops sending traffic when client disassociates	Passed	
WLJ8102S_Reg_189	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	
WLJ8102S_Reg_190	LS client receiving MC2UC traffic roam between APs in the flexconnect group	To verify the local-switching client receiving MC2UC traffic roaming between APs in the flexconnect group	Passed	

WLJ8102S_Reg_191	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	
WLJ8102S_Reg_192	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	
WLJ8102S_Reg_193	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	
WLJ8102S_Reg_194	Videstream config sync for LS WLAN in HA setup	To verify whether the videostreaming config for LS WLAN has been synced between the Active and Standby in HA setup	Passed	
WLJ8102S_Reg_195	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	

Network Assurance

Logical ID	Title	Description	Status	Defect ID
WLJ810S_Reg_190	Creating the SSID and connecting the sensor mode AP	Verify that user is able to connect the sensor mode ap as a client	Passed	

WLJ810S_Reg_191	Radius server up/down event data to Network Assurance	Verify that Radius server up/down event data is sending to Network Assurance server or not	Passed	
WLJ810S_Reg_192	Verify that user is able to disabled NAC via CLI	Checking that user is able to disable NAC via CLI or not	Passed	
WLJ810S_Reg_193	Verify that JSON data is sending out from WLC	Checking that JSON data is sending out from WLC to NA server or not	Passed	
WLJ810S_Reg_194	WLC CLI allowing XOR radio as sensor even when WSA is disabled	Checking that user is able to XOR radio as a sensor while WSA disabled	Passed	
WLJ810S_Reg_195	Verify that WLC sends nearestAP neighbours data to NA server correctly or not	Checking that WLC sends nearestAP neighbours data to NA server correctly or not	Passed	
WLJ810S_Reg_196	Verify that wlan changes are reflecting in client event reason type for retries or not	Checking that WLAN changes are reflecting in NA server or not	Passed	
WLJ810S_Reg_197	Verify that wsa server url confit is syncing to standby wlc or not	Checking that wsa confit syncing with standby in HA mode	Passed	
WLJ810S_Reg_198	Verify that WLC able to resolve url if dns server ip is updated of NA server	Checking that wlc able to resolve the url of NA server if NA server ip address changes	Passed	
WLJ810S_Reg_199	Configuring PSK key for wsa backhaul said	Verify that user is able to confit psk key in backhaul said as normal WLAN or not	Passed	
WLJ810S_Reg_200	Verifying that mac filtering working properly for sensor mode ap debug	Checking that mac-filtering working properly for sensor mode ap debug or not	Passed	

AP 4800 Support

Logical ID	Title	Description	Status	Defect ID
WLJ810S_Reg_38	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	
WLJ810S_Reg_39	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	
WLJ810S_Reg_40	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	
WLJ810S_Reg_41	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	
WLJ810S_Reg_42	Moving AP from 3504 controller to 5520 through High availability	To check if the AP moves from 3504 WLC to 5520 WLC through high availability.	Passed	
WLJ810S_Reg_43	Performing Intra controller roaming of Windows J OS client	To check whether intra controller roaming of windows clients works properly or not in WLC	Passed	
WLJ810S_Reg_44	Performing Intra controller roaming of Android client	To check whether intra controller roaming of Android clients works properly or not	Passed	

WLJ810S_Reg_45	Performing Intra controller roaming of IOS client	To check whether intra controller roaming of IOS clients works properly or not in WLC	Passed	
WLJ810S_Reg_46	Performing Intra controller roaming of Mac OS client	To check whether intra controller roaming of MacOS clients works properly or not	Passed	
WLJ810S_Reg_47	Performing Inter controller roaming of Windows J OS client	To check whether inter controller roaming of windows clients works properly or not	Passed	
WLJ810S_Reg_48	Performing Inter controller roaming of Android client	To check whether inter controller roaming of Android clients works properly or not	Passed	
WLJ810S_Reg_49	Performing Inter controller roaming of IOS client	To check whether inter controller roaming of IOS clients works properly or not	Passed	
WLJ810S_Reg_50	Performing Inter controller roaming of Mac OS client	To check whether inter controller roaming of Mac OS clients works properly or not	Passed	
WLJ810S_Reg_51	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	
WLJ810S_Reg_52	Verifying AP-Image Pre-download with primary image to the 4800 AP	To verify the AP-Pre download with primary images is successfully or not.	Failed	CSCvq53848

WLJ810S_Reg_53	Verifying AP-Image Pre-download with primary image to the 4800 AP	To verify the AP-Pre download with primary images is successfully or not.	Passed	

ATF On Mesh

Logical ID	Title	Description	Status	Defect ID
WLJ810S_Reg_253	Config Mesh setup and apply confit on Mesh Aps	To verify that Mesh setup configured and ATF applied on Mesh Aps	Failed	CSCvq57674 /CSCvq46668
WLJ810S_Reg_254	Apply ATF Enforcement mode on MESH AP	To verify that ATF Enforcement mode applied on MESH AP or not	Passed	
WLJ810S_Reg_255	Apply ATF policy on wlan and connect Android client	To verify that policy applied on WLAN or not and client connected successfully	Passed	
WLJ810S_Reg_256	Mac OS client connectivity with l2 security WLAN which having different Policy weight	To verify the client connectivity with two SSID having different weight	Passed	
WLJ810S_Reg_257	Apply ATF Enforcement mode on AP group	To verify that ATF Enforcement mode applied on AP group or not	Passed	
WLJ810S_Reg_258	Airtime allocation override on universal client access radio 802.11a	To verify that ATF override on universal client access radio 802.11a is enable or not	Passed	
WLJ810S_Reg_259	Airtime allocation override on universal client access radio 802.11b	To verify that ATF override on universal client access radio 802.11b is enable or not	Passed	
WLJ810S_Reg_260	Disable Enforced mode of network for 802.11a radio on GUI	To verify that optimization is disable for network , 802.11 a radio	Passed	

Flexconnect IOS Parity: AAA Override of VLAN Name template

Logical ID	Title	Description	Status	Defect ID
WLJ810S_Reg_361	Checking the AAA override for VLAN name id	To verify whether AAA overriding happening or not with VLAN name	Passed	
WLJ810S_Reg_362	Configuring VLAN name id for AAA override at the time of VLAN support in disable state	To verify whether AAA override is happening or not when VLAN support is in disable state	Passed	
WLJ810S_Reg_363	After configure the WLAN-VLAN support checking the details	To verify whether WLAN-VLAN details are applying or not after configure and disable the VLAN support	Passed	
WLJ810S_Reg_364	Checking the details in AP after VLAN name id Exchange	To verify details are showing in AP cli or not	Passed	
WLJ810S_Reg_365	Checking the debug details at the time of VLAN name id details	To verify whether details are showing successfully or not at the time of VLAN name id exchange	Passed	
WLJ810S_Reg_366	Rebooting the WLC after AAA override with VLAN name ID	To verify whether Client are getting AAA override details or not after reboot	Passed	
WLJ810S_Reg_367	Checking the details in Roaming	To verify whether Roaming is happening with AAA override for VLAN name id	Passed	

Location Analytics

Logical ID	Title	Description	Status	Defect ID

WLJ810S_Reg_295	Adding access points to Floor map	To verify whether client devices are displayed in the floor map or not	Passed	
WLJ810S_Reg_296	Checking windows Client Location is displaying in Floor map	To verify whether windows client devices are displayed in the floor map or not	Passed	
WLJ810S_Reg_297	Checking Android Client Location is displaying in Floor map	To verify whether android client devices are displayed in the floor map or not	Passed	
WLJ810S_Reg_298	Performing filter operation for connected client by MAC address/IP/SSID	To verify whether client device can be searched by specifying its MAC address/IP/SSID or not	Passed	
WLJ810S_Reg_299	Interferers in Floor map	To verify whether interferers are displayed in the floor map or not	Passed	
WLJ810S_Reg_300	Checking Rogue Devices are displaying in Floor map	To verify whether rogues are displayed in the floor map or not	Passed	
WLJ810S_Reg_301	Client movement history playback	To verify whether client's movement history is shown or not	Passed	
WLJ810S_Reg_302	Creating New Report for building and floor	To verify whether new report can be created or not	Passed	

Flexconnect IOS Parity: AAA Override bi-directional rate limit per client/BSSID

Logical ID	Title	Description	Status	Defect ID
WLJ810S_Reg_353	Configuring the downstream and upstream value as "0" per User	To verify whether downstream and upstream values are no restrictions for configured values as "0" per User or not	Passed	

WLJ810S_Reg_354	Configuring the downstream and upstream value as "0" per SSID	To verify whether downstream and upstream values are no restrictions for configured values as "0" per SSID or not	Passed	
WLJ810S_Reg_355	Configuring the downstream and upstream value as certain range per User	To verify whether downstream and upstream values access with restrictions for configured values as per User or not	Passed	
WLJ810S_Reg_356	Configuring the downstream and upstream value as certain range per SSID	To verify whether downstream and upstream values access with restrictions for configured values as per SSID	Passed	
WLJ810S_Reg_357	Resetting the WLC after configure the Client and SSID values	To verify whether Client and SSID values are proper or not	Passed	
WLJ810S_Reg_358	Clearing the values after AAA override enable	To verify whether values are clearing or not	Passed	
WLJ810S_Reg_359	Checking the roaming scenario	To verify whether after client roam between controllers client accessing proper bandwidth or not	Passed	
WLJ810S_Reg_360	Checking the bandwidth for client and SSID in standalone mode	To verify whether clients are getting proper connection for standalone or nor	Passed	

Facebook WIFI

Logical ID	Title	Description	Status	Defect ID
WLJ810S_Reg_286	Redirection to Facebook Page	To verify redirection to Facebook page for logging in is successful or not	Passed	

WLJ810S_Reg_287	Restricting free internet access for unauthenticated Windows client	To verify denial of internet access for unauthenticated Windows users is successful or not	Passed	
WLJ810S_Reg_288	Http Redirection for Continuing Browsing in Android Phone	To Verify Redirection to the Http page initially requested by the Android user is successful or not	Passed	
WLJ810S_Reg_289	Https Redirection for Continuing Browsing in Windows Laptop	To Verify Redirection to the Https page initially requested by the Windows Laptop user is successful or not	Passed	
WLJ810S_Reg_290	Show Logs tab	To Verify successful download of each individual log file listed in the show logs tab	Passed	
WLJ810S_Reg_291	User data statistics	To verify whether the user's data statistics are displayed correctly or not	Passed	
WLJ810S_Reg_292	KNOWN Users	To verify whether authenticated users are listed in the user data tab or not	Passed	
WLJ810S_Reg_293	UNKNOWN Users	To verify whether users not authenticated are listed in the user data tab or not	Passed	
WLJ810S_Reg_294	IN-AUTH Users	To verify whether users attempting to get authenticated are listed in the user data tab or not	Passed	

Inter Release Controller Mobility

Logical ID	Title	Description	Status	Defect ID

WLJ810S_Reg_467	Performing Inter Controller roaming of Windows JOS client between 9800 Controller and 5520 WLC	To check whether Inter Controller roaming works properly or not for Windows JOS clients between 5520 WLC and 9800 Controller with secure mobility tunnel config	Passed	
WLJ810S_Reg_468	Performing 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	
WLJ810S_Reg_469	Checking the Anchor controller functionality during the roaming of Windows JOS Client	To check whether Anchor controller functionality works properly or not in Cat 9800 Controller during the roaming of Windows JOS Client	Passed	
WLJ810S_Reg_470	Checking the roamed clients status in PI during HA failover	To check whether clients status shown properly or not in PI for WLC's during force failover	Passed	
WLJ810S_Reg_471	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	
WLJ810S_Reg_472	Verifying the roaming clients status during RADIUS (ISE) fallback	To check whether roaming works properly or not for clients between 5520 WLC and 9800 Controller during RADIUS fallback	Passed	

WLJ810S_Reg_473	Configuring the Mobility group parameters via TACACS login with Controller access	To check whether mobility groups can be configured or not via TACACS Controller login	Passed	
WLJ810S_Reg_474	Trying to configure the Mobility group parameters via TACACS login with read only access	To check whether mobility groups can be configured or not via TACACS login with read only access	Passed	
WLJ810S_Reg_475	Verifying 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	
WLJ810S_Reg_476	Verifying 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	
WLJ810S_Reg_477	Checking the Anchor controller functionality during the roaming of MAC OS Client	To check whether Anchor controller functionality works properly or not in Cat 9800 Controller during the roaming of MAC OS Client	Passed	
WLJ810S_Reg_478	Performing Inter Controller roaming of Windows JOS client between 9800 Controller and 8540 WLC	To check whether Inter Controller roaming works properly or not for Windows JOS clients between 8540 WLC and 9800 Controller with secure mobility tunnel config	Passed	
WLJ810S_Reg_479	Setting UP the secure mobility tunnel between 9800 Controller & 5520 WLC	To check whether both Control & Data path gets UP or not between 5520 WLC & 9800 Controller	Passed	

WLJ810S_Reg_480	Performing Inter Controller roaming of MAC client between 9800 Controller and 3504 WLC	To check whether Inter Controller roaming works properly or not for MAC clients between 3504 WLC and 9800 Controller with secure mobility tunnel config	Passed	
WLJ810S_Reg_481	Performing Inter Controller roaming of Android client between 9800 Controller and 3504 WLC	To check whether Inter Controller roaming works properly or not for Android clients between 3504 WLC and 9800 Controller with secure mobility tunnel config	Passed	
WLJ810S_Reg_482	Performing Inter Controller roaming of iOS client between 9800 Controller and 5520 WLC	To check whether Inter Controller roaming works properly or not for iOS clients between 5520 WLC and 9800 Controller with secure mobility tunnel config	Passed	
WLJ810S_Reg_483	Performing Inter Controller roaming of iOS client between 9800 Controller and 8540 WLC	To check whether Inter Controller roaming works properly or not for iOS clients between 8540 WLC and 9800 Controller with secure mobility tunnel config	Passed	
WLJ810S_Reg_484	Performing Inter Controller roaming of iOS client between 9800 Controller and 3504 WLC	To check whether Inter Controller roaming works properly or not for iOS clients between 3504 WLC and 9800 Controller with secure mobility tunnel config	Passed	

WLJ810S_Reg_485	Performing Inter Controller roaming of Windows JOS client between 9800 Controller and 3504 WLC	To check whether Inter Controller roaming works properly or not for Windows JOS clients between 3504 WLC and 9800 Controller with secure mobility tunnel config	Passed	
WLJ810S_Reg_486	Checking the Anchor controller functionality during the roaming of Android Client	To check whether Anchor controller functionality works properly or not in Cat 9800 Controller during the roaming of Android Client	Passed	
WLJ810S_Reg_487	Checking the Anchor controller functionality during the roaming of iOS Client	To check whether Anchor controller functionality works properly or not in Cat 9800 Controller during the roaming of iOS Client	Passed	
WLJ810S_Reg_488	Performing Inter Controller roaming of MAC client between 9800 Controller and 5520 WLC	To check whether Inter Controller roaming works properly or not for MAC clients between 5520 WLC and 9800 Controller with secure mobility tunnel config	Passed	
WLJ810S_Reg_489	Performing Inter Controller roaming of MAC client between 9800 Controller and 8540 WLC	To check whether Inter Controller roaming works properly or not for MAC clients between 8540 WLC and 9800 Controller with secure mobility tunnel config	Passed	

WLJ810S_Reg_490	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	
WLJ810S_Reg_491	Performing Inter Controller roaming of Android client between 9800 Controller and 8540 WLC	To check whether Inter Controller roaming works properly or not for Android clients between 8540 WLC and 9800 Controller with secure mobility tunnel config	Passed	
WLJ810S_Reg_492	Checking the Anchor controller functionality during the roaming of Anyconnect Client	To check whether Anchor controller functionality works properly or not in Cat 9800 Controller during the roaming of Anyconnect Client	Passed	
WLJ810S_Reg_493	Performing Inter Controller roaming of different OS clients between 9800 Controller and 8540 WLC with WPA2+dot1x (LEAP)	To check whether Inter Controller roaming works properly or not for clients between 5520 WLC and 9800 Controller with security type WPA2+dot1x (LEAP)	Passed	
WLJ810S_Reg_494	Performing Inter Controller roaming of different OS clients between 9800 Controller and 3504 WLC with WPA2+dot1x (EAP-TLS)	To check whether Inter Controller roaming works properly or not for clients between 5520 WLC and 9800 Controller with security type WPA2+dot1x (EAP-TLS)	Passed	

WLJ810S_Reg_495	Configuring the Anchor controller option in a WLAN in WLC UI	To check whether Anchor option can be configured or not in a WLAN for WLC's and 9800 Controller	Passed	
WLJ810S_Reg_496	Check if AVC rules created in PI are deployed to WLC	To check if AVC rules created in PI are deployed to WLC	Failed	CSCvq37536
WLJ810S_Reg_497	Check different details like location,Interference data in clients and user page	To check different details like location,Interference data in clients and user page	Failed	CSCvq57362
WLJ8102S_Reg_344	Checking the roamed clients status in PI	To check whether clients status shown properly or not in PI for WLC's	Passed	
WLJ8102S_Reg_345	Checking the roamed clients status in PI during HA failover	To check whether clients status shown properly or not in PI for WLC's during force failover	Passed	
WLJ8102S_Reg_346	Creating the custom reports for the roamed clients status in PI	To check whether custom reports are created or not for roamed client status in PI	Passed	
WLJ8102S_Reg_347	Monitoring the roamed clients between 9800 Controller and 8540 WLC with WPA2+dot1x (LEAP) in PI	To check whether clients staus shown properly or not after roamed between 5520 WLC and 9800 Controller with security type WPA2+dot1x (LEAP) in PI	Passed	
WLJ8102S_Reg_348	Monitoring the roamed clients between 9800 Controller and 3504 WLC with WPA2+dot1x (EAP-TLS) in PI	To check whether clients staus shown properly or not after roamed between between 5520 WLC and 9800 Controller with security type WPA2+dot1x (EAP-TLS) in PI	Passed	

WLJ8102S_Reg_349	Monitoring the clients between 9800 Controller and 5520 WLC with WPA2+dot1x (PEAP) in PI	To check whether clients staus shown properly or not after roamed between between 5520 WLC and 9800 Controller with security type WPA2+dot1x (PEAP) in PI	Passed	

Reboot APs by groups

Logical ID	Title	Description	Status	Defect ID
WLJ810S_Reg_14	Creating a site tag in eWLC UI	To create a site tag in eWLC UI and check if the site tag is created or not.	Passed	
WLJ810S_Reg_15	Creating a site tag in eWLC CLI	To create a site tag in eWLC CLI and check if the site tag is created or not.	Passed	
WLJ810S_Reg_16	Mapping a AP profile to the site tag using eWLC UI	To map a AP profile to the site tag and check if the AP profile is mapped to site tag or not.	Passed	
WLJ810S_Reg_17	Mapping a Site to AP in eWLC UI	To map a AP profile to the site tag and check if the AP profile is mapped to site tag or not.	Passed	
WLJ810S_Reg_18	Adding one COS AP to site and rebooting the AP	To add one COS AP to site and applying the site reboot command and check if the AP gets reeboted	Passed	
WLJ810S_Reg_19	Adding 3 COS AP to site and rebooting the AP	To add 3 COS AP to site and applying the site reboot command and check if all the AP gets reeboted and joins the eWLC again	Passed	

WLJ810S_Reg_20	Adding COS AP to site and rebooting the AP with different AP modes	To add COS AP to site and applying the site reboot command and check if the AP gets rebooted in all modes or not	Passed	
WLJ810S_Reg_21	Adding one IOS AP to the site and rebooting the AP through AP site reset command	To add one IOS to the site creates and giving the AP reboot command through CLI to check if the AP gets rebooted or not.	Passed	
WLJ810S_Reg_22	Adding 3 IOS AP to site and rebooting the AP	To add 3 IOS AP to site and applying the site reboot command and check if all the AP gets reeboted and joins the eWLC again	Passed	
WLJ810S_Reg_23	Adding IOS AP to site and rebooting the AP with different AP modes	To add IOS AP to site and applying the site reboot command and check if the AP gets rebooted in all modes or not	Passed	
WLJ810S_Reg_24	Adding 1810 AP to site and rebooting the AP with different AP modes	To add 1810 AP to site and applying the site reboot command and check if the AP gets rebooted in all modes or not	Passed	
WLJ810S_Reg_25	Trying to reboot the AP with a non existing site name	To give the reboot command using site name with a non existing site name and check if the AP is rebooting or not .	Passed	
WLJ810S_Reg_26	Trying to reboot the AP which is already rebooting using site reboot command	To reboot the AP using AP site reboot command which is already being rebooted .	Passed	
WLJ8102S_Reg_34	Creating a site tag in eWLC UI	To create a site tag in eWLC UI and check if the site tag is created or not.	Passed	

WLJ8102S_Reg_35	Creating a site tag in eWLC CLI	To create a site tag in eWLC CLI and check if the site tag is created or not.	Passed	
WLJ8102S_Reg_36	Mapping a AP profile to the site tag using eWLC UI	To map a AP profile to the site tag and check if the AP profile is mapped to site tag or not.	Passed	
WLJ8102S_Reg_37	Mapping a Site to AP in eWLC UI	To map a AP profile to the site tag and check if the AP profile is mapped to site tag or not.	Passed	
WLJ8102S_Reg_38	Adding one COS AP to site and rebooting the AP	To add one COS AP to site and applying the site reboot command and check if the AP gets reeboted	Passed	
WLJ8102S_Reg_39	Adding 3 COS AP to site and rebooting the AP	To add 3 COS AP to site and applying the site reboot command and check if all the AP gets reeboted and joins the eWLC again	Passed	
WLJ8102S_Reg_40	Adding COS AP to site and rebooting the AP with different AP modes	To add COS AP to site and applying the site reboot command and check if the AP gets rebooted in all modes or not	Passed	
WLJ8102S_Reg_41	Adding one IOS AP to the site and rebooting the AP through AP site reset command	To add one IOS to the site creates and giving the AP reboot command through CLI to check if the AP gets rebooted or not.	Passed	
WLJ8102S_Reg_42	Adding 3 IOS AP to site and rebooting the AP	To add 3 IOS AP to site and applying the site reboot command and check if all the AP gets reeboted and joins the eWLC again	Passed	

WLJ8102S_Reg_43	Adding IOS AP to site and rebooting the AP with different AP modes	To add IOS AP to site and applying the site reboot command and check if the AP gets rebooted in all modes or not	Passed	
WLJ8102S_Reg_44	Adding 1810 AP to site and rebooting the AP with different AP modes	To add 1810 AP to site and applying the site reboot command and check if the AP gets rebooted in all modes or not	Passed	
WLJ8102S_Reg_45	Trying to reboot the AP with a non existing site name	To give the reboot comand using site name with a non existing site name and check if the AP is rebooting or not .	Passed	
WLJ8102S_Reg_46	Trying to reboot the AP which is already rebooting using site reboot command	To reboot the AP using AP site reboot command which is already being rebooted .	Passed	

High Availability & Monitoring HA

Logical ID	Title	Description	Status	Defect ID
WLJ810S_Reg_368	Configuring HA pair up- WLC 5520 /8540 by using the cli command	To verify whether the HA pair(ACTIVE:STANDBY) is up successfully by using the cli command	Passed	
WLJ810S_Reg_369	Configuring HA pair up- WLC 5520 /8540 by using the cli command	To verify whether the HA pair(ACTIVE:STANDBY) is up successfully by using the cli command	Passed	
WLJ810S_Reg_370	Configuring HA pair up- WLC 5520 /8540 by using the cli command	To verify whether the HA pair(ACTIVE:STANDBY) is up successfully by using the cli command	Passed	

WLJ810S_Reg_371	Configuring HA pair up- WLC 5520 /8540 by using the cli command	To verify whether the HA pair(ACTIVE:STANDBY) is up successfully by using the cli command	Passed	
WLJ810S_Reg_372	Configuring HA pair up- WLC 5520 /8540 by using the cli command	To verify whether the HA pair(ACTIVE:STANDBY) is up successfully by using the cli command	Passed	
WLJ810S_Reg_373	Configuring HA pair up- WLC 5520 /8540 by using the cli command	To verify whether the HA pair(ACTIVE:STANDBY) is up successfully by using the cli command	Passed	
WLJ810S_Reg_374	Configuring HA pair up- WLC 5520 /8540 by using the cli command	To verify whether the HA pair(ACTIVE:STANDBY) is up successfully by using the cli command	Passed	
WLJ810S_Reg_375	Configuring HA pair up- WLC 5520 /8540 by using the cli command	To verify whether the HA pair(ACTIVE:STANDBY) is up successfully by using the cli command	Passed	
WLJ810S_Reg_376	Configuring HA pair up- WLC 5520 /8540 by using the cli command	To verify whether the HA pair(ACTIVE:STANDBY) is up successfully by using the cli command	Passed	
WLJ810S_Reg_377	Configuring HA pair up- WLC 5520 /8540 by using the cli command	To verify whether the HA pair(ACTIVE:STANDBY) is up successfully by using the cli command	Passed	
WLJ810S_Reg_378	Configuring HA pair up- WLC 5520 /8540 by using the cli command	To verify whether the HA pair(ACTIVE:STANDBY) is up successfully by using the cli command	Passed	
WLJ810S_Reg_379	Configuring HA pair up- WLC 5520 /8540 by using the cli command	To verify whether the HA pair(ACTIVE:STANDBY) is up successfully by using the cli command	Passed	

WLJ810S_Reg_380	Configuring HA pair up- WLC 5520 /8540 by using the cli command	To verify whether the HA pair(ACTIVE:STANDBY) is up successfully by using the cli command	Failed	CSCvr31372
WLJ810S_Reg_381	Configuring HA pair up- WLC 5520 /8540 by using the cli command	To verify whether the HA pair(ACTIVE:STANDBY) is up successfully by using the cli command	Passed	

1815 RLAN Features

Logical ID	Title	Description	Status	Defect ID
WLJ810S_Reg_447	Checking the client connectivity to RLAN configured with Open security and macfiltering	To verify whether client is connecting to RLAN with open security and macfiltering	Passed	
WLJ810S_Reg_448	Enabling the 802.1x security and MAC filtering to RLAN	To create a RLAN with 802.1x security and MAC filtering connecting a windows client to the RLAN and check if the client gets connected to the RLAN port in the AP or not	Passed	
WLJ810S_Reg_449	Configuring RLAN with open security and connect three wired clients (windows,MAC and JOS)	To verify whether three wired clients gets connected with open security	Passed	
WLJ810S_Reg_450	Configuring RLAN with open+macfilter security and connect three wired clients (windows,MAC and JOS)	To verify whether three wired clients gets connected with open+macfilter security	Passed	
WLJ810S_Reg_451	Configuring RLAN with 802.1X security and connect three wired clients (windows,MAC and JOS)	To verify whether three wired clients gets connected with 802.1X security	Passed	

WLJ810S_Reg_452	Configuring RLAN with 802.1X+macfilter security and connect three wired clients (windows,MAC and JOS)	To verify whether three wired clients gets connected with 802.1X+macfilter security	Passed	
WLJ810S_Reg_453	Connecting the client to the RLAN configuring with 802.1x security and host mode as single Host	To verify whether a windows client connecting to the RLAN with 802.1x security and host mode as single Host	Passed	
WLJ810S_Reg_454	Configuring RLAN with 802.1x security and host mode as multi host and connect the client	To verify whether a client connecting to RLAN with 802.1x security and host mode as multi host	Passed	
WLJ810S_Reg_455	Configuring RLAN with 802.1x security and host mode as multi domain and connect the client	To verify whether a client connecting to RLAN with 802.1x security and host mode as multi domain	Passed	
WLJ810S_Reg_456	Checking the client connectivity with 802.1x and MAB mode enabled	To verify whether a client connecting to a RLAN with 802.1x security and enabling the MAB mode ,	Passed	
WLJ810S_Reg_457	Checking the client connectivity to a RLAN with 802.1x security and AVC profile is applied	To create a RLAN with 802.1x security and applying AVC profile, connecting a windows client to the RLAN and check if the AVC profile gets applied to the client connecting to it or not.	Passed	

WLJ810S_Reg_458	Checking the client connectivity with 802.1x security and host mode as single Host and violation mode as Replace	To verify whether client connecting to a RLAN with 802.1x security and host mode as single host along with violation mode as Replace	Passed	
WLJ810S_Reg_459	Checking the client connectivity with 802.1x security and host mode as single Host and violation mode as Shutdown	To verify whether client connecting to a RLAN with 802.1x security and host mode as single host along with violation mode as Shutdown	Passed	
WLJ810S_Reg_460	Checking the client connectivity with 802.1x security and host mode as single Host and violation mode as protect	To verify whether client connecting to a RLAN with 802.1x security and host mode as single host along with violation mode as Protect	Passed	
WLJ810S_Reg_461	Checking the client connectivity to RLAN configured with 802.1x security and preauthentication enabled	To verify whether client connecting to a RLAN with 802.1x security and preauthentication enabling	Passed	
WLJ810S_Reg_462	Rebooting the controller after connecting the client to RLAN	Checking whether RLAN configurations showing same or different after rebooting	Passed	
WLJ810S_Reg_463	Downgrading the controller after configuring RLAN and connect the client	Checking whether RLAN configurations showing same or different after downgrading controller and also verifying client connectivity	Passed	

WLJ810S_Reg_464	Upgrade the controller after configuring RLAN and connect the client	Checking whether RLAN configurations showing same or different after upgrading the controller and also verifying client connectivity	Passed	
WLJ810S_Reg_465	uploading and downloading the confit file and checking the RLAN configuration	To verify whether RLAN configurations showing same or different after uploading and downloading file to controller and also verifying client connectivity	Passed	
WLJ810S_Reg_466	Deploying RLAN from PI to controller	To verify whether user able to deploy RLAN from PI to controller	Passed	
WLJ8102S_Reg_324	Checking the client connectivity to RLAN configured with Open security and macfiltering	To verify whether client is connecting to RLAN with open security and macfiltering	Passed	
WLJ8102S_Reg_325	Enabling the 802.1x security and MAC filtering to RLAN	To create a RLAN with 802.1x security and MAC filtering connecting a windows client to the RLAN and check if the client gets connected to the RLAN port in the AP or not	Passed	
WLJ8102S_Reg_326	Configuring RLAN with open security and connect three wired clients (windows,MAC and JOS)	To verify whether three wired clients gets connected with open security	Passed	

WLJ8102S_Reg_327	Configuring RLAN with open+macfilter security and connect three wired clients (windows,MAC and JOS)	To verify whether three wired clients gets connected with open+macfilter security	Passed	
WLJ8102S_Reg_328	Configuring RLAN with 802.1X security and connect three wired clients (windows,MAC and JOS)	To verify whether three wired clients gets connected with 802.1X security	Passed	
WLJ8102S_Reg_329	Configuring RLAN with 802.1X+macfilter security and connect three wired clients (windows,MAC and JOS)	To verify whether three wired clients gets connected with 802.1X+macfilter security	Passed	
WLJ8102S_Reg_330	Connecting the client to the RLAN configuring with 802.1x security and host mode as single Host	To verify whether a windows client connecting to the RLAN with 802.1x security and host mode as single Host	Passed	
WLJ8102S_Reg_331	Configuring RLAN with 802.1x security and host mode as multi host and connect the client	To verify whether a client connecting to RLAN with 802.1x security and host mode as multi host	Passed	
WLJ8102S_Reg_332	Configuring RLAN with 802.1x security and host mode as multi domain and connect the client	To verify whether a client connecting to RLAN with 802.1x security and host mode as multi domain	Passed	
WLJ8102S_Reg_333	Checking the client connectivity with 802.1x and MAB mode enabled	To verify whether a client connecting to a RLAN with 802.1x security and enabling the MAB mode ,	Passed	

WLJ8102S_Reg_334	Checking the client connectivity to a RLAN with 802.1x security and AVC profile is applied	To create a RLAN with 802.1x security and applying AVC profile, connecting a windows client to the RLAN and check if the AVC profile gets applied to the client connecting to it or not.	Passed	
WLJ8102S_Reg_335	Checking the client connectivity with 802.1x security and host mode as single Host and violation mode as Replace	To verify whether client connecting to a RLAN with 802.1x security and host mode as single host along with violation mode as Replace	Passed	
WLJ8102S_Reg_336	Checking the client connectivity with 802.1x security and host mode as single Host and violation mode as Shutdown	To verify whether client connecting to a RLAN with 802.1x security and host mode as single host along with violation mode as Shutdown	Passed	
WLJ8102S_Reg_337	Checking the client connectivity with 802.1x security and host mode as single Host and violation mode as protect	To verify whether client connecting to a RLAN with 802.1x security and host mode as single host along with violation mode as Protect	Passed	
WLJ8102S_Reg_338	Checking the client connectivity to RLAN configured with 802.1x security and preauthentication enabled	To verify whether client connecting to a RLAN with 802.1x security and preauthentication enabling	Passed	
WLJ8102S_Reg_339	Rebooting the controller after connecting the client to RLAN	Checking whether RLAN configurations showing same or different after rebooting	Passed	

WLJ8102S_Reg_340	Downgrading the controller after configuring RLAN and connect the client	Checking whether RLAN configurations showing same or different after downgrading controller and also verifying client connectivity	Passed	
WLJ8102S_Reg_341	Upgrade the controller after configuring RLAN and connect the client	Checking whether RLAN configurations showing same or different after upgrading the controller and also verifying client connectivity	Passed	
WLJ8102S_Reg_342	uploading and downloading the config file and checking the RLAN configuration	To verify whether RLAN configurations showing same or different after uploading and downloading file to controller and also verifying client connectivity	Passed	
WLJ8102S_Reg_343	Deploying RLAN from PI to controller	To verify whether user able to deploy RLAN from PI to controller	Passed	

IPv4 DNS Filtering for BYOD

Logical ID	Title	Description	Status	Defect ID
WLJ810S_Reg_417	Connecting Android client with single said Byod network	Verify that Android client is getting connected or not with single SSID	Passed	
WLJ810S_Reg_418	Connecting ios client with single said Byod network	Verify that IOS client is getting connected or not with single SSID	Passed	

WLJ810S_Reg_419	Connecting windows client with single said Byod network	Verify that windows client is getting connected or not with single SSID	Passed	
WLJ810S_Reg_420	Connecting android client with dual said Byod network	Verify that android client is getting connected or not with dual SSID	Passed	
WLJ810S_Reg_421	Connecting ios client with dual said Byod network	Verify that IOS client is getting connected or not with dual SSID	Passed	
WLJ810S_Reg_422	Connecting windows client with dual said Byod network	Verify that windows client is getting connected or not with dual SSID	Passed	
WLJ810S_Reg_423	Debugging the BYoD client connection	Verify that user is able to take debug the Byod Client or not	Passed	
WLJ810S_Reg_424	Connecting JOS client with single said Byod network	Verify that JOS client is connected with single said byod network or not	Passed	
WLJ810S_Reg_425	Connecting JOS client with dual said Byod network	Verify that JOS client is connected with dual said byod network or not	Passed	
WLJ810S_Reg_426	Configuring the maximum URL ACL via GUI/CLI/PI	Verify that user is able to configure maximum url acl or not	Passed	

Limit clients per Radio

Logical ID	Title	Description	Status	Defect ID
WLJ810S_Reg_382	Configuring maximum Allowed Clients Per AP Radio with radio policy as 2.4 GHz and connecting client with different security policy.	To configure maximum allowed client Per AP radio with radio policy as 2.4GHz and connecting a client.	Passed	

WLJ810S_Reg_383	Configuring maximum Allowed Clients Per AP Radio with radio policy as 5 GHz and connecting client with different security policy.	To configure maximum allowed client Per AP radio with radio policy as 5 GHz and connecting a client.	Passed	
WLJ810S_Reg_384	Configuring maximum Allowed Clients Per AP Radio with radio policy as 2.4 GHz and connecting client to different AP's.	To connect client to different AP's configuring maximum allowed client per AP radio and check if the configured client alone gets authenticated.	Passed	
WLJ810S_Reg_385	Configuring maximum Allowed Clients Per AP Radio with radio policy as 5 GHz and connecting client to different AP's.	To connect client to different AP's configuring maximum allowed client per AP radio and check if the configured client alone gets authenticated.	Passed	
WLJ810S_Reg_386	Configuring maximum allowed client Per AP radio with radio policy as 2.4 GHz with central switching WLAN	To configure maximum allowed client Per AP radio as 2.4 GHZ with central switching and connecting a clients to it.	Passed	
WLJ810S_Reg_387	Configuring maximum allowed client Per AP radio with radio policy as 2.4 GHz with local switching WLAN	To configure maximum allowed client Per AP radio as 2.4 GHZ with Local switching and connecting a clients to it.	Passed	
WLJ810S_Reg_388	Configuring maximum allowed client Per AP radio with radio policy as 2.4 GHz with local switching and local authentication	To configure maximum allowed client Per AP radio as 2.4 GHZ with local switching and local authentication and connecting a clients to it.	Passed	

WLJ810S_Reg_389	Configuring maximum allowed client Per AP radio with radio policy as 5 GHz with central switching WLAN	To configure maximum allowed client Per AP radio as 5 GHZ with central switching and connecting a clients to it.	Passed	
WLJ810S_Reg_390	Configuring maximum allowed client Per AP radio as 5 GHz with local switching WLAN	To configure maximum allowed client Per AP radio as 5 GHZ with Local switching and connecting a clients to it.	Passed	
WLJ810S_Reg_391	Configuring maximum allowed client Per AP radio as 5 GHz with local switching and local authentication	To configure maximum allowed client Per AP radio as 5 GHZ with local switching and local authentication and connecting a clients to it.	Passed	
WLJ810S_Reg_392	Configuring maximum allowed client Per AP radio as 2.4 GHz and try connecting 5 GHZ client.	To configuring maximum allowed client Per AP radio as 2.4 GHz and try connecting 5 GHZ client . check if only 2.4 GHz clients gets connected and 5 GHz client does not get connected.	Passed	
WLJ810S_Reg_393	Configuring maximum allowed client Per AP radio as 5 GHz and try connecting 2.4 GHZ client.	To configuring maximum allowed client Per AP radio as 5 GHz and try connecting 5 GHZ client . check if only 2.4 GHz clients gets connected and 2.4 GHz client does not get connected.	Passed	

WLJ810S_Reg_394	Deleting one already existing client in 2.4 GHz when max limit reached and try connecting new client .	To delete one existing client in 2.4 GHz when the client limit is reached to maximum and try connecting a new client and check if the clients gets connected to it .	Passed	
WLJ810S_Reg_395	Deleting one already existing client in 5 GHz when max limit reached and try connecting new client .	To delete one existing client in 5 GHz when the client limit is reached to maximum and try connecting a new client and check if the clients gets connected to it .	Passed	
WLJ810S_Reg_396	Trying AP failover priority when clients connected to a AP .	To try AP failover priority when clients connected and the HA WLC has the same WLAN with radio as 2.4 GHz .The WLAN is configured with maximum allowed client Per AP	Passed	
WLJ810S_Reg_397	Intra roaming of clients configuring maximum allowed client Per AP radio	To try intra roaming of clients on the same WLC in a WLAN configured with maximum allowed client Per AP radio and check if the client roam from one AP to another AP.	Passed	
WLJ810S_Reg_398	Inter roaming of clients configuring maximum allowed client Per AP radio	To try inter roaming of clients configuring maximum allowed client per AP radio and check if only the configured limit of clients alone gets connected.	Passed	

DNS Pre-auth ACLs Wave 2 Aps

Logical ID	Title	Description	Status	Defect ID
WLJ810S_Reg_63	Configure WebAuth ACL through 1800/2800/3800/1542 AP level with permit action and connect the clients	To verify whether Windows client getting connected through WebAuth ACL at AP level	Passed	
WLJ810S_Reg_64	Configure WebAuth ACL through 1800/2800/3800 AP level mapping with deny action and connect the clients	To verify whether Windows client getting connected and denied through WebAuth ACL at AP level	Passed	
WLJ810S_Reg_65	Configure WebAuth ACL through Policies on flexconnect group with permit action and connect the clients	To verify whether Windows client getting connected through WebAuth ACL at Policies	Passed	
WLJ810S_Reg_66	Configure WebAuth ACL through Policies on flexconnect group with deny actions and connect the clients	To verify whether Windows client getting connected and denied through WebAuth ACL at Policies	Passed	
WLJ810S_Reg_67	Configure WebAuth ACL through Policies on AP level with permit action and connect the clients	To verify whether Windows client getting connected and permitted through WebAuth ACL using Policies	Passed	
WLJ810S_Reg_68	Configure WebAuth ACL through Policies on and AP level with deny action and connect the clients	To verify whether Windows client getting connected and denied through WebAuth ACL using Policies	Passed	

WLJ810S_Reg_69	Configure URL ACL on the controller map with local policy permiting action and connect the clients	To verify whether policy URL overridies WLAN URL ACL	Passed	
WLJ810S_Reg_70	Configure URL ACL on the controller map with local policy denying action and connect the clients	To verify whether policy URL overridies WLAN URL ACL	Passed	
WLJ810S_Reg_71	Configuring RLAN with URL ACL rule on the controller and connect the clients	To verify whether clients gets connected and redirected to URL	Passed	
WLJ810S_Reg_72	Configuring RLAN with URL ACL rule on the controller and connect the clients	To verify whether clients gets connected and redirected to URL	Passed	
WLJ810S_Reg_73	Configure WebAuth ACL through AAA Vlan-ACL mapping and connect the clients	To verify whether Windows client getting connected and redirected through WebAuth ACL at AAA-ACL mapping	Passed	
WLJ8102S_Reg_47	Configure WebAuth ACL through 1800/2800/3800/1542 AP level with permit action and connect the clients	To verify whether Windows client getting connected through WebAuth ACL at AP level	Passed	
WLJ8102S_Reg_48	Configure WebAuth ACL through 1800/2800/3800 AP level mapping with deny action and connect the clients	To verify whether Windows client getting connected and denied through WebAuth ACL at AP level	Passed	

WLJ8102S_Reg_49	Configure WebAuth ACL through Policies on flexconnect group with permit action and connect the clients	To verify whether Windows client getting connected through WebAuth ACL at Policies	Passed	
WLJ8102S_Reg_50	Configure WebAuth ACL through Policies on flexconnect group with deny actions and connect the clients	To verify whether Windows client getting connected and denied through WebAuth ACL at Policies	Passed	
WLJ8102S_Reg_51	Configure WebAuth ACL through Policies on AP level with permit action and connect the clients	To verify whether Windows client getting connected and permitted through WebAuth ACL using Policies	Passed	
WLJ8102S_Reg_52	Configure WebAuth ACL through Policies on and AP level with deny action and connect the clients	To verify whether Windows client getting connected and denied through WebAuth ACL using Policies	Passed	
WLJ8102S_Reg_53	Configure URL ACL on the controller map with local policy permiting action and connect the clients	To verify whether policy URL overridies WLAN URL ACL	Passed	
WLJ8102S_Reg_54	Configure URL ACL on the controller map with local policy denying action and connect the clients	To verify whether policy URL overridies WLAN URL ACL	Passed	
WLJ8102S_Reg_55	Configuring RLAN with URL ACL rule on the controller and connect the clients	To verify whether clients gets connected and redirected to URL	Passed	

WLJ8102S_Reg_56	Configuring RLAN with URL ACL rule on the controller and connect the clients	To verify whether clients gets connected and redirected to URL	Passed	
WLJ8102S_Reg_57	Configure WebAuth ACL through AAA Vlan-ACL mapping and connect the clients	To verify whether Windows client getting connected and redirected through WebAuth ACL at AAA-ACL mapping	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