Test Results Summary for Cisco Wireless LAN Controller AireOS 8.0, IOS XE 3.6/3.7, for Japan (Release Version AireOS 8.0.100.0, 8.0.110.0/IOS XE 03.06.00.E, 03.07.00E)

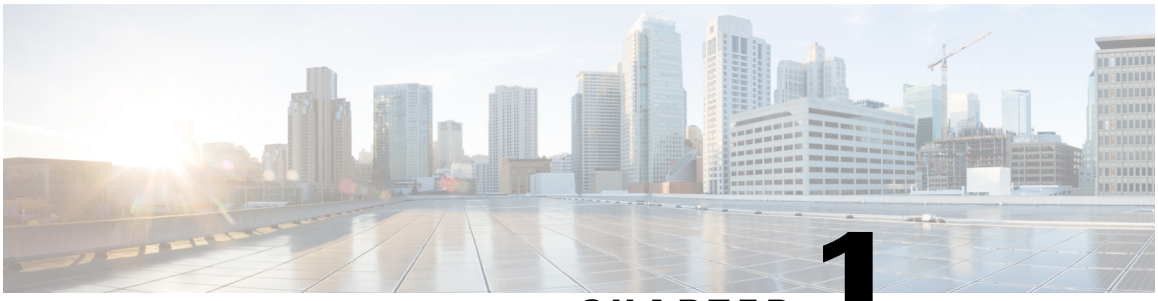
First Published: October 01, 2014

Last Modified: February 05, 2015

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

Text Part Number:

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 8.0
- Customer found defects in selected wireless products
- 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 5508
- Cisco Wireless LAN Controller 2500
- Cisco Wireless LAN Controller 5760
- Cisco Wireless LAN Flex Controller 7500
- Cisco Wireless LAN Flex Controller 8500
- Cisco Catalyst 3850 Switch
- WiSM2 Controller
- Virtual Controller

- Access Point 3500
- Access Point 1042
- Access Point 1142
- Access Point 1262
- Access Point 3600
- Access Point 3700
- Access Point 2600
- Access Point 1530
- Access Point 1550
- Access Point 1600
- Access Point 2700
- Access Point 702
- Cisco OEAP 602
- Cisco Prime Network Control System
- Cisco Prime Infrastructure
- ISE Virtual Appliance
- Cisco Secure ACS
- Cisco Mobility Service Engine (MSE)
- Cisco AnyConnect VPN Client

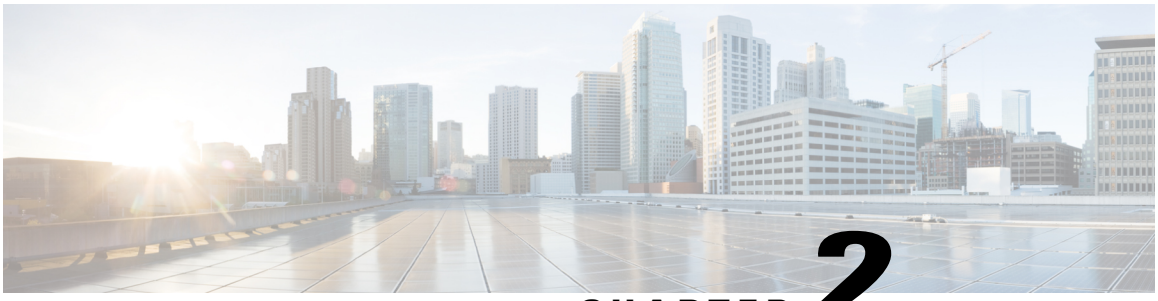
Acronyms

Acronym	Description
AAA	Authentication Authorization and Accounting
ACL	Access Control List
ACS	Access Control Server
AKM	Authentication Key Management
AP	Access Point
AVC	Application Visibility and Control.
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

Acronym	Description
CCX	Cisco Compatible Extensions
CDP	Cisco Discovery Protocol
CKIP	Cisco Key Integrity Protocol
CMX	Connected Mobile Experience
CVBF	Cisco Vector Beam Forming
CWA	Central Web Authentication
DCA	Dynamic Channel Assignment
DMZ	Demilitarized Zone
DNS	Domain Name System
DTIM	Delivery Traffic Indication Map
DSCP	Differentiated Services Code Point
DTLS	Datagram Transport Layer Security
EAP	Extensible Authentication Protocol
EULA	End User Licence Agreement
FLA	Flex Local Authentication
FLS	Flex Local Switching
FT	Fast Transition
FTP	File Transfer Protocol
FW	Firm Ware
HA	High Availability
H-REAP	Hybrid Remote Edge Access Point
IOS	Internetwork Operating System
ISE	Identity Service Engine
LAG	Link Aggregation
LEAP	Lightweight Extensible Authentication Protocol
LSS	Location Specific Services
LWAPP	Lightweight Access Point Protocol
MCS	Modulation Coding Scheme
MFP	Management Frame Protection
mDNS	multicast Domain Name System
MIC	Message Integrity Check

Acronym	Description
MSE	Mobility Service Engine
MTU	Maximum Transmission Unit
NAC	Network Admission Control
NAT	Network Address Translation
NBAR	Network Based Application Recognition
NCS	Network Control System
NGWC	Next Generation Wiring closet
NMSP	Network Mobility Services Protocol
OEAP	Office Extended Access Point
PEAP	Protected Extensible Authentication Protocol
PEM	Policy Enforcement Module
PI	Prime Infrastructure
PMF	Protected Management Frame
POI	Point of Interest
PPPoE	Point-to-Point Protocol over Ethernet
PSK	Pre-shared Key
RADIUS	Remote Authentication Dial-In User Service
RP	Redundancy Port
RRM	Radio Resource Management
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

Acronym	Description
vWLC	Virtual Wireless LAN Controller
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WGB	Workgroup Bridge
wIPS	Wireless Intrusion Prevention System
WiSM	Wireless Service Module
WLAN	Wireless LAN
WLC	Wireless LAN Controller
WPA	Wi-Fi Protected Access

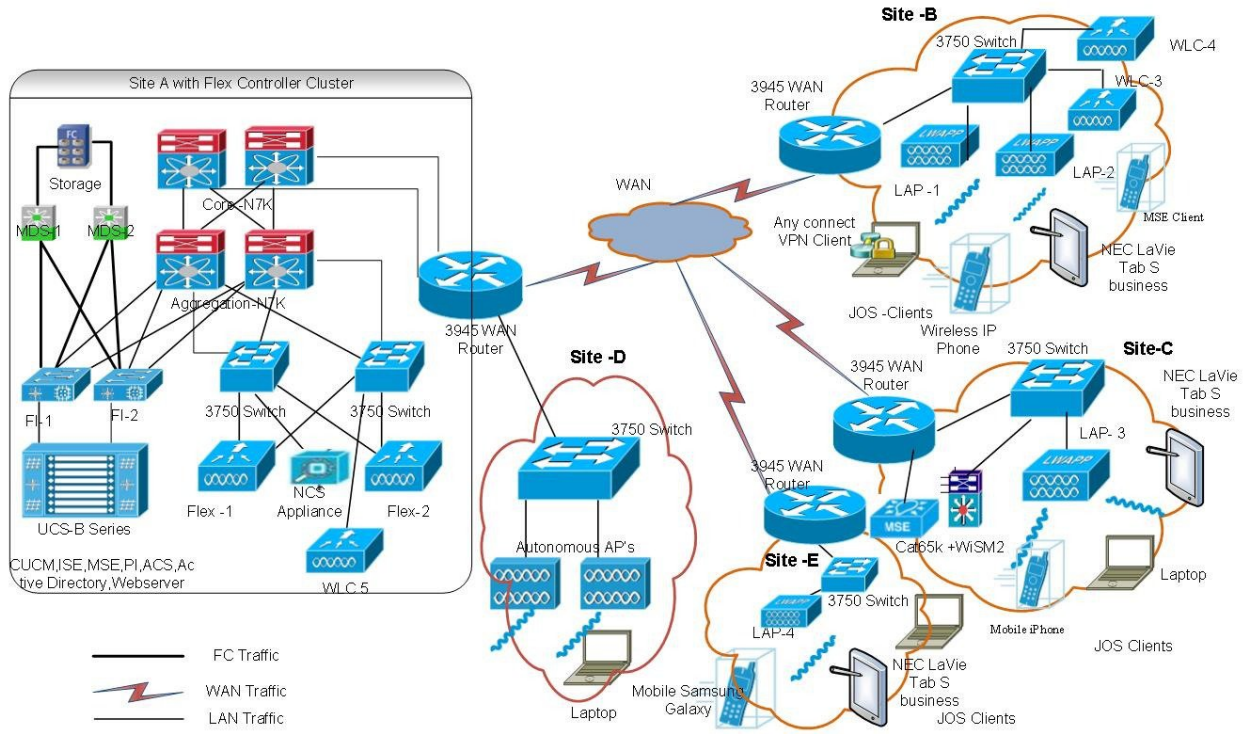


CHAPTER 2

Test Topology and Environment Matrix

Test Topology

Figure 1: Topology In Use



Environment Matrix

Category	Component	Version
Controller	Wireless LAN controller 5508	8.0.100.0 /8.0.110.0
	Flex Controller 7500	8.0.100.0 /8.0.110.0
	Wireless LAN Controller 2500	8.0.100.0 /8.0.110.0
	Wireless LAN Controller 8500	8.0.100.0 /8.0.110.0
	WiSM2	8.0.100.0 /8.0.110.0
	Virtual controller	8.0.100.0 /8.0.110.0
	NGWC 5760	03.06.00.E /3.7.0E (ED)

Category	Component	Version
Application	PI (Physical, VM)	2.1.0.0.87
	ISE(VM)	1.2.0.899
	Secure ACS (VM)	5.5.0.46
	MSE (Physical, VM)	8.0.100.0
Call control	Cisco Unified Communications Manager	10.5.1-10000-7/10.5.1.1000-1(JP)
Access Point	Cisco AP 3500	15.3
	Cisco AP 3600	15.3
	Cisco AP 3700	15.3
	Cisco AP 2600	15.3
	Cisco AP 2700	15.3
	Cisco AP 1600	15.3
	Cisco AP 1262	15.3
	Cisco OEAP 602	15.3
	Cisco AP 702I	15.3
	Cisco AP 702W	15.3
	Cisco AP 1550	15.3
	Cisco AP 1530	15.3
Switch	Cisco 3750V2 switch	15.0(2)SE2
	Cisco Cat 6509-E	15.1(1)SY1
	Cisco Cat 3850	03.06.00.E /3.7.0E (ED)
Chipset	5300, 6300 AGN	15.13.0.1
	Airport Extreme	7.7

Category	Component	Version
Client	Operating System(JOS)	Windows 7 Enterprise
		Windows 8 Enterprise
		Windows 8.1 Enterprise
		Windows XP Professional
	Apple Mac Book Pro (JP Locale)	Mac OS 10.9.4
	iPhone 4(JP Locale)	iOS 7.1.2(11D257)
	iPhone 5(JP Locale)	iOS 7.1.2(11D257)
	Samsung Galaxy S-II and S4	Android 4.3
	Wireless IP Phone 7921G	1.4.5.3
	Wireless IP Phone 7925G	1.4.5.3
	Wireless IP Phones 7926G	1.4.5.3
	NEC LaVie Tab S business	Android 4.4
	Cisco AnyConnect VPN Client	Windows 7 Enterprise/3.1.05178
		Apple Mac OS 10.9.4/3.1.05178
		Windows 8.1/4.0.00061
		Samsung Galaxy S-II/ 3.0.09431
Active Directory	AD	Windows 2008R2Enterprise
Browsers	IE	8.9,10
	Opera	11.5
	Mozilla Firefox	30.0
	Safari	7.0.4
	Chrome	37,40

What's New ?

WLC AireOS

- DHCP Relay Option
- Show Running Config
- Flex: Video Stream Support
- Flex : Upgrade Time Reduction

- 8500 Support As MC
- HA Enhancements
- HTTPS Support for Web-Auth
- NBAR Engine
- Rate Limiting Per Client
- AAA Override for AVC Profile Name
- DCA RF Profiles
- Cleanair Express - Skyros
- FlexConnect on Mesh
- Clean Air Support for Xmas Ale Module
- 11ac Module - CCX Lite
- OEAP Enhancements
- L2TPv3 Over UDP
- 3700 Autonomous

MSE

- CMX Visitor Connect
- Real Path
- Zone Based Analytics
- CMX Napp Store

Open Caveats

Defect ID	Defect Title
CSCun59052	Page error occurs after applying the config in Vlan mapping page
CSCun78876	Unable to select multiple date option for the Zone analysis
CSCup77825	Unable to change MSE Notification Parameter Queue limit in VM machine
CSCup82047	Syslog trap level for AP is inconsistent in controller
CSCup87391	Attached Clients count isn't removed from AP radio in WLC CLI
CSCuo56629	MSE HA Failover and failback working inconsistently
CSCur00347	Deleted VLAN is showing in Autonomous AP CLI.
CSCur08583	AP CLI:show command in non-privileged mode
CSCur12267	Creating WLAN profile and SSID names as empty gets accepted in CLI

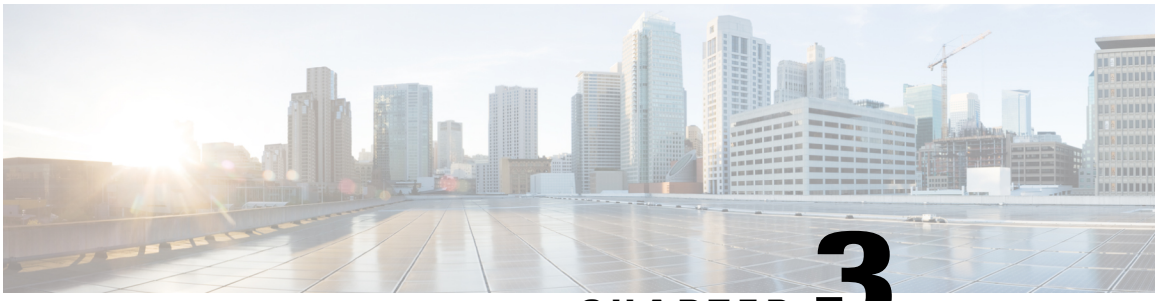
Defect ID	Defect Title
CSCun55413	Incorrect Username appears after configuring HTTP account in NGWC
CSCun96815	OEAP ACL's & Network lists gets deleted after upload/download the config
CSCus60566	Unable to block the Hangouts (Gtalk) messenger in AVC
CSCus68028	Gmail works in Android Client when Gmail application WLC is blocked in AVC

Resolved Caveats

Defect ID	Defect Title
CSCup93585	CAS event messages is not triggered correctly for multiple facility
CSCup21225	NMSP status is not consistently active
CSCum12763	Secondary MSE is not active when primary is shutdown
CSCup59088	CLI description is missing for module3G in command "config ap ?"
CSCun89585	Context Aware notifications are not updated properly
CSCuo37342	Device Port Summary dashlet shows wrong info for controllers
CSCuq94587	EAP profile name display as Junk character if created in UTF-8 character
CSCuq89168	LED Flash state description is missing in OLH page for All APs details
CSCuq82767	System Configuration of AP in AP GUI
CSCuq93760	Custom Webauth and Webauth ACL config in AAP
CSCup86941	GUI: Policy type for "Static WEP" clients is showing as N/A
CSCum84944	Some options missing in WLAN>Advanced>Flexconnect in OLH page

Limitations

Defect ID	Defect Title
CSCun75576	Accessibility issue using analytics tab
CSCun76218	PI Maps is not synchronized with MSE while copying the exiting Maps
CSCun78279	Zone based analytics shows wrong display for multiple zone selection
CSCun78862	Deleted real path is displayed in most popular path analysis
CSCup56865	Unable to login PI CLI after changing hostname/IP upon PI re-setup
CSCuo53852	Export the path outputs



CHAPTER 3

New Features - Test Summary

WLC AireOS

DHCP Relay Options

Logical ID	Title	Description	Status	Defects
WLJ80S_DHCP_01	Configuration of DHCP Relay options - Link Select option in WLC 5500	To check if DHCP relay option 82 with link/subnet select suboption 5 can be enabled via CLI in WLC 5500	Passed	
WLJ80S_DHCP_02	Configuration of DHCP Relay options - VPN id or VRF selection option in WLC 5500	To check if DHCP relay option 82 with VPN id /VRF select suboption 151 and 152 is enabled via CLI in WLC 5500	Passed	
WLJ80S_DHCP_03	DHCP relay options (link/ VPN select)is enabled only when the DHCP proxy enabled in WLC 5500	To check if DHCP relay options (link/VPN select) is enabled only when the DHCP proxy is enabled in WLC 5500	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_DHCP_04	VPN id or the VRF can be configured inside VPN select configuration but not both together from CLI, UI in WLC 5500	To check if VPN id or the VRF can be configured inside VPN select configuration but not both together from CLI, UI in WLC 5500	Passed	
WLJ80S_DHCP_05	Relay src interface name should be a valid interface present on the WLC 5500	To check if Relay src interface name configured should be a valid interface present on the WLC 5500	Passed	
WLJ80S_DHCP_06	Link select and the VPN select can be enabled together per interface in WLC 5500	To check if both link select and the VPN select can be enabled together per interface in WLC 5500	Passed	
WLJ80S_DHCP_07	DHCP discover and request packets are padded with the option 82 with suboption 5 when link select configured within interface for WLC 5500	To check if DHCP discover and request packets are padded with the option 82 and suboption 5 based on Interface configuration for WLC 5500	Passed	
WLJ80S_DHCP_08	DHCP discover and request packets are padded with the option 82 with suboption 151 and 152 when VPN select is configured with the VPN id per interface in WLC 5500	To check if DHCP discover and request packets are padded with the option 82 with suboption 151 and 152 when VPN select is configured with the VPN id per interface in WLC 5500	Passed	
WLJ80S_DHCP_09	DHCP discover and request packets are padded with the option 82 with suboption 151 and 152 when VRF select is configured with the VRF per interface in WLC 5500	To check if DHCP discover and request packets are padded with the option 82 with suboption 151 and 152 when VRF select is configured with the VRF name per interface in WLC 5500	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_DHCP_10	DHCP relay option with HA in WLC 5500	To check if DHCP relay option with HA. Ensure that the relay options configurations are synced to the standby WLC in WLC 5500	Passed	
WLJ80S_DHCP_11	DHCP relay options configuration upload and download in WLC 5500	To check if config upload and download is successfully maintaining the DHCP relay options config in WLC 5500	Passed	
WLJ80S_DHCP_12	AAA override with relay options in WLC 5500	To check if the DHCP relay option 82 with both link and VPN select suboption works with AAA override enabled in WLC 5500	Passed	
WLJ80S_DHCP_13	Debug messages in WLC 5500	To check if there are adequate debug messages for the DHCP relay options in WLC 5500	Passed	
WLJ80S_DHCP_14	Flex central switching in WLC 5500	To check if DHCP relay options for both link and VPN select works fine with Flex central switching in WLC 5500	Passed	
WLJ80S_DHCP_15	L2/L3 Roaming with DHCP relay options in WLC 5500	To check if the L2 intra controller works with DHCP relay option 82 enabled in WLC 5500	Passed	
WLJ80S_DHCP_16	DHCP OFFER and ACK packets are unpadded with option 82 in WLC 5500	To check if the DHCP OFFER and ACK packets have the option 82 unpadded in WLC 5500	Passed	
WLJ80S_DHCP_17	DHCP OFFER and ACK packets are checked by WLC for option 82 with suboption 152 and if present the Critical error has to be logged in WLC 5500	To check if the DHCP OFFER and ACK packets are checked by WLC for option 82 with suboption 152 in WLC 5500 and if present the Critical error has to be logged in syslog server and SNMP trap has to be sent to NCS. Client should not be denied IP address at any point	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_DHCP_18	DHCP relay option 82 with link select or VPN / VRF select is configured along with invalid or non reachable DHCP server in WLC 5500	To Check the behavior when the DHCP relay option 82 with link select or VPN / VRF select is configured along with invalid or non reachable DHCP server in WLC 5500Ensure that all the DHCP discover /Req packets that are retried from the client and relayed by WLC carries the option 82 with either suboption 5 / 151and152	Passed	
WLJ80S_DHCP_19	DHCP relay option 82 with link select or VPN / VRF select is configured along with invalid or non reachable primary DHCP server and it falls back to reachable secondary DHCP server in WLC 5500	To Check the behavior when the DHCP relay option 82 with link select and VPN / VRF select is configured along with invalid or non reachable primary DHCP server and it falls back to reachable secondary DHCP server in WLC 5500Ensure that all the DHCP discover/req packets that are retried from the client and relayed by WLC to the primary and secondary DHCP server carries the option 82 with either suboption 5 / 151and152	Passed	
WLJ80S_DHCP_20	Configuration of DHCP Relay options - Link Select option in WLC 7500	To check if DHCP relay option 82 with link/subnet select suboption 5 can be enabled via CLI in WLC 7500	Passed	
WLJ80S_DHCP_21	Configuration of DHCP Relay options - VPN id or VRF selection option in WLC 7500	To check if DHCP relay option 82 with VPN id /VRF select suboption 151 and 152 is enabled via CLI in WLC 7500	Passed	
WLJ80S_DHCP_22	DHCP relay options (link/VPN select)is enabled only when the DHCP proxy enabled in WLC 7500	To check if DHCP relay options (link/VPN select) is enabled only when the DHCP proxy is enabled in WLC 7500	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_DHCP_23	VPN id or the VRF can be configured inside VPN select configuration but not both together from CLI, UI in WLC 7500	To check if VPN id or the VRF can be configured inside VPN select configuration but not both together from CLI, UI in WLC 7500	Passed	
WLJ80S_DHCP_24	Relay src interface name should be a valid interface present on the WLC 7500	To check if Relay src interface name configured should be a valid interface present on the WLC 7500	Passed	
WLJ80S_DHCP_25	Link select and the VPN select can be enabled together per interface in WLC 7500	To check if both link select and the VPN select can be enabled together per interface in WLC 7500	Passed	
WLJ80S_DHCP_26	DHCP discover and request packets are padded with the option 82 with suboption 5 when link select configured within interface for WLC 7500	To check if DHCP discover and request packets are padded with the option 82 and suboption 5 based on Interface configuration for WLC 7500	Passed	
WLJ80S_DHCP_27	DHCP discover and request packets are padded with the option 82 with suboption 151 and 152 when VPN select is configured with the VPN id per interface in WLC 7500	To check if DHCP discover and request packets are padded with the option 82 with suboption 151 and 152 when VPN select is configured with the VPN id per interface in WLC 7500	Passed	
WLJ80S_DHCP_28	DHCP discover and request packets are padded with the option 82 with suboption 151 and 152 when VRF select is configured with the VRF per interface in WLC 7500	To check if DHCP discover and request packets are padded with the option 82 with suboption 151 and 152 when VRF select is configured with the VRF name per interface in WLC 7500	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_DHCP_29	DHCP relay option with HA in WLC 7500	To check if DHCP relay option with HA. Ensure that the relay options configurations are synced to the standby WLC in WLC 7500	Passed	
WLJ80S_DHCP_30	DHCP relay options configuration upload and download in WLC 7500	To check if config upload and download is successfully maintaining the DHCP relay options config in WLC 7500	Passed	
WLJ80S_DHCP_31	AAA override with relay options in WLC 7500	To check if the DHCP relay option 82 with both link and VPN select suboption works with AAA override enabled in WLC 7500	Passed	
WLJ80S_DHCP_32	Debug messages in WLC 7500	To check if there are adequate debug messages for the DHCP relay options in WLC 7500	Passed	
WLJ80S_DHCP_33	Flex central switching in WLC 7500	To check if DHCP relay options for both link and VPN select works fine with Flex central switching in WLC 7500	Passed	
WLJ80S_DHCP_34	L2/L3 Roaming with DHCP relay options in WLC 7500	To check if the L2 intra controller works with DHCP relay option 82 enabled in WLC 7500	Passed	
WLJ80S_DHCP_35	DHCP OFFER and ACK packets are unpadded with option 82 in WLC 7500	To check if the DHCP OFFER and ACK packets have the option 82 unpadded in WLC 7500	Passed	
WLJ80S_DHCP_36	DHCP OFFER and ACK packets are checked by WLC for option 82 with suboption 152 and if present the Critical error has to be logged in WLC 7500	To check if the DHCP OFFER and ACK packets are checked by WLC for option 82 with suboption 152 in WLC 7500 and if present the Critical error has to be logged in syslog server and SNMP trap has to be sent to NCS. Client should not be denied IP address at any point	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_DHCP_37	DHCP relay option 82 with link select or VPN / VRF select is configured along with invalid or non reachable DHCP server in WLC 7500	To Check the behavior when the DHCP relay option 82 with link select or VPN / VRF select is configured along with invalid or non reachable DHCP server in WLC 7500Ensure that all the DHCP discover /Req packets that are retried from the client and relayed by WLC carries the option 82 with either suboption 5 / 151and152	Passed	
WLJ80S_DHCP_38	DHCP relay option 82 with link select or VPN / VRF select is configured along with invalid or non reachable primary DHCP server and it falls back to reachable secondary DHCP server in WLC 7500	To Check the behavior when the DHCP relay option 82 with link select and VPN / VRF select is configured along with invalid or non reachable primary DHCP server and it falls back to reachable secondary DHCP server in WLC 7500Ensure that all the DHCP discover/req packets that are retried from the client and relayed by WLC to the primary and secondary DHCP server carries the option 82 with either suboption 5 / 151and152	Passed	
WLJ80S_DHCP_39	Configuration of DHCP Relay options - Link Select option in WLC 8500	To check if DHCP relay option 82 with link/subnet select suboption 5 can be enabled via CLI in WLC 8500	Passed	
WLJ80S_DHCP_40	Configuration of DHCP Relay options - VPN id or VRF selection option in WLC 8500	To check if DHCP relay option 82 with VPN id /VRF select suboption 151 and 152 is enabled via CLI in WLC 8500	Passed	
WLJ80S_DHCP_41	DHCP relay options (link/VPN select)is enabled only when the DHCP proxy enabled in WLC 8500	To check if DHCP relay options (link/VPN select) is enabled only when the DHCP proxy is enabled in WLC 8500	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_DHCP_42	VPN id or the VRF can be configured inside VPN select configuration but not both together from CLI, UI in WLC 8500	To check if VPN id or the VRF can be configured inside VPN select configuration but not both together from CLI, UI in WLC 8500	Passed	
WLJ80S_DHCP_43	Relay src interface name should be a valid interface present on the WLC 8500	To check if Relay src interface name configured should be a valid interface present on the WLC 8500	Passed	
WLJ80S_DHCP_44	Link select and the VPN select can be enabled together per interface in WLC 8500	To check if both link select and the VPN select can be enabled together per interface in WLC 8500	Passed	
WLJ80S_DHCP_45	DHCP discover and request packets are padded with the option 82 with suboption 5 when link select configured within interface for WLC 8500	To check if DHCP discover and request packets are padded with the option 82 and suboption 5 based on Interface configuration for WLC 8500	Passed	
WLJ80S_DHCP_46	DHCP discover and request packets are padded with the option 82 with suboption 151 and 152 when VPN select is configured with the VPN id per interface in WLC 8500	To check if DHCP discover and request packets are padded with the option 82 with suboption 151 and 152 when VPN select is configured with the VPN id per interface in WLC 8500	Passed	
WLJ80S_DHCP_47	DHCP discover and request packets are padded with the option 82 with suboption 151 and 152 when VRF select is configured with the VRF per interface in WLC 8500	To check if DHCP discover and request packets are padded with the option 82 with suboption 151 and 152 when VRF select is configured with the VRF name per interface in WLC 8500	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_DHCP_48	DHCP relay option with HA in WLC 8500	To check if DHCP relay option with HA. Ensure that the relay options configurations are synced to the standby WLC in WLC 8500	Passed	
WLJ80S_DHCP_49	DHCP relay options configuration upload and download in WLC 8500	To check if config upload and download is successfully maintaining the DHCP relay options config in WLC 8500	Passed	
WLJ80S_DHCP_50	AAA override with relay options in WLC 8500	To check if the DHCP relay option 82 with both link and VPN select suboption works with AAA override enabled in WLC 8500	Passed	
WLJ80S_DHCP_51	Debug messages in WLC 8500	To check if there are adequate debug messages for the DHCP relay options in WLC 8500	Passed	
WLJ80S_DHCP_52	Flex central switching in WLC 8500	To check if DHCP relay options for both link and VPN select works fine with Flex central switching in WLC 8500	Passed	
WLJ80S_DHCP_53	L2/L3 Roaming with DHCP relay options in WLC 8500	To check if the L2 intra controller works with DHCP relay option 82 enabled in WLC 8500	Passed	
WLJ80S_DHCP_54	DHCP OFFER and ACK packets are unpadded with option 82 in WLC 8500	To check if the DHCP OFFER and ACK packets have the option 82 unpadded in WLC 8500	Passed	
WLJ80S_DHCP_55	DHCP OFFER and ACK packets are checked by WLC for option 82 with suboption 152 and if present the Critical error has to be logged in WLC 8500	To check if the DHCP OFFER and ACK packets are checked by WLC for option 82 with suboption 152 in WLC 8500 and if present the Critical error has to be logged in syslog server and SNMP trap has to be sent to NCS. Client should not be denied IP address at any point	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_DHCP_56	DHCP relay option 82 with link select or VPN / VRF select is configured along with invalid or non reachable DHCP server in WLC 8500	To Check the behavior when the DHCP relay option 82 with link select or VPN / VRF select is configured along with invalid or non reachable DHCP server in WLC 8500Ensure that all the DHCP discover /Req packets that are retried from the client and relayed by WLC carries the option 82 with either suboption 5 / 151and152	Passed	
WLJ80S_DHCP_57	DHCP relay option 82 with link select or VPN / VRF select is configured along with invalid or non reachable primary DHCP server and it falls back to reachable secondary DHCP server in WLC 8500	To Check the behavior when the DHCP relay option 82 with link select and VPN / VRF select is configured along with invalid or non reachable primary DHCP server and it falls back to reachable secondary DHCP server in WLC 8500Ensure that all the DHCP discover/req packets that are retried from the client and relayed by WLC to the primary and secondary DHCP server carries the option 82 with either suboption 5 / 151and152	Passed	

Show Running Config

Logical ID	Title	Description	Status	Defects
WLJ80S_RC_01	Show run-config _commands for WLC 2500	To check the format of show run-config commands for WLC 2500	Passed	
WLJ80S_RC_02	Show run-config _startup-commands for WLC 2500	To check that the command is working without error from WLC 2500	Passed	
WLJ80S_RC_03	Show run-config _commands for WLC 5500	To check the format of show run-config commands for WLC 5500	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_RC_04	Show run-config _startup-commands for WLC 5500	To check that the command is working without error from WLC 5500	Passed	
WLJ80S_RC_05	Show run-config_ commands for WLC 7500	To check the format of show run-config commands for WLC 7500	Passed	
WLJ80S_RC_06	Show run-config _startup-commands for WLC 7500	To check that the command is working without error from WLC 7500	Passed	
WLJ80S_RC_07	Show run-config _commands for WLC 8500	To check the format of show run-config commands for WLC 8500	Passed	
WLJ80S_RC_08	Show run-config _startup-commands for WLC 8500	To check that the command is working without error from WLC 8500	Passed	

Flexconnect video streaming

Logical ID	Title	Description	Status	Defects
WLJ80S_FLSV_01	Enabling/disabling Video Stream for FLS WLAN	To verify whether Video Stream functionality is enabled/disabled for flexconnect local-switching WLAN	Passed	
WLJ80S_FLSV_02	Debug and show commands for FLS Video Streaming	To verify the debug and show commands supported for flexconnect local-switching Video Stream	Passed	
WLJ80S_FLSV_03	MC2UC traffic to local-switching client	To verify that the local-switching client subscribed to Video Streaming receives MC2UC traffic	Passed	
WLJ80S_FLSV_04	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	

Logical ID	Title	Description	Status	Defects
WLJ80S_FLSV_05	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	
WLJ80S_FLSV_06	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	
WLJ80S_FLSV_07	Client disassociates when receiving MC2UC traffic	To verify whether AP stops sending traffic when client disassociates	Passed	
WLJ80S_FLSV_08	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	
WLJ80S_FLSV_09	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	
WLJ80S_FLSV_10	Central Switching and Local switching client with MC2UC enabled	To verify whether AP has no entry for the central switching client with MC2UC enabled	Passed	
WLJ80S_FLSV_11	Local switching clients with MC2UC enabled and disabled	To verify whether the local switching clients with MC2UC enabled receives MC2UC traffic and LS client with Media stream disabled receives normal multicast	Passed	
WLJ80S_FLSV_12	Flex AP in standalone mode retains the Video Stream config	To verify whether Flexconnect AP in standalone retains its Video Stream config	Passed	
WLJ80S_FLSV_13	Flex AP in standalone mode retains the Video Stream config after reboot	To verify whether Flexconnect AP in standalone retains its Video Stream config after reboot	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_FLSV_14	Flex AP from standalone to connected mode can load the updated config	To verify whether the flexconnect AP can load the updated config when switch from standalone to connected mode	Passed	
WLJ80S_FLSV_15	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	
WLJ80S_FLSV_16	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	
WLJ80S_FLSV_17	Flex AP reboot in connected mode when Flex LS client receiving MC2UC traffic	To verify whether client re-associates and receives MC2UC traffic when flex AP is rebooted in connected mode.	Passed	
WLJ80S_FLSV_18	Flex AP reboot in SA mode when Flex LS client receiving MC2UC traffic	To verify whether client re-associates and receives MC2UC traffic when flex AP is rebooted in standalone mode	Passed	
WLJ80S_FLSV_19	AP admin mode disabled when LS client receiving MC2UC traffic	To verify whether the client entries are removed when AP admin mode is disabled	Passed	
WLJ80S_FLSV_20	AP radios shut disabled when LS client receiving MC2UC traffic	To verify whether the client entries are removed when AP radios are shut	Passed	
WLJ80S_FLSV_21	Software Upgrade to the latest image with video stream config at AP	To verify whether upgrading the WLC with latest supported image retains the Video Stream configuration for local-switching WLAN	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_FLSV_22	Software downgrade to the unsupported image with video stream config at AP	To verify whether upgrading the WLC with unsupported image clears the Video Stream configuration for local-switching WLAN	Passed	
WLJ80S_FLSV_23	Video stream config sync for LS WLAN in HA setup	To verify whether the Video Streaming config for LS WLAN has been synced between the Active and Standby in HA setup	Passed	
WLJ80S_FLSV_24	AP SSO with MC2UC enabled for LS WLAN	To verify whether flex AP retains the Video Streaming config post switchover	Passed	
WLJ80S_FLSV_25	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	

Flexconnect Upgrade Time Reduction

Logical ID	Title	Description	Status	Defects
WLJ80S_FC_01	AP mode change from local to flexconnect using WLC CLI	To verify whether changing the AP mode from local to flexconnect using WLC CLI is successful without rebooting the AP	Passed	
WLJ80S_FC_02	AP mode change from local to flexconnect using WLC GUI	To verify whether changing the AP mode from local to flexconnect using WLC GUI is successful without rebooting the AP	Passed	
WLJ80S_FC_03	Basic flex configuration after AP mode change	To verify whether basic flex configurations have been applied to AP after mode change	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_FC_04	Client authentication with AP after mode change to flexconnect_Central Switching	To verify whether client has been successfully authenticated after AP mode has been changed to flexconnect with central switching WLAN	Passed	
WLJ80S_FC_05	Client authentication with AP after mode change to flexconnect_Local Switching ,Central auth	To verify whether client has been successfully authenticated after AP mode has been changed to flexconnect with local switching, central auth WLAN	Passed	
WLJ80S_FC_06	Client association with AP in standalone mode and FT	To verify whether client has been associated successfully to AP in standalone mode and fault tolerance	Passed	
WLJ80S_FC_07	AP reboot in connected/standalone mode, for converted flex AP	To verify whether converted flex AP retains all config when AP is rebooted in connected/standalone mode	Passed	
WLJ80S_FC_08	Client association with AP reboot in connected/standalone mode	To verify the client association with AP reboot in connected/standalone mode, for AP converted to flex	Passed	
WLJ80S_FC_09	Software upgrade/downgrade	To verify whether the AP retains its flex configuration after software upgrade/downgrade	Passed	
WLJ80S_FC_10	HA support for mode change	To verify the AP mode change in HA setup, whether AP mode is synched to standby	Passed	
WLJ80S_FC_11	AP mode change with auto conversion on WLC	To verify the AP mode with auto conversion on WLC	Passed	
WLJ80S_FC_12	Intra-Controller roam, local switching WLAN	To verify the roaming within the controller is successful	Passed	
WLJ80S_FC_13	Inter-Controller roam, central switching WLAN	To verify the inter-controller roaming is successful	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_FC_14	AP mode change for few Aps	To verify whether change of AP mode for few Aps are successful	Passed	
WLJ80S_FC_15	Mode change from local > flex > local	To verify whether changing the mode from local > flex > local for few times are working properly	Passed	
WLJ80S_FC_16	Mode change to flexconnect then to submode wIPS	To verify the mode change to flexconnect and then to WIPS	Passed	

8500 As Mobility Controller

Logical ID	Title	Description	Status	Defects
WLJ80S_MC_01	Enabling New Mobility from CLI & GUI of 8500	To check if "New Mobility" could be successfully enabled from the CLI and GUI	Passed	
WLJ80S_MC_02	Configuring Mobility group members from GUI and CLI of 8500	To check if the mobility group members are successfully added from GUI and CLI	Passed	
WLJ80S_MC_03	Enable/Disable Mobility Multicast mode from CLI & GUI of 8500	To check if the multicast mode can be enabled/disabled from CLI and GUI and check for the changes to have taken effect	Passed	
WLJ80S_MC_04	Create and delete Switch Peer group from GUI & CLI in 8500	To create / delete a Switch peer group from the CLI and GUI and check the changes to have taken effect.	Passed	
WLJ80S_MC_05	Add switch peer group member from the GUI & CLI in 8500	To add a switch peer group member to a created switch peer group from CLI and GUI and check if the configurations are successful.	Passed	
WLJ80S_MC_06	Client Intra MA roaming when 8500 is the MC(open L2 security on the WLAN)	To verify if intra Switch / MA roaming occurs smoothly when 8500 is acting as MC having a WLAN with open authentication	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_MC_07	Client Intra MA roaming when 8500 is the MC (802.1x on the WLAN)	To verify if intra Switch / MA roaming occurs smoothly when 8500 is acting as MC with a WLAN having 802.1x security type.	Passed	
WLJ80S_MC_08	Client Intra MA roaming when 8500 is the MC (WEP/WPA2 on the WLAN)	To verify if intra Switch / MA roaming occurs smoothly when 8500 is acting as MC with a WLAN having WEP or WPA2 security type.	Passed	
WLJ80S_MC_09	Intra switch Peer group roaming when 8500 is acting as the MC for the particular peer group (WLAN having 'none' as L2 security)	To verify if intra switch peer group roaming occurs smoothly when 8500 is acting as MC with a WLAN having open security type.	Passed	
WLJ80S_MC_10	Intra switch Peer group roaming when 8500 is acting as the MC for the particular peer group (WLAN having 'WEP' as L2 security)	To verify if intra switch peer group roaming occurs smoothly when 8500 is acting as MC with a WLAN having "WEP" security type.	Passed	
WLJ80S_MC_11	Intra switch Peer group roaming when 8500 is acting as the MC for the particular peer group (WLAN having '802.1x' as L2 security)	To verify if intra switch peer group roaming occurs smoothly when 8500 is acting as MC with a WLAN having "802.1x" security type.	Passed	
WLJ80S_MC_12	Intra switch Peer group roaming when 8500 is acting as the MC for the particular peer group (WLAN having 'WPA2-PSK' as L2 security)	To verify if intra switch peer group roaming occurs smoothly when 8500 is acting as MC with a WLAN having "WPA-2-PSK" security type.	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_MC_13	Intra switch Peer group dual roaming roaming when 8500 is acting as the MC for the particular peer group (WLAN having 'WPA2-PSK' as L2 security)	To verify if intra switch peer group dual roaming occurs smoothly when 8500 is acting as MC with a WLAN having "WPA-2-PSK" security type.	Passed	
WLJ80S_MC_14	Intra switch Peer group dual roaming roaming when 8500 is acting as the MC for the particular peer group (WLAN having 'none' as L2 security)	To verify if intra switch peer group dual roaming occurs smoothly when 8500 is acting as MC with a WLAN having "none" as the security type.	Passed	
WLJ80S_MC_15	Intra switch Peer group dual roaming roaming when 8500 is acting as the MC for the particular peer group (WLAN having 'WEP' as L2 security)	To verify if intra switch peer group dual roaming occurs smoothly when 8500 is acting as MC with a WLAN having "WEP" as the security type.	Passed	
WLJ80S_MC_16	Intra switch Peer group dual roaming roaming when 8500 is acting as the MC for the particular peer group (WLAN having '802.1x' as L2 security)	To verify if intra switch peer group dual roaming occurs smoothly when 8500 is acting as MC with a WLAN having "802.1x" as the security type.	Passed	
WLJ80S_MC_17	Intra SPG roaming with sticky anchor when 8500 controller is acting as MC on a WLAN with open authentication	To verify if the PoP stays the same and PoA moves to new MA after roaming with sticky anchor (default behavior) on a WLAN with 'none' as L2 security	Passed	
WLJ80S_MC_18	Intra SPG roaming with sticky anchor when 8500 controller is acting as MC on a WLAN with 'WEP' as L2 security type.	To verify if the PoP stays the same and PoA moves to new MA after roaming with sticky anchor (default behavior) on a WLAN with 'WEP' as L2 security	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_MC_19	Intra SPG roaming with sticky anchor when 8500 controller is acting as MC on a WLAN with '802.1x' as L2 security type.	To verify if the PoP stays the same and PoA moves to new MA after roaming with sticky anchor (default behavior) on a WLAN with '802.1x' as L2 security	Passed	
WLJ80S_MC_20	Intra SPG roaming with sticky anchor when 8500 controller is acting as MC on a WLAN with 'WPA2-PSK' as L2 security type.	To verify if the PoP stays the same and PoA moves to new MA after roaming with sticky anchor (default behavior) on a WLAN with 'WPA-PSK' as L2 security	Passed	
WLJ80S_MC_21	Intra SPG roaming without sticky anchor when 8500 controller is acting as MC on a WLAN with open authentication	To verify if the PoP and PoA moves to new MA after roaming without sticky anchor on a WLAN with 'none' as L2 security	Passed	
WLJ80S_MC_22	Intra SPG roaming without sticky anchor when 8500 controller is acting as MC on a WLAN with WEP security	To verify if the PoP and PoA moves to new MA after roaming without sticky anchor on a WLAN with 'Static WEP' as L2 security	Passed	
WLJ80S_MC_23	Intra SPG roaming without sticky anchor when 8500 controller is acting as MC on a WLAN with 802.1x security	To verify if the PoP and PoA moves to new MA after roaming without sticky anchor on a WLAN with '802.1x' as L2 security	Passed	
WLJ80S_MC_24	Intra SPG roaming without sticky anchor when 8500 controller is acting as MC on a WLAN with WPA2-PSK security	To verify if the PoP and PoA moves to new MA after roaming without sticky anchor on a WLAN with 'WPA2-PSK' as L2 security	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_MC_25	Inter SPG L2 roaming when 8500 is the MC with a WLAN having open authentication	To verify if roaming between APs belonging to MA's in different SPGs works fine when 8500 is acting as MC with a WLAN having "open" l2 security.	Passed	
WLJ80S_MC_26	Inter SPG L2 roaming when 8500 is the MC with a WLAN having WEP	To verify if roaming between APs belonging to MA's in different SPGs works fine when 8500 is acting as MC with a WLAN having "WEP" l2 security.	Passed	
WLJ80S_MC_27	Inter SPG L2 roaming when 8500 is the MC with a WLAN having "802.1x" at L2 security	To verify if roaming between APs belonging to MA's in different SPGs works fine when 8500 is acting as MC with a WLAN having "802.1x" l2 security.	Passed	
WLJ80S_MC_28	Inter SPG L2 roaming when 8500 is the MC with a WLAN having "WPA2-PSK" at L2 security	To verify if roaming between APs belonging to MA's in different SPGs works fine when 8500 is acting as MC with a WLAN having "WPA2-PSK" l2 security.	Passed	
WLJ80S_MC_29	PoP, PoA and traffic flow in inter SPG roaming with sticky roaming when 8500 is acting as MC with a WLAN having "none" as L2 security	To verify if the PoP stays the same in inter-SPG roaming with sticky roaming, PoA changes and traffic flow takes the path New MA->MC->old MA on other SPG	Passed	
WLJ80S_MC_30	PoP, PoA and traffic flow in inter SPG roaming with sticky roaming when 8500 is acting as MC with a WLAN having "WEP" as L2 security	To verify if the PoP stays the same in inter-SPG roaming with sticky roaming, PoA changes and traffic flow takes the path New MA->MC->old MA on other SPG	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_MC_31	PoP, PoA and traffic flow in inter SPG roaming with sticky roaming when 8500 is acting as MC with a WLAN having "WEP" as L2 security	To verify if the PoP stays the same in inter-SPG roaming with sticky roaming, PoA changes and traffic flow takes the path New MA->MC->old MA on other SPG	Passed	
WLJ80S_MC_32	PoP, PoA and traffic flow in inter SPG roaming with sticky roaming when 8500 is acting as MC with a WLAN having "WEP" as L2 security	To verify if the PoP stays the same in inter-SPG roaming with sticky roaming, PoA changes and traffic flow takes the path New MA->MC->old MA on other SPG	Passed	
WLJ80S_MC_33	PoP, PoA and traffic flow in inter SPG roaming without sticky roaming when 8500 is acting as MC with a WLAN having "none" as L2 security	To verify if the PoP and PoA moves to the new MA in inter-SPG roaming without sticky roaming and traffic flow takes the path New MA-> datacenter	Passed	
WLJ80S_MC_34	PoP, PoA and traffic flow in inter SPG roaming without sticky roaming when 8500 is acting as MC with a WLAN having "WEP" as L2 security	To verify if the PoP and PoA moves to the new MA in inter-SPG roaming without sticky roaming and traffic flow takes the path New MA-> datacenter	Passed	
WLJ80S_MC_35	PoP, PoA and traffic flow in inter SPG roaming without sticky roaming when 8500 is acting as MC with a WLAN having "WPA2-PSK" as L2 security	To verify if the PoP and PoA moves to the new MA in inter-SPG roaming without sticky roaming and traffic flow takes the path New MA-> datacenter	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_MC_36	PoP, PoA and traffic flow in inter SPG roaming without sticky roaming when 8500 is acting as MC with a WLAN having "802.1X" as L2 security	To verify if the PoP and PoA moves to the new MA in inter-SPG roaming without sticky roaming and traffic flow takes the path New MA-> datacenter	Passed	
WLJ80S_MC_37	Inter SPG roaming within 3 separate SPGs with 8500 ac MC having a WLAN with 'open' authentication	To verify if the roaming of client from an AP associated to MA of a SPG ->SPG1->SPG2 works fine when 8500 is acting as MC with a WLAN having "none" as L2 security type.	Passed	
WLJ80S_MC_38	Inter SPG roaming within 3 separate SPGs with 8500 ac MC having a WLAN with 'WEP' as L2 security method.	To verify if the roaming of client from an AP associated to MA of a SPG ->SPG1->SPG2 works fine when 8500 is acting as MC with a WLAN having "WEP" as L2 security type.	Passed	
WLJ80S_MC_39	Inter SPG roaming within 3 separate SPGs with 8500 ac MC having a WLAN with '802.1x' authentication	To verify if the roaming of client from an AP associated to MA of a SPG ->SPG1->SPG2 works fine when 8500 is acting as MC with a WLAN having "802.1x" as L2 security type.	Passed	
WLJ80S_MC_40	Inter SPG roaming within 3 separate SPGs with 8500 ac MC having a WLAN with 'WPA2-PSK' authentication	To verify if the roaming of client from an AP associated to MA of a SPG ->SPG1->SPG2 works fine when 8500 is acting as MC with a WLAN having "WPA2-PASK" as L2 security type.	Passed	
WLJ80S_MC_41	Inter SPG L3 roaming when 8500 is the MC with a WLAN having open authentication	To verify if roaming between APs belonging to MA's in different SPGs on different subnet works fine when 8500 is acting as MC with a WLAN having "open" l2 security.	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_MC_42	Inter SPG L3 roaming when 8500 is the MC with a WLAN having 'WEP' as L2 security	To verify if roaming between APs belonging to MA's in different SPGs on different subnet works fine when 8500 is acting as MC with a WLAN having "WEP" l2 security.	Passed	
WLJ80S_MC_43	Inter SPG L3 roaming when 8500 is the MC with a WLAN having '802.1x' as L2 security	To verify if roaming between APs belonging to MA's in different SPGs on different subnet works fine when 8500 is acting as MC with a WLAN having "802.1x" l2 security.	Passed	
WLJ80S_MC_44	Inter SPG L3 roaming when 8500 is the MC with a WLAN having 'WPA2-PSK' as L2 security	To verify if roaming between APs belonging to MA's in different SPGs on different subnet works fine when 8500 is acting as MC with a WLAN having "WPA2-PSK" l2 security.	Passed	
WLJ80S_MC_45	Roaming between two 8500 Mobility Controllers in the same subnet when the WLAN has 'none' as L2 security	To verify if the L2 roam between two MC's works fine when the WLAN has 'none' as L2 security.	Passed	
WLJ80S_MC_46	Roaming between two 8500 Mobility Controllers in the same subnet when the WLAN has '802.1x' as L2 security	To verify if the L2 roam between two MC's works fine when the WLAN has '802.1x' as L2 security.	Passed	
WLJ80S_MC_47	Roaming between two 8500 Mobility Controllers in the same subnet when the WLAN has 'WEP' as L2 security	To verify if the L2 roam between two MC's works fine when the WLAN has 'WEP' as L2 security.	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_MC_48	Roaming between two 8500 Mobility Controllers in the same subnet when the WLAN has 'WPA2-PSK' as L2 security	To verify if the L2 roam between two MC's works fine when the WLAN has 'WPA2-PSK' as L2 security.	Passed	
WLJ80S_MC_49	Roaming between two 8500 Mobility Controllers in different subnet when the WLAN has 'none' as L2 security	To verify if the L2 roam between two MC's in different subnet works fine when the WLAN has 'none' as L2 security.	Passed	
WLJ80S_MC_50	Roaming between two 8500 Mobility Controllers in different subnet when the WLAN has 'WEP' as L2 security	To verify if the L2 roam between two MC's in different subnet works fine when the WLAN has 'WEP' as L2 security.	Passed	
WLJ80S_MC_51	Roaming between two 8500 Mobility Controllers in different subnet when the WLAN has '802.1x' as L2 security	To verify if the L2 roam between two MC's in different subnet works fine when the WLAN has '802.1x' as L2 security.	Passed	
WLJ80S_MC_52	Roaming between two 8500 Mobility Controllers in different subnet when the WLAN has 'WPA2-PSK' as L2 security	To verify if the L2 roam between two MC's in different subnet works fine when the WLAN has 'WPA2-PSK' as L2 security.	Passed	
WLJ80S_MC_53	Addition of NAT functionality between two 8500 MCs	To verify if the mobility tunnel gets established between two 8500 MCs when one of the Controllers Private IP address is NAT'ed	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_MC_54	L2 roaming of Static ip 5300 agn Wireless clients within the subdomain of the 8500 MC	To verify if the L2 roaming of Static IP 5300 agn wireless client within the subdomain works fine .	Passed	
WLJ80S_MC_55	L2 roaming of Static IP MAC Wireless clients within the subdomain of the 8500 MC	To verify if the L2 roaming of Static IP MAC wireless client within the subdomain works fine .	Passed	
WLJ80S_MC_56	L3 roaming of Static IP 5300 agn Wireless clients within the subdomain of the 8500 MC	To verify if the L3 roaming of Static IP 5300 agn wireless client within the Subdomain works fine .	Passed	
WLJ80S_MC_57	L3 roaming of Static IP MAC Wireless clients within the subdomain of the 8500 MC	To verify if the L3 roaming of Static IP MAC wireless client within the Subdomain works fine .	Passed	
WLJ80S_MC_58	Initial association of Wired Guest client to the MA when 8500 is acting as MC.	To verify if the client gets anchored to the corresponding MC-anchor when connected in Wireless to the MA where the associated MC-is acting foreign controller.	Passed	
WLJ80S_MC_59	Initial association of Wireless Guest client to the MA when 8500 is acting as MC.	To verify if the client gets anchored to the corresponding MC-anchor when wired to the MA where the associated MC-is acting a foreign controller.	Passed	
WLJ80S_MC_60	Roaming of guest clients within the 8500 MCs	To verify if the L2 and L3 roaming of Guest clients happens successfully between two MC's.	Passed	

HA Enhancements

HA Pair up by connecting RP back-to-back

Internal DHCP support

Logical ID	Title	Description	Status	Defects
WLJ80S_HA_Enh_01	Internal DHCP config in HA pair through CLI	To verify whether Internal DHCP has been configured when HA is enabled through CLI	Passed	
WLJ80S_HA_Enh_02	Internal DHCP config in HA pair through GUI	To verify whether Internal DHCP has been configured when HA is enabled through GUI	Passed	
WLJ80S_HA_Enh_03	Internal DHCP config sync in Standby-Hot	To verify whether the Internal DHCP config through Active CLI/GUI is synced to the Standby-Hot WLC in a HA pair	Passed	
WLJ80S_HA_Enh_04	Internal DHCP config during Incremental sync	To verify the Internal DHCP config during Incremental sync	Passed	
WLJ80S_HA_Enh_05	Internal DHCP config during Bulk sync	To verify the Internal DHCP config during Bulk sync	Passed	
WLJ80S_HA_Enh_06	Internal DHCP config in new Active	To verify the Internal DHCP config in new Active WLC.	Passed	
WLJ80S_HA_Enh_07	Client obtaining IP through Internal DHCP config	To verify whether the client obtaining IP address from the Internal DHCP config	Passed	
WLJ80S_HA_Enh_08	Client IP address after a switchover	To verify whether the client obtaining IP address from the Internal DHCP after a switchover	Passed	
WLJ80S_HA_Enh_09	Upload/download of Internal DHCP config	To verify the Internal DHCP config upload/download from Active and peer	Passed	
WLJ80S_HA_Enh_10	Upgrade/downgrade of HA pair with Internal DHCP config with 8.0 image	To verify the Internal DHCP config is persistent across upgrade/downgrade of HA pair	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_HA_Enh_11	Downgrade WLC pair to 7.6/7.5 with Internal DHCP config	To verify Internal DHCP config is not allowed when downgraded to 7.6/7.5	Passed	

Sleeping Client Sync

Logical ID	Title	Description	Status	Defects
WLJ80S_HA_Enh_12	Sleeping Client sync in Standby- Internal web auth	To verify the sleeping client entry sync to the standby WLC- Internal web authentication	Passed	
WLJ80S_HA_Enh_13	Sleeping Client sync in Standby- customized web auth	To verify the sleeping client entry sync to the standby WLC- Customized web authentication	Passed	
WLJ80S_HA_Enh_14	Sleeping Client sync in Standby- external web auth	To verify the sleeping client entry sync to the standby WLC- External web authentication	Passed	
WLJ80S_HA_Enh_15	Sleeping Client sync in Standby- Dot1x + web auth	To verify the sleeping client entry sync to the standby WLC- Dot1x + web auth	Passed	
WLJ80S_HA_Enh_16	Sleeping Client entry bulk sync- internal and customized web authentication	To verify the sleeping client entry in bulk sync to the standby- internal and customized web authentication	Passed	
WLJ80S_HA_Enh_17	Sleeping Client entry bulk sync- external and dot1x+web auth.	To verify the sleeping client entry in bulk sync to the standby- external and dot1x + web-auth	Passed	
WLJ80S_HA_Enh_18	Sleeping client entry sync in Flexconnect local switching	To verify the sleeping client entry sync in standby enabling Flexconnect local switching	Passed	
WLJ80S_HA_Enh_19	Sleeping client status after switchover- internal web auth	To verify the sleeping client status after switchover with Internal/customized web auth	Passed	
WLJ80S_HA_Enh_20	Sleeping client status after switchover- external web auth	To verify the sleeping client status after switchover with external/dot1x+ web auth	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_HA_Enh_21	Sleeping client entry deletion sync	To verify the sleeping client entry deletion sync between Active and Standby	Passed	
WLJ80S_HA_Enh_22	Sleeping Client in new Active after sleep timer expires	To verify the Sleeping client status after sleep timer expires in new Active after switchover	Passed	

SSO support for OEAP

Logical ID	Title	Description	Status	Defects
WLJ80S_HA_Enh_23	OEAP sync between Active and Standby WLC upon joining	To verify whether OEAP is synced between Active and Standby WLC	Passed	
WLJ80S_HA_Enh_24	OEAP sync between Active and Standby WLC when removed	To verify whether the OEAP is removed from Active and Standby WLC when powered down the AP	Passed	
WLJ80S_HA_Enh_25	OEAP after switchover	To verify whether OEAP switchovers in a seamless manner to the new Active upon switchover	Passed	
WLJ80S_HA_Enh_26	Sync of Client connected to corporate SSID	To verify whether the clients connected through corporate SSID are synced to Standby	Passed	
WLJ80S_HA_Enh_27	Sync of Client connected to personal SSID	To verify whether the clients connected through personal SSID are synced to Standby	Passed	
WLJ80S_HA_Enh_28	Client connected to corporate SSID after switchover	To verify the client connected to Corporate SSID after switchover	Passed	
WLJ80S_HA_Enh_29	Client connected to personal SSID after switchover	To verify the client connected to Personal SSID after switchover	Passed	
WLJ80S_HA_Enh_30	OEAP join statistics and Counters sync	To verify the Join statistics and counters sync of OEAP	Passed	
WLJ80S_HA_Enh_31	Client SSO with OEAP	To verify the client SSO with OEAP	Passed	
WLJ80S_HA_Enh_32	Voice client connected to OEAP after switchover	To verify the voice client status connected to OEAP after switchover	Passed	

CAC statistics sync

Logical ID	Title	Description	Status	Defects
WLJ80S_HA_Enh_33	Voice CAC summary in new Active WLC	To verify the voice CAC summary in new Active WLC after switchover	Passed	
WLJ80S_HA_Enh_34	Voice CAC stats in new Active WLC	To verify the voice CAC stats in new Active WLC after switchover	Passed	
WLJ80S_HA_Enh_35	Voice stats in AP stats after switchover	To verify the voice stats in AP stats after switchover	Passed	

HA Pair up by connecting RP via a L2 switch

Internal DHCP support

Logical ID	Title	Description	Status	Defects
WLJ80S_HA_Enh_36	Internal DHCP config in HA pair through CLI	To verify whether Internal DHCP has been configured when HA is enabled through CLI	Passed	
WLJ80S_HA_Enh_37	Internal DHCP config in HA pair through GUI	To verify whether Internal DHCP has been configured when HA is enabled through GUI	Passed	
WLJ80S_HA_Enh_38	Internal DHCP config sync in Standby-Hot	To verify whether the Internal DHCP config through Active CLI/GUI is synced to the Standby-Hot WLC in a HA pair	Passed	
WLJ80S_HA_Enh_39	Internal DHCP config during Incremental sync	To verify the Internal DHCP config during Incremental sync	Passed	
WLJ80S_HA_Enh_40	Internal DHCP config during Bulk sync	To verify the Internal DHCP config during Bulk sync	Passed	
WLJ80S_HA_Enh_41	Internal DHCP config in new Active	To verify the Internal DHCP config in new Active WLC.	Passed	
WLJ80S_HA_Enh_42	Client obtaining IP through Internal DHCP config	To verify whether the client obtaining IP address from the Internal DHCP config	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_HA_Enh_43	Client IP address after a switchover	To verify whether the client obtaining IP address from the Internal DHCP after a switchover	Passed	
WLJ80S_HA_Enh_44	Upload/download of Internal DHCP config	To verify the Internal DHCP config upload/download from Active and peer	Passed	
WLJ80S_HA_Enh_45	Upgrade/downgrade of HA pair with Internal DHCP config with 8.0 image	To verify the Internal DHCP config is persistent across upgrade/downgrade of HA pair	Passed	
WLJ80S_HA_Enh_46	Downgrade WLC pair to 7.6/7.5 with Internal DHCP config	To verify Internal DHCP config is removed when downgraded to 7.6/7.5	Passed	

Sleeping Client Sync

Logical ID	Title	Description	Status	Defects
WLJ80S_HA_Enh_47	Sleeping Client sync in Standby- Internal web auth	To verify the sleeping client entry sync to the standby WLC- Internal web authentication	Passed	
WLJ80S_HA_Enh_48	Sleeping Client sync in Standby- customized web auth	To verify the sleeping client entry sync to the standby WLC- Customized web authentication	Passed	
WLJ80S_HA_Enh_49	Sleeping Client sync in Standby- external web auth	To verify the sleeping client entry sync to the standby WLC- External web authentication	Passed	
WLJ80S_HA_Enh_50	Sleeping Client sync in Standby- Dot1x + web auth	To verify the sleeping client entry sync to the standby WLC- Dot1x + web auth	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_HA_Enh_51	Sleeping Client entry bulk sync-internal and customized web authentication	To verify the sleeping client entry in bulk sync to the standby- internal and customized web authentication	Passed	
WLJ80S_HA_Enh_52	Sleeping Client entry bulk sync-external and dot1x+web auth.	To verify the sleeping client entry in bulk sync to the standby- external and dot1x + web-auth	Passed	
WLJ80S_HA_Enh_53	Sleeping client entry sync in Flexconnect local switching	To verify the sleeping client entry sync in standby enabling Flexconnect local switching	Passed	
WLJ80S_HA_Enh_54	Sleeping client status after switchover- internal web auth	To verify the sleeping client status after switchover with Internal/customized web auth	Passed	
WLJ80S_HA_Enh_55	Sleeping client status after switchover- external web auth	To verify the sleeping client status after switchover with external/dot1x+ web auth	Passed	
WLJ80S_HA_Enh_56	Sleeping client entry deletion sync	To verify the sleeping client entry deletion sync between Active and Standby	Passed	
WLJ80S_HA_Enh_57	Sleeping Client in new Active after sleep timer expires	To verify the Sleeping client status after sleep timer expires in new Active after switchover	Passed	

SSO support for OEAP

Logical ID	Title	Description	Status	Defects
WLJ80S_HA_Enh_58	OEAP sync between Active and Standby WLC upon joining	To verify whether OEAP is synced between Active and Standby WLC	Passed	
WLJ80S_HA_Enh_59	OEAP sync between Active and Standby WLC when removed	To verify whether the OEAP is removed from Active and Standby WLC when powered down the AP	Passed	
WLJ80S_HA_Enh_60	OEAP after switchover	To verify whether OEAP switchovers in a seamless manner to the new Active upon switchover	Passed	
WLJ80S_HA_Enh_61	Sync of Client connected to corporate SSID	To verify whether the clients connected through corporate SSID are synced to Standby	Passed	
WLJ80S_HA_Enh_62	Sync of Client connected to personal SSID	To verify whether the clients connected through personal SSID are synced to Standby	Passed	
WLJ80S_HA_Enh_63	Client connected to corporate SSID after switchover	To verify the client connected to Corporate SSID after switchover	Passed	
WLJ80S_HA_Enh_64	Client connected to personal SSID after switchover	To verify the client connected to Personal SSID after switchover	Passed	
WLJ80S_HA_Enh_65	OEAP join statistics and Counters sync	To verify the Join statistics and counters sync of OEAP	Passed	
WLJ80S_HA_Enh_66	Client SSO with OEAP	To verify the client SSO with OEAP	Passed	
WLJ80S_HA_Enh_67	Voice client connected to OEAP after switchover	To verify the voice client status connected to OEAP after switchover	Passed	

CAC statistics sync

Logical ID	Title	Description	Status	Defects
WLJ80S_HA_Enh_68	Voice CAC summary in new Active WLC	To verify the voice CAC summary in new Active WLC after switchover	Passed	
WLJ80S_HA_Enh_69	Voice CAC stats in new Active WLC	To verify the voice CAC stats in new Active WLC after switchover	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_HA_Enh_70	Voice stats in AP stats after switchover	To verify the voice stats in AP stats after switchover	Passed	

HTTPS Support

HTTPS Support for Web-Auth

Logical ID	Title	Description	Status	Defects
WLJ80S_HTTPS_01	Associating Win 7 client to web-auth security and checking the redirection of HTTPS URL in 7500 WLC.	To check whether HTTPS URL gets redirected or not to web-auth login page when client gets connected and browses the internet access.	Passed	
WLJ80S_HTTPS_02	Associating two clients(Win 7 and Macbook) to web-auth security and checking the redirection of HTTPS URL in both clients in 7500 WLC.	To check whether HTTPS URL gets redirected or not to web-auth login page when clients gets connected and browses the internet and also checking the Ping function works or not between them.	Passed	
WLJ80S_HTTPS_03	Associating two clients(Win 7 and Win 8) to web-auth security and checking the redirection of HTTPS URL in both clients in 7500 WLC.	To check whether HTTPS URL gets redirected or not to web-auth login page when clients gets connected and browses the internet and also checking the Ping function works or not between them.	Passed	
WLJ80S_HTTPS_04	Associating Samsung S4 to web-auth security and checking the redirection of HTTPS URL in its browser in 7500 WLC.	To check whether HTTPS URL gets redirected or not to web-auth login page when client gets connected and browses the internet access.	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_HTTPS_05	Associating Apple Iphone to web-auth security and checking the redirection of HTTPS URL in its browser in 7500 WLC.	To check whether HTTPS URL gets redirected or not to web-auth login page when client gets connected and browses the internet access.	Passed	
WLJ80S_HTTPS_06	Associating Win 7 client to web-auth security and checking the redirection of HTTPS URL in 5500 WLC.	To check whether HTTPS URL gets redirected or not to web-auth login page when client gets connected and browses the internet access.	Passed	
WLJ80S_HTTPS_07	Associating two clients(Win 7 and Macbook) to web-auth security and checking the redirection of HTTPS URL in both clients in 5500 WLC.	To check whether HTTPS URL gets redirected or not to web-auth login page when clients gets connected and browses the internet and also checking the Ping function works or not between them.	Passed	
WLJ80S_HTTPS_08	Associating two clients(Win 7 and Win 8) to web-auth security and checking the redirection of HTTPS URL in both clients in 5500 WLC.	To check whether HTTPS URL gets redirected or not to web-auth login page when clients gets connected and browses the internet and also checking the Ping function works or not between them.	Passed	
WLJ80S_HTTPS_09	Associating Samsung S4 to web-auth security and checking the redirection of HTTPS URL in its browser in 5500 WLC.	To check whether HTTPS URL gets redirected or not to web-auth login page when client gets connected and browses the internet access.	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_HTTPS_10	Associating Apple Iphone to web-auth security and checking the redirection of HTTPS URL in its browser in 5500 WLC.	To check whether HTTPS URL gets redirected or not to web-auth login page when client gets connected and browses the internet access.	Passed	
WLJ80S_HTTPS_11	Associating Win 7 client to web-auth security and checking the redirection of HTTPS URL in 2500 WLC.	To check whether HTTPS URL gets redirected or not to web-auth login page when client gets connected and browses the internet access.	Passed	
WLJ80S_HTTPS_12	Associating two clients(Win 7 and Macbook) to web-auth security and checking the redirection of HTTPS URL in both clients in 2500 WLC.	To check whether HTTPS URL gets redirected or not to web-auth login page when clients gets connected and browses the internet and also checking the Ping function works or not between them.	Passed	
WLJ80S_HTTPS_13	Associating two clients(Win 7 and Win 8) to web-auth security and checking the redirection of HTTPS URL in both clients in 2500 WLC.	To check whether HTTPS URL gets redirected or not to web-auth login page when clients gets connected and browses the internet and also checking the Ping function works or not between them.	Passed	
WLJ80S_HTTPS_14	Associating Samsung S4 to web-auth security and checking the redirection of HTTPS URL in its browser in 2500 WLC.	To check whether HTTPS URL gets redirected or not to web-auth login page when client gets connected and browses the internet access.	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_HTTPS_15	Associating Apple Iphone to web-auth security and checking the redirection of HTTPS URL in its browser in 2500 WLC.	To check whether HTTPS URL gets redirected or not to web-auth login page when client gets connected and browses the internet access.	Passed	
WLJ80S_HTTPS_16	Associating Win 7 client to web-auth security and checking the redirection of HTTPS URL in WiSM2.	To check whether HTTPS URL gets redirected or not to web-auth login page when client gets connected and browses the internet access.	Passed	
WLJ80S_HTTPS_17	Associating two clients(Win 7 and Macbook) to web-auth security and checking the redirection of HTTPS URL in both clients in WiSM2.	To check whether HTTPS URL gets redirected or not to web-auth login page when clients gets connected and browses the internet and also checking the Ping function works or not between them.	Passed	
WLJ80S_HTTPS_18	Associating two clients(Win 7 and Win 8) to web-auth security and checking the redirection of HTTPS URL in both clients in WiSM2.	To check whether HTTPS URL gets redirected or not to web-auth login page when clients gets connected and browses the internet and also checking the Ping function works or not between them.	Passed	
WLJ80S_HTTPS_19	Associating Samsung S4 to web-auth security and checking the redirection of HTTPS URL in its browser in WiSM2.	To check whether HTTPS URL gets redirected or not to web-auth login page when client gets connected and browses the internet access.	Passed	
WLJ80S_HTTPS_20	Associating Apple Iphone to web-auth security and checking the redirection of HTTPS URL in its browser in WiSM2.	To check whether HTTPS URL gets redirected or not to web-auth login page when client gets connected and browses the internet access.	Passed	

NBAR Engine 3.10 - 8.0

Logical ID	Title	Description	Status	Defects
WLJ80S_AVC_01	Check AVC visibility on upgrade from older release to 8.0 with changing protocol pack in 2500	This is to verify that after upgrade from an older release that supports older AVC engine to 8.0 does not break the basic classification functionality of AVC. The older release will be uploaded with the latest protocol pack 6.0 and then upgraded to 8.0	Passed	
WLJ80S_AVC_02	Check AVC visibility on downgrade from 8.0 to an older release with the latest protocol pack uploaded in 8.0 image in 2500	This is to verify that after downgrade from 8.0 to an older release AVC functionality should not break and AVC config maintained across wlans. The 8.0 image by default will have 4.1 AVC protocol pack which will be upgraded to the latest 6.0 protocol pack before downgrading	Passed	
WLJ80S_AVC_03	Check netflow flow-cache is updated every 90s and traffic sent with dscp values in 2500	This test case is to verify netflow behavior with 8.0 WLC image with 3.10 engine version. The test will also check if DSCP marking is sent in the net flow records and 90s flow cache update happens	Passed	
WLJ80S_AVC_04	Verify AVC classifies multiple applications for multiple clients associated to a single WLC 2500	This is to verify that after upgrade to 8.0 multiple applications for multiple clients are classified as expected.	Passed	
WLJ80S_AVC_05	Check netflow flow-cache is updated every 90s and traffic sent with dscp values in 5500	This test case is to verify netflow behavior with 8.0 WLC image with 3.10 engine version. The test will also check if DSCP marking is sent in the net flow records and 90s flow cache update happens	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_AVC_06	Check netflow flow-cache is updated every 90s and traffic sent with dscp values in WiSM2	This test case is to verify netflow behavior with 8.0 WLC image with 3.10 engine version. The test will also check if DSCP marking is sent in the net flow records and 90s flow cache update happens	Passed	
WLJ80S_AVC_07	Check netflow flow-cache is updated every 90s and traffic sent with dscp values in 8500	This test case is to verify netflow behavior with 8.0 WLC image with 3.10 engine version. The test will also check if DSCP marking is sent in the net flow records and 90s flow cache update happens	Passed	
WLJ80S_AVC_08	Check AVC visibility on upgrade from older release to 8.0 with changing protocol pack in 5500	This is to verify that after upgrade from an older release that supports older AVC engine to 8.0 does not break the basic classification functionality of AVC. The older release will be uploaded with the latest protocol pack 6.0 and then upgraded to 8.0	Passed	
WLJ80S_AVC_09	Check AVC visibility on upgrade from older release to 8.0 with changing protocol pack in WiSM2	This is to verify that after upgrade from an older release that supports older AVC engine to 8.0 does not break the basic classification functionality of AVC. The older release will be uploaded with the latest protocol pack 6.0 and then upgraded to 8.0	Passed	
WLJ80S_AVC_10	Check AVC visibility on upgrade from older release to 8.0 with changing protocol pack in 8500	This is to verify that after upgrade from an older release that supports older AVC engine to 8.0 does not break the basic classification functionality of AVC. The older release will be uploaded with the latest protocol pack 6.0 and then upgraded to 8.0	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_AVC_11	Check AVC visibility on downgrade from 8.0 to an older release with the latest protocol pack uploaded in 8.0 image in 5500	This is to verify that after downgrade from 8.0 to an older release AVC functionality should not break and AVC config maintained across wlans. The 8.0 image by default will have 4.1 AVC protocol pack which will be upgraded to the latest 6.0 protocol pack before downgrading	Passed	
WLJ80S_AVC_12	Check AVC visibility on downgrade from 8.0 to an older release with the latest protocol pack uploaded in 8.0 image in 8500	This is to verify that after downgrade from 8.0 to an older release AVC functionality should not break and AVC config maintained across wlans. The 8.0 image by default will have 4.1 AVC protocol pack which will be upgraded to the latest 6.0 protocol pack before downgrading	Passed	
WLJ80S_AVC_13	Check AVC visibility on downgrade from 8.0 to an older release with the latest protocol pack uploaded in 8.0 image in WiSM2	This is to verify that after downgrade from 8.0 to an older release AVC functionality should not break and AVC config maintained across wlans. The 8.0 image by default will have 4.1 AVC protocol pack which will be upgraded to the latest 6.0 protocol pack before downgrading	Passed	
WLJ80S_AVC_14	Verify AVC classifies multiple applications for multiple clients associated to a single WLC 5500	This is to verify that after upgrade to 8.0 multiple applications for multiple clients are classified as expected.	Passed	
WLJ80S_AVC_15	Verify AVC classifies multiple applications for multiple clients associated to a single WLC 8500	This is to verify that after upgrade to 8.0 multiple applications for multiple clients are classified as expected.	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_AVC_16	Verify AVC classifies multiple applications for multiple clients associated to a single WLC WiSM2	This is to verify that after upgrade to 8.0 multiple applications for multiple clients are classified as expected.	Passed	
WLJ80S_AVC_17	Check AVC profile integration with Local policy CLI along with RADIUS using SSH in 2500	This is to verify that CLI configuration for AVC profile with Local policy engine is configurable as expected and also check RADIUS with ACS	Passed	
WLJ80S_AVC_18	Check AVC profile integration with Local policy CLI along with RADIUS using Telnet in 2500	This is to verify that CLI configuration for AVC profile with Local policy engine is configurable as expected and also check RADIUS with ACS	Passed	
WLJ80S_AVC_19	Check AVC profile integration with Local policy CLI along with RADIUS using SSH in 5500	This is to verify that CLI configuration for AVC profile with Local policy engine is configurable as expected and also check RADIUS with ACS	Passed	
WLJ80S_AVC_20	Check AVC profile integration with Local policy CLI along with RADIUS using SSH in 8500	This is to verify that CLI configuration for AVC profile with Local policy engine is configurable as expected and also check RADIUS with ACS	Passed	
WLJ80S_AVC_21	Check AVC profile integration with Local policy CLI along with RADIUS using SSH in WiSM2	This is to verify that CLI configuration for AVC profile with Local policy engine is configurable as expected and also check RADIUS with ACS	Passed	
WLJ80S_AVC_22	Check AVC profile integration with Local policy CLI along with RADIUS using Telnet in 5500	This is to verify that CLI configuration for AVC profile with Local policy engine is configurable as expected and also check RADIUS with ACS	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_AVC_23	Check AVC profile integration with Local policy CLI along with RADIUS using Telnet in 8500	This is to verify that CLI configuration for AVC profile with Local policy engine is configurable as expected and also check RADIUS with ACS	Passed	
WLJ80S_AVC_24	Check AVC profile integration with Local policy CLI along with RADIUS using Telnet in WiSM2	This is to verify that CLI configuration for AVC profile with Local policy engine is configurable as expected and also check RADIUS with ACS	Passed	
WLJ80S_AVC_25	Check AVC profile integration with Local policy GUI along with RADIUS using 2500	This is to verify that GUI configuration for AVC profile with Local policy engine is configurable as expected and also check RADIUS with ACS	Passed	
WLJ80S_AVC_26	Check AVC profile integration with Local policy GUI along with RADIUS using 5500	This is to verify that GUI configuration for AVC profile with Local policy engine is configurable as expected and also check RADIUS with ACS	Passed	
WLJ80S_AVC_27	Check AVC profile integration with Local policy GUI along with RADIUS using 8500	This is to verify that GUI configuration for AVC profile with Local policy engine is configurable as expected and also check RADIUS with ACS	Passed	
WLJ80S_AVC_28	Check AVC profile integration with Local policy GUI along with RADIUS using WiSM2	This is to verify that GUI configuration for AVC profile with Local policy engine is configurable as expected and also check RADIUS with ACS	Passed	
WLJ80S_AVC_29	To check AVC integration with Local policy configuration from SNMP using 2500	This is to verify that AVC Local policy configuration from SNMP	Passed	
WLJ80S_AVC_30	To check AVC integration with Local policy configuration from SNMP using 5500	This is to verify that AVC Local policy configuration from SNMP	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_AVC_31	To check AVC integration with Local policy configuration from SNMP using 8500	This is to verify that AVC Local policy configuration from SNMP	Passed	
WLJ80S_AVC_32	To check AVC integration with Local policy configuration from SNMP using WiSM2	This is to verify that AVC Local policy configuration from SNMP	Passed	
WLJ80S_AVC_33	Config download check for AVC local policy config	This is to verify AVC Local Policy config and AVC behavior after config upload and download	Passed	
WLJ80S_AVC_34	Upgrade / Downgrade check for AVC Local policy config	This is to verify AVC Local policy intersection with upgrade and downgrade	Passed	
WLJ80S_AVC_35	Verify AVC profile through Local policy functionality	This is to verify that AVC profile is applied based on Cisco AV pair attribute role value from Local Policy to a specific client	Passed	
WLJ80S_AVC_36	Verify AVC profile through Local policy functionality with multiple match types and actions enabled	This is to verify that AVC profile is applied based on Cisco AV pair attribute role value from Local Policy to a specific client with multiple match types and action values	Passed	

Rate Limit

Logical ID	Title	Description	Status	Defects
WLJ80S_rate_01	Check AVC profile per application rate limiting configuration and DSCP marking per application from CLI using SSH along with RADIUS	Verify if that CLI configuration for AVC profile per application rate limiting is configurable as expected and also check in RADIUS (ACS)	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_rate_02	Check AVC profile per application rate limiting configuration and DSCP marking per application from CLI using Telnet along with RADIUS	Verify if that CLI configuration for AVC profile per application rate limiting is configurable as expected and also check in RADIUS (ACS)	Passed	
WLJ80S_rate_03	Check AVC profile per application rate limiting configuration and DSCP marking per application from CLI	Verify if that CLI configuration for AVC profile per application rate limiting is configurable as expected.	Passed	
WLJ80S_rate_04	Check AVC profile per application rate limiting configuration and DSCP marking per application from GUI along with RADIUS	Verify if that GUI configuration for AVC profile per application rate limiting is configurable as expected and also check in RADIUS (ACS)	Passed	
WLJ80S_rate_05	To check AVC rate limiting and DSCP directional marking configuration from SNMP	Verify if that AVC rate limiting and DSCP direction marking configuration from SNMP	Passed	
WLJ80S_rate_06	Upgrade check for AVC rate limit and DSCP directional marking config	Verify if AVC rate limiting, DSCP directional marking config and AVC behavior after upgrade	Passed	
WLJ80S_rate_07	Downgrade check for AVC rate limit and DSCP directional marking config	Verify if AVC rate limiting, DSCP directional marking config and AVC behavior after downgrade	Passed	
WLJ80S_rate_08	Config upload check for AVC rate limit	Verify if AVC rate limiting config and AVC behavior after config upload	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_rate_09	Config download check for AVC rate limit	Verify if AVC rate limiting config and AVC behavior after config download	Passed	
WLJ80S_rate_10	Verify all rate limit application in a AVC profile in 2500	Verify if AVC raterlimit is applied for all the application configured and results are as expected.	Passed	
WLJ80S_rate_11	Verify all rate limit application in a AVC profile in 5500	Verify if AVC raterlimit is applied for all the application configured and results are as expected.	Passed	
WLJ80S_rate_12	Verify all rate limit application in a AVC profile in 8500	Verify if AVC raterlimit is applied for all the application configured and results are as expected.	Passed	
WLJ80S_rate_13	Verify all rate limit application in a AVC profile in WiSM2	Verify if AVC raterlimit is applied for all the application configured and results are as expected.	Passed	
WLJ80S_rate_14	Check AVC rate limiting precedence over Per SSID Bandwidth contract in 2500	Verify if AVC rate limit is applied after per SSID bandwidth contract values.	Passed	
WLJ80S_rate_15	Check AVC rate limiting precedence over Per SSID Bandwidth contract in 5500	Verify if AVC rate limit is applied after per SSID bandwidth contract values.	Passed	
WLJ80S_rate_16	Check AVC rate limiting precedence over Per SSID Bandwidth contract in 8500	Verify if AVC rate limit is applied after per SSID bandwidth contract values.	Passed	
WLJ80S_rate_17	Check AVC rate limiting precedence over Per SSID Bandwidth contract in WiSM2	Verify if AVC rate limit is applied after per SSID bandwidth contract values.	Passed	
WLJ80S_rate_18	Check AVC rate limiting precedence over Per User Bandwidth contract in 2500	Verify if AVC rate limit is applied after per User bandwidth contract values.	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_rate_19	Check AVC rate limiting precedence over Per User Bandwidth contract in 5500	Verify if AVC rate limit is applied after per User bandwidth contract values.	Passed	
WLJ80S_rate_20	Check AVC rate limiting precedence over Per User Bandwidth contract in 8500	Verify if AVC rate limit is applied after per User bandwidth contract values.	Passed	
WLJ80S_rate_21	Check AVC rate limiting precedence over Per User Bandwidth contract in WiSM2	Verify if AVC rate limit is applied after per User bandwidth contract values.	Passed	
WLJ80S_rate_22	Verify all rate limit and directional DSCP application in a dot1x WLAN using 2500	Verify if AVC rate limit and directional DSCP behavior with a dot1x WLAN	Passed	
WLJ80S_rate_23	Verify all rate limit and directional DSCP application in a dot1x WLAN using 5500	Verify if AVC rate limit and directional DSCP behavior with a dot1x WLAN	Passed	
WLJ80S_rate_24	Verify all rate limit and directional DSCP application in a dot1x WLAN using 8500	Verify if AVC rate limit and directional DSCP behavior with a dot1x WLAN	Passed	
WLJ80S_rate_25	Verify all rate limit and directional DSCP application in a dot1x WLAN using WiSM2	Verify if AVC rate limit and directional DSCP behavior with a dot1x WLAN	Passed	
WLJ80S_rate_26	Verify all rate limit and directional DSCP application in a no encryption and static key WLAN using 2500	Verify if AVC rate limit and directional DSCP behavior with a static PSK WLAN and no encryption WLAN	Passed	
WLJ80S_rate_27	Verify all rate limit and directional DSCP application in a no encryption and static key WLAN using 5500	Verify if AVC rate limit and directional DSCP behavior with a static PSK WLAN and no encryption WLAN	Passed	
WLJ80S_rate_28	Verify all rate limit and directional DSCP application in a no encryption and static key WLAN using 8500	Verify if AVC rate limit and directional DSCP behavior with a static PSK WLAN and no encryption WLAN	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_rate_29	Verify all rate limit and directional DSCP application in a no encryption and static key WLAN using WiSM2	Verify if AVC rate limit and directional DSCP behavior with a static PSK WLAN and no encryption WLAN	Passed	
WLJ80S_rate_30	Verify all rate limit and directional DSCP application in a webauth WLAN using 2500	Verify if AVC rate limit and directional DSCP behavior with a webauth WLAN	Passed	
WLJ80S_rate_31	Verify all rate limit and directional DSCP application in a webauth WLAN using 5500	Verify if AVC rate limit and directional DSCP behavior with a webauth WLAN	Passed	
WLJ80S_rate_32	Verify all rate limit and directional DSCP application in a webauth WLAN using 8500	Verify if AVC rate limit and directional DSCP behavior with a webauth WLAN	Passed	
WLJ80S_rate_33	Verify all rate limit and directional DSCP application in a webauth WLAN using WiSM2	Verify if AVC rate limit and directional DSCP behavior with a webauth WLAN	Passed	
WLJ80S_rate_34	Verify AVC rate limit when the rate limit rules dynamically using 2500	Verify if AVC rate limit behavior on a client when the rate limit rule change values dynamically when the client is still associated with the AVC profile name	Passed	
WLJ80S_rate_35	Verify AVC rate limit when the rate limit rules dynamically 5500	Verify if AVC rate limit behavior on a client when the rate limit rule change values dynamically when the client is still associated with the AVC profile name	Passed	
WLJ80S_rate_36	Verify AVC rate limit when the rate limit rules dynamically 8500	Verify if AVC rate limit behavior on a client when the rate limit rule change values dynamically when the client is still associated with the AVC profile name	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_rate_37	Verify AVC rate limit when the rate limit rules dynamically WisM2	Verify if AVC rate limit behavior on a client when the rate limit rule change values dynamically when the client is still associated with the AVC profile name	Passed	
WLJ80S_rate_38	Verify AVC DSCP marking with netflow using 2500	Verify if DSCP values marked based on direction (either upstream / downstream) are updated on the flow data records sent in netflow	Passed	
WLJ80S_rate_39	Verify AVC DSCP marking with netflow using 5500	Verify if DSCP values marked based on direction (either upstream / downstream) are updated on the flow data records sent in netflow	Passed	
WLJ80S_rate_40	Verify AVC DSCP marking with netflow using 8500	Verify if DSCP values marked based on direction (either upstream / downstream) are updated on the flow data records sent in netflow	Passed	
WLJ80S_rate_41	Verify AVC DSCP marking with netflow using WiSM2	Verify if DSCP values marked based on direction (either upstream / downstream) are updated on the flow data records sent in netflow	Passed	

AAA Override for AVC Profile Name

Logical ID	Title	Description	Status	Defects
WLJ80S_AAA_01	Verify AVC profile AAA override from authentication server	This is to verify that AVC profile is applied using AAA override from authentication server when the wlan is central switching.	Passed	
WLJ80S_AAA_02	Verify AVC profile AAA override from authentication server in a split-tunnel wlan config	This is to verify that AVC profile is applied using AAA override from authentication server when the wlan is central switching and split tunneling configured	Passed	
WLJ80S_AAA_03	Verify AVC profile AAA override from authentication server	This is to verify that AVC profile is applied using AAA override from authentication server when the WLAN is L3 enabled.	Passed	
WLJ80S_AAA_04	Verify AVC profile AAA override from authentication server when wlan is configured for mac filtering	This is to verify that AVC profile is applied using AAA override from authentication server when the wlan is configured for mac filtering	Passed	
WLJ80S_AAA_05	Verify AVC profile AAA override with Radius NAC enabled	This is to verify that AVC profile is applied using AAA override from ISE when client goes through CWA / posturing.	Passed	
WLJ80S_AAA_06	Check if after re-authentication AVC profile is still applied to the client.	This is to verify that AVC profile is applied using AAA override from authentication server even after session timeout is expired.	Passed	
WLJ80S_AAA_07	To validate AAA override Radius session time out	To validate AAA override Radius session time out	Passed	
WLJ80S_AAA_08	Check if after re-authentication AVC profile is still applied to the client even if the AVC name change on the AAA.	This is to verify that the same AVC profile is applied using AAA override from authentication server even after session timeout is expired.	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_AAA_09	Verify AVC profile AAA override from authentication server with max number of clients	This is to verify that AVC profile is applied using AAA override from authentication server accordingly with max number of clients.	Passed	
WLJ80S_AAA_10	Verify AVC profile AAA override from authentication server with invalid profile name	This is to verify the AVC profile behavior when applied from AAA with an invalid name which is not configured on the WLC.	Passed	
WLJ80S_AAA_11	Verify AVC profile AAA override from authentication server with additional AAA attributes like Vlan, session timeout and ACL name	This is to verify the AVC profile behavior when applied from AAA with additional attributes like ACL name, session timeout and Vlan id.	Passed	
WLJ80S_AAA_12	Verify AVC profile AAA override from authentication server with radius failover	This is to verify the AVC profile behavior when applied from AAA with additional attributes like ACL name, session timeout and Vlan id.	Passed	
WLJ80S_AAA_13	Verify AVC profile AAA override from authentication server with AAA override disabled for the wlan	This is to verify the AVC profile behavior when applied from AAA when AAA override is disabled on the wlan, but AAA server returning a AVC profile name	Passed	
WLJ80S_AAA_14	Verify AVC profile through Local policy functionality when AAA override enabled and AVC-profile-name is configured on the AAA	This is to verify that AVC profile is applied from local policy based on Cisco AV pair attribute role value to a specific client when AAA override is enabled is enabled and cisco-av-pair AVC-profile-name and role name attribute is received after authentication from AAA server	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_AAA_15	Verify AVC profile through Local policy functionality when AAA override disabled and AVC-profile-name is configured on the AAA	This is to verify that AVC profile is applied from local policy based on Cisco AV pair attribute role value to a specific client when AAA override is disabled and cisco-av-pair AVC-profile-name and role name attribute is received after authentication from AAA server	Passed	
WLJ80S_AAA_16	Verify AVC profile through Local policy functionality when AAA override disabled and AVC-profile-name and role is not configured on the AAA	This is to verify that AVC profile is applied from default wlan AVC profile name when role and AVC-profile-name is not configured on the AAA server and local policy configured on the WLAN with a AVC profile name	Passed	

Rf Profile

Logical ID	Title	Description	Status	Defects
WLJ80S_RF_01	RF profile DCA list-GUI	To Configure few channels on Global DCA list. Try to configure a channel on RF profile DCA list which is not part of Global list via the GUI. Verify GUI throws error	Passed	
WLJ80S_RF_02	RF profile DCA list-CLI	To Configure few channels on Global DCA list. Try to configure a channel on RF profile DCA list which is not part of Global list via the CLI. Verify CLI throws error	Passed	
WLJ80S_RF_03	Show CLI command related to RF profile for DCA feature	"To Verify the CLI -""show rf-profile details <RF-Profile>"", shows parameters configured for DCA and Threshold for traps."	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_RF_04	Upload / Download of the Config and check for Channel width parameter on DCA RF profile	To Verify Config is successfully uploaded and CW is seen as 20 MHz. Change the channel width to 40 MHz on the uploaded config. Download the changed config and verify CW on RF profile is set to 40 MHz	Passed	
WLJ80S_RF_05	Configure RF profile DCA parameters via the CLI	To Configure various RF profile DCA parameters via the CLI and verify configs are successful	Passed	
WLJ80S_RF_06	Upload/Download of the Config and check for Avoid Foreign AP interference parameter on DCA RF profile	Verify Config is successfully uploaded and Avoid Foreign AP interference is seen as enabled.	Passed	
WLJ80S_RF_07	Upload/Download of the Config and check for threshold trap values on RF profile	To Verify config is successfully uploaded. Change few threshold values on uploaded config. Download the config and verify the changed values	Passed	
WLJ80S_RF_08	RF profile, threshold for traps via the GUI	To Configure various threshold for traps via the GUI and verify configs are successful	Passed	
WLJ80S_RF_09	RF profile DCA parameters via the CLI	To Configure various RF profile DCA parameters via the CLI and verify configs are successful	Passed	
WLJ80S_RF_10	RF profile DCA parameters via the GUI	To verify Configure various RF profile DCA parameters via the GUI and verify configs are successful	Passed	
WLJ80S_RF_11	RF profile, threshold for traps via the CLI	To verify Configure various threshold for traps via the CLI and verify configs are successful	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_RF_12	RF profile, threshold for traps via the GUI	To verify Configure various threshold for traps via the GUI and verify configs are successful	Passed	
WLJ80S_RF_13	Controller should retain the config across controller reset	Configure DCA and threshold for traps on RF profile. Reset the Controller and verify the configs are retained	Passed	

Cleanair-skyros

Logical ID	Title	Description	Status	Defects
WLJ80S_CAE_01	Enable/Disable CleanAir in the GUI of 5508 and WiSM2 controller.	To verify if the cleanAir functionality can be enabled/disabled from the GUI of the WLC	Passed	
WLJ80S_CAE_02	Enable/Disable CleanAir in the GUI of 7500 and 8500 controller.	To verify if the cleanAir functionality can be enabled/disabled from the GUI of the WLC	Passed	
WLJ80S_CAE_03	Enabling/disabling CleanAir from the CLI of 5508 and WiSM2 controllers	To verify if the cleanAir functionality can be enabled/disabled from the CLI of the WLC	Passed	
WLJ80S_CAE_04	Enabling/disabling CleanAir from the CLI of 7500 and 8500 controllers	To verify if the cleanAir functionality can be enabled/disabled from the CLI of the WLC	Passed	
WLJ80S_CAE_05	Detecting Bluetooth interferences using 1600 AP in 5508 and WiSM2 controllers	To verify if the AP is able to detect Bluetooth interferences in the 802.11b/g/n range.	Passed	
WLJ80S_CAE_06	Detecting Bluetooth interferences using 1600 AP in 7500/8500 controllers	To verify if the AP is able to detect Bluetooth interferences in the 802.11b/g/n range.	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_CAE_07	Air Quality Index trap after setting the AQI alarm threshold in the 5508 and WiSM2 controller to which a 1600 AP is associated	To verify if the alarm if triggered if the Air Quality reaches the threshold value or below in a controller where the 1600 AP is associated	Passed	
WLJ80S_CAE_08	Air Quality Index trap after setting the AQI alarm threshold in the 7500/8500 controller to which a 1600 AP is associated	To verify if the alarm if triggered if the Air Quality reaches the threshold value or below in a controller where the 1600 AP is associated	Passed	
WLJ80S_CAE_09	Trap for unclassified interferences using 1600 AP associated to the 5508/WiSM2 controller	To enable trap for unclassified interferences, set the threshold for the same and verify if the trap is passed for bluetooth and other interference types	Passed	
WLJ80S_CAE_10	Trap for unclassified interferences using 1600 AP associated to the 7500/8500 controller	To enable trap for unclassified interferences, set the threshold for the same and verify if the trap is passed for bluetooth and other interference types	Passed	
WLJ80S_CAE_11	Trigger spectrum event-driven radio resource management (RRM) when a CleanAir enabled 1600 AP is associated to 5508/WiSM2 controller	To verify if the RRM initiated DCA which changes the channel of the affected access point radio if possible to improve network performance when the interference for the access point rises above the threshold level	Passed	
WLJ80S_CAE_12	Trigger spectrum event-driven radio resource management (RRM) when a CleanAir enabled 1600 AP is associated to 7500/8500 controller	To verify if the RRM initiated DCA which changes the channel of the affected access point radio if possible to improve network performance when the interference for the access point rises above the threshold level	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_CAE_13	Enabling CleanAir from the Access point configure page in 1600 AP	To verify if the CleanAir configuration on the AP page is correctly and the changes reflect.	Passed	
WLJ80S_CAE_14	Monitoring Interference device from the Controller GUI	To verify if the interferences detected by 1600 AP can be correctly monitored from the WLC GUI.	Passed	
WLJ80S_CAE_15	Monitor Persistent devices on a 1600 Access Point	To verify if the persistent devices could be monitored on a specific 1600 Series Access Point	Passed	
WLJ80S_CAE_16	Detecting Wifi direct interferences using 1600 AP in 5508 and WiSM2 controllers	To verify if the AP is able to detect Wifi direct interferences.	Passed	
WLJ80S_CAE_17	Detecting Wifi direct interferences using 1600 AP in 7500/8500 controllers	To verify if the AP is able to detect Wifi direct interferences.	Passed	
WLJ80S_CAE_18	Monitoring the Air Quality of Radio Bands from the 5508/WiSM2 Controller GUI and CLI	To verify if the Air Quality if Radio bands can be viewed from the GUI of controller and CLI.	Passed	
WLJ80S_CAE_19	Monitoring the Air Quality of Radio Bands from the 7500/8500 Controller GUI and CLI	To verify if the Air Quality if Radio bands can be viewed from the GUI of controller and CLI.	Passed	
WLJ80S_CAE_20	Cisco Prime Infrastructure Reports on CleanAir	To verify if the Cisco Prime Infrastructure report for CleanAir is generated correctly .	Passed	
WLJ80S_CAE_21	Location of known non-WiFi interferers using a CleanAir enabled 1600 series AP	To verify if the location of the known non-WiFi interferers is detected by the CleanAir enabled 1600 series AP	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_CAE_22	SE-Connect mode in CleanAir enabled 1600 series AP	To verify if the SE-connect mode can be turned on in a CleanAir enabled 1600 series AP	Passed	
WLJ80S_CAE_23	CleanAir enabled 1600 AP for Spectrum Expert function	To verify if we can obtain detailed spectrum data that can be used to generate RF analysis plots similar to those provided by a spectrum analyzer.	Passed	
WLJ80S_CAE_24	CleanAir enabled 1600 AP for Spectrum Expert function enabling from Cisco Prime Infrastructure	To verify if the Spectrum Expert enabling done from the PI is working fine	Passed	

Flexconnect on Mesh

Logical ID	Title	Description	Status	Defects
WLJ80S_Mesh_01	AP conversion from Local to Flex+bridge mode	To verify whether changing the AP mode from local to flex+bridge works properly	Passed	
WLJ80S_Mesh_02	AP conversion from Flexconnect to Flex+bridge mode for RAP	To verify whether changing the RAP mode from Flexconnect to Flex+bridge works properly	Passed	
WLJ80S_Mesh_03	AP conversion from Flexconnect to Flex+bridge mode for MAP	To verify whether changing the MAP mode from Flexconnect to Flex+bridge works properly	Passed	
WLJ80S_Mesh_04	AP conversion from Flexconnect to Flex+bridge mode for RAP/MAP	To verify whether changing the mode from flexconnect to Flex+bridge works properly for RAP/MAP	Passed	
WLJ80S_Mesh_05	Show commands for Flex+bridge mode	To verify all the show commands for Flex+bridge mode	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_Mesh_06	VLAN/WLAN mapping for flexconnect local-switching	To verify the VLAN/WLAN mapping for flexconnect group with local-switching	Passed	
WLJ80S_Mesh_07	Default AP group with VLAN/WLAN mapping	To verify the default AP group with VLAN/WLAN mapping	Passed	
WLJ80S_Mesh_08	AP mode after upgrade	To verify whether the AP mode retains after upgrading the WLC to latest software	Passed	
WLJ80S_Mesh_09	VLAN/WLAN mapping config upon WLC reset	To verify the VLAN/WLAN mapping config for flexconnect LS after WLC reset	Passed	
WLJ80S_Mesh_10	Client status when Flex+bridge AP is in standalone mode	To verify the client status	Passed	

Cleanair

Logical ID	Title	Description	Status	Defects
WLJ80S_CleanAir_01	Clean Air Event Driven RRM	To verify the Airt event driven RRM	Passed	
WLJ80S_CleanAir_02	Confirm Air Quality updates are sent by access points	To verify the Air Quality updates	Passed	
WLJ80S_CleanAir_03	Interference detection in Flex Connect	Verify if a Bluetooth is detected by AP / WLC in Flexconnect mode.	Passed	

OEAP Enhancements

Basic Firewall

Logical ID	Title	Description	Status	Defects
WLJ80S_OEAP_BF_01	Associating OEAP to 5500 WLC	To check whether OEAP gets joined or not with 5500 WLC	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_OEAP_BF_02	Enabling the Firewall in OEAP GUI.	To check whether Firewall is getting enabled or not in OEAP GUI.	Passed	
WLJ80S_OEAP_BF_03	Enabling the Firewall in OEAP GUI and checking the internet access for a Lan client.	To check whether Lan clients access is denied or not after enabling Firewall in OEAP GUI.	Passed	
WLJ80S_OEAP_BF_04	Enabling the Lan application access for HTTP & HTTPS in OEAP GUI.	To check whether HTTP & HTTPS application access are allowed or not for a Lan client.	Passed	
WLJ80S_OEAP_BF_05	Enabling the Lan application access for TFTP & Telnet in OEAP GUI.	To check whether TFTP & Telnet application access are allowed or not for a Lan client when it is connected to Lan port no.1	Passed	
WLJ80S_OEAP_BF_06	Associating three Lan clients and checking the Firewall function	To check whether all three clients gets denied or not when Firewall is enabled.	Passed	
WLJ80S_OEAP_BF_07	Denying specific Lan ip address using port forwarding rules	To check whether specific Lan ip address access to internet is denied or not by configuring ip address in Port Forwarding.	Passed	
WLJ80S_OEAP_BF_08	Allowing specific Lan ip address using port forwarding rules	To check whether specific Lan ip address access to internet is allowed or not by configuring ip address in Port Forwarding.	Passed	
WLJ80S_OEAP_BF_09	Creating Local WLAN and associating a client to this Local WLAN.	To check whether client is connected or not to Local WLAN created in OEAP GUI.	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_OEAP_BF_10	Checking the Firewall function to a Local WLAN client	To check whether Firewall getting applied to Local WLAN client or not.	Passed	
WLJ80S_OEAP_BF_11	Enabling the Lan application access for HTTP & HTTPS in OEAP GUI and checking for Local WLAN client	To check whether HTTP & HTTPS application access are allowed or not for a Local WLAN client.	Passed	
WLJ80S_OEAP_BF_12	Enabling the Lan application access for TFTP & Telnet in OEAP GUI and checking for Local WLAN client.	To check whether TFTP & Telnet application access are allowed or not for a Local WLAN client.	Passed	
WLJ80S_OEAP_BF_13	Enabling Mac Filter in OEAP GUI and checking the Firewall function for Win 7 Client by adding its Mac address.	To check whether Firewall function works or not in Win 7 client by associating it to Personal SSID in OEAP with Security-MacFiltering.	Passed	
WLJ80S_OEAP_BF_14	Enabling Mac Filter in OEAP GUI and checking the Firewall function for Win 8 Client by adding its Mac address.	To check whether Firewall function works or not in Win 8 client by associating it to Personal SSID in OEAP with Security-MacFiltering.	Passed	
WLJ80S_OEAP_BF_15	Enabling Mac Filter in OEAP GUI and checking the Firewall function for MacBook Client by adding its Mac address.	To check whether Firewall function works or not in MacBook client by associating it to Personal SSID in OEAP with Security-MacFiltering.	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_OEAP_BF_16	Enabling Mac Filter in OEAP GUI and checking the Firewall function for Samsung S4 Client by adding its Mac address.	To check whether Firewall function works or not in Samsung S4 client by associating it to Personal SSID in OEAP with Security-MacFiltering.	Passed	
WLJ80S_OEAP_BF_17	Enabling Mac Filter in OEAP GUI and checking the Firewall function for Apple Iphone Client by adding its Mac address.	To check whether Firewall function works or not in Apple Iphone client by associating it to Personal SSID in OEAP with Security-MacFiltering.	Passed	
WLJ80S_OEAP_BF_18	Associating Win 7 client to Personal SSID -WPA2+PSK and checking the firewall function.	To verify whether Firewall functions works or not for Win 7 client associated to Personal SSID with Security - WPA2+PSK.	Passed	
WLJ80S_OEAP_BF_19	Associating MacBook client to Personal SSID -WPA2+PSK and checking the firewall function.	To verify whether Firewall functions works or not for MacBook client associated to Personal SSID with Security - WPA2+PSK.	Passed	
WLJ80S_OEAP_BF_20	Creating a DMZ ip address and checking its function.	To check whether client able to access the internet or not via DMZ.	Passed	

End User GUI Enhancements

Logical ID	Title	Description	Status	Defects
WLJ80S_OEAP_UI_01	Associating OEAP to 5500 WLC and checking the Network Diagnostics tab in WLC GUI	To check whether Network Diagnostics tab is present or not in WLC GUI for OEAP.	Passed	
WLJ80S_OEAP_UI_02	Starting the Network Diagnostics in OEAP GUI	To check whether network diagnostics works or not in OEAP GUI.	Passed	
WLJ80S_OEAP_UI_03	Starting the Network Diagnostics in 7500 WLC GUI	To check whether network diagnostics works or not in 7500 WLC GUI.	Passed	
WLJ80S_OEAP_UI_04	Starting the Network Diagnostics in 7500 WLC CLI	To check whether network diagnostics works or not in 7500 WLC CLI.	Passed	
WLJ80S_OEAP_UI_05	Starting the Network Diagnostics in 2500 WLC GUI	To check whether network diagnostics works or not in 2500 WLC GUI.	Passed	
WLJ80S_OEAP_UI_06	Starting the Network Diagnostics in 2500 WLC CLI	To check whether network diagnostics works or not in 2500 WLC CLI.	Passed	
WLJ80S_OEAP_UI_07	Starting the Network Diagnostics in 8500 WLC GUI	To check whether network diagnostics works or not in 8500 WLC GUI.	Passed	
WLJ80S_OEAP_UI_08	Starting the Network Diagnostics in 8500 WLC CLI	To check whether network diagnostics works or not in 8500 WLC CLI.	Passed	
WLJ80S_OEAP_UI_09	Starting the Network Diagnostics in WiSM2 GUI	To check whether network diagnostics works or not in WiSM2 GUI.	Passed	
WLJ80S_OEAP_UI_10	Starting the Network Diagnostics in 8500 WiSM2 CLI	To check whether network diagnostics works or not in WiSM2 CLI.	Passed	

Split Tunnel for Internet Traffic

Logical ID	Title	Description	Status	Defects
WLJ80S_OEAP_ST_01	Enabling Split tunnel configuration globally.	To check whether split tunnel configuration is enabled globally or not in WLC.	Passed	
WLJ80S_OEAP_ST_02	Creating a OEAP ACL in WLC GUI and mapping it to a WLAN.	To check whether OEAP ACL is created and mapped to a WLAN successfully or not in WLC GUI.	Passed	
WLJ80S_OEAP_ST_03	Creating a OEAP ACL in WLC CLI and mapping it to a WLAN.	To check whether OEAP ACL is created and mapped to a WLAN successfully or not in WLC CLI.	Passed	
WLJ80S_OEAP_ST_04	Associating a Win 7 client to a WLAN in which split tunnel is enabled in 7500 WLC	To check whether Win 7 client associated successfully to the WLAN in 7500 WLC and able to access the internet via gateway as mentioned in WLAN under OEAP parameters.	Passed	
WLJ80S_OEAP_ST_05	Associating a Macbook client to a WLAN in which split tunnel is enabled in 7500 WLC	To check whether MacBook client associated successfully to the WLAN in 7500 WLC and able to access the internet via gateway as mentioned in WLAN under OEAP parameters.	Passed	
WLJ80S_OEAP_ST_06	Associating a Win 8 client to a WLAN in which split tunnel is enabled in 7500 WLC	To check whether Win 8 client associated successfully to the WLAN in 7500 WLC and able to access the internet via gateway as mentioned in WLAN under OEAP parameters.	Passed	
WLJ80S_OEAP_ST_07	Associating a Samsung S4 client to a WLAN in which split tunnel is enabled in 7500 WLC	To check whether Samsung S4 client associated successfully to the WLAN in 7500 WLC and able to access the internet via gateway as mentioned in WLAN under OEAP parameters.	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_OEAP_ST_08	Associating Apple Iphone client to a WLAN in which split tunnel is enabled in 7500 WLC	To check whether Apple Iphone client associated successfully to the WLAN in 7500 WLC and able to access the internet via gateway as mentioned in WLAN under OEAP parameters.	Passed	
WLJ80S_OEAP_ST_09	Associating a Win 7 client to a WLAN in which split tunnel is enabled in 5500 WLC	To check whether Win 7 client associated successfully to the WLAN in 5500 WLC and able to access the internet via gateway as mentioned in WLAN under OEAP parameters.	Passed	
WLJ80S_OEAP_ST_10	Associating a Macbook client to a WLAN in which split tunnel is enabled in 5500 WLC	To check whether MacBook client associated successfully to the WLAN in 5500 WLC and able to access the internet via gateway as mentioned in WLAN under OEAP parameters.	Passed	
WLJ80S_OEAP_ST_11	Associating a Win 8 client to a WLAN in which split tunnel is enabled in 5500 WLC	To check whether Win 8 client associated successfully to the WLAN in 5500 WLC and able to access the internet via gateway as mentioned in WLAN under OEAP parameters.	Passed	
WLJ80S_OEAP_ST_12	Associating a Samsung S4 client to a WLAN in which split tunnel is enabled in 5500 WLC	To check whether Samsung S4 client associated successfully to the WLAN in 5500 WLC and able to access the internet via gateway as mentioned in WLAN under OEAP parameters.	Passed	
WLJ80S_OEAP_ST_13	Associating Apple Iphone client to a WLAN in which split tunnel is enabled in 5500 WLC	To check whether Apple Iphone client associated successfully to the WLAN in 5500 WLC and able to access the internet via gateway as mentioned in WLAN under OEAP parameters.	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_OEAP_ST_14	Associating a Win 7 client to a WLAN in which split tunnel is enabled in 2500 WLC	To check whether Win 7 client associated successfully to the WLAN in 2500 WLC and able to access the internet via gateway as mentioned in WLAN under OEAP parameters.	Passed	
WLJ80S_OEAP_ST_15	Associating a Macbook client to a WLAN in which split tunnel is enabled in 2500 WLC	To check whether MacBook client associated successfully to the WLAN in 2500 WLC and able to access the internet via gateway as mentioned in WLAN under OEAP parameters.	Passed	

Voice QOS Enhancements

Logical ID	Title	Description	Status	Defects
WLJ80S_OEAP_QOS_01	Associating OEAP to 5500 WLC and checking the Radio statistics page in WLC GUI.	To check whether OEAP Queue stats are present or not in Radio's detail page of 7500 WLC GUI for OEAP.	Passed	
WLJ80S_OEAP_QOS_02	Associating OEAP to 7500 WLC and checking the Radio statistics page in WLC GUI.	To check whether OEAP Queue stats are present or not in Radio's detail page of 7500 WLC GUI for OEAP.	Passed	
WLJ80S_OEAP_QOS_03	Associating voice clients to OEAP and checking the Radio statistics page in 5500 WLC GUI.	Checking the voice packets stats in Radio details page of 5500 WLC GUI when connecting voice clients to OEAP and passing the voice traffic between the clients.	Passed	
WLJ80S_OEAP_QOS_04	Associating voice clients to OEAP and checking the Radio statistics page in 5500 WLC CLI.	Checking the voice packets stats in 5500 WLC CLI when connecting voice clients to OEAP and passing the voice traffic between the clients.	Passed	
WLJ80S_OEAP_QOS_05	Associating video clients to OEAP and checking the Radio statistics page in 5500 WLC GUI.	Checking the video packets stats in Radio details page of 5500 WLC GUI when connecting video clients to OEAP.	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_OEAP_QOS_06	Associating video clients to OEAP and checking the Radio statistics page in 5500WLC CLI.	Checking the video packets stats in Radio details page of 5500 WLC CLI when connecting video clients to OEAP.	Passed	
WLJ80S_OEAP_QOS_07	Associating voice clients to OEAP and checking the Radio statistics page in 7500 WLC GUI.	Checking the voice packets stats in Radio details page of 7500 WLC GUI when connecting voice clients to OEAP and passing the voice traffic between the clients.	Passed	
WLJ80S_OEAP_QOS_08	Associating voice clients to OEAP and checking the Radio statistics page in 7500 WLC CLI.	Checking the voice packets stats in 7500 WLC CLI when connecting voice clients to OEAP and passing the voice traffic between the clients.	Passed	
WLJ80S_OEAP_QOS_09	Associating video clients to OEAP and checking the Radio statistics page in 7500 WLC GUI.	Checking the video packets stats in Radio details page of 7500 WLC GUI when connecting video clients to OEAP.	Passed	
WLJ80S_OEAP_QOS_10	Associating video clients to OEAP and checking the Radio statistics page in 7500 WLC CLI.	Checking the video packets stats in Radio details page of 7500 WLC CLI when connecting video clients to OEAP.	Passed	

L2TPv3 over UDP

Logical ID	Title	Description	Status	Defects
WLJ80S_L2TPv3_01	L2TPV3 over UDP configuration	To verify the L2TPv3 over UDP configuration in AP	Passed	
WLJ80S_L2TPv3_02	l2tpv3 over UDP tunnel establishment-AP 3500	To verify whether tunnel status is Up	Passed	

3700 Autonomous AP

Logical ID	Title	Description	Status	Defects
WLJ80S_aap_01	Client Association with no security	Verify client association	Passed	
WLJ80S_aap_02	Client Association with WEP	Verify client association	Passed	
WLJ80S_aap_03	Client Association with WPA	Verify client association	Passed	
WLJ80S_aap_04	WGB Mode	Verify WGB association	Passed	
WLJ80S_aap_05	Autonomous AP management access	Verify the Autonomous AP management access	Passed	
WLJ80S_aap_06	Traffic flow between two wireless clients	To Verify the Traffic flow between two wireless clients	Passed	
WLJ80S_aap_07	Monitoring of connected client	To verify the connected client in AP management page	Passed	
WLJ80S_aap_08	Trap logs for connected client	To verify the Trap Logs for connected client	Passed	
WLJ80S_aap_09	Management users	To verify the management user creation	Passed	
WLJ80S_aap_10	Enabling/Disabling the radio	To verify the radio enable/disable status	Passed	
WLJ80S_aap_11	Client Association with TKIP	Verify client association	Passed	
WLJ80S_aap_12	Client Association with AES-CCMP	Verify client association	Passed	
WLJ80S_aap_13	Client Association with TKIP +WEP	Verify client association	Passed	
WLJ80S_aap_16	Transmit and Receive antenna	Verify Transmit and Receive antenna	Passed	
WLJ80S_aap_17	Data rates change	Verify the client association after changing the data rates	Passed	
WLJ80S_aap_18	CDP neighbor details	To verify the CDP neighbor details	Passed	

11ac CCX Lite

Logical ID	Title	Description	Status	Defects
WLJ80S_CCX_01	CCX IE verification	To verify the CCX IE content from 11ac interface	Passed	
WLJ80S_CCX_04	Initial Client association with CCKM enabled-Netgear client	To verify the initial client association with CCKM enabled-Netgear client	Passed	
WLJ80S_CCX_07	Fast re-authentication of 11ac client with CCKM enabled-Netgear client	To verify the Fast re-authentication with CCKM enabled under roaming conditions- Netgear client	Passed	

MSE

CMX Visitor Connect

Logical ID	Title	Description	Status	Defects
WLJ80S_Visitor_01	Creating Template Fields in CMX Connect and Engage UI	To verify created New Template Field is listed in the Splash Templates Tab or not	Passed	
WLJ80S_Visitor_02	Editing Template Fields in CMX Connect and Engage UI	To verify whether Editing the existing Template Field in CMX Connect and Engage UI is successful or not	Passed	
WLJ80S_Visitor_03	Deleting Template Fields in CMX Connect and Engage UI	To verify whether Deleting the existing Template Field in CMX Connect and Engage UI is successful or not	Passed	
WLJ80S_Visitor_04	Creating Social Connectors in CMX Connect and Engage UI	To verify created New Social Connector is listed in the Splash Templates Tab or not	Passed	
WLJ80S_Visitor_05	Editing Social Connectors in CMX Connect and Engage UI	To verify whether Editing the existing Social Connectors in CMX Connect and Engage UI is successful or not	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_Visitor_06	Deleting Social Connectors in CMX Connect and Engage UI	To verify whether Deleting the existing Social Connectors in CMX Connect and Engage UI is successful or not	Passed	
WLJ80S_Visitor_07	Creating Splash Templates in CMX Connect and Engage UI	To verify creation of New Splash Template is successful or not	Passed	
WLJ80S_Visitor_08	Editing Splash Templates in CMX Connect and Engage UI	To verify Editing the existing Splash Template is successful or not	Passed	
WLJ80S_Visitor_09	Deleting Splash Templates in CMX Connect and Engage UI	To verify Deleting the existing Splash Template is successful or not	Passed	
WLJ80S_Visitor_10	Splash Templates assigned to the Social Connectors	To verify displaying of Splash Templates assigned to the Social Connectors is successful or not	Passed	
WLJ80S_Visitor_11	Assigning a Splash Template to a floor	To verify assignation of Splash Template to a Floor is successful or not	Passed	
WLJ80S_Visitor_12	Default User Groups	To verify whether Default User Groups are Displayed in CMX Connect and Engage UI or not	Passed	
WLJ80S_Visitor_13	User Groups	To verify the Redirection of a client to the Splash Page is successful or not	Passed	
WLJ80S_Visitor_14	User Groups	To verify whether Basic User is de-authentication after using 100 MB or not	Passed	
WLJ80S_Visitor_15	User Groups	To verify whether Social User is de-authentication after using 500 MB or not	Passed	
WLJ80S_Visitor_16	NMSP Message for De-authenticating window 7 client	To verify whether the MSE issues NMSP Message for De-auth Packet or not	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_Visitor_17	NMSP Message for De-authenticating Apple mac book client	To verify whether the MSE issues NMSP Message for De-auth Packet or not	Passed	
WLJ80S_Visitor_18	NMSP Message for De-authenticating Apple iphone client	To verify whether the MSE issues NMSP Message for De-auth Packet or not	Passed	
WLJ80S_Visitor_19	NMSP Message for De-authenticating Samsung s4 mobile client	To verify whether the MSE issues NMSP Message for De-auth Packet or not	Passed	
WLJ80S_Visitor_20	User Bandwidth	To verify that the Bandwidth is tracked or not when the Limit is set to Zero	Passed	
WLJ80S_Visitor_21	New Windows 7 Visitors	To verify Whether New Windows 7 Visitors are Displayed in the CMX Connect and Engage UI or not	Passed	
WLJ80S_Visitor_22	New Apple mac book Visitors	To verify Whether New Apple mac book Visitors are Displayed in the CMX Connect and Engage UI or not	Passed	
WLJ80S_Visitor_23	New Apple iphone Visitors	To verify Whether New Apple iphone Visitors are Displayed in the CMX Connect and Engage UI or not	Passed	
WLJ80S_Visitor_24	New Samsung s4 mobile Visitors	To verify Whether New Samsung s4 mobile Visitors are Displayed in the CMX Connect and Engage UI or not	Passed	
WLJ80S_Visitor_25	Repeated Windows 7 Visitors	To verify Whether Repeated Windows 7 Visitors are Displayed in the CMX Connect and Engage UI or not	Passed	
WLJ80S_Visitor_26	Repeated Apple mac book Visitors	To verify Whether Repeated Apple mac book Visitors are Displayed in the CMX Connect and Engage UI or not	Passed	
WLJ80S_Visitor_27	Repeated Apple iphone Visitors	To verify Whether Repeated Apple iphone Visitors are Displayed in the CMX Connect and Engage UI or not	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_Visitor_28	Repeated Samsung s4 mobile Visitors	To verify Whether Repeated Samsung s4 mobile Visitors are Displayed in the CMX Connect and Engage UI or not	Passed	
WLJ80S_Visitor_29	Active Windows 7 Visitors	To verify Whether Active Windows 7 Visitors are Displayed in the CMX Connect and Engage UI or not	Passed	
WLJ80S_Visitor_30	Active Apple mac book Visitors	To verify Whether Active Apple mac book Visitors are Displayed in the CMX Connect and Engage UI or not	Passed	
WLJ80S_Visitor_31	Active Apple iphone Visitors	To verify Whether Active Apple iphone Visitors are Displayed in the CMX Connect and Engage UI or not	Passed	
WLJ80S_Visitor_32	Active Samsung s4 mobile Visitors	To verify Whether Active Samsung s4 mobile Visitors are Displayed in the CMX Connect and Engage UI or not	Passed	

Real-Path

Logical ID	Title	Description	Status	Defects
WLJ80S_MSE_RP_01	Real path configuration icons function for the selected floor	To verify whether all the real path configuration icons function for the selected floor	Passed	
WLJ80S_MSE_RP_02	Imports the path created	To verify whether can import the path created and saved	Passed	
WLJ80S_MSE_RP_03	Export the path outputs	To verify whether can export the path created	Failed	CSCuo53852
WLJ80S_MSE_RP_04	Clear function for the real path	To verify whether clear function is working fine	Passed	
WLJ80S_MSE_RP_05	Reload function for the real path with saved	To verify whether reload function is working fine when saved the real paths created	Passed	
WLJ80S_MSE_RP_06	Reload function for the real path without saved	To verify whether reload function is working fine without save the real paths created	Passed	

Zone Based Analytics

Logical ID	Title	Description	Status	Defects
WLJ80S_MSE_ZB_01	Zone-Based Analytics, Local AP L2 Roaming, Same floor	To verify whether Zone Based Analytics using Local APs with L2 roaming on the same floor able to roam and pass the traffic successfully	Passed	
WLJ80S_MSE_ZB_02	Zone-Based Analytics, Local AP L3 Roaming, Same floor	To verify whether Zone Based Analytics using Local APs with L3 roaming on the same floor able to roam and pass the traffic successfully	Passed	
WLJ80S_MSE_ZB_03	Zone-Based Analytics, Local AP L2 Roaming, Different floors	To verify whether Zone Based Analytics using Local APs with L2 roaming on the different floor able to roam and pass the traffic successfully	Passed	
WLJ80S_MSE_ZB_04	Zone-Based Analytics, Local AP L3 Roaming, Different floors	To verify whether Zone Based Analytics using Local APs with L3 roaming on the different floor able to roam and pass the traffic successfully	Passed	
WLJ80S_MSE_ZB_05	Zone-Based Analytics, Flex AP L2 Roaming, Same floor	To verify whether Zone Based Analytics using Flex APs with L2 roaming on same floor able to roam and pass the traffic successfully	Passed	
WLJ80S_MSE_ZB_06	Zone-Based Analytics, Flex AP L3 Roaming, Same floor	To verify whether Zone Based Analytics using Flex APs with L3 roaming on same floor able to roam and pass the traffic successfully	Passed	
WLJ80S_MSE_ZB_07	Zone-Based Analytics, Flex AP L2 Roaming, Different floor	To verify whether Zone Based Analytics using Flex APs with L2 roaming with different floor able to roam and pass the traffic successfully	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_MSE_ZB_08	Zone-Based Analytics, Flex AP L3 Roaming, Different floor	To verify whether Zone Based Analytics using Flex APs with L3 roaming with different floor able to roam and pass the traffic successfully	Passed	

CMX NAPP Store

Logical ID	Title	Description	Status	Defects
WLJ80S_NAPP_01	Checking MSE admin view UI	To verify all web apps and services are displayed in the MSE admin view or not	Passed	
WLJ80S_NAPP_02	Moving web app inside the MSE admin view UI	To verify whether web apps can be dragged and dropped in the MSE admin view UI	Passed	
WLJ80S_NAPP_03	Creating new folder in MSE admin view UI	To verify creation of new folder in CMX NAPP Store in virtual MSE is successful or not	Passed	
WLJ80S_NAPP_04	Search bar in CMX NAPP Store	To verify whether or not any particular web app is returned once after the search is completed successfully	Passed	
WLJ80S_NAPP_05	Updates in MSE admin view UI	To verify that all the updates are listed in the admin view or not	Passed	
WLJ80S_NAPP_06	What's New? App in MSE admin view UI	To verify whether What's New ? App is successfully launched	Passed	
WLJ80S_NAPP_07	Settings app in MSE admin view UI	To verify whether settings page is loaded successfully from the admin view UI of MSE or not	Passed	
WLJ80S_NAPP_08	Adding trap destination in settings app launched from MSE admin view UI	To verify whether trap destinations can be newly added from the settings app or not	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_NAPP_09	Downloading logs from settings app launched from MSE admin view UI	To verify whether logs is successfully downloaded from the settings app or not	Passed	
WLJ80S_NAPP_10	Creating a wish and sending feedback	To verify successful creation of a wish and sending feedback	Passed	

702 AP

Logical ID	Title	Description	Status	Defects
WLJ80S_702AP_01	Joining 702 AP to 2500 Controller	To verify whether 702 AP is joined or not with 2500 Controller	Passed	
WLJ80S_702AP_02	Associating a client to a WLC using 702 AP (Local Mode) with L2 Security - WEP using 2500	To verify whether client gets connected or not to a WLC using 702 AP with L2 Security - WEP using 2500	Passed	
WLJ80S_702AP_03	Associating a client to a WLC using 702 AP (Local Mode) with L2 Security - WPA+WPA2-PSK using 2500	To verify whether client gets connected or not to a WLC using 702 AP with L2 Security - WPA2+PSK using 2500	Passed	
WLJ80S_702AP_04	Associating a client to a WLC using 702 AP (Local Mode) with L2 Security -802.1x using 2500	To verify whether client gets connected or not to a WLC using 702 AP with L2 Security - 802.1x using 2500	Passed	
WLJ80S_702AP_05	Associating a client to a WLC using 702 AP (Flexconnect Mode) with L2 Security - WEP using 2500	To verify whether client gets connected or not to a WLC using 702 AP with L2 Security - WEP using 2500	Passed	

WLJ80S_702AP_06	Associating a client to a WLC using 702 AP (Flexconnect Mode) with L2 Security - WPA+WPA2-PSK using 2500	To verify whether client gets connected or not to a WLC using 702 AP with L2 Security - WPA2+PSK using 2500	Passed	
WLJ80S_702AP_07	Associating a client to a WLC using 702 AP (Flexconnect Mode) with L2 Security - 802.1x using 2500	To verify whether client gets connected or not to a WLC using 702 AP with L2 Security - 802.1x using 2500	Passed	
WLJ80S_702AP_08	Adding 702 AP in Flexconnect group and making it as AAA server for LEAP clients.	To verify whether 702 AP acts as AAA server or not for LEAP clients by enabling Local Authentication check box and LEAP check box in a Flex group.	Passed	
WLJ80S_702AP_09	Adding 702 AP in Flexconnect group and making it as AAA server for PEAP clients.	To verify whether 702 AP acts as AAA server or not for PEAP clients by enabling Local Authentication check box and LEAP check box in a Flex group.	Passed	
WLJ80S_702AP_10	HREAP fault tolerance between connected and standalone AP-2.4 GHz	To verify whether the client associated to flexconnect AP will get reassociated in case of fault tolerance	Passed	
WLJ80S_702AP_11	HREAP fault tolerance between standalone and connected AP-2.4 GHz	To verify whether the client associated to flexconnect AP will get reassociated in case of fault tolerance	Passed	

WLJ80S_702AP_12	HREAP fault tolerance between connected and standalone AP-2.4 GHz	To verify whether the client associated to flexconnect AP will get reassociated in case of fault tolerance	Passed	
WLJ80S_702AP_13	HREAP fault tolerance between standalone and connected AP-2.4 GHz	To verify whether the client associated to flexconnect AP will get reassociated in case of fault tolerance	Passed	
WLJ80S_702AP_14	11r Client Association with AKM PSK - FlexConnect Central Switch	To verify client's initial association to a wlan with 11r enabled with ft-psk AKM Suite in flexconnect central switching.	Passed	
WLJ80S_702AP_15	11r Client Association with AKM PSK - FlexConnect Local Switch Central Auth	Verify client's initial association to a wlan with 11r enabled with ft-psk AKM Suite in flexconnect local switch central auth.	Passed	
WLJ80S_702AP_16	Client association through Primary RADIUS server(ISE) at site level with L2 Security WPA2+Dot1x(PEAP)	To verify whether the Client authentication is done via Primary RADIUS server configured in flexconnect group	Passed	
WLJ80S_702AP_17	Client association through Secondary RADIUS server(ISE)at site level with L2 Security WPA2+Dot1x(PEAP)	To verify whether the Client authentication is done via Secondary RADIUS server configured in flexconnect group	Passed	
WLJ80S_702AP_18	Client association through Primary RADIUS server(ACS) at site level with L2 Security WPA2+Dot1x(PEAP)	To verify whether the Client authentication is done via Primary RADIUS server configured in flexconnect group	Passed	

WLJ80S_702AP_19	Client association through Secondary RADIUS server(ACS) at site level with L2 Security WPA+Dot1x(PEAP)	To verify whether the Client authentication is done via Secondary RADIUS server configured in flexconnect group	Passed	
WLJ80S_702AP_20	Associating client -L3 security "Web-Auth" using 2500	To check whether the client is associated successfullyor not into the network through Web-Auth using 2500	Passed	
WLJ80S_702AP_21	Authentication for the association of clients-WPA	Checking for the Authentication of the clients when connected to an AP using WPA+WPA2 security .	Passed	
WLJ80S_702AP_22	Authentication for the association of clients-802.1X	Checking for the Authentication of the clients when connected to an AP using 802.1X security.	Passed	
WLJ80S_702AP_23	Authentication for the association of clients-Static WEP	Checking for the Authentication of the clients when connected to an AP using Static WEP security.	Passed	
WLJ80S_702AP_24	Authentication for the association of clients- Static WEP+802.1X	Checking for the Authentication of the clients when connected to an AP using Static WEP+802.1X security.	Passed	
WLJ80S_702AP_25	Performing MAC Filtering with Clients registered in ACS server-WiSM2 Controller	To check whether registered client is successfully authenticated and associated with WLANS enabled MAC Filtering	Passed	

WLJ80S_702AP_26	Performing MAC Filtering with Clients registered in ACS server- 2500 Controller	To check whether registered client is successfully authenticated and associated with WLANS enabled MAC Filtering	Passed	
WLJ80S_702AP_27	Performing MAC Filtering with Clients registered in ACS server- 7500 Controller	To check whether registered client is successfully authenticated and associated with WLANS enabled MAC Filtering	Passed	
WLJ80S_702AP_28	Verify AVC rule to drop an application works fine	Apply an AVC profile with a rule to block an application and check if that application is dropped when tried to open and notification is send via snmp trap	Passed	
WLJ80S_702AP_29	AVC profile should work fine in AP SSO	To verify that after creating a new AVC profile works, it works fine in AP SSO using 5508	Passed	
WLJ80S_702AP_30	application traffic flow from client to AP when AP in local mode and centrally switched flexconnect - 5508,7500 &2500 WLC	To verify the Application traffic flow from client to AP when AP is in local mode and centrally switched flexconnect using the 5508, 7500 and 2500 controllers	Passed	
WLJ80S_702AP_31	Configuring and verifying custom DSCP value for AVC	To verify if custom DSCP value is configured and applied successfully for a AVC rule	Passed	

WLJ80S_702AP_32	Bandwidth contract Rate limit applied per-SSID on downstream traffic in 2500	To Verify if bandwidth contract applied per-SSID on downstream traffic works fine using a 2500 controller	Passed	
WLJ80S_702AP_33	Override Per-user bandwidth contract on downstream and upstream traffic	To verify if Override Per-user bandwidth contract on downstream and upstream traffic works fine	Passed	
WLJ80S_702AP_34	Authentication of client with Security Static WEP and Web-Auth -2500, 5508, WiSM2 and 7500 Controller.	Checking for the Authentication of the client when connected to a WLAN in which Static WEP and Web-Auth is enabled.	Passed	
WLJ80S_702AP_35	Authentication of client - Win 7 with Security Static WEP+Dot1x and Web-Auth using ISE-2500, 5508, WiSM2 and 7500 Controller.	Checking for the Authentication of the clients when connected to a WLAN in which Static WEP+Dot1x and Web-Auth is enabled.	Passed	
WLJ80S_702AP_36	Authentication of clients - Win 7 with Security Dot1x using ISE and Web-Auth-2500, 5508, WiSM2 and 7500 Controller.	Checking for the Authentication of the clients when connected to a WLAN in which Dot1x and Web-Auth is enabled.	Passed	
WLJ80S_702AP_37	Client Association with no security	To configure the radio interface and to check and Verify the client association with open security	Passed	
WLJ80S_702AP_38	Client Association with WEP	To check and verify the client association with the Security type as WEP	Passed	

WLJ80S_702AP_39	Client Association with WPA	To check and verify client association with the Security type as WPA	Passed	
WLJ80S_702AP_40	Verify WGB association	To Check and verify WGB association with root AP	Passed	
WLJ80S_702AP_41	Autonomous AP management access	To check and verify the Autonomous AP management access by http and telnet	Passed	
WLJ80S_702AP_42	Traffic flow between two wireless clients	To check and verify the Traffic flow between two wireless clients	Passed	
WLJ80S_702AP_43	Monitoring of connected client	To verify the connected client in AP management page	Passed	
WLJ80S_702AP_44	Trap logs for connected client	To check and verify the Trap Logs for connected client	Passed	
WLJ80S_702AP_45	Management users creation	To verify the management user creation	Passed	
WLJ80S_702AP_46	Enabling/Disabling the radio	To verify the radio enable/disable status	Passed	
WLJ80S_702AP_47	Client Association with TKIP	To check and verify client association with TKIP	Passed	
WLJ80S_702AP_48	Client Association with AES-CCMP	To check and verify client association with AES-CCMP	Passed	
WLJ80S_702AP_49	Client Association with TKIP +WEP	To check and verify client association with TKIP+WEP	Passed	
WLJ80S_702AP_50	Client Association with CKIP	To check and verify client association with CKIP	Passed	
WLJ80S_702AP_51	Client Association with Local radius server	To check and verify client association with local radius server	Passed	

WLJ80S_702AP_52	Transmit and Receive antenna	To check and verify Transmit and Receive antenna	Passed	
WLJ80S_702AP_53	Data rates change	Verify the client association after changing the data rates	Passed	
WLJ80S_702AP_54	CDP neighbor details	To verify the CDP neighbor details using show cdp	Passed	
WLJ80S_702AP_55	Client Association with no security	To check and verify client association with no/open security	Passed	
WLJ80S_702AP_56	Client Association with WEP	To check and verify client association with WEP	Passed	
WLJ80S_702AP_57	Client Association with WPA	To check and verify client association with WPA	Passed	
WLJ80S_702AP_58	WGB Mode	To check and verify WGB association with root AP	Passed	
WLJ80S_702AP_59	Autonomous AP management access	To check and verify the Autonomous AP management access by http and telnet	Passed	
WLJ80S_702AP_60	Traffic flow between two wireless clients	To check and verify the Traffic flow between two wireless clients	Passed	
WLJ80S_702AP_61	Monitoring of connected client	To verify the monitoring option of connected client in AP management page	Passed	
WLJ80S_702AP_62	Trap logs for connected client	To check and verify the Trap Logs for connected client	Passed	

WLJ80S_702AP_63	RF profile DCA list-GUI	To Configure few channels on Global DCA list. Try to configure a channel on RF profile DCA list which is not part of Global list via the GUI. Verify GUI throws error	Passed	
WLJ80S_702AP_64	RF profile DCA list-CLI	To Configure few channels on Global DCA list. Try to configure a channel on RF profile DCA list which is not part of Global list via the CLI. Verify CLI throws error	Passed	
WLJ80S_702AP_65	Show CLI command related to RF profile for DCA feature	To Verify the CLI - "show rf-profile details <RF-Profile>", shows parameters configured for DCA and Threshold for traps.	Passed	
WLJ80S_702AP_66	Upload/Download of the Config and check for Channel width parameter on DCA RF profile	To Verify Config is successfully uploaded and CW is seen as 20 MHz. Change the channel width to 40 Mhz on the uploaded config. Download the changed config and verify CW on RF profile is set to 40 MHz	Passed	
WLJ80S_702AP_67	Configure RF profile DCA parameters via the CLI	To Configure various RF profile DCA parameters via the CLI and verify configs are successful	Passed	

WLJ80S_702AP_68	Upload/Download of the Config and check for Avoid Foreign AP interference parameter on DCA RF profile	Verify Config is successfully uploaded and Avoid Foreign AP interference is seen as enabled.	Passed	
WLJ80S_702AP_69	Upload/Download of the Config and check for threshold trap values on RF profile	To Verify config is successfully uploaded. Change few threshold values on uploaded config. Download the config and verify the changed values	Passed	
WLJ80S_702AP_70	RF profile, threshold for traps via the GUI	To Configure various threshold for traps via the GUI and verify configs are successful	Passed	
WLJ80S_702AP_71	RF profile DCA parameters via the CLI	To Configure various RF profile DCA parameters via the CLI and verify configs are successful	Passed	
WLJ80S_702AP_72	RF profile DCA parameters via the GUI	To verify Configure various RF profile DCA parameters via the GUI and verify configs are successful	Passed	
WLJ80S_702AP_73	RF profile, threshold for traps via the CLI	To verify Configure various threshold for traps via the CLI and verify configs are successful	Passed	
WLJ80S_702AP_74	RF profile, threshold for traps via the GUI	To verify Configure various threshold for traps via the GUI and verify configs are successful	Passed	

WLJ80S_702AP_75	Controller should retain the config across controller reset	Configure DCA and threshold for traps on RF profile. Reset the Controller and verify the configs are retained	Passed	
WLJ80S_702AP_76	Joining 702 AP to 5500 Controller	To verify whether 702 AP is joined or not with 5500 Controller	Passed	
WLJ80S_702AP_77	Joining 702 AP to 7500 Controller	To verify whether 702 AP is joined or not with 7500 Controller	Passed	
WLJ80S_702AP_78	Joining 702 AP to 8500 Controller	To verify whether 702 AP is joined or not with 8500 Controller	Passed	
WLJ80S_702AP_79	Joining 702 AP to WiSM2 Controller	To verify whether 702 AP is joined or not with WiSM2 Controller	Passed	
WLJ80S_702AP_80	Associating a client to a WLC using 702 AP (Local Mode) with L2 Security - WEP using 5500	To verify whether client gets connected or not to a WLC using 702 AP with L2 Security - WEP using 5500	Passed	
WLJ80S_702AP_81	Associating a client to a WLC using 702 AP (Local Mode) with L2 Security - WEP using 7500	To verify whether client gets connected or not to a WLC using 702 AP with L2 Security - WEP using 7500	Passed	
WLJ80S_702AP_82	Associating a client to a WLC using 702 AP (Local Mode) with L2 Security - WEP using 8500	To verify whether client gets connected or not to a WLC using 702 AP with L2 Security - WEP using 8500	Passed	

WLJ80S_702AP_83	Associating a client to a WLC using 702 AP (Local Mode) with L2 Security - WEP using WISM2	To verify whether client gets connected or not to a WLC using 702 AP with L2 Security - WEP using WISM2	Passed	
WLJ80S_702AP_84	Associating a client to a WLC using 702 AP (Local Mode) with L2 Security - WPA+WPA2-PSK using 5500	To verify whether client gets connected or not to a WLC using 702 AP with L2 Security - WPA2+PSK using 5500	Passed	
WLJ80S_702AP_85	Associating a client to a WLC using 702 AP (Local Mode) with L2 Security - WPA+WPA2-PSK using 7500	To verify whether client gets connected or not to a WLC using 702 AP with L2 Security - WPA2+PSK using 7500	Passed	
WLJ80S_702AP_86	Associating a client to a WLC using 702 AP (Local Mode) with L2 Security - WPA+WPA2-PSK using 8500	To verify whether client gets connected or not to a WLC using 702 AP with L2 Security - WPA2+PSK using 8500	Passed	
WLJ80S_702AP_87	Associating a client to a WLC using 702 AP (Local Mode) with L2 Security - WPA+WPA2-PSK using WISM2	To verify whether client gets connected or not to a WLC using 702 AP with L2 Security - WPA2+PSK using WISM2	Passed	
WLJ80S_702AP_88	Associating a client to a WLC using 702 AP (Local Mode) with L2 Security -802.1x using 5500	To verify whether client gets connected or not to a WLC using 702 AP with L2 Security - 802.1x using 5500	Passed	
WLJ80S_702AP_89	Associating a client to a WLC using 702 AP (Local Mode) with L2 Security -802.1x using 7500	To verify whether client gets connected or not to a WLC using 702 AP with L2 Security - 802.1x using 7500	Passed	

WLJ80S_702AP_90	Associating a client to a WLC using 702 AP (Local Mode) with L2 Security -802.1x using 8500	To verify whether client gets connected or not to a WLC using 702 AP with L2 Security - 802.1x using 8500	Passed	
WLJ80S_702AP_91	Associating a client to a WLC using 702 AP (Local Mode) with L2 Security -802.1x using WISM2	To verify whether client gets connected or not to a WLC using 702 AP with L2 Security - 802.1x using WISM2	Passed	
WLJ80S_702AP_92	Associating a client to a WLC using 702 AP (Flexconnect Mode) with L2 Security - WEP using 5500	To verify whether client gets connected or not to a WLC using 702 AP with L2 Security - WEP using 5500	Passed	
WLJ80S_702AP_93	Associating a client to a WLC using 702 AP (Flexconnect Mode) with L2 Security - WEP using 7500	To verify whether client gets connected or not to a WLC using 702 AP with L2 Security - WEP using 7500	Passed	
WLJ80S_702AP_94	Associating a client to a WLC using 702 AP (Flexconnect Mode) with L2 Security - WEP using 8500	To verify whether client gets connected or not to a WLC using 702 AP with L2 Security - WEP using 8500	Passed	
WLJ80S_702AP_95	Associating a client to a WLC using 702 AP (Flexconnect Mode) with L2 Security - WEP using WISM2	To verify whether client gets connected or not to a WLC using 702 AP with L2 Security - WEP using WISM2	Passed	
WLJ80S_702AP_96	Associating a client to a WLC using 702 AP (Flexconnect Mode) with L2 Security - WPA+WPA2-PSK using 5500	To verify whether client gets connected or not to a WLC using 702 AP with L2 Security - WPA2+PSK using 5500	Passed	

WLJ80S_702AP_97	Associating a client to a WLC using 702 AP (Flexconnect Mode) with L2 Security - WPA+WPA2-PSK using 7500	To verify whether client gets connected or not to a WLC using 702 AP with L2 Security - WPA2+PSK using 7500	Passed	
WLJ80S_702AP_98	Associating a client to a WLC using 702 AP (Flexconnect Mode) with L2 Security - WPA+WPA2-PSK using 8500	To verify whether client gets connected or not to a WLC using 702 AP with L2 Security - WPA2+PSK using 8500	Passed	
WLJ80S_702AP_99	Associating a client to a WLC using 702 AP (Flexconnect Mode) with L2 Security - WPA+WPA2-PSK using WISM2	To verify whether client gets connected or not to a WLC using 702 AP with L2 Security - WPA2+PSK using WISM2	Passed	
WLJ80S_702AP_100	Associating a client to a WLC using 702 AP (Flexconnect Mode) with L2 Security - 802.1x using 5500	To verify whether client gets connected or not to a WLC using 702 AP with L2 Security - 802.1x using 5500	Passed	
WLJ80S_702AP_101	Associating a client to a WLC using 702 AP (Flexconnect Mode) with L2 Security - 802.1x using 7500	To verify whether client gets connected or not to a WLC using 702 AP with L2 Security - 802.1x using 7500	Passed	
WLJ80S_702AP_102	Associating a client to a WLC using 702 AP (Flexconnect Mode) with L2 Security - 802.1x using 8500	To verify whether client gets connected or not to a WLC using 702 AP with L2 Security - 802.1x using 8500	Passed	
WLJ80S_702AP_103	Associating a client to a WLC using 702 AP (Flexconnect Mode) with L2 Security - 802.1x using WISM2	To verify whether client gets connected or not to a WLC using 702 AP with L2 Security - 802.1x using WISM2	Passed	

WLJ80S_702AP_104	Associating client -L3 security "Web-Auth" using 5500	To check whether the client is associated successfully or not into the network through Web-Auth using 5500	Passed	
WLJ80S_702AP_105	Associating client -L3 security "Web-Auth" using 7500	To check whether the client is associated successfully or not into the network through Web-Auth using 7500	Passed	
WLJ80S_702AP_106	Associating client -L3 security "Web-Auth" using 8500	To check whether the client is associated successfully or not into the network through Web-Auth using 8500	Passed	
WLJ80S_702AP_107	Associating client -L3 security "Web-Auth" using WISM2	To check whether the client is associated successfully or not into the network through Web-Auth using WISM2	Passed	
WLJ80S_702AP_108	Apply an AVC profile with a rule to block an application and check if that application is dropped when tried to open using 2500	To verify AVC rule to drop an application works fine in 2500	Passed	
WLJ80S_702AP_109	Apply an AVC profile with a rule to block an application and check if that application is dropped when tried to open using 5500	To verify AVC rule to drop an application works fine in 5500	Passed	

WLJ80S_702AP_110	Apply an AVC profile with a rule to block an application and check if that application is dropped when tried to open using 7500	To verify AVC rule to drop an application works fine in 7500	Passed	
WLJ80S_702AP_111	Apply an AVC profile with a rule to block an application and check if that application is dropped when tried to open using 8500	To verify AVC rule to drop an application works fine in 8500	Passed	
WLJ80S_702AP_112	Apply an AVC profile with a rule to block an application and check if that application is dropped when tried to open using WISM2	To verify AVC rule to drop an application works fine in WISM2	Passed	
WLJ80S_702AP_113	Apply an AVC profile with a rule to mark an application and check if that application is marked when tried to open using WISM2	To verify AVC rule to mark an application works fine in WISM2	Passed	
WLJ80S_702AP_114	Apply an AVC profile with a rule to mark an application and check if that application is marked when tried to open using 2500	To verify AVC rule to mark an application works fine in 2500	Passed	
WLJ80S_702AP_115	Apply an AVC profile with a rule to mark an application and check if that application is marked when tried to open using 5500	To verify AVC rule to mark an application works fine in 5500	Passed	

WLJ80S_702AP_116	Apply an AVC profile with a rule to mark an application and check if that application is marked when tried to open using 7500	To verify AVC rule to mark an application works fine in 7500	Passed	
WLJ80S_702AP_117	Apply an AVC profile with a rule to mark an application and check if that application is marked when tried to open using 8500	To verify AVC rule to mark an application works fine in 8500	Passed	
WLJ80S_702AP_118	Bandwidth contract Rate limit applied per-SSID on downstream traffic in 5500	To Verify if bandwidth contract applied per-SSID on downstream traffic works fine	Passed	
WLJ80S_702AP_119	Bandwidth contract Rate limit applied per-SSID on downstream traffic in 7500	To Verify if bandwidth contract applied per-SSID on downstream traffic works fine	Passed	
WLJ80S_702AP_120	Bandwidth contract Rate limit applied per-SSID on downstream traffic in 8500	To Verify if bandwidth contract applied per-SSID on downstream traffic works fine	Passed	

2700 AP

Logical ID	Title	Description	Status	Defects
WLJ80S_2700AP_01	Joining 2700 AP to 2500 Controller	To verify whether 2700 AP is joined or not with 2500 Controller.	Passed	
WLJ80S_2700AP_02	Associating a client to a WLC using 2700 AP (Local Mode) with L2 Security - WEP using 2500	To verify whether client gets connected or not to a WLC using 2700 AP with L2 Security - WEP using 2500	Passed	

WLJ80S_2700AP_03	Associating a client to a WLC using 2700 AP (Local Mode) with L2 Security - WPA+WPA2-PSK using 2500	To verify whether client gets connected or not to a WLC using 2700 AP with L2 Security - WPA2+PSK using 2500	Passed	
WLJ80S_2700AP_04	Associating a client to a WLC using 2700 AP (Local Mode) with L2 Security -802.1x using 2500	To verify whether client gets connected or not to a WLC using 2700 AP with L2 Security - 802.1x using 2500	Passed	
WLJ80S_2700AP_05	Associating a client to a WLC using 2700 AP (Flexconnect Mode) with L2 Security - WEP using 2500	To verify whether client gets connected or not to a WLC using 2700 AP with L2 Security - WEP using 2500	Passed	
WLJ80S_2700AP_06	Associating a client to a WLC using 2700 AP (Flexconnect Mode) with L2 Security - WPA+WPA2-PSK using 2500	To verify whether client gets connected or not to a WLC using 2700 AP with L2 Security - WPA2+PSK using 2500	Passed	
WLJ80S_2700AP_07	Associating a client to a WLC using 2700 AP (Flexconnect Mode) with L2 Security - 802.1x using 2500	To verify whether client gets connected or not to a WLC using 2700 AP with L2 Security - 802.1x using 2500	Passed	
WLJ80S_2700AP_08	Adding 2700 AP in Flexconnect group and making it as AAA server for LEAP clients.	To verify whether 2700 AP acts as AAA server or not for LEAP clients by enabling Local Authentication check box and LEAP check box in a Flex group.	Passed	

WLJ80S_2700AP_09	Adding 2700 AP in Flexconnect group and making it as AAA server for PEAP clients.	To verify whether 2700 AP acts as AAA server or not for PEAP clients by enabling Local Authentication check box and LEAP check box in a Flex group.	Passed	
WLJ80S_2700AP_10	HREAP fault tolerance between connected and standalone AP-2.4 GHz	To verify whether the client associated to flexconnect AP will get reassociated in case of fault tolerance	Passed	
WLJ80S_2700AP_11	HREAP fault tolerance between standalone and connected AP-2.4 GHz	To verify whether the client associated to flexconnect AP will get reassociated in case of fault tolerance	Passed	
WLJ80S_2700AP_12	HREAP fault tolerance between connected and standalone AP-2.4 GHz	To verify whether the client associated to flexconnect AP will get reassociated in case of fault tolerance	Passed	
WLJ80S_2700AP_13	HREAP fault tolerance between standalone and connected AP-2.4 GHz	To verify whether the client associated to flexconnect AP will get reassociated in case of fault tolerance	Passed	
WLJ80S_2700AP_14	11r Client Association with AKM PSK - FlexConnect Central Switch	To verify client's initial association to a wlan with 11r enabled with ft-psk AKM Suite in flexconnect central switching.	Passed	
WLJ80S_2700AP_15	11r Client Association with AKM PSK - FlexConnect Local Switch Central Auth	Verify client's initial association to a wlan with 11r enabled with ft-psk AKM Suite in flexconnect local switch central auth.	Passed	

WLJ80S_2700AP_16	Client association through Primary RADIUS server(ISE) at site level with L2 Security WPA2+Dot1x(PEAP)	To verify whether the Client authentication is done via Primary RADIUS server configured in flexconnect group	Passed	
WLJ80S_2700AP_17	Client association through Secondary RADIUS server(ISE)at site level with L2 Security WPA2+Dot1x(PEAP)	To verify whether the Client authentication is done via Secondary RADIUS server configured in flexconnect group	Passed	
WLJ80S_2700AP_18	Client association through Primary RADIUS server(ACS) at site level with L2 Security WPA2+Dot1x(PEAP)	To verify whether the Client authentication is done via Primary RADIUS server configured in flexconnect group	Passed	
WLJ80S_2700AP_19	Client association through Secondary RADIUS server(ACS) at site level with L2 Security WPA+Dot1x(PEAP)	To verify whether the Client authentication is done via Secondary RADIUS server configured in flexconnect group	Passed	
WLJ80S_2700AP_20	Associating client -L3 security "Web-Auth" using 2500	To check whether the client is associated successfullyor not into the network through Web-Auth using 2500	Passed	
WLJ80S_2700AP_21	Authentication for the association of clients-WPA	Checking for the Authentication of the clients when connected to an AP using WPA+WPA2 security .	Passed	
WLJ80S_2700AP_22	Authentication for the association of clients-802.1X	Checking for the Authentication of the clients when connected to an AP using 802.1X security.	Passed	

WLJ80S_2700AP_23	Authentication for the association of clients-Static WEP	Checking for the Authentication of the clients when connected to an AP using Static WEP security.	Passed	
WLJ80S_2700AP_24	Authentication for the association of clients- Static WEP+802.1X	Checking for the Authentication of the clients when connected to an AP using Static WEP+802.1X security.	Passed	
WLJ80S_2700AP_25	Performing MAC Filtering with Clients registered in ACS server- WiSM2 Controller	To check whether registered client is successfully authenticated and associated with WLANS enabled MAC Filtering	Passed	
WLJ80S_2700AP_26	Performing MAC Filtering with Clients registered in ACS server- 2500 Controller	To check whether registered client is successfully authenticated and associated with WLANS enabled MAC Filtering	Passed	
WLJ80S_2700AP_27	Performing MAC Filtering with Clients registered in ACS server- 7500 Controller	To check whether registered client is successfully authenticated and associated with WLANS enabled MAC Filtering	Passed	
WLJ80S_2700AP_28	Verify AVC rule to drop an application works fine	Apply an AVC profile with a rule to block an application and check if that application is dropped when tried to open and notification is send via snmp trap	Passed	

WLJ80S_2700AP_29	AVC profile should work fine in AP SSO	To verify that after creating a new AVC profile works, it works fine in AP SSO using 5508	Passed	
WLJ80S_2700AP_30	application traffic flow from client to AP when AP in local mode and centrally switched flexconnect - 5508,7500 &2500 WLC	To verify the Application traffic flow from client to AP when AP is in local mode and centrally switched flexconnect using the 5508, 7500 and 2500 controllers	Passed	
WLJ80S_2700AP_31	Configuring and verifying custom DSCP value for AVC	To verify if custom DSCP value is configured and applied successfully for a AVC rule	Passed	
WLJ80S_2700AP_32	Bandwidth contract Rate limit applied per-SSID on downstream traffic in 2500	To Verify if bandwidth contract applied per-SSID on downstream traffic works fine using a 2500 controller	Passed	
WLJ80S_2700AP_33	Override Per-user bandwidth contract on downstream and upstream traffic	To verify if Override Per-user bandwidth contract on downstream and upstream traffic works fine	Passed	
WLJ80S_2700AP_34	Authentication of client with Security Static WEP and Web-Auth -2500,5508, WiSM2 and 7500 Controller.	Checking for the Authentication of the client when connected to a WLAN in which Static WEP and Web-Auth is enabled.	Passed	
WLJ80S_2700AP_35	Authentication of client - Win 7 with Security Static WEP+Dot1x and Web-Auth using ISE-2500, 5508, WiSM2 and 7500 Controller.	Checking for the Authentication of the clients when connected to a WLAN in which Static WEP+Dot1x and Web-Auth is enabled.	Passed	

WLJ80S_2700AP_36	Authentication of client - Win 7 with Security Dot1x using ISE and Web-Auth -2500, 5508, WiSM2 and 7500 Controller.	Checking for the Authentication of the clients when connected to a WLAN in which Dot1x and Web-Auth is enabled.	Passed	
WLJ80S_2700AP_37	Client Association with no security	To configure the radio interface and to check and Verify the client association with open security	Passed	
WLJ80S_2700AP_38	Client Association with WEP	To check and verify the client association with the Security type as WEP	Passed	
WLJ80S_2700AP_39	Client Association with WPA	To check and verify client association with the Security type as WPA	Passed	
WLJ80S_2700AP_40	Verify WGB association	To Check and verify WGB association with root AP	Passed	
WLJ80S_2700AP_41	Autonomous AP management access	To check and verify the Autonomous AP management access by http and telnet	Passed	
WLJ80S_2700AP_42	Traffic flow between two wireless clients	To check and verify the Traffic flow between two wireless clients	Passed	
WLJ80S_2700AP_43	Monitoring of connected client	To verify the connected client in AP management page	Passed	
WLJ80S_2700AP_44	Trap logs for connected client	To check and verify the Trap Logs for connected client	Passed	
WLJ80S_2700AP_45	Management users	To verify the management user creation	Passed	

WLJ80S_2700AP_46	Enabling/Disabling the radio	To verify the radio enable/disable status	Passed	
WLJ80S_2700AP_47	Client Association with TKIP	To check and verify client association with TKIP	Passed	
WLJ80S_2700AP_48	Client Association with AES-CCMP	To check and verify client association with AES-CCMP	Passed	
WLJ80S_2700AP_49	Client Association with TKIP +WEP	To check and verify client association with TKIP+WEP	Passed	
WLJ80S_2700AP_50	Client Association with CKIP	To check and verify client association with CKIP	Passed	
WLJ80S_2700AP_51	Client Association with Local radius server	To check and verify client association with local radius server	Passed	
WLJ80S_2700AP_52	Transmit and Receive antenna	To check and verify Transmit and Receive antenna	Passed	
WLJ80S_2700AP_53	Data rates change	Verify the client association after changing the data rates	Passed	
WLJ80S_2700AP_54	CDP neighbor details	To verify the CDP neighbor details using show cdp	Passed	
WLJ80S_2700AP_55	Client Association with no security	To check and verify client association with no/open security	Passed	
WLJ80S_2700AP_56	Client Association with WEP	To check and verify client association with WEP	Passed	
WLJ80S_2700AP_57	Client Association with WPA	To check and verify client association with WPA	Passed	
WLJ80S_2700AP_58	WGB Mode	To check and verify WGB association with root AP	Passed	

WLJ80S_2700AP_59	Autonomous AP management access	To check and verify the Autonomous AP management access by http and telnet	Passed	
WLJ80S_2700AP_60	Traffic flow between two wireless clients	To check and verify the Traffic flow between two wireless clients	Passed	
WLJ80S_2700AP_61	Monitoring of connected client	To verify the monitoring option of connected client in AP management page	Passed	
WLJ80S_2700AP_62	Trap logs for connected client	To check and verify the Trap Logs for connected client	Passed	
WLJ80S_2700AP_63	RF profile DCA list-GUI	To Configure few channels on Global DCA list. Try to configure a channel on RF profile DCA list which is not part of Global list via the GUI. Verify GUI throws error	Passed	
WLJ80S_2700AP_64	RF profile DCA list-CLI	To Configure few channels on Global DCA list. Try to configure a channel on RF profile DCA list which is not part of Global list via the CLI. Verify CLI throws error	Passed	
WLJ80S_2700AP_65	Show CLI command related to RF profile for DCA feature	To Verify the CLI - "show rf-profile details <RF-Profile>", shows parameters configured for DCA and Threshold for traps.	Passed	

WLJ80S_2700AP_66	Upload/Download of the Config and check for Channel width parameter on DCA RF profile	To Verify Config is successfully uploaded and CW is seen as 20 MHz. Change the channel width to 40 Mhz on the uploaded config. Download the changed config and verify CW on RF profile is set to 40 MHz	Passed	
WLJ80S_2700AP_67	Configure RF profile DCA parameters via the CLI	To Configure various RF profile DCA parameters via the CLI and verify configs are successful	Passed	
WLJ80S_2700AP_68	Upload/Download of the Config and check for Avoid Foreign AP interference parameter on DCA RF profile	Verify Config is successfully uploaded and Avoid Foreign AP interference is seen as enabled.	Passed	
WLJ80S_2700AP_69	Upload/Download of the Config and check for threshold trap values on RF profile	To Verify config is successfully uploaded. Change few threshold values on uploaded config. Download the config and verify the changed values	Passed	
WLJ80S_2700AP_70	RF profile, threshold for traps via the GUI	To Configure various threshold for traps via the GUI and verify configs are successful	Passed	
WLJ80S_2700AP_71	RF profile DCA parameters via the CLI	To Configure various RF profile DCA parameters via the CLI and verify configs are successful	Passed	

WLJ80S_2700AP_72	RF profile DCA parameters via the GUI	To verify Configure various RF profile DCA parameters via the GUI and verify configs are successful	Passed	
WLJ80S_2700AP_73	RF profile, threshold for traps via the CLI	To verify Configure various threshold for traps via the CLI and verify configs are successful	Passed	
WLJ80S_2700AP_74	RF profile, threshold for traps via the GUI	To verify Configure various threshold for traps via the GUI and verify configs are successful	Passed	
WLJ80S_2700AP_75	Controller should retain the config across controller reset	Configure DCA and threshold for traps on RF profile. Reset the Controller and verify the configs are retained	Passed	
WLJ80S_2700AP_76	Joining 2700 AP to 5500 Controller	To verify whether 2700 AP is joined or not with 5500 Controller	Passed	
WLJ80S_2700AP_77	Joining 2700 AP to 7500 Controller	To verify whether 2700 AP is joined or not with 7500 Controller	Passed	
WLJ80S_2700AP_78	Joining 2700 AP to 8500 Controller	To verify whether 2700 AP is joined or not with 8500 Controller	Passed	
WLJ80S_2700AP_79	Joining 2700 AP to WiSM2 Controller	To verify whether 2700 AP is joined or not with WiSM2 Controller	Passed	
WLJ80S_2700AP_80	Associating a client to a WLC using 2700 AP (Local Mode) with L2 Security - WEP using 5500	To verify whether client gets connected or not to a WLC using 2700 AP with L2 Security - WEP using 5500	Passed	

WLJ80S_2700AP_81	Associating a client to a WLC using 2700 AP (Local Mode) with L2 Security - WEP using 7500	To verify whether client gets connected or not to a WLC using 2700 AP with L2 Security - WEP using 7500	Passed	
WLJ80S_2700AP_82	Associating a client to a WLC using 2700 AP (Local Mode) with L2 Security - WEP using 8500	To verify whether client gets connected or not to a WLC using 2700 AP with L2 Security - WEP using 8500	Passed	
WLJ80S_2700AP_83	Associating a client to a WLC using 2700 AP (Local Mode) with L2 Security - WEP using WISM2	To verify whether client gets connected or not to a WLC using 2700 AP with L2 Security - WEP using WISM2	Passed	
WLJ80S_2700AP_84	Associating a client to a WLC using 2700 AP (Local Mode) with L2 Security - WPA+WPA2-PSK using 5500	To verify whether client gets connected or not to a WLC using 2700 AP with L2 Security - WPA2+PSK using 5500	Passed	
WLJ80S_2700AP_85	Associating a client to a WLC using 2700 AP (Local Mode) with L2 Security - WPA+WPA2-PSK using 7500	To verify whether client gets connected or not to a WLC using 2700 AP with L2 Security - WPA2+PSK using 7500	Passed	
WLJ80S_2700AP_86	Associating a client to a WLC using 2700 AP (Local Mode) with L2 Security - WPA+WPA2-PSK using 8500	To verify whether client gets connected or not to a WLC using 2700 AP with L2 Security - WPA2+PSK using 8500	Passed	
WLJ80S_2700AP_87	Associating a client to a WLC using 2700 AP (Local Mode) with L2 Security - WPA+WPA2-PSK using WISM2	To verify whether client gets connected or not to a WLC using 2700 AP with L2 Security - WPA2+PSK using WISM2	Passed	

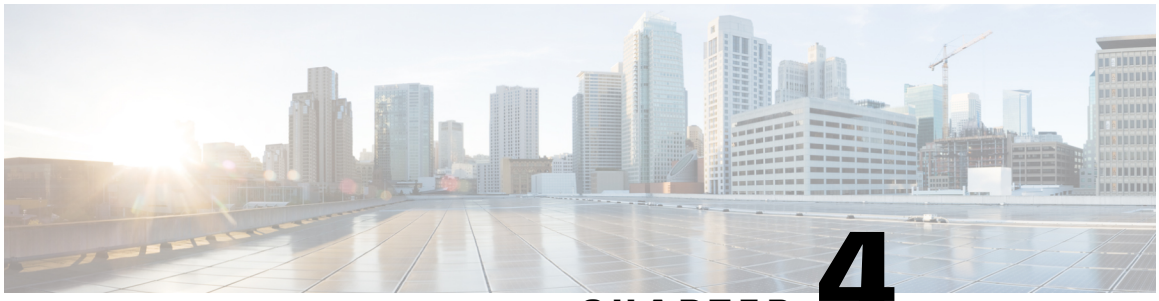
WLJ80S_2700AP_88	Associating a client to a WLC using 2700 AP (Local Mode) with L2 Security -802.1x using 5500	To verify whether client gets connected or not to a WLC using 2700 AP with L2 Security - 802.1x using 5500	Passed	
WLJ80S_2700AP_89	Associating a client to a WLC using 2700 AP (Local Mode) with L2 Security -802.1x using 7500	To verify whether client gets connected or not to a WLC using 2700 AP with L2 Security - 802.1x using 7500	Passed	
WLJ80S_2700AP_90	Associating a client to a WLC using 2700 AP (Local Mode) with L2 Security -802.1x using 8500	To verify whether client gets connected or not to a WLC using 2700 AP with L2 Security - 802.1x using 8500	Passed	
WLJ80S_2700AP_91	Associating a client to a WLC using 2700 AP (Local Mode) with L2 Security -802.1x using WISM2	To verify whether client gets connected or not to a WLC using 2700 AP with L2 Security - 802.1x using WISM2	Passed	
WLJ80S_2700AP_92	Associating a client to a WLC using 2700 AP (Flexconnect Mode) with L2 Security - WEP using 5500	To verify whether client gets connected or not to a WLC using 2700 AP with L2 Security - WEP using 5500	Passed	
WLJ80S_2700AP_93	Associating a client to a WLC using 2700 AP (Flexconnect Mode) with L2 Security - WEP using 7500	To verify whether client gets connected or not to a WLC using 2700 AP with L2 Security - WEP using 7500	Passed	
WLJ80S_2700AP_94	Associating a client to a WLC using 2700 AP (Flexconnect Mode) with L2 Security - WEP using 8500	To verify whether client gets connected or not to a WLC using 2700 AP with L2 Security - WEP using 8500	Passed	

WLJ80S_2700AP_95	Associating a client to a WLC using 2700 AP (Flexconnect Mode) with L2 Security - WEP using WISM2	To verify whether client gets connected or not to a WLC using 2700 AP with L2 Security - WEP using WISM2	Passed	
WLJ80S_2700AP_96	Associating a client to a WLC using 2700 AP (Flexconnect Mode) with L2 Security - WPA+WPA2-PSK using 5500	To verify whether client gets connected or not to a WLC using 2700 AP with L2 Security - WPA2+PSK using 5500	Passed	
WLJ80S_2700AP_97	Associating a client to a WLC using 2700 AP (Flexconnect Mode) with L2 Security - WPA+WPA2-PSK using 7500	To verify whether client gets connected or not to a WLC using 2700 AP with L2 Security - WPA2+PSK using 7500	Passed	
WLJ80S_2700AP_98	Associating a client to a WLC using 2700 AP (Flexconnect Mode) with L2 Security - WPA+WPA2-PSK using 8500	To verify whether client gets connected or not to a WLC using 2700 AP with L2 Security - WPA2+PSK using 8500	Passed	
WLJ80S_2700AP_99	Associating a client to a WLC using 2700 AP (Flexconnect Mode) with L2 Security - WPA+WPA2-PSK using WISM2	To verify whether client gets connected or not to a WLC using 2700 AP with L2 Security - WPA2+PSK using WISM2	Passed	
WLJ80S_2700AP_100	Associating a client to a WLC using 2700 AP (Flexconnect Mode) with L2 Security - 802.1x using 5500	To verify whether client gets connected or not to a WLC using 2700 AP with L2 Security - 802.1x using 5500	Passed	
WLJ80S_2700AP_101	Associating a client to a WLC using 2700 AP (Flexconnect Mode) with L2 Security - 802.1x using 7500	To verify whether client gets connected or not to a WLC using 2700 AP with L2 Security - 802.1x using 7500	Passed	

WLJ80S_2700AP_102	Associating a client to a WLC using 2700 AP (Flexconnect Mode) with L2 Security - 802.1x using 8500	To verify whether client gets connected or not to a WLC using 2700 AP with L2 Security - 802.1x using 8500	Passed	
WLJ80S_2700AP_103	Associating a client to a WLC using 2700 AP (Flexconnect Mode) with L2 Security - 802.1x using WISM2	To verify whether client gets connected or not to a WLC using 2700 AP with L2 Security - 802.1x using WISM2	Passed	
WLJ80S_2700AP_104	Associating client -L3 security "Web-Auth" using 5500	To check whether the client is associated successfully or not into the network through Web-Auth using 5500	Passed	
WLJ80S_2700AP_105	Associating client -L3 security "Web-Auth" using 7500	To check whether the client is associated successfully or not into the network through Web-Auth using 7500	Passed	
WLJ80S_2700AP_106	Associating client -L3 security "Web-Auth" using 8500	To check whether the client is associated successfully or not into the network through Web-Auth using 8500	Passed	
WLJ80S_2700AP_107	Associating client -L3 security "Web-Auth" using WISM2	To check whether the client is associated successfully or not into the network through Web-Auth using WISM2	Passed	

WLJ80S_2700AP_108	Apply an AVC profile with a rule to block an application and check if that application is dropped when tried to open using 2500	To verify AVC rule to drop an application works fine in 2500	Passed	
WLJ80S_2700AP_109	Apply an AVC profile with a rule to block an application and check if that application is dropped when tried to open using 5500	To verify AVC rule to drop an application works fine in 5500	Passed	
WLJ80S_2700AP_110	Apply an AVC profile with a rule to block an application and check if that application is dropped when tried to open using 7500	To verify AVC rule to drop an application works fine in 7500	Passed	
WLJ80S_2700AP_111	Apply an AVC profile with a rule to block an application and check if that application is dropped when tried to open using 8500	To verify AVC rule to drop an application works fine in 8500	Passed	
WLJ80S_2700AP_112	Apply an AVC profile with a rule to block an application and check if that application is dropped when tried to open using WISM2	To verify AVC rule to drop an application works fine in WISM2	Passed	
WLJ80S_2700AP_113	Apply an AVC profile with a rule to mark an application and check if that application is marked when tried to open using WISM2	To verify AVC rule to mark an application works fine in WISM2	Passed	

WLJ80S_2700AP_114	Apply an AVC profile with a rule to mark an application and check if that application is marked when tried to open using 2500	To verify AVC rule to mark an application works fine in 2500	Passed	
WLJ80S_2700AP_115	Apply an AVC profile with a rule to mark an application and check if that application is marked when tried to open using 5500	To verify AVC rule to mark an application works fine in 5500	Passed	
WLJ80S_2700AP_116	Apply an AVC profile with a rule to mark an application and check if that application is marked when tried to open using 7500	To verify AVC rule to mark an application works fine in 7500	Passed	
WLJ80S_2700AP_117	Apply an AVC profile with a rule to mark an application and check if that application is marked when tried to open using 8500	To verify AVC rule to mark an application works fine in 8500	Passed	
WLJ80S_2700AP_118	Bandwidth contract Rate limit applied per-SSID on downstream traffic in 5500	To Verify if bandwidth contract applied per-SSID on downstream traffic works fine	Passed	
WLJ80S_2700AP_119	Bandwidth contract Rate limit applied per-SSID on downstream traffic in 7500	To Verify if bandwidth contract applied per-SSID on downstream traffic works fine	Passed	
WLJ80S_2700AP_120	Bandwidth contract Rate limit applied per-SSID on downstream traffic in 8500	To Verify if bandwidth contract applied per-SSID on downstream traffic works fine	Passed	



CHAPTER 4

Regression Features - Test Summary

WLC AireOS

Re-instating PPPoE Modules

Logical ID	Title	Description	Status	Defects
WLJ80S_PPPoE_01	Enabling submode PPPoE in AP3702 and associating it to WLC 7500.	To check whether PPPoE submode is enabled or not in AP3702 and check whether AP gets associated or not to WLC 7500 with submode as PPPoE	Passed	
WLJ80S_PPPoE_02	Enabling submode PPPoE in AP1532 and associating it to WLC 7500.	To check whether PPPoE submode is enabled or not in AP1532 and check whether AP gets associated or not to WLC 7500 with submode as PPPoE	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_PPPoE_03	Enabling submode PPPoE in AP702I and associating it to WLC 7500.	To check whether PPPoE submode is enabled or not in AP702I and check whether AP gets associated or not to WLC 7500 with submode as PPPoE	Passed	
WLJ80S_PPPoE_04	Associating Win 7 client to AP 3702(Submode PPPoE) with L2 security Mac Filtering in WLC 7500	To check whether Win 7 client able to get associated successfully or not to AP 3702 with L2 Security Mac Filtering.	Passed	
WLJ80S_PPPoE_05	Associating MacBook client to AP 702(Submode PPPoE) with L2 security Mac Filtering in WLC 7500	To check whether Mac Book client able to get associated successfully or not to AP 702 with L2 Security Mac Filtering.	Passed	
WLJ80S_PPPoE_06	Associating Samsung S4 and Iphone clients to AP 3702(Submode PPPoE) with L2 security Mac Filtering in WLC 7500	To check whether Samsung S4 andIphone clients able to get associated successfully or not to AP 3702 with L2 Security Mac Filtering.	Passed	
WLJ80S_PPPoE_07	Associating Win 7 client to AP 1532(Submode PPPoE) with L2 security Dot1x in WLC 7500	To check whether Win 7 client able to get associated successfully or not to AP 1532 with L2 Security Dot1x.	Passed	
WLJ80S_PPPoE_08	Associating MacBook client to AP 3702(Submode PPPoE) with L2 security Dot1x in WLC 7500	To check whether Mac Book client able to get associated successfully or not to AP 3702 with L2 Security Dot1x.	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_PPPoE_09	Associating Samsung S4 and Iphone clients to AP 702(Submode PPPoE) with L2 security Dot1x in WLC 7500	To check whether Samsung S4 and Iphone clients able to get associated successfully or not to AP 702 with L2 Security Dot1x.	Passed	
WLJ80S_PPPoE_10	Performing 3702AP(Submode PPPoE) Fallback from Primary to Secondary WLC	To check whether 3702 AP getting Fallback or not to Secondary WLC when Primary WLC is down.	Passed	
WLJ80S_PPPoE_11	Performing 1532AP(Submode PPPoE) Fallback from Primary to Secondary WLC	To check whether 1532 AP getting Fallback or not to Secondary WLC when Primary WLC is down.	Passed	
WLJ80S_PPPoE_12	Performing 702AP(Submode PPPoE) Fallback from Primary to Secondary WLC	To check whether 702 AP getting Fallback or not to Secondary WLC when Primary WLC is down.	Passed	
WLJ80S_PPPoE_13	Performing 3702AP(Submode PPPoE) Fallback from Primary to Secondary WLC with association of clients(Win 7 and MacBook).	To check whether 3702 AP getting Fallback or not to Secondary WLC when Primary WLC is down and also check whether clients(Win 7 and MacBook) able to access the network in Secondary WLC.	Passed	
WLJ80S_PPPoE_14	Performing 702AP(Submode PPPoE) Fallback from Primary to Secondary WLC with association of clients(Samsung S4 and Iphone).	To check whether 702 AP getting Fallback or not to Secondary WLC when Primary WLC is down and also check whether clients(Samsung S4 and Iphone) and MacBook) able to access the network in Secondary WLC.	Passed	
WLJ80S_PPPoE_15	Adding 3702 AP(submode as PPPoE) in Flexconnect group and making it as AAA server for LEAP clients.	To verify whether 3702 AP acts as AAA server or not for LEAP clients by enabling Local Authentication check box and LEAP check box in a Flex group.	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_PPPoE_16	Adding 1532 AP(submode as PPPoE) in Flexconnect group and making it as AAA server for PEAP clients.	To verify whether 1532 AP(submode as PPPoE) acts as AAA server or not for PEAP clients by enabling Local Authentication check box and LEAP check box in a Flex group.	Passed	
WLJ80S_PPPoE_17	Adding 2 702 AP's in Flex group and performing roaming between AP's with LEAP clients.	To verify whether roaming occurs seamlessly or not between AP's within a Flex group.	Passed	
WLJ80S_PPPoE_18	Adding 2 1532 AP's in Flex group and performing roaming between AP's with PEAP clients.	To verify whether roaming occurs seamlessly or not between AP's within a Flex group.	Passed	
WLJ80S_PPPoE_19	Associating clients to AP 1532(Submode PPPoE) with L3 security Web-Authentication in WLC 7500	To check whether clients able to get associated successfully or not to AP 1532 with L3 Security Web-Auth.	Passed	
WLJ80S_PPPoE_20	Associating clients to AP 702(Submode PPPoE) with L3 security Web-Authentication in WLC 5500	To check whether clients able to get associated successfully or not to AP 702 with L3 Security Web-Auth.	Passed	

L2 Security

Logical ID	Title	Description	Status	Defects
WLJ80S_SR_L2_09	Associating 7921G IP phone - WEP	To check whether the 7921G IP phone is associated successfully into the network through WEP authentication method	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_SR_L2_10	Associating 7921G IP phone - WPA	To check whether the 7921G IP phone is associated successfully into the network through WPA authentication method	Passed	
WLJ80S_SR_L2_11	7921G IP Phone Association through WEP(RADIUS Server Authentication)	To verify the 7921G IP Phone is successfully authenticated and associated through WEP	Passed	
WLJ80S_SR_L2_12	Authentication for the association of clients-WPA	Checking for the Authentication of the clients when connected to an AP.	Passed	
WLJ80S_SR_L2_13	Authentication for the association of clients-802.1X	Checking for the Authentication of the clients when connected to an AP.	Passed	
WLJ80S_SR_L2_14	Authentication for the association of clients-Static WEP	Checking for the Authentication of the clients when connected to an AP.	Passed	
WLJ80S_SR_L2_15	Authentication for the association of clients- Static WEP+802.1X	Checking for the Authentication of the clients when connected to an AP.	Passed	

L3 Security

Logical ID	Title	Description	Status	Defects
WLJ80S_SR_L3_01	Configuring Customized (Downloaded) web-auth using NCS	To check the Customized(Downloaded) web-auth configuration in NCS reflects in WLC.	Passed	
WLJ80S_SR_L3_02	CT2500: Customized (Downloaded) login page for the controller.	To verify the successful customized web login page with Internal Authentication.	Passed	
WLJ80S_SR_L3_03	CT2500: Download customized login page for the controller.	To verify the customized web login page bundle is downloaded successfully.	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_SR_L3_04	Customized web auth login page for the controller-Laptop	To verify the successful customized web login page with internal authentication	Passed	
WLJ80S_SR_L3_05	Downloading the customized login page	To verify the successful download of customized login page	Passed	
WLJ80S_SR_L3_06	Customized web login page for the controller	To verify the successful customized web login page with internal authentication	Passed	
WLJ80S_SR_L3_07	CT2500: Default login page for the controller.	To verify the successful default web login page with Internal Authentication.	Passed	
WLJ80S_SR_L3_08	Default web login page for the controller	To verify the successful default web login page with Internal authentication	Passed	

Link Aggregation Mode

Logical ID	Title	Description	Status	Defects
WLJ80S_LAG_19	Enable Link Aggregation on the controller- LAP Local Mode	To verify the Light Weight Access Point Registration/Join status on controller - Local Mode	Passed	
WLJ80S_LAG_20	Enable Link Aggregation on the controller -LAP Flex Connect Mode	To verify the Light Weight Access Point Registration status on controller - Flex Connect Mode	Passed	
WLJ80S_LAG_21	Client Association with Light Weight Access Point after Link Aggregation failover	To verify the successful association of wireless client with Light Weight Access Point	Passed	
WLJ80S_LAG_22	LAG failover -Ping, FTP (Refer-CSCth12513)	To verify the successful PING, FTP packets during LAG failover	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_LAG_23	LAG Port status Trap Log with SNMP Manager (Refer: CSCto58101 Delay in Port Up down causes issues with LAG working on WLC	To verify the successful LAG port status message in SNMP manager	Passed	
WLJ80S_LAG_24	Active controller ports status when it is in Link Aggregation (LAG) failover	To check active controller ports status in Link Aggregation failover	Passed	

High Availability

Logical ID	Title	Description	Status	Defects
WLJ80S_SR_HA_25	Bringing HA pair up- WLC 5508	To verify whether the HA pair(ACTIVE:STANDBY) is up successfully	Passed	
WLJ80S_SR_HA_26	Bringing HA pair up- WLC 7500	To verify whether the HA pair(ACTIVE:STANDBY) is up successfully	Passed	
WLJ80S_SR_HA_27	Controller HA pair with different hardware models	To verify the role negotiation between the controllers with different hardware models	Passed	
WLJ80S_SR_HA_28	Controller HA pair with different software versions	To verify the role negotiation between the controllers with different software versions	Passed	
WLJ80S_SR_HA_29	Controller mode when the redundancy port loses connectivity	To verify the HA pair controller modes after disconnecting the redundancy port	Passed	
WLJ80S_SR_HA_30	Controller mode when the Gateway is not reachable to the STANDBY controller	To verify the HA pair controller modes when the Gateway is not reachable from the STANDBY controller	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_SR_HA_31	Controller mode when the Gateway is not reachable to the ACTIVE controller	To verify the HA pair controller modes when the Gateway is not reachable from the ACTIVE controller	Passed	
WLJ80S_SR_HA_32	Controller mode when the Gateway is not reachable to both the controller	To verify the HA pair controller modes when the Gateway is not reachable to both the controllers	Passed	
WLJ80S_SR_HA_33	Controller modes(HA pair) after power failure	To verify the controller modes after power failure on both the controllers	Passed	
WLJ80S_SR_HA_34	HA mode after resetting the peer system from ACTIVE	To verify the HA mode after resetting the peer system from ACTIVE controller	Passed	
WLJ80S_SR_HA_35	Client status during AP SSO after active failover-Web Authentication	To check whether the Client gets disassociated and forced to re-join to the controller after AP SSO	Passed	

Roaming

Logical ID	Title	Description	Status	Defects
WLJ80S_11r_36	11r Client Association with AKM PSK - FlexConnect Central Switch	To verify client's initial association to a wlan with 11r enabled with ft-PSK AKM Suite in flexconnect central switching.	Passed	
WLJ80S_11r_37	11r Client Association with AKM PSK - FlexConnect Local Switch Central Auth	Verify client's initial association to a wlan with 11r enabled with ft-PSK AKM Suite in flexconnect local switch central auth.	Passed	
WLJ80S_11r_38	Over the Air Intra-controller roaming - flexconnect Central Switch	To verify fast transition client roaming over the air within the same controller in flexconnect central auth.	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_11r_39	Over the DS Intra-controller roaming - Flexconnect Central Switch VLAN Pooling	Verify fast transition client roaming over the DS within the same controller in flexconnect central switch.	Passed	
WLJ80S_11r_40	Open Security Over-the-Air Roaming - controller	Verify open security 11r Over-the-Air Roaming	Passed	
WLJ80S_11r_41	Open Security Over-the-Air Roaming -NCS	Verify open security 11r Over-the-Air Roaming	Passed	
WLJ80S_11r_42	Roaming of wireless data clients within APs of one Flex connect group when controller is Down.	To check for the successful and seamless roaming of wireless data clients between APs of same Flex connect group when controller is "Down".	Passed	
WLJ80S_11r_44	Roaming of data clients between APs in same Flex connect group.	To check for the seamless roaming from one AP to another from the same Flex Connect group.	Passed	

AAA

Logical ID	Title	Description	Status	Defects
WLJ80S_aaa_01	Configure an access point in PI	To verify the access point configuration in PI GUI	Passed	
WLJ80S_aaa_02	Change the access point parameters in PI	To verify the access point parameters (name, mode, admin status, etc) are able to change when PI is integrated with ACS server	Passed	
WLJ80S_aaa_03	Configure an access point in virtual PI	To verify the access point configuration in virtual PI GUI	Passed	

WLJ80S_aaa_04	Change the access point parameters in virtual PI	To verify the access point parameters (name, mode, admin status, etc) are able to change when virtual PI is integrated with ACS server	Passed	

Flexconnect Enhancements

Logical ID	Title	Description	Status	Defects
WLJ80S_FLEX_48	WGB Association, WGB client registration through Flexconnect AP in connected mode.	To verify whether the WGB associates and the clients are registered to the controller through Flexconnect AP.	Passed	
WLJ80S_FLEX_49	WGB Association, WGB client registration through Flexconnect AP in standalone mode	To verify whether the WGB associates and the clients are registered to the controller through Flexconnect AP in standalone mode.	Passed	
WLJ80S_FLEX_50	WGB Association through Local authenticated WLAN.	To verify whether the WGB associates with the flexconnect through local authenticated WLAN	Passed	
WLJ80S_FLEX_51	WGB disassociation from the controller	To verify whether the WGB disassociates from the controller upon deletion	Passed	
WLJ80S_FLEX_52	WGB client de-registration with the flexconnect in standalone mode to connected mode	To verify whether the WGB disassociates from the controller upon deletion	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_FLEX_53	Flexconnect AP reload in connected mode when WGB is associated-Central auth locally switched	To verify whether WGB and WGB clients re-associates to the controller after flexconnect AP reloads	Passed	
WLJ80S_FLEX_54	Flexconnect AP reload in standalone mode when WGB is associated-Local authentication	To verify whether WGB and WGB clients re-associates to the controller after flexconnect AP reloads	Passed	
WLJ80S_FLEX_55	WGB Clients roaming to a different flexconnect on the same controller	To verify the WGB client re-associates successfully to a different flexConnect after roaming within the controller	Passed	

HREAP

Logical ID	Title	Description	Status	Defects
WLJ80S_SR_Fault_56	HREAP fault tolerance between connected and standalone AP-2.4 GHz	To verify whether the client associated to flexconnect AP will get re-associated in case of fault tolerance	Passed	
WLJ80S_SR_Fault_57	HREAP fault tolerance between standalone and connected AP-2.4 GHz	To verify whether the client associated to flexconnect AP will get re-associated in case of fault tolerance	Passed	

Anyconnect VPN

Logical ID	Title	Description	Status	Defects
WLJ80S_Any_58	WPA+WPA2 network(AnyConnect) in Win7 client	To check whether the Anyconnect VPN is connecting or not using WPA+WPA2 layer2 security in Win7 client	Passed	
WLJ80S_Any_59	Static WEP network(AnyConnect) in Win7 client	To check whether the AnyConnect VPN is connecting or not, using Static WEP layer2 security in Win7 client	Passed	
WLJ80S_Any_60	Layer 2 security None for open auth (AnyConnect) in Win7 client	To check whether the AnyConnect VPN is connect or not using "None" Layer 2 security in Win7 client	Passed	
WLJ80S_Any_61	WPA+WPA2 network(AnyConnect) using MacBook client	To check whether the Anyconnect VPN is connect or not, using WPA+WPA2 layer2 security in MacBook client	Passed	
WLJ80S_Any_62	Static WEP network (AnyConnect) in MacBook Client	To check whether the Anyconnect VPN is connect or not using Static WEP layer2 security in MacBook Client	Passed	
WLJ80S_Any_63	Layer 2 security "None" for open auth network (AnyConnect) in MacBook Client	To check whether the Anyconnect VPN is connect or not , using "None" Layer 2 security in MacBook Client	Passed	
WLJ80S_Any_64	WPA+WPA2 network (AnyConnect) using Samsung Galaxy sII client	To check whether the Anyconnect VPN is connect or not, using WPA+WPA2 layer2 security in Samsung Galaxy sII client	Passed	
WLJ80S_Any_65	Static WEP network (AnyConnect) in Samsung Galaxy sII client	To check whether the Anyconnect VPN is connect or not using Static WEP layer2 security in Samsung Galaxy sII Client	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_Any_66	Layer 2 security "None" for open auth network (Anyconnect) in Samsung Galaxy sII client.	To check whether the Anyconnect VPN is connect or not , using "None" Layer 2 security in Samsung Galaxy sII Client.	Passed	

Dot1x and Web-Auth Support

Logical ID	Title	Description	Status	Defects
WLJ80S_SR_Web_67	Authentication of client(Apple Mac Book) with Security Static WEP and Web-Auth -2500,5508, WiSM2 and 7500 Controller.	Checking for the Authentication of the client when connected to a WLAN in which Static WEP and Web-Auth is enabled.	Passed	
WLJ80S_SR_Web_68	Authentication of clients(Apple Mac Book and Win 7) with Security Static WEP+Dot1x and Web-Auth using ISE-2500,5508, WiSM2 and 7500 Controller.	Checking for the Authentication of the clients when connected to a WLAN in which Static WEP+Dot1x and Web-Auth is enabled.	Passed	
WLJ80S_SR_Web_69	Authentication of clients(Apple Mac Book and Win 7) with Security Dot1x using ISE and Web Auth-2500 ,5508 , WiSM2 and 7500 Controller.	Checking for the Authentication of the clients when connected to a WLAN in which Dot1x and Web-Auth is enabled.	Passed	

Multiple RADIUS Server Per SSID

Logical ID	Title	Description	Status	Defects
WLJ80S_Rad_70	Performing Dot1x authentication over PPPoE AP with RADIUS servers configured(Primary)-2500,5508,WiSM2 and 7500 WLC	To verify whether Dot1x authentication can be performed successfully to the clients associated via the Primary RADIUS server over the PPPoE connection with the Vlan mapped	Passed	
WLJ80S_Rad_71	Performing Dot1x authentication over PPPoE AP with RADIUS servers configured(Secondary)-2500,5508,WiSM2 and 7500 WLC	To verify whether Dot1x authentication can be performed successfully to the clients associated via the secondary RADIUS server over the PPPoE connection with the Vlan mapped	Passed	
WLJ80S_Rad_72	Performing Dot1x authentication over PPPoE AP with RADIUS servers configured(Primary failover)-2500,5508,WiSM2 and 7500 WLC	To verify whether Dot1x authentication can be performed successfully to the clients associated via the secondary RADIUS server over the PPPoE connection with the Vlan mapped	Passed	
WLJ80S_Rad_73	Performing Dot1x authentication over FlexConnect AP with RADIUS servers configured(Primary)-2500,5508,WiSM2 and 7500 WLC	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	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_Rad_74	Performing Dot1x authentication over FlexConnect AP with RADIUS servers configured(Secondary)-2500,5508,WiSM2 and 7500 WLC	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	Passed	
WLJ80S_Rad_75	Performing Dot1x authentication over FlexConnect AP with RADIUS servers configured(Primary failover)-2500,5508,WiSM2 and 7500 WLC	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	Passed	

Secure FTP

Logical ID	Title	Description	Status	Defects
WLJ80S_SFTP__76	Transfer download of controller image with SFTP method- WLC 5500series , WiSM2 , 2500 series	To verify controller able to download the image using SFTP method and installs properly	Passed	
WLJ80S_SFTP__77	Transfer of controller configuration with SFTP method - WLC 5500 , 2500 , WiSM2.	To verify controller able to download a configuration and upload the current configuration using SFTP transfer method	Passed	
WLJ80S_SFTP__78	Transfer download of controller certificates with SFTP method - WLC Virtual and 7500	To verify controller is able to download all the supported certificates using SFTP transfer method	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_SFTP__79	SFTP Transfer validation with other configuration items like, path, filename, server IP and port number - All Controllers	Verify controller validates properly the transfer parameters like server IP address, Port number, filename, and path. Transfer is aborted if any of the above configuration parameters are in-correct or server issues - All controllers	Passed	
WLJ80S_SFTP__80	Transfer upload of other data type files with SFTP method - WLC 5500 series , 2500 and WiSM2	To verify controller is able to upload all the other supported data type files using SFTP transfer method- WLC 5500 , 2500 & WiSM2.	Passed	

NBAR

Logical ID	Title	Description	Status	Defects
WLJ80S_NBAR_82	Apply an AVC profile with a rule to block an application and check if that application is dropped when tried to open and notification is send via SNMP trap	To verify AVC rule to drop an application works fine	Passed	
WLJ80S_NBAR_83	AVC profile should work fine in AP SSO	To verify if AVC profile works fine after AP SSO	Passed	
WLJ80S_NBAR_84	application traffic flow from client to AP when AP in local mode and centrally switched flexconnect - 5508,7500 &2500 WLC	To verify the IP traffic flow from client to AP when AP is in local mode and centrally switched flexconnect	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_NBAR_85	Configuring and verifying custom DSCP value for AVC	To verify if custom DSCP value is configured and applied successfully for a AVC rule	Passed	
WLJ80S_NBAR_86	Bandwidth contract Rate limit applied per-SSID on downstream traffic	To Verify if bandwidth contract applied per-SSID on downstream traffic works fine	Passed	
WLJ80S_NBAR_87	Override Per-user bandwidth contract on downstream and upstream traffic	To verify if Override Per-user bandwidth contract on downstream and upstream traffic works fine	Passed	
WLJ80S_NBAR_88	AVC Monitoring	To verify the AVC monitoring .	Passed	

PI

NCS Maps

Logical ID	Title	Description	Status	Defects
WLJ80SS_MAP_16	Copy and Replace AP-Map	To verify the successful copy and replace	Passed	

Autonomous to LWAPP Migration

Logical ID	Title	Description	Status	Defects
WLJ80S_Migration_01	Autonomous to LWAPP Migration	To migrate the autonomous to LWAPP	Passed	
WLJ80S_Migration_02	NCS: migrating autonomous AP to LWAPP using the "Schedule for later date /time	To verify if autonomous AP is migrating to LAP immediately using the option " Schedule for later date/time"	Passed	

Backup And Restore of PI

Logical ID	Title	Description	Status	Defects
WLJ80S_BnR_81	Performing Backup and restore in PI	To verify the PI backup and restore is successful	Passed	

PI HA

Logical ID	Title	Description	Status	Defects
WLJ76S_PI_HA_01	PI HA- When primary server is down(HW failure) and Failover type as "Manual"	To check whether PI has been switchover to the secondary when there is a primary server(HW) failure-failover type as "Manual"	Passed	
WLJ76S_PI_HA_02	PI HA- When primary server is down(HW failure) and Failover type as "Automatic"	To check whether PI has been switchover to the secondary when there is a primary server(HW) failure-failover type as "Automatic"	Passed	
WLJ76S_PI_HA_03	PI HA- When primary server is down(Network failure) and Failover type as "Manual"	To check whether PI has been switchover to the secondary when there is a primary server(NW) failure-failover type as "Manual"	Passed	
WLJ76S_PI_HA_04	PI HA- When primary server is down(Network failure) and Failover type as "Manual"	To check whether PI has been switchover to the secondary when there is a primary server(NW) failure-failover type as "Automatic"	Passed	
WLJ76S_PI_HA_05	PI HA- Failback to Primary server once it has been recovered from HW failure	To check whether the failback operation is successful after the primary server has been recovered from HW failure	Passed	
WLJ76S_PI_HA_06	PI HA- Failback to Primary server once it has been recovered from NW failure	To check whether the failback operation is successful after the primary server has been recovered from NW failure	Passed	

MSE

MSE HA

Logical ID	Title	Description	Status	Defects
WLJ76S_MSE_HA_01	MSE system hardware shutdown in Direct Connect Link deployment	To verify whether MSE HA failover and fail back works when MSE system hardware shutdown in Direct Connect Link deployment.	Failed	CSCum12763
WLJ76S_MSE_HA_01	MSE system hardware shutdown in Non-Direct Connect Link deployment	To verify whether MSE HA failover and fail back works when MSE system hardware shutdown in Non-Direct Connect Link deployment.	Failed	CSCum12763
WLJ76S_MSE_HA_02	MSE network shutdown in Direct Connect Link deployment	To verify whether MSE HA failover and fail back works when MSE network shutdown in Direct Connect Link deployment.	Failed	CSCum12763
WLJ76S_MSE_HA_02	MSE network shutdown in Direct Non-Connect Link deployment	To verify whether MSE HA failover and fail back works when MSE network shutdown in Non-Direct Connect Link deployment.	Failed	CSCum12763

SR Test Cases

Button in Report Launch pad

Logical ID	Title	Description	Status	Defects
WLJ80S_Reg_01	PI: Save/Run button in Report Launch pad	To verify whether "Save", "Run and Save" button is working in Report Launch pad in PI	Passed	

Map Location in Copy and Replace

Logical ID	Title	Description	Status	Defects
WLJ80S_Reg_02	Map Location in Copy and Replace	To verify the successful copy and replace with Map Location	Passed	

Upload File

Logical ID	Title	Description	Status	Defects
WLJ80S_Reg_03	CT5508: Controller configuration Upload using TFTP server	To verify whether the configuration upload from a controller is successful	Passed	
WLJ80S_Reg_04	CT7500: Controller configuration Upload using TFTP server	To verify whether the configuration upload from a controller is successful	Passed	
WLJ80S_Reg_05	CT2504: Controller configuration Upload using TFTP server	To verify whether the configuration upload from a controller is successful	Passed	

HREAP

Logical ID	Title	Description	Status	Defects
WLJ80S_Reg_06	HREAP fault tolerance between connected and standalone AP-2.4 GHz	To verify whether the client associated to flexconnect AP will get re-associated in case of fault tolerance	Passed	
WLJ80S_Reg_07	HREAP fault tolerance between standalone and connected AP-2.4 GHz	To verify whether the client associated to flexconnect AP will get re-associated in case of fault tolerance	Passed	

AP Fallback

Logical ID	Title	Description	Status	Defects
WLJ80S_SR_01	Performing AP fallback from Secondary to Primary WLC	To verify whether the client gets disconnected or not when AP Fallback from Secondary to Primary WLC with enabling "AP Fallback" option in Primary WLC once it is UP.	Passed	
WLJ80S_SR_02	Performing AP fallback from Secondary to Primary WLC	To verify whether the client gets disconnected or not when AP Fallback from Secondary to Primary WLC with enabling "AP Fallback" option in Primary WLC at all time.	Passed	

Fault Tolerance

Logical ID	Title	Description	Status	Defects
WLJ80S_SR_03	Performing Fault tolerance of Flex AP from Primary to Secondary WLC	To verify whether AP resets its radio or not when it is moving from Primary to Secondary WLC after trying to join Primary WLC for long time.	Passed	
WLJ80S_SR_04	Performing Fault tolerance of Flex AP from Primary to Secondary WLC	To verify whether AP resets its radio or not when it is moving from Primary to Secondary WLC .	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_SR_05	Performing Fault tolerance of AP in Local mode from Primary to Secondary WLC	To verify whether AP resets its radio or not when it is moving from Primary to Secondary WLC after trying to join Primary WLC for long time.	Passed	
WLJ80S_SR_06	Performing Fault tolerance of AP in Local mode from Primary to Secondary WLC	To verify whether AP resets its radio or not when it is moving from Primary to Secondary WLC .	Passed	

ISE

Logical ID	Title	Description	Status	Defects
WLJ80S_SR_07	Checking the end user device for HTTP probe in ISE	To Verify whether ISE shows the end user device correctly or not for HTTP probe.	Passed	

FlexConnect Enhancement

Logical ID	Title	Description	Status	Defects
WLJ80S_SR_08	Performing VLAN mapping for a WLAN in a FlexConnect Group with 1142 AP - L2 Security "Dot1x-Leap"	To verify whether VLAN mapping is done or not from AP level WLAN-VLAN mapping in a FlexConnect Group	Passed	
WLJ80S_SR_09	Performing VLAN mapping for a WLAN in a FlexConnect Group with 1142 AP - L2 Security "Dot1x-Peap"	To verify whether VLAN mapping is done or not from AP level WLAN-VLAN mapping in a FlexConnect Group	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_SR_10	Performing VLAN mapping for a WLAN in a FlexConnect Group with 1262 AP - L2 Security "Dot1x-Leap"	To verify whether VLAN mapping is done or not from AP level WLAN-VLAN mapping in a FlexConnect Group	Passed	
WLJ80S_SR_11	Performing VLAN mapping for a WLAN in a FlexConnect Group with 1262 AP - L2 Security "Dot1x-Peap"	To verify whether VLAN mapping is done or not from AP level WLAN-VLAN mapping in a FlexConnect Group	Passed	

WLC

Logical ID	Title	Description	Status	Defects
WLJ80S_SR_12	Channel Width of RF Channel Assignment is changed	To verify Channel Width of RF Channel Assignment is not changing	Passed	

PI

Logical ID	Title	Description	Status	Defects
WLJ80S_SR_13	Validating ms-lync application in PI	To verify if ms-lync application is recognized or not in PI	Passed	
WLJ80S_SR_14	Dashlet data is refreshed when time period in dashlet is changed	To verify if dashlet data is refreshed when time period in dashlet is changed	Passed	

Fix Verification

Logical ID	Title	Description	Status	Defects
WLJ80S_Fix_01	AP name in debug client output on the 5508 controller	To verify if the debug client output on the 5508 controller shows the AP name along with BSSID	Passed	
WLJ80S_Fix_02	AP name in debug client output on the 7500 and 8500 controller	To verify if the debug client output on the 7500 and 8500 controller shows the AP name along with BSSID	Passed	
WLJ80S_Fix_03	AP name in debug client output on the WiSM2 controller	To verify if the debug client output on the WiSM2 controller shows the AP name along with BSSID	Passed	
WLJ80S_Fix_04	WLAN and Profile name in the show client output on 5508 series controller	To verify if the "show client detail mac-address" output shows the WLAN and profile name in 5508 controller.	Passed	
WLJ80S_Fix_05	WLAN and Profile name in the show client output on 7500/8500 series controller	To verify if the "show client detail mac-address" output shows the WLAN and profile name in 7500/8500 controller.	Passed	
WLJ80S_Fix_06	WLAN and Profile name in the show client output on WiSM2 series controller	To verify if the "show client detail mac-address" output shows the WLAN and profile name in WiSM2 controller.	Passed	
WLJ80S_Fix_07	LSC only authentication for MAP in 5508 series controller	To verify if the MAP are authenticated in the 5508 controller using LSC	Passed	
WLJ80S_Fix_08	LSC only authentication for MAP in 7500/8500 series controller	To verify if the MAP are authenticated in the 7500/8500 controller using LSC	Passed	
WLJ80S_Fix_09	LSC only authentication for MAP in WiSM2 series controller	To verify if the MAP are authenticated in WiSM2 controller using LSC	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_Fix_10	MAC filter authentication for MAP in 5508 Series Controller	To verify if the old behavior of MAC filter authentication for Mesh APs is not affected in 5508 Controllers.	Passed	
WLJ80S_Fix_11	MAC filter authentication for MAP in 7500 Series Controller	To verify if the old behavior of MAC filter authentication for Mesh APs is not affected in 7500 Controllers.	Passed	
WLJ80S_Fix_12	MAC filter authentication for MAP in WiSM2 Controller	To verify if the old behavior of MAC filter authentication for Mesh APs is not affected in WiSM2 Controllers.	Passed	
WLJ80S_Fix_13	Enable/Disable Flexconnect ARP cache from GUI of the 5508 Series and WiSM2 Controller	To enable/disable 'Flexconnect ARP cache' in 5508 and WiSM2 controllers from GUI and check if it could be applied successfully	Passed	
WLJ80S_Fix_14	Enable/Disable Flexconnect ARP cache from GUI of the 7500 and 8500 series Controller	To enable/disable 'Flexconnect ARP cache' in 7500 and 8500 controllers from GUI and check if it could be applied successfully	Passed	
WLJ80S_Fix_15	Enable/Disable Flexconnect ARP cache from CLI of the 5508 Series and WiSM2 Controller	To enable/disable 'Flexconnect ARP cache' in 5508 and WiSM2 controllers from CLI and check if it could be applied successfully	Passed	
WLJ80S_Fix_16	Enable/Disable Flexconnect ARP cache from CLI of the 7500 and 8500 series Controller	To enable/disable 'Flexconnect ARP cache' in 7500 and 8500 controllers from CLI and check if it could be applied successfully	Passed	
WLJ80S_Fix_17	Flexconnect ARP cache on locally switched WLANs in 5508 and WiSM2 controllers.	To check if the ARP request from wired side doesn't reach the Wireless client when the client is attached to a Flexconnect AP with locally switched WLAN.	Passed	
WLJ80S_Fix_18	Flexconnect ARP cache on locally switched WLANs in 7500 and 8500 controllers.	To check if the ARP request from wired side doesn't reach the Wireless client when the client is attached to a Flexconnect AP with locally switched WLAN.	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_Fix_19	Flexconnect ARP cache on locally switched WLANs in all the model controllers when using NGWC switch	To check if the ARP request from NGWC switch doesn't reach the Wireless client when the client is attached to a Flexconnect AP with locally switched WLAN.	Passed	
WLJ80S_Fix_20	Global Telnet/SSH command on all Lightweight APs which are joined to the controller	To check the functionality of the global Telnet/SSH enable option in the controller for the APs which are registered to the controller	Passed	
WLJ80S_Fix_21	Telnet/SSH on a Mesh AP which has not joined the controller , but obtained an IP address	To check if the user is able to Telnet/SSH a Mesh AP which has obtained an IP address, but not joined any controllers.	Passed	
WLJ80S_Fix_22	The new controller CLI format for Telnet /SSH	To check the working of the new CLI command format for Telnet /SSH in terms of configuration and functionality	Passed	
WLJ80S_Fix_23	A per-AP configured Telnet/SSH setting functionality when controller's global Telnet/SSH setting is enabled	To check if the Per-AP configured Telnet/SSH setting doesn't get overridden by the controller's global Telnet/SSH enabled setting.	Passed	
WLJ80S_Fix_24	Configuring the AP 3600 to Local mode from the CLI	To configure the 3600 AP to local mode from CLI of the AP and verify if the configuration applies correctly	Passed	
WLJ80S_Fix_25	Configuring the AP 3600 to bridge mode from the CLI	To configure the 3600 AP to bridge mode from CLI of the AP and verify if the configuration applies correctly	Passed	
WLJ80S_Fix_26	Configuring the AP 1602 to Local mode from the CLI	To configure the 1602 AP to local mode from CLI of the AP and verify if the configuration applies correctly	Passed	
WLJ80S_Fix_27	Configuring the AP 1602 to bridge mode from the CLI	To configure the 1602 AP to bridge mode from CLI of the AP and verify if the configuration applies correctly	Passed	
WLJ80S_Fix_28	Configuring the AP 1532 to Local mode from the CLI	To configure the 1532 AP to local mode from CLI of the AP and verify if the configuration applies correctly	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_Fix_29	Configuring the AP 1532 to bridge mode from the CLI	To configure the 1532 AP to bridge mode from CLI of the AP and verify if the configuration applies correctly	Passed	
WLJ80S_Fix_30	WLAN Id attribute with Dot1x L2 security on a WLAN	To verify if Dot1X is rejected if Airespace-WLAN-id does not match value returned from AAA	Passed	
WLJ80S_Fix_31	WLAN Id attribute with Mac filtering on a WLAN	To verify if Mac filtering is rejected if Airespace-WLAN-id does not match value returned from AAA	Passed	
WLJ80S_Fix_32	SSID attribute with Dot1x auth with single SSID	To verify if Dot1X is rejected on a SSID based on values returned from AAA server	Passed	
WLJ80S_Fix_33	SSID attribute with Mac filtering auth with single SSID	To verify if Mac filtering is rejected on a SSID based on values returned from AAA server	Passed	
WLJ80S_Fix_34	SSID attribute with Dot1x Auth with multiple SSIDs	To verify if Dot1x is rejected on a SSID based on values returned from AAA server	Passed	
WLJ80S_Fix_35	SSID attribute with Mac filtering with multiple SSIDs	To verify if Mac filtering is rejected on a SSID based on values returned from AAA server	Passed	
WLJ80S_Fix_36	WLAN Id attribute with Web-auth on a WLAN	To verify if Web-auth is rejected if Airespace-WLAN-id does not match value returned from AAA	Passed	
WLJ80S_Fix_37	SSID attribute with Web-auth with single SSID	To verify if Web-auth is rejected on a SSID based on values returned from AAA server	Passed	
WLJ80S_Fix_38	SSID attribute with Web-Auth with multiple SSIDs	To verify if Web-auth is rejected on a SSID based on values returned from AAA server	Passed	
WLJ80S_Fix_39	Multiple event definition triggered by location change	To verify if multiple events((3 events) are configured as triggering by Location Change, "distance" value in CAS notification for the second and third event in addition to the first event isa non-zero value	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_Fix_40	Multiple event definition triggered by location change	To verify if multiple events(5 events) are configured as triggering by Location Change, "distance" value in CAS notification for the second and third event in addition to the first event isa non-zero value	Passed	
WLJ80S_Fix_41	Notification for Missing client	To verify if notification configuration for probing clients which are tracked by CAS/MSE, the notifications over SOAP/Syslog are sent only once when the notification has "Non Recurring" as Frequency configuration	Passed	
WLJ80S_Fix_42	Notification for Missing client	To verify if notification configuration for probing clients which are tracked by CAS/MSE, the notifications over SOAP/Syslog are sent at a periodic interval when the notification has " Recurring" as Frequency configuration	Passed	
WLJ80S_Fix_43	MAC filtering parameter cache	To check if the MAC filtering tracking is faster .	Passed	
WLJ80S_Fix_44	CAPWAP data keep alive support	To verify if the CAPWAP data keep alive support exists or not from the AP to WLC when a NAT gateway exists between them.	Passed	
WLJ80S_Fix_45	Tx Power level in 3600 AP in Q domain	To verify if the Transmit power level remains the same in the AP when the Transmit power level is set to 5 in the controller >Wireless> 802.11a and b radio settings.	Passed	
WLJ80S_Fix_46	Tx Power level in 2600 AP in Q domain	To verify if the Transmit power level remains the same in the AP when the Transmit power level is set to 5 in the controller >Wireless> 802.11a and b radio settings.	Passed	
WLJ80S_Fix_47	Tx Power level in 1042 AP in A domain	To verify if the Transmit power level remains the same in the AP when the Transmit power level is set to 5 in the controller >Wireless> 802.11a and b radio settings.	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_Fix_48	Tx Power level in 3700 AP in Q domain	To verify if the Transmit power level remains the same in the AP when the Transmit power level is set to 5 in the controller >Wireless> 802.11a and b radio settings.	Passed	

TAC

Logical ID	Title	Description	Status	Defect
WLJ80S_Fix_01	AP name in debug client output on the 5508 controller	To verify if the debug client output on the 5508 controller shows the AP name along with BSSID	Passed if the debug output shows the AP name along with BSSID	CSCua30068
WLJ80S_Fix_02	AP name in debug client output on the 7500 and 8500 controller	To verify if the debug client output on the 7500 and 8500 controller shows the AP name along with BSSID	Passed if the debug output shows the AP name along with BSSID	CSCua30068
WLJ80S_Fix_03	AP name in debug client output on the WiSM2 controller	To verify if the debug client output on the WiSM2 controller shows the AP name along with BSSID	Passed if the debug output shows the AP name along with BSSID	CSCua30068
WLJ80S_Fix_04	WLAN and Profile name in the show client output on 5508 series controller	To verify if the "show client detail mac-address" output shows the WLAN and profile name in 5508 controller.	Passed if the debug output shows the WLAN and profile name .	CSCug72744
WLJ80S_Fix_05	WLAN and Profile name in the show client output on 7500/8500 series controller	To verify if the "show client detail mac-address" output shows the WLAN and profile name in 7500/8500 controller.	Passed if the debug output shows the WLAN and profile name .	CSCug72744

Logical ID	Title	Description	Status	Defect
WLJ80S_Fix_06	WLAN and Profile name in the show client output on WiSM2 series controller	To verify if the "show client detail mac-address" output shows the WLAN and profile name in WiSM2 controller.	Passed if the debug output shows the WLAN and profile name .	CSCug72744
WLJ80S_Fix_07	LSC only authentication for MAP in 5508 series controller	To verify if the MAP are authenticated in the 5508 controller using LSC	Passed if the MAP is authenticated using LSC only.	CSCud56704
WLJ80S_Fix_08	LSC only authentication for MAP in 7500/8500 series controller	To verify if the MAP are authenticated in the 7500/8500 controller using LSC	Passed if the MAP is authenticated using LSC only.	CSCud56704
WLJ80S_Fix_09	LSC only authentication for MAP in WiSM2 series controller	To verify if the MAP are authenticated in WiSM2 controller using LSC	Passed if the MAP is authenticated using LSC only.	CSCud56704
WLJ80S_Fix_10	MAC filter authentication for MAP in 5508 Series Controller	To verify if the old behavior of MAC filter authentication for Mesh APs is not affected in 5508 Controllers.	Passed if the old behavior is not affected	CSCud56704
WLJ80S_Fix_11	MAC filter authentication for MAP in 7500 Series Controller	To verify if the old behavior of MAC filter authentication for Mesh APs is not affected in 7500 Controllers.	Passed if the old behavior is not affected	CSCud56704
WLJ80S_Fix_12	MAC filter authentication for MAP in WiSM2 Controller	To verify if the old behavior of MAC filter authentication for Mesh APs is not affected in WiSM2 Controllers.	Passed if the old behavior is not affected	CSCud56704

Logical ID	Title	Description	Status	Defect
WLJ80S_Fix_13	Enable/Disable Flexconnect ARP cache from GUI of the 5508 Series and WiSM2 Controller	To enable/disable 'Flexconnect ARP cache' in 5508 andWiSM2 controllers from GUI and check if it could be applied successfully	Passed if the Flexconnect ARP cache can be enabled/disabled without any issue.	CSCty04398
WLJ80S_Fix_14	Enable/Disable Flexconnect ARP cache from GUI of the 7500 and8500 series Controller	To enable/disable 'Flexconnect ARP cache' in 7500 and 8500 controllers from GUI and check if it could be applied successfully	Passed if the Flexconnect ARP cache can be enabled/disabled without any issue.	CSCty04398
WLJ80S_Fix_15	Enable/Disable Flexconnect ARP cache from CLI of the 5508 Series and WiSM2 Controller	To enable/disable 'Flexconnect ARP cache' in 5508 andWiSM2 controllers from CLI and check if it could be applied successfully	Passed if the Flexconnect ARP cache can be enabled/disabled without any issue.	CSCty04398
WLJ80S_Fix_16	Enable/Disable Flexconnect ARP cache from CLI of the 7500 and8500 series Controller	To enable/disable 'Flexconnect ARP cache' in 7500 and 8500 controllers from CLI and check if it could be applied successfully	Passed if the Flexconnect ARP cache can be enabled/disabled without any issue.	CSCty04398
WLJ80S_Fix_17	Flexconnect ARP cache on locally switched WLANs in 5508 and WiSM2 controllers.	To check if the ARP request from wired side doesn't reach the Wireless client when the client is attached to a Flexconnect AP with locally switched WLAN.	Passed if the ARP request doesn't reach the wireless client and the AP replies to the wired side.	CSCty04398

Logical ID	Title	Description	Status	Defect
WLJ80S_Fix_18	Flexconnect ARP cache on locally switched WLANs in 7500 and 8500 controllers.	To check if the ARP request from wired side doesn't reach the Wireless client when the client is attached to a Flexconnect AP with locally switched WLAN.	Passed if the ARP request doesn't reach the wireless client and the AP replies to the wired side.	CSCty04398
WLJ80S_Fix_19	Flexconnect ARP cache on locally switched WLANs in all the model controllers when using NGWC switch	To check if the ARP request from NGWC switch doesn't reach the Wireless client when the client is attached to a Flexconnect AP with locally switched WLAN.	Passed if the ARP request doesn't reach the wireless client and the AP replies to the wired side.	CSCty04398
WLJ80S_Fix_20	Global Telnet /SSH command on all Lightweight APs which are joined to the controller	To check the functionality of the global Telnet /SSH enable option in the controller for the APs which are registered to the controller	Passed if the Telnet/SSH is working as expected.	CSCud56714
WLJ80S_Fix_21	Telnet/SSH on a Mesh AP which has not joined the controller , but obtained an IP address	To check if the user is able to Telnet/SSH a Mesh AP which has obtained an IP address, but not joined any controllers.	Passes if the user is able to Telnet/SSH the Mesh AP	CSCud56714
WLJ80S_Fix_22	The new controller CLI format for Telnet/SSH	To check the working of the new CLI command format for Telnet/SSH interims of configuration and functionality	Passed if worked as expected	CSCud56714

Logical ID	Title	Description	Status	Defect
WLJ80S_Fix_23	A per-AP configured Telnet/SSH setting functionality when controller's global Telnet/SSH setting is enabled	To check if the Per-AP configured Telnet /SSH setting doesn't get overridden by the controller's global Telnet /SSH enabled setting.	Passed if the global setting doesn't override the per-AP configured Telnet /SSH setting	CSCud56714
WLJ80S_Fix_24	Configuring the AP 3600 to Local mode from the CLI	To configure the 3600 AP to local mode from CLI of the AP and verify if the configuration applies correctly	Passed if the AP mode is changed to local	CSCug82223
WLJ80S_Fix_25	Configuring the AP 3600 to bridge mode from the CLI	To configure the 3600 AP to bridge mode from CLI of the AP and verify if the configuration applies correctly	Passed if the AP mode is changed to bridge.	CSCug82223
WLJ80S_Fix_26	Configuring the AP 1602 to Local mode from the CLI	To configure the 1602 AP to local mode from CLI of the AP and verify if the configuration applies correctly	Passed if the AP mode is changed to local	CSCug82223
WLJ80S_Fix_27	Configuring the AP 1602 to bridge mode from the CLI	To configure the 1602 AP to bridge mode from CLI of the AP and verify if the configuration applies correctly	Passed if the AP mode is changed to bridge.	CSCug82223
WLJ80S_Fix_28	Configuring the AP 1532 to Local mode from the CLI	To configure the 1532 AP to local mode from CLI of the AP and verify if the configuration applies correctly	Passed if the AP mode is changed to local	CSCug82223
WLJ80S_Fix_29	Configuring the AP 1532 to bridge mode from the CLI	To configure the 1532 AP to bridge mode from CLI of the AP and verify if the configuration applies correctly	Passed if the AP mode is changed to bridge.	CSCug82223

Logical ID	Title	Description	Status	Defect
WLJ80S_Fix_30	"WLAN Id attribute with Dot1x L2 security on a WLAN "	To verify if Dot1X is rejected if Airespace-WLAN-id does not match value returned from AAA	Passed if worked as expected	CSCsj27376
WLJ80S_Fix_31	"WLAN Id attribute with Mac filtering on a WLAN"	To verify if Mac filtering is rejected if Airespace-WLAN-id does not match value returned from AAA	Passed if worked as expected	CSCsj27376
WLJ80S_Fix_32	"SSID attribute with Dot1x auth with single SSID"	To verify if Dot1X is rejected on a SSID based on values returned from AAA server	Passed if worked as expected	CSCsj27376
WLJ80S_Fix_33	"SSID attribute with Mac filtering auth with single SSID"	To verify if Mac filtering is rejected on a SSID based on values returned from AAA server	Passed if worked as expected	CSCsj27376
WLJ80S_Fix_34	SSID attribute with Dot1x Auth with multiple SSIDs	To verify if Dot1x is rejected on a SSID based on values returned from AAA server	Passed if worked as expected	CSCsj27376
WLJ80S_Fix_35	SSID attribute with Mac filtering with multiple SSIDs	To verify if Mac filtering is rejected on a SSID based on values returned from AAA server	Passed if worked as expected	CSCsj27376
WLJ80S_Fix_36	"WLAN Id attribute with Web-auth on a WLAN"	To verify if Web-auth is rejected if Airespace-WLAN-id does not match value returned from AAA	Passed if worked as expected	CSCsj27376
WLJ80S_Fix_37	"SSID attribute with Web-auth with single SSID"	To verify if Web-auth is rejected on a SSID based on values returned from AAA server	Passed if worked as expected	CSCsj27376

Logical ID	Title	Description	Status	Defect
WLJ80S_Fix_38	SSID attribute with Web-Auth with multiple SSIDs	To verify if Web-auth is rejected on a SSID based on values returned from AAA server	Passed if worked as expected	CSCsj27376
WLJ80S_Fix_39	Multiple event definition triggered by location change	"To verify if multiple events((3 events) are configured as triggering by Location Change,""distance"" value in CAS notification for the second and third event in addition to the first event isa non-zero value "	Passed if the CAS notification for the second and third event is also received to a non-zero value	CSCuh00581
WLJ80S_Fix_40	Multiple event definition triggered by location change	"To verify if multiple events(5 events) are configured as triggering by Location Change,""distance"" value in CAS notification for the second and third event in addition to the first event isa non-zero value "	Passed if the CAS notification for the second and third event is also received to a non-zero value	CSCuh00581
WLJ80S_Fix_41	Notification for Missing client	To verify if notification configuration for probing clients which are tracked by CAS/MSE, the notifications over SOAP/Syslog are sent only once when the notification has "Non Recurring" as Frequency configuration	Passed if the notification is sent only once	CSCuj12261

Logical ID	Title	Description	Status	Defect
WLJ80S_Fix_42	Notification for Missing client	To verify if notification configuration for probing clients which are tracked by CAS/MSE, the notifications over SOAP/Syslog are sent at a periodic interval when the notification has " Recurring" as Frequency configuration	Passed if the notifications is sent out at the configured interval In a recurring fashion	CSCuj12261
WLJ80S_Fix_43	MAC filtering parameter cache	To check if the MAC filtering tracking is faster .	Passed if worked as expected.	CSCug46654
WLJ80S_Fix_44	CAPWAP data keep alive support	To verify if the CAPWAP data keep alive support exists or not from the AP to WLC when a NAT gateway exists between them.	Passed if the persists	CSCsq48449

WLC_Security

Logical ID	Title	Description	Status	Defects
WLJ80S_Sec_01	Performing EAP-Identity function in Win 7 client with Dot1x security	To check whether Win 7 client gets de-authenticated or not before EAP-identity timeout expires.	Passed	
WLJ80S_Sec_02	Performing EAP-Identity function in Win 7 client with WPA2+Dot1x security	To check whether Win 7 client gets de-authenticated or not before EAP-identity timeout expires.	Passed	

WLJ80S_Sec_03	Performing EAP-Identity function in Win 8 client with Dot1x security	To check whether Win 8 client gets de-authenticated or not before EAP-identity timeout expires.	Passed	
WLJ80S_Sec_04	Performing EAP-Identity function in Apple MacBook client with Dot1x security	To check whether Apple MacBook client gets de-authenticated or not before EAP-identity timeout expires.	Passed	
WLJ80S_Sec_05	Roaming a client between AP's in 5500 WLC with AAA override enabled.	To check whether Win 7 client roams between AP's in a 5500 WLC and gets ip from vlan mapped in that WLAN with AAA override enabled.	Passed	
WLJ80S_Sec_06	Roaming a client between AP's in 2500 WLC with AAA override enabled.	To check whether Win 7 client roams between AP's in a 2500 WLC and gets ip from vlan mapped in that WLAN with AAA override enabled.	Passed	
WLJ80S_Sec_07	Performing EAP-TLS method with Win 7 client.	To check whether Win 7 client is associated or not to Dot1x WLAN with EAP-TLS method.	Passed	
WLJ80S_Sec_08	Performing EAP-TLS method with Apple MacBook client.	To check whether Apple MacBook client is associated or not to Dot1x WLAN with EAP-TLS method.	Passed	
WLJ80S_Sec_09	Performing Dot1x in 5500 & 2500 WLC's and checking the nas-id in AAA server.	To check whether nas-id shown in AAA server is "system nas-id" or nas-id mapped in WLAN while performing dot1x security.	Passed	

WLJ80S_Sec_10	Performing Dot1x in 8500 & vWLC's and checking the nas-id in AAA server.	To check whether nas-id shown in AAA server is "system nas-id" or nas-id mapped in WLAN while performing dot1x security.	Passed	
WLJ80S_Sec_11	Configuring Router as NTP server in 5500 WLC & NCS and checking the sync via SNMP Trap log.	To check whether NTP sever & WLC are in sync or not via SNMP Trap log while rebooting the WLC.	Passed	
WLJ80S_Sec_12	Configuring 5500 WLC as NTP server in NCS and checking the Sync via SNMP Trap log.	To check whether NTP sever & WLC are in sync or not via SNMP Trap log while rebooting the WLC.	Passed	
WLJ80S_Sec_13	Configuring Router as NTP server in 8500 WLC & NCS and checking the sync via SNMP Trap log.	To check whether NTP sever & WLC are in sync or not via SNMP Trap log while rebooting the WLC.	Passed	
WLJ80S_Sec_14	Configuring 8500 WLC as NTP server in NCS and checking the Sync via SNMP Trap log.	To check whether NTP sever & WLC are in sync or not via SNMP Trap log while rebooting the WLC.	Passed	
WLJ80S_Sec_15	Configuring Router as NTP server in vWLC & NCS and checking the sync via SNMP Trap log.	To check whether NTP sever & WLC are in sync or not via SNMP Trap log while rebooting the WLC.	Passed	
WLJ80S_Sec_16	Configuring vWLC as NTP server in NCS and checking the Sync via SNMP Trap log.	To check whether NTP sever & WLC are in sync or not via SNMP Trap log while rebooting the WLC.	Passed	
WLJ80S_Sec_17	Enabling RADIUS NAC for a WLAN in 5500 WLC.	To check whether the configurations of Radius NAC is retained or not once WLC gets rebooted.	Passed	

WLJ80S_Sec_18	Enabling RADIUS NAC for a WLAN in 8500 WLC.	To check whether the configurations of Radius NAC is retained or not once WLC gets rebooted.	Passed	
WLJ80S_Sec_19	Enabling RADIUS NAC for a WLAN in vWLC.	To check whether the configurations of Radius NAC is retained or not once WLC gets rebooted.	Passed	
WLJ80S_Sec_20	Checking the Radius NAC configuration in WLC GUI after Upload/download the config file via TFTP.	To check whether the configurations of Radius NAC is retained or not after Upload/download the config file via TFTP.	Passed	
WLJ80S_Sec_21	Roaming a Win 7 client from 5500 HA WLC to 8500 WLC.	To check whether Win 7 client gets roamed or not from HA WLC to 8500 WLC and also checking whether error message displays or not in Syslog messages.	Passed	
WLJ80S_Sec_22	Roaming a Win 8 client from 5500 HA WLC to 8500 WLC.	To check whether Win 8 client gets roamed or not from HA WLC to 8500 WLC and also checking whether error message displays or not in Syslog messages.	Passed	
WLJ80S_Sec_23	Roaming a Apple MacBook client from 5500 HA WLC to 8500 WLC.	To check whether Apple MacBook client gets roamed or not from HA WLC to 8500 WLC and also checking whether error message displays or not in Syslog messages.	Passed	

WLJ80S_Sec_24	Checking the configurations of Local policy in 5500 WLC after Upload/download the config file.	To check whether Local policies(name which contain special characters) gets retained or not in WLC after Upload/download the config file.	Passed	
WLJ80S_Sec_25	Checking the configurations of Local policy in 2500 WLC after Upload/download the config file.	To check whether Local policies(name which contain special characters) gets retained or not in WLC after Upload/download the config file.	Passed	
WLJ80S_Sec_26	Checking the configurations of Local policy in 8500 WLC after Upload/download the config file.	To check whether Local policies(name which contain special characters) gets retained or not in WLC after Upload/download the config file.	Passed	
WLJ80S_Sec_27	Checking the configurations of Local policy in WiSM2 after Upload/download the config file.	To check whether Local policies(name which contain special characters) gets retained or not in WLC after Upload/download the config file.	Passed	
WLJ80S_Sec_28	Enabling Nac-Alert in 5500 WLC and checking the SNMP Traplog's while associating a nac-client.	To check whether nac-alert is shown in SNMP Trap log list or not when nac-client is associated to WLC.	Passed	
WLJ80S_Sec_29	Enabling Nac-Alert in 2500 WLC and checking the SNMP Traplog's while associating a nac-client.	To check whether nac-alert is shown in SNMP Trap log list or not when nac-client is associated to WLC.	Passed	
WLJ80S_Sec_30	Enabling Nac-Alert in 8500 WLC and checking the SNMP Traplog's while associating a nac-client.	To check whether nac-alert is shown in SNMP Trap log list or not when nac-client is associated to WLC.	Passed	

WLJ80S_Sec_31	Creating 150 WLAN's & 100 APgroups in 5500 WLC and checking the WLC Console.	To check whether error message dispayed or not in WLC console when 150 WLAN's & 100 Apgroups are created in WLC GUI.	Passed	
WLJ80S_Sec_32	Associating a Win 7 client to a WLAN(WPA2+PSK) with WEP in 5500 WLC and checking the message log.	To check whether when client tries to associate a WLAN with different L2 Security but SSID being same and checking the message log whether it displays correct error message or not.	Passed	
WLJ80S_Sec_33	Associating a Win 7 client to a WLAN(WPA2+PSK) with WEP in 8500 WLC and checking the message log.	To check whether when client tries to associate a WLAN with different L2 Security but SSID being same and checking the message log whether it displays correct error message or not.	Passed	
WLJ80S_Sec_34	Associating a Win 7 client to a WLAN(WPA2+PSK) with WEP in vWLC and checking the message log.	To check whether when client tries to associate a WLAN with different L2 Security but SSID being same and checking the message log whether it displays correct error message or not.	Passed	
WLJ80S_Sec_35	Associating a Win 7 client to a WLAN(WPA2+PSK) with WEP in WiSM2 and checking the message log.	To check whether when client tries to associate a WLAN with different L2 Security but SSID being same and checking the message log whether it displays correct error message or not.	Passed	

WLJ80S_Sec_36	Associating 7921 IPphone to CCKM enabled WLAN in 5500 WLC.	To check whether 7921 IPphone able to associate or not with CCKM enabled WLAN.	Passed	
WLJ80S_Sec_37	Associating 7925 IPphone to CCKM enabled WLAN in 5500 WLC.	To check whether 7925 IPphone able to associate or not with CCKM enabled WLAN.	Passed	
WLJ80S_Sec_38	Associating 7921 IPphone to CCKM enabled WLAN in 8500 WLC.	To check whether 7921 IPphone able to associate or not with CCKM enabled WLAN.	Passed	
WLJ80S_Sec_39	Associating 7925 IPphone to CCKM enabled WLAN in 8500 WLC.	To check whether 7925 IPphone able to associate or not with CCKM enabled WLAN.	Passed	
WLJ80S_Sec_40	Associating 7921 & 7925 IPphones to CCKM enabled WLAN in WLC and checking the voice call between them.	To check whether 7921 &7925 IPphones are associated or not with CCKM enabled WLAN and checking the voice call between them.	Passed	
WLJ80S_Sec_41	Associate a Win 7 client to WLAN with security Dot1x and change the credentials periodically.	To check whether by changing the credentials periodically from Machine to user credentials and checking whether clients gets de-authenticated or not while credentials change.	Passed	
WLJ80S_Sec_42	Associate a MacBook client to WLAN with security Dot1x and change the credentials periodically.	To check whether by changing the credentials periodically from Machine to user credentials and checking whether clients gets de-authenticated or not while credentials change.	Passed	

WLJ80S_Sec_43	Associate a Win 7 client to WLAN with security Dot1x and change the credentials periodically with Fast SSID enabled.	To check whether by changing the credentials periodically from Machine to user credentials and checking whether clients gets de-authenticated or not while credentials change with Fast SSID change enabled.	Passed	
WLJ80S_Sec_44	Associate a Apple MacBook client to WLAN with security Dot1x and change the credentials periodically with Fast SSID enabled.	To check whether by changing the credentials periodically from Machine to user credentials and checking whether clients gets de-authenticated or not while credentials change with Fast SSID change enabled.	Passed	
WLJ80S_Sec_45	Checking the Sync of Radius Server configuration in HA WLC's.	To check whether Radius server configuration getting sync or not between Active & Standby WLC's.	Passed	
WLJ80S_Sec_46	Changing the name of User while Win 7 client associating to Dot1x security.	To check whether client gets connected or not when name of the User changed slightly while connecting second time.	Passed	
WLJ80S_Sec_47	Changing the name of User while MacBook client associating to Dot1x security.	To check whether client gets connected or not when name of the User changed slightly while connecting second time.	Passed	

WLJ80S_Sec_48	Changing the name of User and also changing the EAP methods while Win 7 client associating to Dot1x security.	To check whether client gets connected or not when name of the User changed slightly while connecting second time and also changing the EAP method during association of second time.	Passed	
WLJ80S_Sec_49	Associating Win 8 client to WPA2+ AES+ PSK in 5500 WLC.	To check whether Win 8 client gets associated or not with WPA2+AES+PSK enabled WLAN in 5500 WLC.	Passed	
WLJ80S_Sec_50	Associating Win 8 client to WPA2+ AES+ PSK in 8500 WLC.	To check whether Win 8 client gets associated or not with WPA2+AES+PSK enabled WLAN in 8500 WLC.	Passed	
WLJ80S_Sec_51	Associating Win 8 client to WPA2+ AES+ PSK in vWLC.	To check whether Win 8 client gets associated or not with WPA2+AES+PSK enabled WLAN in vWLC.	Passed	
WLJ80S_Sec_52	Associating Win 8 client to WPA2+ AES+ Dot1x in 5500 WLC.	To check whether Win 8 client gets associated or not with WPA2+AES+Dot1x enabled WLAN in 5500 WLC.	Passed	
WLJ80S_Sec_53	Associating Win 8 client to WPA2+ AES+ Dot1x in 8500 WLC.	To check whether Win 8 client gets associated or not with WPA2+AES+Dot1x enabled WLAN in 8500 WLC.	Passed	
WLJ80S_Sec_54	Associating Win 8 client to WPA2+ AES+ Dot1x in vWLC.	To check whether Win 8 client gets associated or not with WPA2+AES+Dot1x enabled WLAN in vWLC.	Passed	

WLJ80S_Sec_55	Associating Win 8 client to WPA2+ AES+ Dot1x in WiSM2.	To check whether Win 8 client gets associated or not with WPA2+AES+Dot1x enabled WLAN in WiSM2.	Passed	
WLJ80S_Sec_56	Capturing the Radius Access-Request packet using Wireshark.	To check whether Message authenticator code goes to zero bits or not in Radius Access-Request packet when Radius Compatibility mode changed from Cisco ACS to Free RADIUS using Wireshark	Passed	
WLJ80S_Sec_57	Performing Mac Filtering in 5500 WLC using Multiple Radius Server.	To check whether Mac Filtering works or not while using Multiple Radius Server in a Flexconnect group in 5500 WLC.	Passed	
WLJ80S_Sec_58	Performing Mac Filtering in 8500 WLC using Multiple Radius Server.	To check whether Mac Filtering works or not while using Multiple Radius Server in a Flexconnect group in 5500 WLC.	Passed	
WLJ80S_Sec_59	Checking the configuration of client exclusion value in a WLAN after Upload/download the config file in 2500 WLC.	To check whether configurations of client exclusion value gets retained or not after Upload/download the config file in 2500 WLC.	Passed	
WLJ80S_Sec_60	Checking the configuration of client exclusion value in a WLAN after Upload/download the config file in vWLC.	To check whether configurations of client exclusion value gets retained or not after Upload/download the config file in vWLC.	Passed	

WLJ80S_Sec_61	Verfiying Management user login using TACACS server.	To check whether mgmt user login is authenticated or not by TACACS server.	Passed	
WLJ80S_Sec_62	Changing the credentials of Management User for second time in WLC & verfiying it using TACACS server.	To check whether mgmt user login is authenticated or not by TACACS server after changing the credentials in both WLC & TACACS server which is lesser value than first one.	Passed	
WLJ80S_Sec_63	Roaming a Win 7 client between WLC's with Security as Web-auth and checking the Web-auth timeout function.	To check whether error message occurs or not in msglog of WLC-A while client moves to WLC-B & web-auth timeout occurs while associating to WLC-B.	Passed	
WLJ80S_Sec_64	Roaming a Apple MacBook client between WLC's with Security as Web-auth and checking the Web-auth timeout function.	To check whether error message occurs or not in msglog of WLC-A while client moves to WLC-B & web-auth timeout occurs while associating to WLC-B.	Passed	
WLJ80S_Sec_65	Checking the configuration of Static-wep-encryption in a WLAN after Upload/download the config file in 2500 WLC.	To check whether configurations of Static-wep-encryption value gets retained or not after Upload/download the config file in 2500 WLC.	Passed	
WLJ80S_Sec_66	Checking the configuration of Static-wep-encryption in a WLAN after Upload/download the config file in vWLC.	To check whether configurations of Static-wep-encryption value gets retained or not after Upload/download the config file in vWLC.	Passed	

WLJ80S_Sec_67	Checking the configuration of Static-wep-encryption in a WLAN after Upload/download the config file in 8500 WLC.	To check whether configurations of Static-wep-encryption value gets retained or not after Upload/download the config file in 8500 WLC.	Passed	
WLJ80S_Sec_68	Performing Radius Server fallback.	To check whether Radius server fallback occurs or not when Primary Server is down.	Passed	
WLJ80S_Sec_69	Checking the configuration of SNMP parameters(users & communities) after Upload/download the config file in 8500 WLC.	To check whether configurations of SNMP parameters gets retained or not after Upload/download the config file in 8500 WLC.	Passed	
WLJ80S_Sec_70	Checking the configuration of SNMP parameters(users & communities) after Upload/download the config file in 5500 WLC.	To check whether configurations of SNMP parameters gets retained or not after Upload/download the config file in 5500 WLC.	Passed	
WLJ80S_Sec_71	Checking the configuration of SNMP parameters(users & communities) after Upload/download the config file in WiSM2.	To check whether configurations of SNMP parameters gets retained or not after Upload/download the config file in WiSM2.	Passed	
WLJ80S_Sec_72	Checking the configuration of 802.11a advanced parameters after Upload/download the config file in 2500 WLC.	To check whether configurations of 802.11a advanced parameters gets retained or not after Upload/download the config file in 2500 WLC.	Passed	

WLJ80S_Sec_73	Checking the configuration of 802.11a advanced parameters after Upload/download the config file in vWLC.	To check whether configurations of 802.11a advanced parameters gets retained or not after Upload/download the config file in vWLC.	Passed	
WLJ80S_Sec_74	Checking the configuration of 802.11a advanced parameters after Upload/download the config file in 8500 WLC.	To check whether configurations of 802.11a advanced parameters gets retained or not after Upload/download the config file in 8500 WLC.	Passed	
WLJ80S_Sec_75	Associating Win 7 client to Dot1x security in 5500 WLC and checking the message log.	To check whether traceback message occurs or not in 5500 WLC while associating Win 7 client to Dot1x WLAN.	Passed	
WLJ80S_Sec_76	Associating Apple MacBook client to Dot1x security in 8500 WLC and checking the message log.	To check whether traceback message occurs or not in 8500 WLC while associating Apple MacBook client to Dot1x WLAN.	Passed	
WLJ80S_Sec_77	Performing Accounting in 5500 WLC using Radius Server as ISE.	To check whether accounting function works or not in 5500 WLC by associating Win 7 client to ISE.	Passed	
WLJ80S_Sec_79	Checking the wIPS alarm in PI.	To check whether false wIPS alarm is produced or not in PI for neighbor AP's as rogue in other WLC when configured in same mobility group.	Passed	

WLJ80S_Sec_83	Associating 2 clients to WLAN with security Static WEP + Dot1x in 5500 WLC and checking the ping function between the clients.	To check whether clients associated or not to Locally switching WLAN with Static WEP + Dot1x in 5500 WLC and check whether ping function works or not between the clients.	Passed	
WLJ80S_Sec_84	Associating 2 clients to WLAN with security Static WEP + Dot1x in 8500 WLC and checking the ping function between the clients.	To check whether clients associated or not to Locally switching WLAN with Static WEP + Dot1x in 8500 WLC and check whether ping function works or not between the clients.	Passed	
WLJ80S_Sec_85	Checking the CLI command "show client ap 802.11b <Apname>" in 2500 WLC while client is in idle state.	To check whether cli commands displays the output correctly or not when client is associated to AP in 2500 WLC.	Passed	

AP_OEAP

Logical ID	Title	Description	Status	Defects
WLJ80S_oeap_01	Associating OEAP to 5500 WLC and checking the channels in WLC GUI/CLI & OEAP GUI.	To check whether channel is same in WLC GUI/CLI & OEAP GUI after the association of OEAP to 5500 WLC.	Passed	
WLJ80S_oeap_02	Associating OEAP to 2500 WLC and checking the channels in WLC GUI/CLI & OEAP GUI.	To check whether channel is same in WLC GUI/CLI & OEAP GUI after the association of OEAP to 2500 WLC.	Passed	

WLJ80S_oeap_03	Associating OEAP to 8500 WLC and checking the channels in WLC GUI/CLI & OEAP GUI.	To check whether channel is same in WLC GUI/CLI & OEAP GUI after the association of OEAP to 8500 WLC.	Passed	
WLJ80S_oeap_04	Associating a Win 7 Client to OEAP Personal SSID and checking the throughput of the client.	To check whether Win 7 client gets throughput more than 50 Mbps or not when it is connected to Personal SSID of OEAP using FTP.	Passed	
WLJ80S_oeap_05	Associating a Win 8 Client to OEAP Personal SSID and checking the throughput of the client.	To check whether Win 8 client gets throughput more than 50 Mbps or not when it is connected to Personal SSID of OEAP using FTP.	Passed	
WLJ80S_oeap_06	Checking the idle timeout function for Win 7 client when it is connected to OEAP.	To check whether Win 7 client goes to idle state or not when it moves out of range of OEAP.	Passed	
WLJ80S_oeap_07	Checking the idle timeout function for Win 8 client when it is connected to OEAP.	To check whether Win 8 client goes to idle state or not when it moves out of range of OEAP.	Passed	
WLJ80S_oeap_08	Checking the idle timeout function for Apple Macbook client when it is connected to OEAP.	To check whether Apple MacBook client goes to idle state or not when it moves out of range of OEAP.	Passed	
WLJ80S_oeap_09	Checking the idle timeout function for Android client when it is connected to OEAP.	To check whether Android client goes to idle state or not when it moves out of range of OEAP.	Passed	

WLJ80S_oeap_10	Associating OEAP to 5500 WLC and assigning static IP to OEAP in its local GUI and checking AP ip in WLC CLI.	To check whether static ip configured for AP in its local GUI is shown or not in 5500 WLC CLI.	Passed	
WLJ80S_oeap_11	Associating OEAP to 2500 WLC and assigning static IP to OEAP in its local GUI and checking AP ip in WLC CLI.	To check whether static ip configured for AP in its local GUI is shown or not in 2500 WLC CLI.	Passed	
WLJ80S_oeap_12	Associating OEAP to 8500 WLC and assigning static IP to OEAP in its local GUI and checking AP ip in WLC CLI.	To check whether static ip configured for AP in its local GUI is shown or not in 8500 WLC CLI.	Passed	
WLJ80S_oeap_13	Connecting WAN port of OEAP to router port and pinging the private address in router.	To check whether private address is pingable or not from WAN port of OEAP.	Passed	

WLC_HREAP

Logical ID	Title	Description	Status	Defects
WLJ80S_wlchreap_01	Client connection to a WLAN in local switching with DHCP required enabled	To verify whether the client gets stuck in the DHCP required state or not	Passed	
WLJ80S_wlchreap_02	Client connection to a WLAN in central switching with DHCP required enabled	To verify whether the client gets stuck in the DHCP required state or not	Passed	
WLJ80S_wlchreap_03	Ghost client entry in WLC - Local switching	To verify whether the WLC keeps ghost client entry or not	Passed	
WLJ80S_wlchreap_04	Ghost client entry in WLC - Central switching	To verify whether the WLC keeps ghost client entry or not	Passed	

WLJ80S_wlchreap_07	Applying NCS Light Weight AP Template to AP	To verify whether the NCS Light Weight AP Template is correctly applied to the AP or not	Passed	
WLJ80S_wlchreap_08	Applying NCS Light Weight AP Template to AP-3600/3700 with module inserted	To verify whether the NCS Light Weight AP Template is correctly applied to the AP or not	Passed	
WLJ80S_wlchreap_09	Ethernet cable disconnection in AP powered by AC adapter - Windows 7 Client	To verify whether the Windows 7 clients are getting disconnected and connected back or not when ethernet cable is disconnected and connected back to/from the AP powered by AC adapter	Passed	
WLJ80S_wlchreap_10	Ethernet cable disconnection in AP powered by AC adapter - Apple MAC Book Client	To verify whether the Apple MAC Book clients are getting disconnected and connected back or not when ethernet cable is disconnected and connected back to/from the AP powered by AC adapter	Passed	
WLJ80S_wlchreap_11	Ethernet cable disconnection in AP powered by AC adapter - Samsung S4 Mobile Client	To verify whether the Samsung S4 Mobile clients are getting disconnected and connected back or not when ethernet cable is disconnected and connected back to/from the AP powered by AC adapter	Passed	

WLJ80S_wlchreap_12	Ethernet cable disconnection in AP powered by AC adapter - Apple iphone Client	To verify whether the Apple iphone clients are getting disconnected and connected back or not when ethernet cable is disconnected and connected back to/from the AP powered by AC adapter	Passed	
WLJ80S_wlchreap_13	Duplicate association identifier entries for HREAP Windows 7 clients	To verify whether WLC is reporting duplicate association identifier entries for the clients associated to it or not	Passed	
WLJ80S_wlchreap_14	Duplicate association identifier entries for HREAP Apple MAC Book clients	To verify whether WLC is reporting duplicate association identifier entries for the clients associated to it or not	Passed	
WLJ80S_wlchreap_15	Duplicate association identifier entries for HREAP Samsung S4 Mobile clients	To verify whether WLC is reporting duplicate association identifier entries for the clients associated to it or not	Passed	
WLJ80S_wlchreap_16	Duplicate association identifier entries for HREAP Apple iphone clients	To verify whether WLC is reporting duplicate association identifier entries for the clients associated to it or not	Passed	
WLJ80S_wlchreap_19	Receiving broadcasts in wireless clients	To verify whether the broadcasts suchs as ARP are received in the wireless clients or not	Passed	
WLJ80S_wlchreap_20	Receiving broadcasts in wireless clients - with VLAN enabled	To verify whether the broadcasts suchs as ARP are received in the wireless clients or not when VLAN is configured	Passed	

WLJ80S_wlchreap_21	Windows 7 Client IP	To verify whether the Windows 7 client IP address is displayed correctly in the WLC or not	Passed	
WLJ80S_wlchreap_22	Apple MAC Book Client IP	To verify whether the Apple MAC Book client IP address is displayed correctly in the WLC or not	Passed	
WLJ80S_wlchreap_23	Samsung S4 Mobile Client IP	To verify whether the Samsung S4 Mobile client IP address is displayed correctly in the WLC or not	Passed	
WLJ80S_wlchreap_24	Apple iphone Client IP	To verify whether the Apple iphone client IP address is displayed correctly in the WLC or not	Passed	
WLJ80S_wlchreap_25	HREAP VLAN Mapping	To verify whether VLAN mapping is preserved after AP failover or not	Passed	
WLJ80S_wlchreap_26	Bridge-group ID assignation to sub-interfaces in AP	To verify whether different bridge IDs are assigned to the different sub-interfaces of the AP after failover or not	Passed	
WLJ80S_wlchreap_27	Bridge-group ID assignation to sub-interfaces in AP - by configuring AP Group	To verify whether different bridge IDs are assigned to the different sub-interfaces of the AP after failover or not	Passed	
WLJ80S_wlchreap_28	GTK Updates used for broadcast traffic encryption - For Windows 7 Clients	To verify whether AP sends GTK updates used for broadcast traffic encryption to its current Windows 7 clients	Passed	

WLJ80S_wlchreap_29	GTK Updates used for broadcast traffic encryption - For Apple MAC Book Clients	To verify whether AP sends GTK updates used for broadcast traffic encryption to its current Apple MAC clients	Passed	
WLJ80S_wlchreap_30	Client protocol after HREAP fault tolerance - Windows 7 Client	To verify whether the Windows 7 client protocol is displayed correctly in the WLC after HREAP fault tolerance or not	Passed	
WLJ80S_wlchreap_31	Client protocol after HREAP fault tolerance - Apple MAC Book Client	To verify whether the Apple MAC Book client protocol is displayed correctly in the WLC after HREAP fault tolerance or not	Passed	
WLJ80S_wlchreap_32	Client protocol after HREAP fault tolerance - Samsung S4 Mobile Client	To verify whether the Samsung S4 Mobile client protocol is displayed correctly in the WLC after HREAP fault tolerance or not	Passed	
WLJ80S_wlchreap_33	Client protocol after HREAP fault tolerance - Apple iphone Client	To verify whether the Apple iphone client protocol is displayed correctly in the WLC after HREAP fault tolerance or not	Passed	
WLJ80S_wlchreap_34	Web-authentication after inter-controller roaming - Windows 7 Client	To verify whether the Windows 7 client is prompted for web-authentication after inter-controller roaming or not	Passed	
WLJ80S_wlchreap_35	Web-authentication after inter-controller roaming - Apple MAC Book Client	To verify whether the Apple MAC Book client is prompted for web-authentication after inter-controller roaming or not	Passed	

WLJ80S_wlchreap_36	Client count displayed in Attached Clients field - Local switching	To verify whether the client count is displayed correctly in the Attached Clients field or not	Passed with exception	CSCup87391
WLJ80S_wlchreap_37	Client count displayed in Attached Clients field - Central switching	To verify whether the client count is displayed correctly in the Attached Clients field or not	Passed with exception	CSCup87391
WLJ80S_wlchreap_38	VLAN mappings after HREAP Local Switching AP reboot	To verify whether the VLAN mappings are changed after HREAP Local Switching AP reboot or not	Passed	
WLJ80S_wlchreap_39	VLAN mappings after HREAP Central Switching AP reboot	To verify whether the VLAN mappings are changed after HREAP Central Switching AP reboot or not	Passed	
WLJ80S_wlchreap_41	AP and WLC Association Counter - Windows 7 Client	To verify whether both AP and WLC association counter matches or not	Passed	
WLJ80S_wlchreap_42	AP and WLC Association Counter - Apple MAC Book Client	To verify whether both AP and WLC association counter matches or not	Passed	
WLJ80S_wlchreap_43	Transferring run-config - 5500, 2504 Series WLC	To verify whether WLAN and L2ACL config is preserved or not after transferring the run-config from 5500,2504 series WLC	Passed	
WLJ80S_wlchreap_44	Transferring run-config - 7500 Series WLC	To verify whether WLAN and L2ACL config is preserved or not after transferring the run-config from 7500 series WLC	Passed	

WLJ80S_wlchreap_45	Transferring run-config - WISM Series WLC	To verify whether WLAN and L2ACL config is preserved or not after transferring the run-config from WISM series WLC	Passed	

LWAPP-AP-SW

Logical ID	Title	Description	Status	Defects
WLJ80S_lwapp_01	AP using 100 mbps Ethernet Channel - with 5500, 2504 WLC	To verify whether AP's capwap connection to the WLC is lost or not when 100 mbps ethernet channel is used	Passed	
WLJ80S_lwapp_02	AP using 100 mbps Ethernet Channel - with 7500 WLC	To verify whether AP's capwap connection to the WLC is lost or not when 100 mbps ethernet channel is used	Passed	
WLJ80S_lwapp_03	AP using 100 mbps Ethernet Channel - with WISM WLC	To verify whether AP's capwap connection to the WLC is lost or not when 100 mbps ethernet channel is used	Passed	
WLJ80S_lwapp_04	"lwapp ap" Exec AP command for Ease of Deploy	To verify whether "lwapp ap" exec command works in AP CLI or not	Passed	
WLJ80S_lwapp_05	AP IOS Booting up in Recovery image with No Ethernet Link	To verify whether there is any informational trace backs found when AP IOS Booting up in Recovery image with No Ethernet Link	Passed	

WLJ80S_lwapp_06	AP Join process	To verify whether AP joins a WLC or not when both AP and WLC are in different subnets	Passed	

WCM_WEB

Logical ID	Title	Description	Status	Defects
WLJ80S_wcm-web_01	Extended UNII-2 Channels	To verify whether channel 120, 124, 128 are added by Extended UNII-2 channels or not	Passed	
WLJ80S_wcm-web_02	PSK key after WLAN modification	To verify whether PSK key get changed or not after WLAN modifications are done	Passed	
WLJ80S_wcm-web_03	Allowed power level	To verify whether Allowed power level is AP specific or not	Passed	
WLJ80S_wcm-web_04	EAP type mentioned	To verify whether both CLI and GUI output for EAP type matched or not	Passed	
WLJ80S_wcm-web_05	802.11a/n/ac Radio Edit page - Antenna Params	To verify whether the Antenna Parameters are shown appropriately or not in the 802.11a/n/ac radio page	Passed	
WLJ80S_wcm-web_06	802.11b/g/n Radio Edit page - Antenna Params	To verify whether the Antenna Parameters are shown appropriately or not in the 802.11b/g/n radio page	Passed	

WLJ80S_wcm-web_07	802.11a/n/ac Radio Edit page - RF Channel Assignment	To verify whether the RF Channel Assignment is shown appropriately or not in the 802.11a/n/ac radio page	Passed	
WLJ80S_wcm-web_08	802.11b/g/n Radio Edit page - RF Channel Assignment	To verify whether the RF Channel Assignment is shown appropriately or not in the 802.11b/g/n radio page	Passed	

WLC_Web-auth

Logical ID	Title	Description	Status	Defects
WLJ80S_WA_01	Clients reaching Session timeout when attached to a WLAN configured with L2 and L3 authentication	To verify whether both the L2 and L3 re-authentication occurs after the session timeout or not	Passed	
WLJ80S_WA_02	Clients reaching Session timeout when attached to a WLAN configured with L2 and L3 authentication - after roaming from one AP to an another	To verify whether both the L2 and L3 re-authentication occurs after the session timeout or not	Passed	
WLJ80S_WA_03	Web-auth guest access, custom bundle, pass-through with email - Windows 7 Client	To verify whether the custom web-auth page re-appears after entering incorrect email address or not	Passed	
WLJ80S_WA_04	Web-auth guest access, custom bundle, pass-through with email - Apple MAC Book Client	To verify whether the custom web-auth page re-appears after entering incorrect email address or not	Passed	
WLJ80S_WA_05	Web-auth bundle template - Internal Web-Auth	To verify whether the logout option works fine for the web-auth user or not	Passed	

WLJ80S_WA_06	Web-auth bundle template - External Web-Auth	To verify whether the logout option works fine for the web-auth user or not	Passed	
WLJ80S_WA_07	config certificate generate webadmin - Backup file uploaded	To verify whether "config certificate generate webadmin" is present or not in the backup file which is uploaded	Passed	
WLJ80S_WA_08	config certificate generate webadmin - Backup file downloaded	To verify whether "config certificate generate webadmin" is present or not with the backup file which is downloaded	Passed	

Alarms_UI

Logical ID	Title	Description	Status	Defects
WLJ80S_alm-ui_02	Sorting Unclassified Rogue AP's	To verify whether sorting functions works in Unclassified Rogue AP's page or not	Passed	
WLJ80S_alm-ui_03	Sorting Malicious Rogue AP's	To verify whether sorting functions works in Malicious Rogue AP's page or not	Passed	

Client_Mgmt

Logical ID	Title	Description	Status	Defects
WLJ80S_cl-mgnt_01	Reporting Period in Client summary report	To verify whether "1 Hour" can be selected or not as Reporting Period in Client summary report	Passed	

WLJ80S_cl-mgnt_02	NCS Client traffic report	To verify whether Client Traffic reported by each Floor value & Client Traffic reported by Sum of AP by Floor value matches or not	Passed	
WLJ80S_cl-mgnt_03	Client graph updation after service startup	To verify whether there is a break in Client graph updation after restart of services or not	Passed	
WLJ80S_cl-mgnt_04	Authenticated Client Count	To verify whether the Authenticated Client Count shown when Reported by: All and AP By Controller matches	Passed	

MSE_Install

Logical ID	Title	Description	Status	Defects
WLJ80S_install_01	Connection with NCS after upgrading the MSE	To verify whether MSE is getting connected to the NCS once after the MSE is upgraded or not	Passed	
WLJ80S_install_02	Connection with NCS after downgrading the MSE	To verify whether MSE is getting connected to the NCS once after the MSE is downgraded or not	Passed	
WLJ80S_install_03	Eth0 interface status after MSE reboot	To verify whether the eth0 interface is coming up or not after rebooting the MSE	Passed	
WLJ80S_install_04	Eth0 interface status after MSE upgrade	To verify whether the eth0 interface is coming up or not after upgrading the MSE	Passed	
WLJ80S_install_05	Eth0 interface status after MSE downgrade	To verify whether the eth0 interface is coming up or not after downgrading the MSE	Passed	

WLJ80S_install_06	NCS Communication Username and Password - MSE Virtual Appliance	To verify whether NCS Communication Credentials can be changed by invoking setup.sh script or not	Passed	
WLJ80S_install_07	NCS Communication Username and Password - Physical 3355 Series MSE	To verify whether NCS Communication Credentials can be changed by invoking setup.sh script or not	Passed	

NCS-MSE

Logical ID	Title	Description	Status	Defects
WLJ80S_pi-mse_01	MSE License Usage Table summary - Physical 3355 MSE	To verify whether Prime Infrastructure displays the MSE License Usage Table summary or not	Passed	
WLJ80S_pi-mse_02	MSE License Usage Table summary - MSE Virtual appliance	To verify whether Prime Infrastructure displays the MSE License Usage Table summary or not	Passed	
WLJ80S_pi-mse_03	Physical 3355 Series MSE - MSAP Service in NCS	To verify whether MSAP Services can be disabled from the NCS GUI or not	Passed	
WLJ80S_pi-mse_04	Permanent License for MSAP Services - Physical 3355 Series MSE	To verify whether permanent license for MSAP services is displayed or not	Passed	
WLJ80S_pi-mse_05	Virtual Appliance MSE - MSAP Service in NCS	To verify whether MSAP Services can be disabled from the NCS GUI or not	Passed	
WLJ80S_pi-mse_06	Permanent License for MSAP Services - Virtual Appliance MSE	To verify whether permanent license for MSAP services is displayed or not	Passed	

WLC-RRM

Logical ID	Title	Description	Status	Defects
WLJ80s_rrm_01	SNMP data sent from WLC 5508	To check if the format for object cLApDot11IfSlotId is not interpreted wrongly in the SNMP server message logs	Passed	
WLJ80s_rrm_02	SNMP data sent from WLC 2504	To check if the format for object cLApDot11IfSlotId is not interpreted wrongly in the SNMP server message logs	Passed	
WLJ80s_rrm_03	SNMP data sent from WLC 7500/8500	To check if the format for object cLApDot11IfSlotId is not interpreted wrongly in the SNMP server message logs	Passed	
WLJ80s_rrm_04	SNMP data sent from WLC WiSM2/vWLC	To check if the format for object cLApDot11IfSlotId is not interpreted wrongly in the SNMP server message logs	Passed	
WLJ80s_rrm_05	Message log after saving RRM data in 5508 controller	To check the message log in the controller for any save error after configuring any RRM data	Passed	
WLJ80s_rrm_06	Message log after saving RRM data in 7500/8500 controller	To check the message log in the controller for any save error after configuring any RRM data	Passed	
WLJ80s_rrm_07	Message log after saving RRM data in 2504 controller	To check the message log in the controller for any save error after configuring any RRM data	Passed	

WLJ80s_rrm_08	Message log after saving RRM data in WiSM2 controller	To check the message log in the controller for any save error after configuring any RRM data	Passed	
WLJ80s_rrm_09	802.11a monitor mode disable in 5508 Controller	To check if the 802.11a monitor mode can be disabled in 5508 controller after disabling RF group, DCA and TPC.	Passed	
WLJ80s_rrm_10	802.11a monitor mode disable in 7500/8500 Controller	To check if the 802.11a monitor mode can be disabled in 7500/8500 controller after disabling RF group, DCA and TPC.	Passed	
WLJ80s_rrm_11	802.11a monitor mode disable in 2504 Controller	To check if the 802.11a monitor mode can be disabled in 2504 controller after disabling RF group, DCA and TPC.	Passed	
WLJ80s_rrm_12	802.11a monitor mode disable in WiSM2/vWLC Controller	To check if the 802.11a monitor mode can be disabled in WiSM2/vWLC controller after disabling RF group, DCA and TPC.	Passed	
WLJ80s_rrm_13	Upload/Download with RF profile configs in 5508 WLC	To check if the configuration file which has been uploaded after configuring RF profiles can be downloaded into the controller without any issues	Passed	
WLJ80s_rrm_14	Upload/Download with RF profile configs in 7500/8500 WLC	To check if the configuration file which has been uploaded after configuring RF profiles can be downloaded into the controller without any issues	Passed	

WLJ80s_rrm_15	Upload/Download with RF profile configs in 2504 WLC	To check if the configuration file which has been uploaded after configuring RF profiles can be downloaded into the controller without any issues	Passed	
WLJ80s_rrm_16	Upload/Download with RF profile configs in WiSM2/vWLC	To check if the configuration file which has been uploaded after configuring RF profiles can be downloaded into the controller without any issues	Passed	
WLJ80s_rrm_17	Checking the Configuration guide for note	To check if the configuration guide has a note regarding AP channel change	Passed	
WLJ80s_rrm_18	Client Association with Aps in 5508 Controller after some number of HA failovers	To check if the simulated and real clients are able to associate to the AP in controller without any problem after couple of HA failovers	Passed	
WLJ80s_rrm_19	Client Association with Aps in 7500/8500 Controller after some number of HA failovers	To check if the simulated and real clients are able to associate to the AP in controller without any problem after couple of HA failovers	Passed	
WLJ80s_rrm_20	Client Association with Aps in 2504 Controller after some number of HA failovers	To check if the simulated and real clients are able to associate to the AP in controller without any problem after couple of HA failovers	Passed	
WLJ80s_rrm_21	RRM AP Neighbor list sync to HA Standby after switchover in 5508 HA pair	To check if the RRM AP neighbor list is synced to HA pair after switchover	Passed	

WLJ80s_rrm_22	RRM AP Neighbor list sync to HA Standby after switchover in 2504 HA pair	To check if the RRM AP neighbor list is synced to HA pair after switchover	Passed	
WLJ80s_rrm_23	RRM AP Neighbor list sync to HA Standby after switchover in 7500 HA pair	To check if the RRM AP neighbor list is synced to HA pair after switchover	Passed	
WLJ80s_rrm_24	RRM AP Neighbor list sync to HA Standby after switchover in 8500 HA pair	To check if the RRM AP neighbor list is synced to HA pair after switchover	Passed	
WLJ80s_rrm_25	RF profile config in uploaded file from 5508 controller	To check if the RF profile config which is configured in the WLC is present in the uploaded configuration file	Passed	
WLJ80s_rrm_26	RF profile config in uploaded file from 2504 controller	To check if the RF profile config which is configured in the WLC is present in the uploaded configuration file	Passed	
WLJ80s_rrm_27	RF profile config in uploaded file from 7500/8500 controller	To check if the RF profile config which is configured in the WLC is present in the uploaded configuration file	Passed	
WLJ80s_rrm_28	RF profile config in uploaded file from WiSM2/vWLC controller	To check if the RF profile config which is configured in the WLC is present in the uploaded configuration file	Passed	
WLJ80s_rrm_29	Configuring Advance 802.11[a|b] monitor noise out of range in 5508 Controller	To check if the command for advance 802.11a/b monitor noise when configured out of range retains after WLC reboot	Passed	

WLJ80s_rrm_30	Configuring Advance 802.11[a|b] monitor noise out of range in 7500/8500 Controller	To check if the command for advance 802.11a/b monitor noise when configured out of range retains after WLC reboot	Passed	
WLJ80s_rrm_31	Configuring Advance 802.11[a|b] monitor noise out of range in 2504 Controller	To check if the command for advance 802.11a/b monitor noise when configured out of range retains after WLC reboot	Passed	
WLJ80s_rrm_32	Configuring Advance 802.11[a|b] monitor noise out of range in WiSM2/vWLC Controller	To check if the command for advance 802.11a/b monitor noise when configured out of range retains after WLC reboot	Passed	
WLJ80s_rrm_33	CleanAir air-quality summary in Aps joined to 5508 controller	To check if all AQ's are present for entire channel list for monitor mode AP joined to the controller	Passed	
WLJ80s_rrm_34	CleanAir air-quality summary in Aps joined to 7500/8500 controller	To check if all AQ's are present for entire channel list for monitor mode AP joined to the controller	Passed	
WLJ80s_rrm_35	CleanAir air-quality summary in Aps joined to 2504 controller	To check if all AQ's are present for entire channel list for monitor mode AP joined to the controller	Passed	
WLJ80s_rrm_36	CleanAir air-quality summary in Aps joined to WiSM2/vWLC controller	To check if all AQ's are present for entire channel list for monitor mode AP joined to the controller	Passed	
WLJ80s_rrm_37	Disabling 802.11a DCA in WLC 5508	To Disable 802.11a DCA and check if advanced 802.11a summary shows only the supported channels	Passed	

WLJ80s_rrm_38	Disabling 802.11a DCA in WLC 7500/8500	To Disable 802.11a DCA and check if advanced 802.11a summary shows only the supported channels	Passed	
WLJ80s_rrm_39	Disabling 802.11a DCA in WLC 2504	To Disable 802.11a DCA and check if advanced 802.11a summary shows only the supported channels	Passed	
WLJ80s_rrm_40	Disabling 802.11a DCA in WLC WiSM2	To Disable 802.11a DCA and check if advanced 802.11a summary shows only the supported channels	Passed	
WLJ80s_rrm_41	Disabling 802.11a DCA in vWLC	To Disable 802.11a DCA and check if advanced 802.11a summary shows only the supported channels	Passed	
WLJ80s_rrm_42	802.11a channel load/noise / DCA channel lists configurations in the uploaded backup file from controller in 5508 controller	To upload, donwload and upload the config to controller and check for the 802.11 channel load/noise/DCA channel configs	Passed	
WLJ80s_rrm_43	802.11a channel load/noise / DCA channel lists configurations in the uploaded backup file from controller in 7500/8500 controller	To upload, donwload and upload the config to controller and check for the 802.11 channel load/noise/DCA channel configs	Passed	
WLJ80s_rrm_44	802.11a channel load/noise / DCA channel lists configurations in the uploaded backup file from controller in 2504 controller	To upload, donwload and upload the config to controller and check for the 802.11 channel load/noise/DCA channel configs	Passed	

WLJ80s_rrm_45	802.11a channel load/noise / DCA channel lists configurations in the uploaded backup file from controller in WiSM2 controller	To upload, donwload and upload the config to controller and check for the 802.11 channel load/noise/DCA channel configs	Passed	
WLJ80s_rrm_46	802.11a channel load/noise / DCA channel lists configurations in the uploaded backup file from controller in vWLC controller	To upload, donwload and upload the config to controller and check for the 802.11 channel load/noise/DCA channel configs	Passed	
WLJ80s_rrm_47	802.11a DCA channel list after upgrade in 5508 Controller	To check if the congigured 802.11 DCA channel list prevails after upgrade	Passed	
WLJ80s_rrm_48	802.11a DCA channel list after upgrade in 7500/8500 Controller	To check if the congigured 802.11 DCA channel list prevails after upgrade	Passed	
WLJ80s_rrm_49	802.11a DCA channel list after upgrade in 2504 Controller	To check if the congigured 802.11 DCA channel list prevails after upgrade	Passed	
WLJ80s_rrm_50	802.11a DCA channel list after upgrade in WiSM2 Controller	To check if the congigured 802.11 DCA channel list prevails after upgrade	Passed	
WLJ80s_rrm_51	802.11a DCA channel list after upgrade in vWLC Controller	To check if the congigured 802.11 DCA channel list prevails after upgrade	Passed	
WLJ80s_rrm_52	unexpected channels on New Aps	To check if any brand new AP comes up with unexpected channels on it.	Passed	
WLJ80s_rrm_53	Rifs rx disableafter 11n mode disabled/re-enabled in 5508 controller	To check If Rifs rx disable doesn't remain after 11n mode disabled/re-enabled	Passed	

WLJ80s_rrm_54	Rifs rx disableafter 11n mode disabled/re-enabled in 7500/8500 controller	To check If Rifs rx disable doesn't remain after 11n mode disabled/re-enabled	Passed	
WLJ80s_rrm_55	Rifs rx disableafter 11n mode disabled/re-enabled in 2504 controller	To check If Rifs rx disable doesn't remain after 11n mode disabled/re-enabled	Passed	
WLJ80s_rrm_56	Rifs rx disableafter 11n mode disabled/re-enabled in WiSM2 controller	To check If Rifs rx disable doesn't remain after 11n mode disabled/re-enabled	Passed	
WLJ80s_rrm_57	Rifs rx disableafter 11n mode disabled/re-enabled in vWLC controller	To check If Rifs rx disable doesn't remain after 11n mode disabled/re-enabled	Passed	
WLJ80s_rrm_58	Restoring "wlan security static-wep-key encryption" settings to the WLC 5508	To check if the wlan security static-wep-key settings are restored to WLC after uploading and downloading the same config to the WLC	Passed	
WLJ80s_rrm_59	Restoring "wlan security static-wep-key encryption" settings to the WLC 7500	To check if the wlan security static-wep-key settings are restored to WLC after uploading and downloading the same config to the WLC	Passed	
WLJ80s_rrm_60	Restoring "wlan security static-wep-key encryption" settings to the WLC 8500	To check if the wlan security static-wep-key settings are restored to WLC after uploading and downloading the same config to the WLC	Passed	
WLJ80s_rrm_61	Restoring "wlan security static-wep-key encryption" settings to the WLC 2504	To check if the wlan security static-wep-key settings are restored to WLC after uploading and downloading the same config to the WLC	Passed	

WLJ80s_rrm_62	Restoring "wlan security static-wep-key encryption" settings to the WLC WiSM2	To check if the wlan security static-wep-key settings are restored to WLC after uploading and downloading the same config to the WLC	Passed	
WLJ80s_rrm_63	Restoring "wlan security static-wep-key encryption" settings to the vWLC	To check if the wlan security static-wep-key settings are restored to WLC after uploading and downloading the same config to the WLC	Passed	
WLJ80s_rrm_64	Restoring some settings in the WLC 5508	To check if all the configurations are restored correctly in WLC	Passed	
WLJ80s_rrm_65	Restoring some settings in the WLC 7500	To check if all the configurations are restored correctly in WLC	Passed	
WLJ80s_rrm_66	Restoring some settings in the WLC 8500	To check if all the configurations are restored correctly in WLC	Passed	
WLJ80s_rrm_67	Restoring some settings in the WLC 2504	To check if all the configurations are restored correctly in WLC	Passed	
WLJ80s_rrm_68	Restoring some settings in the WLC WiSM2	To check if all the configurations are restored correctly in WLC	Passed	
WLJ80s_rrm_69	Restoring some settings in the vWLC	To check if all the configurations are restored correctly in WLC	Passed	
WLJ80s_rrm_70	INVALID TIMER with traceback in 5508 controller	To check if the Invalid timer traceback is observed when the controller registers AP	Passed	

WLJ80s_rrm_71	INVALID TIMER with traceback in 7500/8500 controller	To check if the Invalid timer traceback is observed when the controller registers AP	Passed	
WLJ80s_rrm_72	INVALID TIMER with traceback in WiSM2/vWLC controller	To check if the Invalid timer traceback is observed when the controller registers AP	Passed	
WLJ80s_rrm_73	INVALID TIMER with traceback in 2504 controller	To check if the Invalid timer traceback is observed when the controller registers AP	Passed	
WLJ80s_rrm_74	Maximum number of allowed clients on a WLAN in 5508 controller	To check if the maximum number of clients per wlan is not exceeded in controller	Passed	
WLJ80s_rrm_75	Maximum number of allowed clients on a WLAN in 7500/8500 controller	To check if the maximum number of clients per wlan is not exceeded in controller	Passed	
WLJ80s_rrm_76	Maximum number of allowed clients on a WLAN in 2504 controller	To check if the maximum number of clients per wlan is not exceeded in controller	Passed	
WLJ80s_rrm_77	Maximum number of allowed clients on a WLAN in WiSM2/vWLC controller	To check if the maximum number of clients per wlan is not exceeded in controller	Passed	
WLJ80s_rrm_78	Show client detail MAC Address	To check if show client detail <Mac address> include client statistics	Passed	

All AP-Radio

Logical ID	Title	Description	Status	Defects

WLJ80S_aprad_01	Radio reset, profile changes, radio bring up in AP1142	To check if the Radio in AP1142 goes into down state with protocol being down after a radio reset, profile changes, radio bring up etc	Passed	
WLJ80S_aprad_02	Radio reset, profile changes, radio bring up in AP1262	To check if the Radio in AP1262 goes into down state with protocol being down after a radio reset, profile changes, radio bring up etc	Passed	
WLJ80S_aprad_03	Radio reset, profile changes, radio bring up in AP2600	To check if the Radio in AP2600 goes into down state with protocol being down after a radio reset, profile changes, radio bring up etc	Passed	
WLJ80S_aprad_04	Radio reset, profile changes, radio bring up in AP3500,3600	To check if the Radio in AP3500,3600 goes into down state with protocol being down after a radio reset, profile changes , radio bring up etc	Passed	
WLJ80S_aprad_05	Radio reset, profile changes, radio bring up in AP3700	To check if the Radio in AP3700 goes into down state with protocol being down after a radio reset, profile changes , radio bring up etc	Passed	
WLJ80S_aprad_06	Multicast traffic after fast roaming in 5508 controllers having Aps	To verify if the multicast traffic works fine even after the fast roaming of the clients on a particular wlan	Passed	
WLJ80S_aprad_07	Multicast traffic after fast roaming in 7500/8500 controllers having Aps	To verify if the multicast traffic works fine even after the fast roaming of the clients on a particular wlan	Passed	

WLJ80S_aprad_08	Multicast traffic after fast roaming in 2504/WiSM2 controllers having Aps	To verify if the multicast traffic works fine even after the fast roaming of the clients on a particular wlan	Passed	
WLJ80S_aprad_09	Transmitting and receiving on 1142 AP	To verify if the clients are able to transfer data without any problem and the transmitting and receiving on the AP radio is smooth.	Passed	
WLJ80S_aprad_10	Transmitting and receiving on 3500/3600 AP's	To verify if the clients are able to transfer data without any problem and the transmitting and receiving on the AP radio is smooth.	Passed	
WLJ80S_aprad_11	Transmitting and receiving on 1262 AP's	To verify if the clients are able to transfer data without any problem and the transmitting and receiving on the AP radio is smooth.	Passed	
WLJ80S_aprad_12	Transmitting and receiving on 3700 AP's	To verify if the clients are able to transfer data without any problem and the transmitting and receiving on the AP radio is smooth.	Passed	

AP-DFS

Logical ID	Title	Description	Status	Defects
WLJ80S_dfs_01	AP association after DFS Scan event in 5508 controller	To check if the AP association to the controller prevails after a DFS	Passed	

WLJ80S_dfs_02	AP association after DFS Scan event in 7500/8500 controller	To check if the AP association to the controller prevails after a DFS	Passed	
WLJ80S_dfs_03	AP association after DFS Scan event in 2504 controller	To check if the AP association to the controller prevails after a DFS	Passed	
WLJ80S_dfs_04	AP association after DFS Scan event in WiSM2/vWLC controller	To check if the AP association to the controller prevails after a DFS	Passed	
WLJ80S_dfs_05	5GHZ channel in 5508 controller	To check if the 5GHz channel doesn't revert back to original configured static channel	Passed	
WLJ80S_dfs_06	5GHZ channel in 7500/8500 controller	To check if the 5GHz channel doesn't revert back to original configured static channel	Passed	
WLJ80S_dfs_07	5GHZ channel in 2504 controller	To check if the 5GHz channel doesn't revert back to original configured static channel	Passed	
WLJ80S_dfs_08	5GHZ channel in WiSM2/vWLC controller	To check if the 5GHz channel doesn't revert back to original configured static channel	Passed	
WLJ80S_dfs_09	AP's behaviour after all available 11a channels are exhausted in 5508 controller	To check if the AP doesn't go to Discovery state after all the available 802.11a channels are exhausted after a DFS event	Passed	
WLJ80S_dfs_10	AP's behaviour after all available 11a channels are exhausted in 5508 controller	To check if the AP doesn't go to Discovery state after all the available 802.11a channels are exhausted after a DFS event	Passed	

WLJ80S_dfs_11	AP's behaviour after all available 11a channels are exhausted in 5508 controller	To check if the AP doesn't go to Discovery state after all the available 802.11a channels are exhausted after a DFS event	Passed	

AP Radio

Logical ID	Title	Description	Status	Defects
WLJ80S_ap-rad_01	Client count check in AP with flexconnect mode	To verify the client count in LAP with Flexconnect mode	Passed	
WLJ80S_ap-rad_02	Client count check in AP with local mode	To verify the client count in LAP with Local mode	Passed	
WLJ80S_ap-rad_03	1142 AP functionality in local mode after upgrading to 7.4 MR3	To verify the 1142 AP performance after upgrading to 7.4 MR3	Passed	
WLJ80S_ap-rad_04	1142 AP functionality in flexconnect mode after upgrading to 7.4 MR3	To verify the 1142 AP performance after upgrading to 7.4 MR4	Passed	
WLJ80S_ap-rad_05	802.11b/g radio disabled and reboot the AP	To verify whether AP comes with 802.11b/g radio disabled after reload	Passed	
WLJ80S_ap-rad_06	Unified images in AP with client traffic	To verify the unified images with client traffic	Passed	
WLJ80S_ap-rad_07	Autonomous ios images in AP	To verify the APS 3500/3600 while boot up with autonomous ios images	Passed	
WLJ80S_ap-rad_08	Recovery ios images in AP	To verify the APS 3500/3600 wile boot up with recovery ios images	Passed	

WLJ80S_ap-rad_17	AP radio performance when stop-on-failure set	To verify whether the radios should not reset frequently when stop-on-failure set	Passed	
WLJ80S_ap-rad_18	AP radio performance when client is frequently associating/disassociting with stop-on-failure set-WLC 5508, 2504	To verify the AP radio performance when client is frequently associating/disassoaciating with stop-on-failure set	Passed	
WLJ80S_ap-rad_19	AP radio performance when client is frequently associating/disassociting with stop-on-failure set-WLC 7500,8500	To verify the AP radio performance when client is frequently associating/disassoaciating with stop-on-failure set	Passed	
WLJ80S_ap-rad_20	AP radio performance when client is frequently associating/disassociting with stop-on-failure set-WLC WiSM2	To verify the AP radio performance when client is frequently associating/disassoaciating with stop-on-failure set	Passed	
WLJ80S_ap-rad_21	AP radio performance when AP fallover between pri/sec with stop-on-failure set-WLC 5508, 2504	To verify the AP radio performance when AP fallover between pri/sec with stop-on-failure set	Passed	
WLJ80S_ap-rad_22	AP radio performance when AP fallover between pri/sec with stop-on-failure set-WLC 7500, 8500	To verify the AP radio performance when AP fallover between pri/sec with stop-on-failure set	Passed	

WLJ80S_ap-rad_23	AP radio performance when AP fallover between pri/sec with stop-on-failure set-WLC WiSM2	To verify the AP radio performance when AP fallover between pri/sec with stop-on-failure set	Passed	
WLJ80S_ap-rad_24	AP radio performance when frequent client ass/disass and/or AP fallback when stop-on-failure disabled	To verify the AP radio performance when frequent client association/disassociation and/or AP fallback between pri/sec with stop-on-failure disabled	Passed	
WLJ80S_ap-rad_25	AP radios operational status in WLC	To verify the AP radios operational status in WLC	Passed	
WLJ80S_ap-rad_26	AP radios operational status in WLC and client connectivity	To verify the AP radios operational status in WLC and client connectivity	Passed	

WLC HA

Logical ID	Title	Description	Status	Defects
WLJ80S_WLCHA_01	ACL config sync between the Active and Standby Hot WLC	To verify whether ACLs has been synced between the Active and Standby Hot WLC	Passed	
WLJ80S_WLCHA_02	Client connectivity with aaa overriden WLAN after switchover-Samsung Galaxy, iPhone	To verify whether clients access details specified in the acls after switchover	Passed	
WLJ80S_WLCHA_03	Client connectivity with aaa overriden WLAN after switchover-Macbook Pro, Windows 7 JOS	To verify whether clients access details specified in the acls after switchover	Passed	

WLJ80S_WLCHA_04	Mobility mac address between Active and Standby WLC	To verify whether Mobility Mac address and redundancy Mac address is shown correctly in Active and Standby WLC	Passed	
WLJ80S_WLCHA_05	Mobility mac address between Active and Standby WLC where primary WLC is replaced with new WLC	To verify whether Mobility Mac address and redundancy Mac address is shown correctly in Active and Standby WLC	Passed	
WLJ80S_WLCHA_06	HA failover after powercycling the Active WLC	To verify whether HA failover is successful after saving the config and powercycling the Active WLC	Passed	
WLJ80S_WLCHA_07	Bulk config sync between the WLCs	To verify whether Bulk config sync is successful between the WLCs in HA pair	Passed	
WLJ80S_WLCHA_08	Incremental config sync between the WLCs	To verify whether run time config has been synced between the WLCs	Passed	
WLJ80S_WLCHA_09	Flexconnect Local switching config sync between the WLCs	To verify whether FLS config has been synced between WLC HA pair	Passed	
WLJ80S_WLCHA_10	FLS config after HA failover	To verify whether the FLS config has been retained after HA switchover	Passed	
WLJ80S_WLCHA_11	Client connectivity with FLS enabled WLAN after WLC switchover-Samsung galaxy, iPhone	To verify whether client serves with local switching after WLC switchover	Passed	
WLJ80S_WLCHA_12	Client connectivity with FLS enabled WLAN after WLC switchover-Macbook pro, windows 7 JOS	To verify whether client serves with local switching after WLC switchover	Passed	

WLJ80S_WLCHA_13	Config upload in HA pair	To verify whether config upload is succesful and all config has been imported to HA pair	Passed	
WLJ80S_WLCHA_14	Disable the mgmt default GW failover and Active mgmt port down	To verify whether there is no switchover when the mgmt default GW failover is disabled and Active mgmt port is down	Passed	
WLJ80S_WLCHA_15	Disable the mgmt default GW failover and Standby mgmt port down	To verify whether there is no reboot occured when the mgmt default GW failover is disabled and Standby mgmt port is down	Passed	
WLJ80S_WLCHA_16	Enable the mgmt default GW failover and Active mgmt port down	To verify whether switchover happens when mgmt default GW is enabled and Active mgmt port is down	Passed	
WLJ80S_WLCHA_17	Enable the mgmt default GW failover and Standby mgmt port down	To verify whether reboot of standby occurs when mgmt default GW is enabled and Standby mgmt port is down	Passed	
WLJ80S_WLCHA_18	SNMP trap notification in case of WLC switchover	To verify whether SNMP trap notification is generated when there is a WLC switchover	Passed	
WLJ80S_WLCHA_19	Unknown messages in msglog/syslog	To verify whether there are no unknown messages in syslog/msglog	Passed	
WLJ80S_WLCHA_20	Unit of secondary box which is converted	To verify whether unit of converted secondary box should show as "Secondary"	Passed	
WLJ80S_WLCHA_22	HA failover during software download to Standby HOT WLC with gw unreachable	To verify the HA failover process during software download to Standby WLC	Passed	

WLJ80S_WLCHA_23	HA failover during software download to Active WLC with GW unreachable to Active	To verify the HA failover process during software download and GW unreachable from Active controller	Passed	
WLJ80S_WLCHA_24	HA failover during software download to Active WLC with GW unreachable to both Active and Standby HOT	To verify the HA failover process during software download to Standby WLC and GW unreachable from both Active and Standby WLC	Passed	
WLJ80S_WLCHA_25	HA failover during SW download to Active and Standby and red port down in Standby WLC	To verify the HA failover process during sw download and red port down in Standby WLC	Passed	
WLJ80S_WLCHA_26	HA failover during SW download to Active and Standby and red port down in Active WLC	To verify the HA failover process during sw download and red port down in Active WLC	Passed	
WLJ80S_WLCHA_27	HA failover during SW download to Active and Standby and red port down in both Active and Standby WLC	To verify the HA failover process during sw download and red port down in Active and StandbyWLC	Passed	
WLJ80S_WLCHA_28	Redundancy laxtiming configurations	To verify whether lax timing is configurable in HA pair	Passed	
WLJ80S_WLCHA_29	HA multiple switchovers with number of Aps added	To verify whether multiple switchovers between the WLCs are working fine with number of Aps added	Passed	
WLJ80S_WLCHA_30	HA false switchover	To verify there is no false switchover between the HA pair	Passed	
WLJ80S_WLCHA_32	Check for no irrelevant HA error messages on syslog or console	To verify there is no unwanted/irrelevant HA related messages printed on console or syslog	Passed	

Backup - Restore

Logical ID	Title	Description	Status	Defects
WLJ80S_BnR_01	PI backup with FTP password set as 16 char - pPI	To verify whether PI backup has been taken when FTP password is set upto 16 chars	Passed	
WLJ80S_BnR_02	PI backup with FTP password set as 16 char - vPI	To verify whether PI backup has been taken when FTP password is set upto 16 chars	Passed	
WLJ80S_BnR_03	PI restore in standalone box with invalid backup file	To verify whether backup of invalid file in standalone box prints the appropriate error message	Passed	
WLJ80S_BnR_04	PI restore in HA enabled box with invalid backup file	To verify whether backup of invalid file in HA enabled box prints the appropriate error message	Passed	
WLJ80S_BnR_05	PI restore with a valid backup file	To verify whether restoring a valid backup file succeeds	Passed	
WLJ80S_BnR_06	PI application backup and restore	To verify the application backup and restore operation is successful	Passed	
WLJ80S_BnR_07	PI appliance backup and restore	To verify the appliance backup and restore operation is successful	Passed	
WLJ80S_BnR_08	PI application backup- automatic and manual	To verify whether automatic and manual backup are working fine in PI application without any issues	Passed	
WLJ80S_BnR_09	PI backup and checking domain maps	To verify whether taking backup internally by filling 75% in /opt and check the domain maps under /opt/CSCOlumos/domainmaps	Passed	

WLJ80S_BnR_10	PI backup and checking domain maps	To verify whether taking backup to an external server by filling 75% in /opt and check the domain maps under /opt/CSCOlumos/domainmaps	Passed	
WLJ80S_BnR_11	PI backup and checking domain maps	To verify whether taking backup internally by filling 95% in /opt and check the domain maps under /opt/CSCOlumos/domainmaps	Passed	
WLJ80S_BnR_12	PI backup and checking domain maps	To verify whether taking backup to an external server by filling 95% in /opt and check the domain maps under /opt/CSCOlumos/domainmaps	Passed	

System

Logical ID	Title	Description	Status	Defects
WLJ80S_Sys_01	PI IP/Hostname change upon re-setup	To verify whether changing the hostname/IP when re-setup starts the PI services completely and works fine	Passed with exception	CSCup56865
WLJ80S_Sys_02	PI external SNMP server config	To verify whether external server config on PI doesnot make the services down	Passed	

NCS HA

Logical ID	Title	Description	Status	Defects

WLJ80S_pi-ha_01	PI HA relationship when secondary shutdown first	To verify the PI HA relationship when primary and secondary servers shutdown at the same time and made secondary to be up first	Passed	
WLJ80S_pi-ha_02	PI HA relationship when primary shutdown first	To verify the PI HA relationship when primary and secondary servers shutdown at the same time and made primary to be up first	Passed	
WLJ80S_pi-ha_03	PI failback to primary server with failover set as "Manual"	To verify whether failback is working fine where failover type is set as "Manual" in case of primary server failure due to hardware issue	Passed	
WLJ80S_pi-ha_04	PI failback to primary server with failover set as "Manual"	To verify whether failback is working fine where failover type is set as "Manual" in case of primary server failure due to network issue	Passed	
WLJ80S_pi-ha_05	PI failback to primary server with failover set as "Automatic"	To verify whether failback is working fine where failover type is set as "Automatic" in case of primary server failure due to hardware issue	Passed	
WLJ80S_pi-ha_06	PI failback to primary server with failover set as "Automatic"	To verify whether failback is working fine where failover type is set as "Automatic" in case of primary server failure due to network issue	Passed	
WLJ80S_pi-ha_07	PI failback to primary where primary server is freshly installed after failover	To verify whether failback to freshly installed primary server is working fine	Passed	

WLJ80S_pi-ha_08	Pi Licensing after failover to secondary when primary server is failed due to HW failure	To verify whether PI license has been initialized in secondary after failover to secondary server in case of primary failed	Passed	
WLJ80S_pi-ha_09	Pi Licensing after failover to secondary when primary server is failed due to NW failure	To verify whether PI license has been initialized in secondary after failover to secondary server in case of primary failed	Passed	

NCS Clean-Air

Logical ID	Title	Description	Status	Defects
WLJ80S_cleanair_01	PI AQ Index Vs Time report	To verify whether AQ Minimum Index should be smaller than AQ Average Index in AQ Index Vs Time report graph	Passed	

NCS Licensing

Logical ID	Title	Description	Status	Defects
WLJ80S_lic_01	PI License works fine	To verify whether PI license is working fine in PI physical appliance	Passed	
WLJ80S_lic_02	PI License works fine	To verify whether PI license is working fine in PI virtual appliance	Passed	

MSE Software

Logical ID	Title	Description	Status	Defects

WLJ80S_msesw_01	check MSE password reset reflect after reboot	To verify whether change password work after the automatic reboot of MSE	Passed	
WLJ80S_msesw_02	Check the MSE services start up in 5mints	To verify whether the MSE services and health monitor started in 5 mints	Passed	
WLJ80S_msesw_03	Check whether the MSE show the error message for Hardware test	To verify the MSE hardware test shows the error message as "No such file or directory"	Passed	
WLJ80S_msesw_04	check the location change distance value on event notification	To verify whether the location change distance value does not zero for event definition	Passed	
WLJ80S_msesw_05	check MSE NMSP status after upgrade	To verify whether MSE reachable from PI and check NMSP status after upgrade	Failed	CSCup21225
WLJ80S_msesw_06	MSE Faiback functionality when secondary MSE comes up first after shutdownof both MSE	To verify whether MSE failover and failback works as expected when shutdown MSE's	Failed	CSCuo56629
WLJ80S_msesw_08	check MSE error message on syslog only error message triggered on the process	To verify whether the error message triggered to syslog when process trigger the error	Passed	
WLJ80S_msesw_09	Context Aware Notifications Multiple event Definitions using syslog	To verify whether the Context Aware Notifications for Multiple event Definitions created	Failed	CSCup93585
WLJ80S_msesw_10	Check MSE display any error after upgrade	To verify whether the MSE displays message for every few seconds after upgrade	Passed	

WLC LAN

Logical ID	Title	Description	Status	Defects
WLJ80S_lan_02	Enable and disable the controller LAG on controller	To verify whether enable and disable of the controller LAG shows any error message	Passed	
WLJ80S_lan_03	check controller send the syslog message when LAG port up and down	To verify whether the controller send LAG down and up message to the syslog server successfully	Passed	
WLJ80S_lan_04	check the access point disconnected during controller image download	To verify whether the access point gets disconnected during downloading wlc image from the TFTP	Passed	
WLJ80S_lan_05	check the GARP request are forward to AP and client	To verify whether the GARP request are not forward to AP and client is successful	Passed	

WLC SNMP

Logical ID	Title	Description	Status	Defects
WLJ80S_snmp_01	install WLC MIB file on SNMP manager	To verify whether can install the WLC MIB file into the SNMP manager successfully	Passed	
WLJ80S_snmp_02	Check whether can add the ip and mask as 0.0.0.0 on WLC SNMP community	To verify the SNMP community ip and mask can be configured as 0.0.0.0	Passed	
WLJ80S_snmp_03	check the restore of WLC SNMP configuration on the new WLC image	To verify whether the SNMP backup configuration restored correctly on the new wlc image	Passed	

WLJ80S_snmp_04	check the controller MIB returns any invalid Tx rate	To verify whether wireless controller does not return any invalid Tx rate s	Passed	
WLJ80S_snmp_05	Restriction for changing access level on the default SNMP public	To verify the whether the deny creation of default SNMP entries works as expected	Passed	

Maps

Logical ID	Title	Description	Status	Defects
WLJ80S_maps_01	check whether the backup of NCS hold the .PNG and .GIF file under domain maps directory	To verify the NCS doesn't delete the .PNG and .GIF files after back completed.	Passed	
WLJ80S_maps_02	Check whether the NCS maps floor view access point protocol setting changes as expected	To verify the access point protocol setting on NCS floor view changes properly	Passed	
WLJ80S_maps_03	Check whether the NCS maps floor view client filter setting changes as expected	To verify the client filter setting on NCS floor view changes properly when saved	Passed	
WLJ80S_maps_04	check whether disabling the AP radio cause noise in NCS heat maps	To verify NCS air quality heat map shows the while noise around after disabling AP radio	Passed	
WLJ80S_maps_05	Check whether center of the heat map is shifted from AP in NCS planning mode	To verify the NCS floor planning mode shows the heat map offset	Passed	
WLJ80S_maps_06	Check whether the AP status on the NCS building view after disable it on WLC	To verify the AP status on NCS building view changes when disable AP administratively	Passed	

WLJ80S_maps_07	Check whether the AP status on the NCS floor view after disable it on WLC	To verify the AP status on NCS floor view changes when disable AP administratively	Passed	
WLJ80S_maps_08	check whether the heat maps load slowly even disable the dynamic heat maps on Maps	To verify the loading of heat maps as expected	Passed	

WLC-Mobility

Logical ID	Title	Description	Status	Defects
WLJ80S_mob_01	Check the DTLS handshake between mobility anchor and mobility controller	To verify whether the DTLS handshake is successful between mobility anchor and mobility controller	Passed	
WLJ80S_mob_02	Check mobility peers can be removed and no controller should be added as mobility anchors	To check if many controllers can be added as Mobility peers , removed etc	Passed	
WLJ80S_mob_03	Create WLC mobility peer with hash value none	To verify whether the mobility peer with hash value as none is created successfully	Passed	
WLJ80S_mob_04	Add the WLC maximum mobility group member as 72	To verify whether the WLC maximum mobility group member 72 added successfully	Passed	

Location

Logical ID	Title	Description	Status	Defects

WLJ80S_WLCLO_01	Check whether the additional config displays after upgrade the WLC	To verify the upgrade of WLC shows additional default config when take the config backup to tftp	Passed	
WLJ80S_WLCLO_02	Check whether default aggregate probe request on wlan as 500msec when client load balancing is not enabled and no MSE connected	To verify the default aggregate probe request on wlan as 500msec when no MSE connected	Passed	
WLJ80S_WLCLO_03	Check whether default aggregate probe request on wlan as 200msec when client load balancing is not enabled and MSE connected	To verify the default aggregate probe request on wlan as 200msec when MSE connected	Passed	
WLJ80S_WLCLO_04	Check whether the location tracking working as expected	To verify the location tracking does not show the invalid rssi -128	Passed	

WLC Multicast

Logical ID	Title	Description	Status	Defects
WLJ80S_MU_01	check the L2 multicast status for uploaded and download config file	To verify whether L2 multicast status as expected when download and upload the config	Passed	
WLJ80S_MU_02	check the disabled multicast on WLAN with flexconnect local switching enabled status after upgrade	To verify whether the multicast on WLAN works as expected after the upgrade successfully	Passed	

AP-Regulatory

Logical ID	Title	Description	Status	Defects
WLJ80S_apreg_01	Check allowed frequency range for the japan regulatory domain	To verify whether the allowed frequency range works as expected successfully	Passed	
WLJ80S_apreg_02	JP World wide marking in Beacon/probe response	To verify whether the JP world wide mode marked in beacon/probe response instead of J4 successfully	Passed	
WLJ80S_apreg_03	Check whether the AP3502 radio interface operation status working as expected	To verify the AP3502 radio interface operation status and beaconing properly	Passed	

WLC DHCP

Logical ID	Title	Description	Status	Defects
WLJ80S_dhcp_02	check the DHCP assignment required is retained on WLAN	To verify whether the DHCP assignment required is retained on WLAN after WLC reboot	Passed	
WLJ80S_dhcp_03	check the DHCP assignment required is retained on WLAN with LAG disabled	To verify whether the DHCP assignment required is retained on WLAN after WLC reboot with LAG disabled	Passed	

WLC Guestaccess

Logical ID	Title	Description	Status	Defects

WLJ80S_GA_01	Check the WLC guest user account expiry	To verify whether the WLC guest user account expired on specified date successfully	Passed	
WLJ80S_GA_02	Check the wlc gets error log for maximum allowed login for the guest account	To verify whether WLC logs gets error message for maximum allowed login successfully	Passed	
WLJ80S_GA_03	Check the wlc gets error log for client entry deletion	To verify whether wlc gets error log for client entry deletion successfully	Passed	
WLJ80S_GA_04	Check the wlc gets error log for the configured user account	To verify whether wlc gets error log for only configured user account	Passed	

WLC NTP

Logical ID	Title	Description	Status	Defects
WLJ80S_ntp_01	Check the Controller NTP synchronization after reboot	To verify whether the controller successfully synchronize with NTP after WLC reboot	Passed	
WLJ80S_ntp_02	Check the controller uses assigned NTP port number for both source and destination port number	To verify whether the controller uses the correct port number for NTP	Passed	

CAPWAP-AP-SW

Logical ID	Title	Description	Status	Defects

WLJ80S_capwap-sw_01	Check the joined AP's name in the controller are correct	To verify whether the AP name in the AP join statistics and in the AP summary are same in the 2504 controller CLI	Passed	
WLJ80S_capwap-sw_02	Check the joined AP's name in the controller are correct	To verify whether the AP name in the AP join statistics and in the AP summary are same in the 2504 controller GUI	Passed	
WLJ80S_capwap-sw_03	Check AP joined to the statically configured controller ip address	To verify whether the AP is joined with statically configured controller ip address by using env_var	Passed	
WLJ80S_capwap-sw_04	Configure the Syslog level for the Lightweight AP	To verify whether the Syslog level for the lightweight AP ia configured successfully	Failed	CSCup82047
WLJ80S_capwap-sw_05	Configure and check the interface availability in the controller	To verify whether the interface is configured and its available after upgrading the image in the 5508 controller	Passed	
WLJ80S_capwap-sw_06	Configure and check the interface availability in the controller	To verify whether the interface is configured and its available after upgrading the image in the 8500 controller	Passed	
WLJ80S_capwap-sw_07	Check flexconnect AP maintains its configured name after joining with the controller	To verify whether the flexconnect AP maintains its configured name after joining with the 5508 controller.	Passed	
WLJ80S_capwap-sw_08	Check flexconnect AP maintains its configured name after joining with the controller	To verify whether the flexconnect AP maintains its configured name after joining with the 8500 controller.	Passed	

WLJ80S_capwap-sw_09	Check AP disassociation alarm in PI	To verify whether the AP disassociation alarm is triggered in PI only when AP gets disjoined from the controller	Passed	
WLJ80S_capwap-sw_10	Check AP disassociation alarm in virtual PI	To verify whether the AP disassociation alarm is triggered in virtual PI only when AP gets disjoined from the controller	Passed	
WLJ80S_capwap-sw_11	Check AP gets image correctly from the controller	To verify whether the AP gets images correctly when multiple images are upgraded in the 5508 controller GUI repeatedly without rebooting	Passed	
WLJ80S_capwap-sw_12	Check AP gets image correctly from the controller	To verify whether the AP gets images correctly when multiple images are upgraded in the 8500 controller GUI repeatedly without rebooting	Passed	

AP-capwap

Logical ID	Title	Description	Status	Defects
WLJ80S_capwap_01	Check the CAPWAP client timers : WLC 5508	To verify whether the CAPWAP client timers is shown in 5508 controller	Passed	
WLJ80S_capwap_02	Check the CAPWAP client timers : WLC 8500	To verify whether the CAPWAP client timers is shown in 8500 controller	Passed	
WLJ80S_capwap_03	Check Ap's are joined with controller	To verify whether the AP's are joined with the controller successfully	Passed	

WLJ80S_capwap_05	Configure the TX power level for the AP in the 5508 controller via GUI	To verify whether the TX power level of the Lightweight AP is configured from the 5508 controller GUI	Passed	
WLJ80S_capwap_06	Configure the TX power level for the AP in the 5508 controller via CLI	To verify whether the TX power level of the Lightweight AP is configured from the 5508 controller CLI	Passed	
WLJ80S_capwap_07	Check the AP association with the controller by enabling DFS	To verify whether the AP is joined with the controller after enabling DFS.	Passed	
WLJ80S_capwap_08	Check the AP association with the controller by disabling proxy arp	To verify whether the AP joined with the controller when they two are in different VLAN and no proxy arp.	Passed	

WLC-License

Logical ID	Title	Description	Status	Defects
WLJ80S_lic_01	Configure the priority for licenses in wlc 5508 CLI	To verify whether the license priority is configured from wlc 5508 CLI	Passed	
WLJ80S_lic_02	Configure the priority for licenses in virtual wlc CLI	To verify whether the license priority is configured from virtual wlc CLI	Passed	
WLJ80S_lic_03	Configure the priority for licenses in wlc 5508 GUI	To verify whether the license priority is configured from wlc 5508 GUI	Passed	
WLJ80S_lic_04	Configure the priority for licenses in virtual wlc GUI	To verify whether the license priority is configured from virtual wlc GUI	Passed	

WLJ80S_lic_05	Check the supported AP count in the licenses in 5508 controller CLI	To check whether the licenses having the maximum ap's supported count as mentioned in the controller - 5508 CLI	Passed	
WLJ80S_lic_06	Check the supported AP count in the licenses in virtual controller CLI	To check whether the licenses having the maximum ap's supported count as mentioned in the controller - virtual CLI	Passed	
WLJ80S_lic_07	Check the supported AP count in the licenses in 5508 controller GUI	To check whether the licenses having the maximum ap's supported count as mentioned in the controller - 5508 GUI	Passed	
WLJ80S_lic_08	Check the supported AP count in the licenses in virtual controller GUI	To check whether the licenses having the maximum ap's supported count as mentioned in the controller - virtual GUI	Passed	
WLJ80S_lic_10	Check the permanent base license removal from the controller	To verify whether the permanent base license is removed from the controller successfully via controller CLI.	Passed	
WLJ80S_lic_11	Check the permanent base license removal from the controller	To verify whether the permanent base license is removed from the controller successfully via controller GUI.	Passed	
WLJ80S_lic_12	WLC 5508: Check HA pair is enabled after removing all licenses	To verify whether after removing licenses also HA pair is enabled between 5508 controllers.	Passed	

WLJ80S_lic_13	WLC 8500: Check HA pair is enabled after removing all licenses	To verify whether after removing licenses also HA pair is enabled between 8500 controllers.	Passed	
WLJ80S_lic_14	WLC 5508: configure HA between the controllers and make a role change	To verify whether HA role change is done between 5508 controllers	Passed	
WLJ80S_lic_15	WLC 8500: configure HA between the controllers and make a role change	To verify whether HA role change is done between 8500 controllers	Passed	
WLJ80S_lic_16	Check the removal of base license without EULA.	To check without accepting end user license agreement, the base license is removed from the 5508 controller.	Passed	
WLJ80S_lic_17	Check the removal of base license without EULA.	To check without accepting end user license agreement, the base license is removed from the virtual controller.	Passed	
WLJ80S_lic_20	Check the evaluation license removal from the controller	To verify whether the deleted evaluation license is present after rebooting the controller	Passed	

AP-GUI

Logical ID	Title	Description	Status	Defects
WLJ80S_apgui_01	Configure power level of radio0 in Autonomous AP GUI	To verify whether the autonomous ap power level for radio0 is configured via GUI	Passed	
WLJ80S_apgui_02	Configure power level of radio0 in Autonomous AP CLI	To verify whether the autonomous ap power level for radio0 is configured via CLI	Passed	

WLJ80S_apgui_03	Configure power level of radio1 in Autonomous AP GUI	To verify whether the autonomous ap power level for radio1 is configured via GUI	Passed	
WLJ80S_apgui_04	Configure power level of radio1 in Autonomous AP CLI	To verify whether the autonomous ap power level for radio1 is configured via CLI	Passed	
WLJ80S_apgui_05	Configure MCS rate for radio0 in Autonomous AP GUI	To verify whether the autonomous ap MCS rate for radio0 is configured via GUI	Passed	
WLJ80S_apgui_06	Configure MCS rate for radio0 in Autonomous AP CLI	To verify whether the autonomous ap MCS rate for radio0 is configured via CLI	Passed	
WLJ80S_apgui_07	Configure MCS rate for radio1 in Autonomous AP GUI	To verify whether the autonomous ap MCS rate for radio1 is configured via GUI	Passed	
WLJ80S_apgui_08	Configure MCS rate for radio1 in Autonomous AP CLI	To verify whether the autonomous ap MCS rate for radio1 is configured via CLI	Passed	
WLJ80S_apgui_09	Configure an VLAN and associate the client in Autonomous AP	To verify whether the VLAN is configured and able to create open authentication SSID in that VLAN and client can able to associate by using that SSID.	Passed	

WLJ80S_apgui_10	Configure an VLAN and associate the client in Autonomous AP CLI	To verify whether the VLAN is configured and able to create open authentication SSID in that VLAN and client can able to associate by using that SSID in Autonomous AP CLI.	Passed	
WLJ80S_apgui_11	Configure RADIUS server in autonomous AP	To verify whether the RADIUS server is configured and able to authenticate the client in autonomous ap.	Passed	
WLJ80S_apgui_12	Configure Open authentication SSID in Autonomous AP GUI	To verify whether the SSID with open authentication is configured in autonomous AP GUI	Passed	
WLJ80S_apgui_13	Configure Open authentication SSID in Autonomous AP CLI	To verify whether the SSID with open authentication is configured in autonomous AP CLI	Passed	
WLJ80S_apgui_14	Configure an SSID with WEP Encryption in AP GUI	To verify whether the SSID with WEP encryption is configured and able to associate with the client in AP GUI	Passed	
WLJ80S_apgui_15	Configure an SSID with WEP Encryption in AP CLI	To verify whether the SSID with WEP encryption is configured and able to associate with the client in AP CLI	Passed	
WLJ80S_apgui_16	Configure an SSID with WPA Pre share key in AP CLI	To verify whether the SSID with WPA pre share key is configured and able to associate with the client in AP CLI	Passed	

WLJ80S_apgui_17	Configure an SSID with WPA Pre share key in AP GUI	To verify whether the SSID with WPA pre share key is configured and able to associate with the client in AP GUI	Passed	

Alarm-Server

Logical ID	Title	Description	Status	Defects
WLJ80S_alm_svr_01	Severity level of AP reboot reason in PI	To verify whether the AP reboot reason alarm is triggered with the configured severity level in PI	Passed	
WLJ80S_alm_svr_02	Severity level of AP reboot reason in virtual PI	To verify whether the AP reboot reason alarm is triggered with the configured severity level in virtual PI	Passed	
WLJ80S_alm_svr_03	AP association alarm in PI	To verify whether the AP association with controller alarm is triggered successfully in PI	Passed	
WLJ80S_alm_svr_04	AP association alarm in virtual PI	To verify whether the AP association with controller alarm is triggered successfully in virtual PI	Passed	
WLJ80S_alm_svr_05	Email notification for Rogue AP in PI	To verify whether the mail server is configured and email notification is sent when rogue ap alarm is triggered in PI	Passed	

WLJ80S_alm_svr_06	Email notification for Rogue AP in virtual PI	To verify whether the mail server is configured and email notification is sent when rogue ap alarm is triggered in virtual PI	Passed	
WLJ80S_alm_svr_07	Appliance power supply failure alarm in PI	To verify whether the Appliance power supply failure alarm is triggered in PI	Passed	
WLJ80S_alm_svr_08	Appliance power supply failure alarm in virtual PI	To verify whether the Appliance power supply failure alarm is triggered in virtual PI	Passed	
WLJ80S_alm_svr_09	Configure Notification Receiver in PI and send traps	To Verify whether notification receiver is configured successfully in PI and able to get traps from PI	Passed	
WLJ80S_alm_svr_10	Configure Notification Receiver in virtual PI and send traps	To Verify whether notification receiver is configured successfully in virtual PI and able to get traps from virtual PI	Passed	

Reports-Wireless

Logical ID	Title	Description	Status	Defects
WLJ80S_RW_01	Report for Rogue AP count summary in PI	To verify the whether the report for rogue ap count summary is generated in PI	Passed	
WLJ80S_RW_02	Report for Rogue AP count summary in virtual PI	To verify the whether the report for rogue ap count summary is generated in virtual PI	Passed	

WLJ80S_RW_03	Report for Rogue AP's in PI	To verify the whether the report for Rogue AP's is generated in PI	Passed	
WLJ80S_RW_04	Report for Rogue AP's in virtual PI	To verify the whether the report for Rogue AP's is generated in virtual PI	Passed	
WLJ80S_RW_05	Report for Client Traffic in PI	To verify the whether the report for Client traffic is generated in PI	Passed	
WLJ80S_RW_06	Report for Client Traffic in virtual PI	To verify the whether the report for Client traffic is generated in virtual PI	Passed	
WLJ80S_RW_07	Report for Client summary in PI	To verify the whether the report for Client summary is generated in virtual PI	Passed	
WLJ80S_RW_08	Report for Client summary in virtual PI	To verify the whether the report for Client summary is generated in virtual PI	Passed	

WLC-TFTP

Logical ID	Title	Description	Status	Defects
WLJ80S_tftp_01	Configure High Availability - WLC 5508	To verify whether the High availability is configured and running in WLC 5508.	Passed	
WLJ80S_tftp_02	Upgrade image in WLC-5508	To verify whether the primary AP bundle image is downloaded to the associated AP's in wlc 5508 after image upgradation was done.	Passed	

WLJ80S_tftp_03	Configure High Availability - WLC 7500	To verify whether the High availability is configured and running in WLC 7500.	Passed	
WLJ80S_tftp_04	Upgrade image in WLC-7500	To verify whether the primary AP bundle image is downloaded to the associated AP's in wlc 7500 after image upgradation was done.	Passed	
WLJ80S_tftp_05	Configure High Availability - WLC 2504	To verify whether the High availability is configured and running in WLC 2504.	Passed	
WLJ80S_tftp_06	Upgrade image in WLC-2504	To verify whether the primary AP bundle image is downloaded to the associated AP's in wlc 2504 after image upgradation was done.	Passed	
WLJ80S_tftp_07	Running Configuration file upload - WLC 5508	To verify whether the running configuration file is uploaded from the WLC 5508 to the tftp server	Passed	
WLJ80S_tftp_08	Running Configuration file upload - WLC 2504	To verify whether the running configuration file is uploaded from the WLC 2504 to the tftp server	Passed	
WLJ80S_tftp_09	Running Configuration file upload - WLC 7500	To verify whether the running configuration file is uploaded from the WLC 7500 to the tftp server	Passed	

Prime-UI

Logical ID	Title	Description	Status	Defects

WLJ80S_prime_01	Change the theme of PI using Chrome browser	To verify the change of PI theme in chrome browser	Passed	
WLJ80S_prime_02	Change the theme of PI using Firefox browser	To verify the change of PI theme in Firefox browser	Passed	
WLJ80S_prime_03	Change the theme of PI using IE browser	To verify the change of PI theme in IE browser	Passed	
WLJ80S_prime_04	Change the theme of virtual PI using Chrome browser	To verify the change of virtual PI theme in chrome browser	Passed	
WLJ80S_prime_05	Change the theme of virtual PI using Firefox browser	To verify the change of virtual PI theme in Firefox browser	Passed	
WLJ80S_prime_06	Change the theme of virtual PI using IE browser	To verify the change of virtual PI theme in IE browser	Passed	
WLJ80S_prime_07	Check the PI clients and users using Chrome browser	To verify the details of clients and users in PI are shown by chrome browser	Passed	
WLJ80S_prime_08	Check the PI clients and users using Firefox browser	To verify the details of clients and users in PI are shown by Firefox browser	Passed	
WLJ80S_prime_09	Check the PI clients and users using IE browser	To verify the details of clients and users in PI are shown by IE browser	Passed	
WLJ80S_prime_10	Check the virtual PI clients and users using Chrome browser	To verify the details of clients and users in virtual PI are shown by chrome browser	Passed	
WLJ80S_prime_11	Check the virtual PI clients and users using Firefox browser	To verify the details of clients and users in virtual PI are shown by Firefox browser	Passed	
WLJ80S_prime_12	Check the virtual PI clients and users using IE browser	To verify the details of clients and users in virtual PI are shown by IE browser	Passed	

Admin

Logical ID	Title	Description	Status	Defects
WLJ80S_admin_01	Severity count in PI	To verify whether the severity count is matched with the specified count in the PI	Passed	
WLJ80S_admin_02	Severity count in Virtual PI	To verify whether the severity count is matched with the specified count in the virtual PI	Passed	
WLJ80S_admin_03	Add FTP server in virtual PI	To verify whether the FTP server is configured in PI	Passed	
WLJ80S_admin_04	Add FTP server in PI	To verify whether the FTP server is configured in virtual PI	Passed	
WLJ80S_admin_05	Update the FTP server credentials in PI	To verify whether the FTP server user credentials are updated and able to access the server from PI	Passed	
WLJ80S_admin_06	Update the FTP server credentials in virtual PI	To verify whether the FTP server user credentials are updated and able to access the server from virtual PI	Passed	

NCS-Upgrade

Logical ID	Title	Description	Status	Defects
WLJ80S_upg_01	Creating a Local repository using PI CLI	To configure local repository from PI CLI	Passed	
WLJ80S_upg_02	Creating a Remote repository using PI CLI	To configure a remote repository from PI CLI	Passed	
WLJ80S_upg_03	View the repository using PI CLI	To view the configured repository from PI CLI	Passed	

WLJ80S_upg_04	Taking application backup using PI CLI	To verify application backup is taken for PI from CLI	Passed	
WLJ80S_upg_05	Taking appliance backup using PI CLI	To verify appliance backup is taken for PI from CLI	Passed	
WLJ80S_upg_06	Scheduling automatic application backup using PI GUI	To verify automatic application backup is taken for PI fromGUI	Passed	
WLJ80S_upg_07	Create Repository using PI GUI	To verify repository is configured from PI GUI	Passed	
WLJ80S_upg_08	Taking application backup using PI GUI	To verify application backup is taken for PI from GUI	Passed	
WLJ80S_upg_09	View backup information using PI CLI	To verify the history of the PI backup	Passed	
WLJ80S_upg_10	View the PI status	To check the status of the PI	Passed	
WLJ80S_upg_11	Stop the PI server	To verify whether the PI is stopped successfully.	Passed	
WLJ80S_upg_12	Upgrading the PI	To verify whether the PI is upgraded successfully	Passed	
WLJ80S_upg_13	Start the PI server	To verify whether the PI is started successfully	Passed	
WLJ80S_upg_14	Restore the application to the PI server	To verify whether the application is restored correctly in the PI	Passed	
WLJ80S_upg_15	Restore the appliance to the PI server	To verify whether the appliance is restored correctly in the PI	Passed	
WLJ80S_upg_16	Add a switch and severity level in PI	To configure a switch in PI and changing the severity level for switch down alarm	Passed	
WLJ80S_upg_17	Check switch down alarm in PI	To verifying the alarm in PI by bringing down the switch.	Passed	

WLJ80S_upg_18	Add a switch and severity level in Virtual PI	To configure a switch in virtual PI and changing the severity level for switch down alarm	Passed	
WLJ80S_upg_19	Check switch down alarm in virtual PI	To verifying the alarm in virtual PI by bringing down the switch.	Passed	

Reporting

Logical ID	Title	Description	Status	Defects
WLJ80S_rep_01	Run button in PI Report launch pad	To verify whether the Run button is working on Report Launch pad in PI	Passed	
WLJ80S_rep_02	Save button in PI Report launch pad	To verify whether the Save button is working on Report Launch pad in PI	Passed	
WLJ80S_rep_03	Run button in virtual PI Report launch pad	To verify whether the Run button is working on Report Launch pad in virtual PI	Passed	
WLJ80S_rep_04	Save button in virtual PI Report launch pad	To verify whether the Save button is working on Report Launch pad in virtual PI	Passed	

AAA

Logical ID	Title	Description	Status	Defects
WLJ80S_aaa_01	Configure an access point in PI	To verify the access point configuration in PI GUI	Passed	

WLJ80S_aaa_02	Change the access point parameters in PI	To verify the access point parameters (name, mode, admin status, etc) are able to change when PI is integrated with ACS server	Passed	
WLJ80S_aaa_03	Configure an access point in virtual PI	To verify the access point configuration in virtual PI GUI	Passed	
WLJ80S_aaa_04	Change the access point parameters in virtual PI	To verify the access point parameters (name, mode, admin status, etc) are able to change when virtual PI is integrated with ACS server	Passed	

AP-HREAP

Logical ID	Title	Description	Status	Defects
WLJ80S_hreap_01	Client connection fails after WLC failover	To verify if client connection failed after WLC failover	Passed	
WLJ80S_hreap_02	Flex Connect Group Creation	To check the creation of Flex group	Passed	
WLJ80S_hreap_03	Flex Connect group with wlan to vlan mapping	To connect flex connect group with wlan to vlan mapping	Passed	
WLJ80S_hreap_04	station-role root fallback shutdown for capwap AP	To verify the 'station-role root fallback shutdown' feature in capwap AP	Passed	
WLJ80S_hreap_05	web-auth with flex connect AP	To verify the web-auth connection in flex connect set up	Passed	
WLJ80S_hreap_06	Verification of bridge group id with single interface	Check whether one bridge-group ID is assigned to single sub-interfaces in H-reap	Passed	

WLJ80S_hreap_07	Client connectivity with Flex Connect Local switching	Check whether SSIDs are stopped beaconing with Flex Connect Local Switching enabled	Passed	
WLJ80S_hreap_08	Checking P2P Blocking action in a WLAN	To verify whether P2P blocking action works or not in a WLAN while associating 2 clients to this WLAN in a single AP.	Passed	

WLC-Web

Logical ID	Title	Description	Status	Defects
WLJ80S_web_01	AP group Name with 14 characters	To verify the Ap group name & status	Passed	
WLJ80S_web_02	AP group name & status verification	To verify the Ap group name & status	Passed	
WLJ80S_web_03	Antenna selection a-antenna (use antenna A)	To verify the antenna selection (A)	Passed	
WLJ80S_web_04	Antenna selection ab-antenna (use antennas A & B)	To verify the antenna selection (A &B)	Passed	
WLJ80S_web_05	Antenna selection ab-antenna (use antennas A & B &C	To verify the antenna selection (A &B &C)	Passed	
WLJ80S_web_06	Antenna selection ab-antenna (use antennas A & B& C& D	To verify the antenna selection (A & B& C& D)	Passed	
WLJ80S_web_07	Status of rifs rx after disbale/Re enable	To verify the status of rifs rx	Passed	

WLJ80S_web_09	Moving a client between different WLANs with AAA override enabled	To check whether client gets ip from mapped vlan or not when it gets moved between different WLANS with different security types.	Passed	

Autonomous_APs

Logical ID	Title	Description	Status	Defects
WLJ80S_AAP_02	Refresh from network fails when Autonomous AP is present on the floor	To verify whether refresh from network fails when Autonomous AP is present on the floor	Passed	
WLJ80S_AAP_03	Unable to download aIOS image for AP3G1/AP3G2 image Family	To verify Aios image for AP3G1/AP3G2 gets download	Passed	
WLJ80S_AAP_04	Unable to download aIOS image for AP3G1/AP3G2 image Family	To verify Aios image for AP3G1/AP3G2 gets download	Passed	
WLJ80S_AAP_05	Unable to download aIOS image for AP3G1/AP3G2 image Family	To verify Aios image for AP3G1/AP3G2 gets download	Passed	
WLJ80S_AAP_06	Unable to download aIOS image for AP3G1/AP3G2 image Family	To verify Aios image for AP3G1/AP3G2 gets download	Passed	

Config

Logical ID	Title	Description	Status	Defects
WLJ80S_config_01	"application reset-config NCS" not doing anything	To verify "application reset-config NCS" functions properly	Passed	

WLJ80S_config_02	Restoring the NCS Database	Check whether services can be started without any issues after back up config restored	Passed	
WLJ80S_config_03	Restoring the NCS Database in a High Availability Environment	Check whether services can be started without any issues after back up config restored	Passed	

WLC-Wlan

Logical ID	Title	Description	Status	Defects
WLJ80S_wlan_02	Voice clients connectivity with Dot11 b/g radios	To verify the clients connectivity with radio policy a/b/g	Passed	
WLJ80S_wlan_03	Voice clients connectivity with Dot11 a radio	To verify the clients connectivity with radio policy a	Passed	

Config-Wireless

Logical ID	Title	Description	Status	Defects
WLJ80S_cfg-wl_01	Audit from PI with office extend AP	Check th PI audit report after the failed WLC refresh	Passed	
WLJ80S_cfg-wl_02	Copy And Replace AP function does not work	To verify copy and replace AP function works	Passed	
WLJ80S_cfg-wl_03	Audit report on NCS for AP	Check the audit mismatch warning report on NCS for the AP slot	Passed	
WLJ80S_cfg-wl_04	Audit report on NCS for AP	Check the audit mismatch warning report on NCS for the AP slot	Passed	

WLJ80S_cfg-wl_05	AP image FTP download in GUI	Check the Autonomous AP image downloaded from server by FTP protocol from PI	Passed	
WLJ80S_cfg-wl_06	AP image TFTP download in GUI	Check the Autonomous AP image downloaded from server by TFTP protocol from PI	Passed	
WLJ80S_cfg-wl_11	WCS apply AP Group template to WLC	Check the application of AP Group template to WLC	Passed	
WLJ80S_cfg-wl_12	WCS apply AP Group template to WLC group	Check the application of AP Group template to WLC group	Passed	
WLJ80S_cfg-wl_13	Configuring AP Fast Heartbeat causes Audit Mismatch status	To verify whether configuring AP Fast Heartbeat causes audit mismatch status	Passed	

SR/CFD

SR/CFD Test cases

CFD Test Cases

Logical ID	Title	Description	Status	Defects
WLJ80S_acap_01	Associate the client to flex connect local switching WLAN	To check whether the client is able to associate with flex connect local switching WLAN	Passed	
WLJ80S_acl_01	ACL Configuration in WLC GUI	To verify whether or not the ACL rule's directions are changed after config upload and download	Passed	

WLJ80S_acl_02	ACL Configuration in WLC CLI	To verify whether or not the ACL rule's directions are changed after config upload and download	Passed	
WLJ80S_alap_01	Check the frequent reload of AP under high throughput condition.	To verify whether any AP reloads or error when associating client under the high traffic condition	Passed	
WLJ80S_alap_02	Check the status of the clients after association with the WLC	To check the status of the clients after their association with the WLC	Passed	
WLJ80S_apcl_01	Cleanair unable to report interference	To check if cleanair is able to report interference	Passed	
WLJ80S_apcli_01	Check Bridge group spanning tree configuration in AP	To configure and check the Bridge group spanning tree configuration in ap and add sub interface	Passed	
WLJ80S_apcrash_01	Configure a High availability in AP via wlc GUI and make AP failover.	To verify whether HA is configured in AP via wlc GUI and able to make AP failover from primary to secondary controller and vice-versa.	Passed	
WLJ80S_apcrash_02	Configure a High availability in AP via wlc CLI and make AP failover.	To verify whether HA is configured in AP via wlc CLI and able to make AP failover from primary to secondary controller and vice-versa.	Passed	
WLJ80S_apdoc_01	Check whether the antenna command options are present in Aironet	To check whether antenna command options are present in the Aironet command reference.	Passed	
WLJ80S_apenc_01	Client connect with TKIP encryption - AP1600	To verify the client connection with TKIP encryption and traffic flow between two TKIP clients	Passed	

WLJ80S_apenc_02	Client connect with TKIP encryption - AP1600	To verify the client connection with TKIP encryption and traffic flow between TKIP and non-TKIP clients	Passed	
WLJ80S_apenc_03	Configure a SSID with WPA+PSK+TKIP security in AP700 GUI and associate client	To verify a client association with the WPA+PSK+TKIP enabled SSID from AP700 GUI	Passed	
WLJ80S_apenc_04	Configure a SSID with WPA+PSK+TKIP security in AP700 CLI and associate client	To verify a client association with the WPA+PSK+TKIP enabled SSID from AP700 CLI	Passed	
WLJ80S_apenc_05	Configure a SSID with WPA+PSK+TKIP security in wlc 5508 and associate client	To verify a client association with the WPA+PSK+TKIP enabled SSID in wlc 5508	Passed	
WLJ80S_apgui_01	Radius Server configuration via CLI reflects in GUI	To check whether the radius server config via new CLI in AP will reflect in Security table of AP GUI	Passed	
WLJ80S_apgui_02	Autonomous AP transmitter power	To verify whether transmitter power is shown properly in GUI or not	Passed	
WLJ80S_apgui_03	Autonomous AP transmitter power	To verify whether transmitter power is shown properly in CLI or not	Passed	
WLJ80S_apios_01	AP bootup after power outage-AP3600	To check whether AP3600 bootup properly without any flash issues after power outage	Passed	
WLJ80S_apios_02	AP bootup after power outage-AP2600	To check whether AP2600 bootup properly without any flash issues after power outage	Passed	

WLJ80S_apios_03	Configure a default route to BVI interface and to gateway for LAP with static ip address	To verify whether the configured default route to BVI interface is removed by configuring the default route to gateway in LAP which holds static ip address and rebooting.	Passed	
WLJ80S_apios_04	Configure a default route to BVI interface and to gateway for LAP with dynamic (DHCP) ip address	To verify whether the configured default route to BVI interface is removed by configuring the default route to gateway in LAP which holds DHCP ip address and rebooting.	Passed	
WLJ80S_appoe_01	"Radio disabled due to inline power"	To check all APs are connected without error message after upgrade	Passed	
WLJ80S_aprad_01	Verifying the radio slot of 3700 AP in 5508 WLC	To verify whether radio slot 0 gets reset automatically or not while installing Radio slot 1 in 3700 AP.	Passed	
WLJ80S_aprad_02	Verifying the radio slot of 3700 AP in vWLC	To verify whether radio slot 0 gets reset automatically or not while installing Radio slot 1 in 3700 AP.	Passed	
WLJ80S_aprad_03	Verifying the radio slot of 1142 AP in 8508 WLC	To verify whether radio slot 0 gets reset automatically or not while installing Radio slot 1 in 1142 AP.	Passed	
WLJ80S_aprad_04	Radio behaviour when large beacon/dtim period is set in its interface	To verify whether there is no tx stop happens when large beacon/dtim period is set in radio interface.	Passed	
WLJ80S_aprrm_01	AP channel width after reboot-AireOS	To verify whether AP starts with 40Mhz after reboot where channel width is configured as 40Mhz and auto	Passed	

WLJ80S_aprrm_02	AP channel width after reboot-IOS-XE	To verify whether AP starts with 40Mhz after reboot where channel width is configured as 40Mhz and auto	Passed	
WLJ80S_apstats_01	Associating 11n clients to Autonomous AP and checking the data transfer between them	To verify whether 11n clients can able to transfer data within them or not while associated to Autonomous AP.	Passed	
WLJ80S_aptx_01	check allowed tx power levels can be configured correctly by converting AP2600 as CAP and SAP	To verify whether the allowed tx power levels can be configured correctly by converting AP2600 as CAP and SAP successfully	Passed	
WLJ80S_apunkn_01	Broadcom Clients in AP 3600 when WMM is enabled	To verify whether broadcom clients are able to associate successfully or not when WMM enabled	Passed	
WLJ80S_apunkn_02	Broadcom Clients in AP 3700 when WMM is enabled	To verify whether broadcom clients are able to associate successfully or not when WMM enabled	Passed	
WLJ80S_apunkn_03	Broadcom Clients in AP 2600 when WMM is enabled	To verify whether broadcom clients are able to associate successfully or not when WMM enabled	Passed	
WLJ80S_apunkn_04	Boot up the 3600 AP	To verify whether 3600 AP is booted up successfully without any unrelated messages.	Passed	
WLJ80S_apunkn_05	Boot up the 2600 AP	To verify whether 2600 AP is booted up successfully without any unrelated messages.	Passed	
WLJ80S_apunkn_06	Boot up the 3700 AP	To verify whether 3700 AP is booted up successfully without any unrelated messages.	Passed	

WLJ80S_apunkn_07	Boot up the 2700 AP	To verify whether 2700 AP is booted up successfully without any unrelated messages.	Passed	
WLJ80S_auap_01	check radio channel setting as per the configuration guide	To verify whether the radio channel setting is working as expected as per the configuration guide	Passed	
WLJ80S_awips_01	wips alarm detection time stamp is ahead of AP clock	To check if wips alarm detedtion time stamp isnt ahead of AP clock	Passed	
WLJ80S_c3p1_01	Bringing HA pair up- WLC 5760	To verify whether the HA pair (ACTIVE:STANDBY) is up successfully	Passed	
WLJ80S_c3p1_02	Controller mode when the Gateway is not reachable to the ACTIVE controller	To verify the HA pair controller modes when the Gateway is not reachable from the ACTIVE controller	Passed	
WLJ80S_capwap_01	Configure a channel for AP's 802.11a interface and check the channel changed message in wlc 5508, physical PI and Virtual PI logs.	To verify whether the AP's 802.11a interface channel is configured and the configured messages shows correctly in wlc 5508, physical PI and virtual PI logs.	Passed	
WLJ80S_capwap_02	Configure a channel for AP's 802.11b interface and check the channel changed message in wlc 5508, physical PI and Virtual PI logs.	To verify whether the AP's 802.11b interface channel is configured and the configured messages shows correctly in wlc 5508, physical PI and virtual PI logs.	Passed	
WLJ80S_capwap_03	Configure a channel for AP's 802.11a interface and check the channel changed message in wlc 8500, physical PI and Virtual PI logs.	To verify whether the AP's 802.11a interface channel is configured and the configured messages shows correctly in wlc 8500, physical PI and virtual PI logs.	Passed	

WLJ80S_capwap_04	Configure a channel for AP's 802.11b interface and check the channel changed message in wlc 8500, physical PI and Virtual PI logs.	To verify whether the AP's 802.11b interface channel is configured and the configured messages shows correctly in wlc 8500, physical PI and virtual PI logs.	Passed	
WLJ80S_capwap_05	Configure a channel for AP's 802.11a interface and check the channel changed message in virtual wlc, physical PI and Virtual PI logs.	To verify whether the AP's 802.11a interface channel is configured and the configured messages shows correctly in virtual wlc, physical PI and virtual PI logs.	Passed	
WLJ80S_capwap_06	Configure a channel for AP's 802.11b interface and check the channel changed message in virtual wlc, physical PI and Virtual PI logs.	To verify whether the AP's 802.11b interface channel is configured and the configured messages shows correctly in virtual wlc, physical PI and virtual PI logs.	Passed	
WLJ80S_capwap_07	Reconnect AP with WLC and check the Handshake messages	To check the DTLS handshake messages for corrupted data after rejoining the AP with WLC	Passed	
WLJ80S_capwap_08	Check the old DTLS data encryption sessions in WLC	To check whether old DTLS data encryption session is still present in the WLC	Passed	
WLJ80S_capwap_09	Check the old DTLS data encryption sessions in WLC with connected AP	To check whether old DTLS data encryption session is still present in the WLC with AP still connected	Passed	
WLJ80S_capwap_10	Check the AP entry available in the database	To check and verify whether the AP entry is available in the database after the AP is associated with the WLC	Passed	

WLJ80S_cmgmt_01	Client traffic filtered based on SSID	To verify whether clients are filtered based on SSID with the time frame more than an hour or not	Passed	
WLJ80S_cmgmt_02	Client traffic filtered based on Device IP Address	To verify whether clients are filtered based on Device IP Address with the time frame more than an hour or not	Passed	
WLJ80S_cmgmt_03	Client traffic filtered based on Device Host Name	To verify whether clients are filtered based on Device Host Name with the time frame more than an hour or not	Passed	
WLJ80S_com_01	AVC visibility for Cisco jabber applications	To verify whether wireless clients running cisco jabber is classified as SSL when client is connected to AVC enabled WLAN	Passed	
WLJ80S_conwl_01	PI-Noise/Interference report for Unified Aps in LC theme	To verify the Nose and interference report has been generated when unified AP is selected in LC > DWC	Passed	
WLJ80S_conwl_02	Checking the neighbor address details in PI	To verify whether Neighbor address details are displayed in Hex or not in PI	Passed	
WLJ80S_dhcp_01	check the client able to get the internal wlc dhcp scope offer	To verify whether the clients are connected using internal DHCP scope offer	Passed	
WLJ80S_doc_01	VLAN isn't marked as dirty when re-connect client cannot get IP via DHCP	To check if client status display appropriately - 2500	Passed	
WLJ80S_doc_02	VLAN isn't marked as dirty when re-connect client cannot get IP via DHCP	To check if client status display appropriately - 5500	Passed	

WLJ80S_doc_03	VLAN isn't marked as dirty when re-connect client cannot get IP via DHCP	To check if client status display appropriately - 7500	Passed	
WLJ80S_doc_04	VLAN isn't marked as dirty when re-connect client cannot get IP via DHCP	To check if client status display appropriately - 8500	Passed	
WLJ80S_doc_05	Checking the update of 2504 Express setup in release notes and checking the dashboard functionality in all browsers.	To verify whether 2504 Express setup supported browsers is updated or not in 7.6Mr3 release notes and check whether dashboards works properly or not in all browsers.	Passed	
WLJ80S_error_01	check the WLC managed from the wireless client when management via wireless enabled	To verify whether the WLC managed from the wireless client	Passed	
WLJ80S_fwd_01	LAG fail-over does not work on CT5508Â	To check if lag fail over works in 5500	Passed	
WLJ80S_fwd_02	LAG fail-over does not work on 7500	To check if lag fail over works in 7500	Passed	
WLJ80S_fwd_03	LAG fail-over does not work on 8500	To check if lag fail over works in 8500	Passed	
WLJ80S_guest_01	Uploading and Downloading guest user configuration in WLC	To verify whether the guest user configuration is retained in a WLC after config upload and download or not	Passed	
WLJ80S_guest_02	Guest user configuration in WLC after rebooting	To verify whether the guest user configuration is retained in a WLC after rebooting or not	Passed	

WLJ80S_guest_03	Check the scheduled guest user is removed from Physical PI and WLC 5508 after its time expired	To verify whether scheduled guest user is created and removed from physical PI and WLC 5508 after its time expired	Passed	
WLJ80S_guest_04	Check the scheduled guest user is removed from virtual PI and WLC 5508 after its time expired	To verify whether scheduled guest user is created and removed from virtual PI and WLC 5508 after its time expired	Passed	
WLJ80S_ha_01	check the controller HA failover false redundancy heartbeat loss	To verify whether the false redundancy hearbeat loss failver occur on WLC HA failover	Passed	
WLJ80S_hreap_01	H-REAP between connected and standalone AP	To verify whether flexconnect AP changes mode when controller (5508) is down/up.	Passed	
WLJ80S_hreap_02	H-REAP between connected and standalone AP	To verify whether flexconnect AP changes mode when controller (2504) is down/up.	Passed	
WLJ80S_hreap_03	H-REAP between connected and standalone AP	To verify whether flexconnect AP changes mode when controller (8500) is down/up.	Passed	
WLJ80S_hreap_04	Check AP connection status to WLC after VLAN mapping config using 7510	To check and verify the AP connection status to WLC after configuring the VLAN mapping	Passed	
WLJ80S_hreap_05	Check AP connection status to WLC after VLAN mapping config	To check and verify the AP connection status to WLC after configuring the VLAN mapping and reconnect the AP with WLC after disconnecting.	Passed	

WLJ80S_hreap_10	Configure a web auth with pre and post auth flex ACL in wlc 5508	To verify whether web auth with flex local switching is able to create and apply pre and post auth flex acl to it and associate client and check web authentication in wlc 5508	Passed	
WLJ80S_hreap_11	Configure a web auth with pre and post auth flex ACL in wlc 8500	To verify whether web auth with flex local switching is able to create and apply pre and post auth flex acl to it and associate client and check web authentication in wlc 8500	Passed	
WLJ80S_idb_01	AP telnet session due to tx load in the interfaces	To verify the aIOS AP telnet session and txload in AP's interfaces	Passed	
WLJ80S_inv_01	check the WLC deleted from PI after upgrade WLC from the old version	To verify whether the WLC deleted succuessfully after upgrade from WLC old version to new version	Passed	
WLJ80S_lan_01	Disabling Multicast state in WLC GUI	To verify whether Multicast state can be disabled in WLC successfully or not	Passed	
WLJ80S_lan_02	Disabling Multicast state in WLC CLI	To verify whether Multicast state can be disabled in WLC successfully or not	Passed	
WLJ80S_lic_01	Trying to remove licenses in WLC	To verify whether licenses can be removed or not in HA SKU WLC other than base license.	Passed	
WLJ80S_logger_01	Add AP to the WLC and check ARP entry to the network using 2500,5508	This is to verify the ARP entry in the network by adding the AP's to the Wireless controller and adding the clients	Passed	

WLJ80S_maps_01	check the heapmap and AP colour status are showing on the floor view	To verify whether the heapmap and AP colour status are showing successfully on the floor view	Passed	
WLJ80S_memry_01	Check the output logs for AP console for memory leaks	To check and find whether any memory leaks occur from the logs of AP	Passed	
WLJ80S_mse_01	MSE Admin View from PI server	To check the MSE admin view launch from PI server	Passed	
WLJ80S_mse_02	PI 1.4 don't display clients and rogue AP on floor view	To check whether pi displays clients and rogue AP in floor view	Passed	
WLJ80S_mseloc_01	Checking the MSE tracking function after sync/resync the Maps.	To verify whether MSE able to track the clients or not after sync/re-sync the Maps.	Passed	
WLJ80S_msesw_01	Suspicious after-hours traffic detected during working hours	To check if there is any suspicious after hours traffic detected during working hours	Passed	
WLJ80S_msesw_02	NTP sync failed due to timed out, nothing received	To check whether there is no timed out error during NTP sync	Passed	
WLJ80S_msesw_03	Setting the DB password in MSE.	To verify whether DB(Database) password is able to config or not in MSE.	Passed	
WLJ80S_msesw_04	Resetting the Oracle DB password in MSE.	To verify whether Oracle DB(Database) password is able to re-config or not in MSE.	Passed	
WLJ80S_msesw_05	Check the logs of mse for the history of the ap's	To check whether ap's are saving the history in the database of the mse	Passed	
WLJ80S_osbt_01	check the Katana/Edison booting after upgrade or rebooting when service configuration completed	To verify whetherthe Katana/Edison is booting up after upgrade when service config is configured	Passed	

WLJ80S_prime_01	Check the compatibility of PI with latest chrome browser	To check the PI full compatibility with the latest upgraded chrome browser	Passed	
WLJ80S_prime_02	Check the compatibility of PI with latest chrome browser	To check the PI full compatibility with the latest upgraded chrome browser	Passed	
WLJ80S_rrm_05	After few failovers None of the Clients get authenticated	To check After a few failovers whether clients get authenticated	Passed	
WLJ80S_rrm_06	After few failovers None of the Clients get authenticated	To check After a few failovers whether clients get authenticated	Passed	
WLJ80S_rrm_07	After few failovers None of the Clients get authenticated	To check After a few failovers whether clients get authenticated	Passed	
WLJ80S_rrm_08	Floor maps in PI fail to load with widget exceptions	To check if Floor maps in PI loads without any exceptions	Passed	
WLJ80S_rrm_09	Configure the AP transmit (Tx) power level for 802.11a from controller GUI	To verify whether the AP Transmit(Tx) power level for 802.11a is configured from the controller GUI	Passed	
WLJ80S_rrm_10	Configure the AP transmit (Tx) power level for 802.11a from controller CLI	To verify whether the AP Transmit(Tx) power level for 802.11a is configured from the controller CLI	Passed	
WLJ80S_rrm_11	Configure the AP transmit (Tx) power level for 802.11b from controller GUI	To verify whether the AP Transmit(Tx) power level for 802.11b is configured from the controller GUI	Passed	
WLJ80S_rrm_12	Configure the AP transmit (Tx) power level for 802.11b from controller CLI	To verify whether the AP Transmit(Tx) power level for 802.11b is configured from the controller CLI	Passed	
WLJ80S_sec_01	check the applied local policy on WLAN is working on specified active hours	To verify whether the applied local policy on wlan is working as expected when active hours defined	Passed	

WLJ80S_sec_02	check the OUI match is happening when use the iPhone5s for native profiling	To verify whether the OUI match is happening successfully for iphone5s native profiling	Passed	
WLJ80S_sec_03	Check the session timeouts for the clients in roaming	To check and verify the session timeouts for the clients associated with wlc while in roaming	Passed	
WLJ80S_sec_04	Check for MFP anomaly messages after enabling the Infrastructure MFP	To enable the Infrastructure MFP in WLC and check for any MFP anomaly messages generated by rogue clients/ap's	Passed	
WLJ80S_sec_05	Check for MFP anomaly messages after disabling the Infrastructure MFP	To disable the Infrastructure MFP in WLC and check for any MFP anomaly messages present in the logs generated by rogue clients/ap's	Passed	
WLJ80S_snmp_01	Modification of default community with non default values in GUI	To verify whether the system accepts modifying default SNMP community or not	Passed	
WLJ80S_snmp_02	Modification of default community with non default values in CLI	To verify whether the system accepts modifying default SNMP community or not	Passed	
WLJ80S_snmp_03	Creation of SNMPV3 user named "default" in GUI	To verify whether the system accepts creation of SNMPV3 user named "default" or not	Passed	
WLJ80S_snmp_04	Creation of SNMPV3 user named "default" in CLI	To verify whether the system accepts creation of SNMPV3 user named "default" or not	Passed	
WLJ80S_snmp_05	Creation of non-default community with non-default values in GUI	To verify whether the system accepts creation of non-default community with non-default values or not	Passed	

WLJ80S_snmp_06	Creation of non-default community with non-default values in CLI	To verify whether the system accepts creation of non-default community with non-default values or not	Passed	
WLJ80S_sys_01	PI server after accessing floor maps-Standalone box	To check on accessing floor maps in PI server(Standalone) doesn't cause the server to crash	Passed	
WLJ80S_sys_02	PI server after accessing floor maps-HA enabled box	To check on accessing floor maps in PI server(HA enabled) doesn't cause the server to crash	Passed	
WLJ80S_sys_03	Adding more number of AP's in Floor maps.	To verify whether PI get crashed or not while accessing floor maps with more number of AP's added in it.	Passed	
WLJ80S_web_01	AP Multicast Mode with blank Multicast Group Address in GUI	To verify whether the show network summary results matches the running config or not	Passed	
WLJ80S_web_02	AP Multicast Mode with blank Multicast Group Address in CLI	To verify whether the show network summary results matches the running config or not	Passed	
WLJ80S_web_03	Japanese DBCS characters in Internal WebAuth	To verify whether the Japanese DBCS characters is garbled or not in internal Webauth login.html page	Passed	
WLJ80S_web_04	Japanese DBCS characters in External WebAuth	To verify whether the Japanese DBCS characters is garbled or not during external Web authentication	Passed	
WLJ80S_web_05	Configure the AP parameters from Controller GUI	To verify Whether ap parameters are able to configure from 5508 controller GUI	Passed	

WLJ80S_web_06	Configure the AP parameters from Controller CLI	To verify Whether ap parameters are able to configure from 5508 controller CLI	Passed	
WLJ80S_web_07	Configure the AP parameters from Controller GUI	To verify Whether ap parameters are able to configure from 8500 controller GUI	Passed	
WLJ80S_web_08	Configure the AP parameters from Controller CLI	To verify Whether ap parameters are able to configure from 8500 controller CLI	Passed	
WLJ80S_webauth_01	Client reconnection to a SSID with different IP address	To verify whether web authentication happens for a client reconnected to an SSID with different IP address or not	Passed	
WLJ80S_webauth_02	Client reconnection to a SSID with same IP address	To verify whether web authentication happens for a client reconnected to an SSID with same IP address or not	Passed	
WLJ80S_webauth_03	Web authentication after renewing the IP address from DHCP	To verify whether web authentication happens for a client after renewing the IP address from the DHCP or not	Passed	
WLJ80S_wlan_01	AP group radio policy by downgrading/upgrading build	To verify the radio policy of WLAN/AP group by upgrading/downgrading the WLC build	Passed	
WLJ80S_wlan_02	AP group radio policy after rebooting the WLC	To verify the radio policy of WLAN/AP group after saving config and rebooting the WLC	Passed	
WLJ80S_wlan_03	AP group radio policy after uploading the backup config	To verify the radio policy of AP group/WLAN after downloading and uploading the config file	Passed	

WLJ80S_wlan_04	AP group radio policy when connecting client with specific radio policy "a only"	To verify the radio policy by connecting clients to the specific radio which is set in WLC "a only"	Passed	
WLJ80S_wlan_05	AP group radio policy when connecting client with specific radio policy "b/g only"	To verify the radio policy by connecting clients to the specific radio which is set in WLC as "b/g only"	Passed	
WLJ80S_wlan_06	WLC 7500: Radio policy in custom AP group- Upgrade	To verify the radio policy of custom ap group has been retained after upgrade WLC 7500	Passed	
WLJ80S_wlan_07	WLC 7500: Radio policy in custom AP group- config restore	To verify the radio policy of custom ap group has been retained after config upload	Passed	
WLJ80S_wlan_08	WLC 7500: Radio policy in custom AP group- Client connectivity	To verify whether clients connect to the explicitly configured radio policy of AP group	Passed	
WLJ80S_wlan_09	NGWC: Checking Radio policy setting	To verify whether clients connect to the explicitly configured radio policy of AP group in NGWC	Passed	
WLJ80S_wlan_10	check the voice clients connects to specified radio policy	To verify whether the clients connects to specified radio policy set on the controller	Passed	
WLJ80S_wlan_11	Timestamp-tolerance in Guest LAN	To verify whether the timestamp-tolerance is shown properly or not in show running-config output	Passed	
WLJ80S_wlan_12	Checking the WLAN state after rebooting the 5508 WLC.	To verify whether Wlan's(ID > 16) state gets disabled or not after rebooting the 5508 WLC.		

WLJ80S_wlan_13	Checking the WLAN state after rebooting the 8500 WLC.	To verify whether Wlan's(ID > 16) state gets disabled or not after rebooting the 8500 WLC.		
WLJ80S_wlan_14	Checking the WLAN state after rebooting the vWLC.	To verify whether Wlan's(ID > 16) state gets disabled or not after rebooting the vWLC.	Passed	
WLJ80S_wlan_15	Checking the WLAN state after upload/download the config file in 5508 WLC.	To verify whether Wlan's(ID > 16) state gets disabled or not after upload/download the config file in 5508 WLC.	Passed	
WLJ80S_wlan_16	Checking the WLAN state after upload/download the config file in 8500 WLC.	To verify whether Wlan's(ID > 16) state gets disabled or not after upload/download the config file in 8500 WLC.	Passed	
WLJ80S_wlan_17	Checking the WLAN state after upload/download the config file in vWLC.	To verify whether Wlan's(ID > 16) state gets disabled or not after upload/download the config file in vWLC.	Passed	
WLJ80S_wlcos_01	Dynamic interface setting in WLC	To verify whether all dynamic interfaces created has been restored after config download	Passed	
WLJ80S_wlcos_02	check the downgrading of WLC show the error AP image bundle is not unbundled	To verify whether the downgrading of WLC image is working as expected	Passed	
WLJ80S_wlcvm_01	Checking the deployment of vWLC with UCS server.	To verify whether vWLC Ova is able to install successfully or not with UCS server.	Passed	

SR Test Cases

Logical ID	Title	Description	Status	Defects

WLJ80S_11AC_01	Enable/disable the 802.11ac network from WLC CLI.	To check and verify enabling/disabling the 802.11ac network from WLC GUI.	Passed	
WLJ80S_11AC_02	Enable/disable the 802.11ac network from WLC GUI.	To check and verify enabling /disabling the 802.11ac network from WLC CLI	Passed	
WLJ80S_APCON_01	Verification of Running config after powe loss	To verify the running config after powe loss	Passed	
WLJ80S_APCON_02	Verification of default route after setting the gateway	To verify the default route after configuring the default gateway	Passed	
WLJ80S_APCON_03	Verification of Running config after reset by WLC GUI	To verify the running config after powe loss	Passed	
WLJ80S_APGRP_01	Checking SSID broadcasting disable when clients are in connected state	To verify the client behaviour when broadcasting SSID is diabled where clients are in connected state	Passed	
WLJ80S_APGRP_02	Session timeout for dot1x associated client	To check that the dot1x authenticated client should not disassocite after session timeout expires	Passed	
WLJ80S_APGRP_03	Client roam across AP groups with WLAN mapped to different VLAN	To check the client roaming form one AP group to another AP group provided WLAN is mapped to multiple AP groups with different VLAN	Passed	
WLJ80S_APGRP_04	Client roam across AP groups with WLAN mapped to different VLAN- FLS enabled	To check the client roaming form one AP group to another AP group provided WLAN is mapped to multiple AP groups with different VLAN where FLS is enabled in the WLAN	Passed	
WLJ80S_APGRP_05	Dynamic VLAN assignment- WLC 2504	To check the dynamic VLAN assignment for a client in WLC 2504	Passed	

WLJ80S_APIOS_01	Checking the default gateway config in show running command of AP CLI.	To check whether default gateway to BVI1 config is present or not in show running command of AP CLI.	Passed	
WLJ80S_APRAD_01	Channel selection in AP	To verify the channel selection in AP	Passed	
WLJ80S_EAP_01	Configuring backup port for Active port of Active HA WLC.	To check whether Active HA WLC goes to standy by WLC or to backup port while primary port is down.	Passed	
WLJ80S_EAP_02	Trying to delete excluded client present in Monitor > Clients page.	To check whether excluded client present in Monitor > Clients page is able to delete or not in WLC GUI.	Passed	
WLJ80S_EAP_04	Deauthenticating more associated dot1x clients and checking the CPU process value in WLC CLI.	To check whether CPU process value getting greater than 1 or not via WLC CLI when 3-4 associated dot1x clients are deauthenticated at once in WLC GUI.	Passed	
WLJ80S_EAP_05	Associating a client to a WLAN with security dot1x+Webauth in 5508 WLC.	To check whether error message occurs or not when a client is getting redirected to web-auth login page while it is getting associated to a WLAN with security dot1x+webauth	Passed	
WLJ80S_EAP_06	Adding Invalid mac address in local mac filter page of 5508 WLC via GUI	To check whether invalid mac address can be added or not in local mac filter page of WLC via GUI.	Passed	
WLJ80S_EAP_07	Adding Invalid mac address in local mac filter page of 5508 WLC via CLI	To check whether invalid mac address can be added or not in local mac filter page of WLC via CLI.	Passed	

WLJ80S_EAP_08	Roaming Samsung S4 client between wlc's with dot1x security.	To check whether Samsung S4 client roams or not between 2 WLC's with dot1x security.	Passed	
WLJ80S_EAP_09	Roaming Apple Iphone client between wlc's with dot1x security.	To check whether Apple Iphone client roams or not between 2 WLC's with dot1x security.	Passed	
WLJ80S_EAP_10	Associating a Win 8 client to a WLAN with security dot1x+Webauth in 8500 WLC.	To check whether win 8 client associated or not to a WLAN with security dot1x+webauth in 8500 WLC.	Passed	
WLJ80S_EAP_11	Associating a Win 8 client to a WLAN with security dot1x+Webauth in vWLC.	To check whether win 8 client associated or not to a WLAN with security dot1x+webauth in vWLC.	Passed	
WLJ80S_EAP_12	Associating Win 8 client to a WLAN with security Dot1x(PEAP with TLS).	To check whether win 8 client gets associated or not to a WLAN with security Dot1x(PEAP with TLS).	Passed	
WLJ80S_EAP_13	Associating wireless clients to 1142 AP with different L2 & L3 security types in 5508 WLC.	To check whether clients gets associated or not to 1142 AP in 5508 WLC with all security types.	Passed	
WLJ80S_EAP_14	Checking the availability of SSID field in "show radius summary" command.	To check whether SSID field is present or not in CLI command of show radius summary.	Passed	
WLJ80S_FLEX_01	WLAN-VLAN mapping for localswitching central auth configuration- FT	To check the WLAN-VLAN mapping for localswitching central auth config in case of fault tolerance	Passed	

WLJ80S_FLEX_02	WLAN-VLAN mapping for localswitching local auth configuration- FT	To check the WLAN-VLAN mapping for localswitching local auth config in case of fault tolerance	Passed	
WLJ80S_FLEX_03	WLAN-VLAN mapping when AP boots in connected mode	To check the WLAN-VLAN mapping when AP boots in connected mode	Passed	
WLJ80S_FLEX_04	WLAN-VLAN mapping when AP boots in SA mode	To check the WLAN-VLAN mapping when AP boots in SA mode	Passed	
WLJ80S_FLEX_05	WLAN-VLAN mapping for localswitching central auth configuration when AP moves from connected to SA mode	To check the WLAN-VLAN mapping for localswitching central auth config when AP moves from connected to Sa mode and vice versa	Passed	
WLJ80S_FLEX_06	WLAN-VLAN mapping for localswitching local auth configuration when AP moves from connected to SA mode	To check the WLAN-VLAN mapping for localswitching local auth config when AP moves from connected to Sa mode and vice versa	Passed	
WLJ80S_FLEX_07	Flexconnect VLAN mapping upon save config in WLC	To check whether configured VLAN mapping is saved upon save config on WLC instead of changing to nativa VLAN	Passed	
WLJ80S_FLEX_08	OEAP setup with WLC 2504	To check the OEAP association with WLC 2504	Passed	
WLJ80S_FLEX_09	FLS clients via AP3502	To verify FLS clients connected via AP3502 shouldn't experience any intermittent disconnection	Passed	

WLJ80S_FLEX_10	Flexconnect AP behavior when reboot in SA mode	To check whether flexconnect AP can be able to service clients when WAN outage and AP is rebooted in SA mode	Passed	
WLJ80S_FLEX_11	iPad Client association to WLC 7500- Central switching	To check whether iPads are able to list the wifi networks and able to connect to it	Passed	
WLJ80S_FLEX_12	iPad Client association to WLC 7500- Local switching	To check whether iPads are able to list the wifi networks and able to connect to it	Passed	
WLJ80S_FLEX_13	FLS clientswhen move from connected to SA mode- WLC 7500	To check whether FLS clients didn't disconnect when AP moves from connected to SA mode	Passed	
WLJ80S_FLEX_14	FLS clientswhen move from SA to connected mode- wlc 7500	To check whether FLS clients didn't disconnect when AP moves from SA to connected mode	Passed	
WLJ80S_FLEX_15	Client connectivity in Flexconnect AP	To check there is no double AID allocation in flexconnect AP while client connectivity	Passed	
WLJ80S_FLEX_16	Client connectivity to OEAP	To check the client connectivity to OEAP	Passed	
WLJ80S_FLEX_17	Flexconnect AP with multiple SSIDs having same name	To check whether the modifiction of one SSID wont affect the other SSID with same name	Passed	
WLJ80S_FLEX_18	Config import by adding ascii/hex key manually in WLC config file	To verify whether clients connected when config file is manually edited with cleartext ascii/hex key	Passed	
WLJ80S_FLEX_19	De-authentication frames	To verify the de-authentication frames for client	Passed	

WLJ80S_Ipv6_01	Disabling the ipv6 on WLC	To verify the ipv6 disable on WLC	Passed	
WLJ80S_LIC_01	check the WLC adder loses after the system reset	To verify whether the WLC adder licsense loses after system reset on WLC	Passed	
WLJ80S_LWAPP_01	To associate a client with controller and ping the network	To check and associate a wireless client with 5500 controller and ping the network through GUI	Passed	
WLJ80S_LWAPP_02	To associate a client with controller and ping the network	To check and associate a wireless client with 5500 controller and ping the network through CLI	Passed	
WLJ80S_LWAPP_03	To upgrade the AP image by pre-download from controller	To verify whether the AP is able to pre-download the image from the controller 5500 using GUI	Passed	
WLJ80S_LWAPP_04	To upgrade the AP image by pre-download from controller	To verify whether the AP is able to pre-download the image from the controller 5500 using CLI	Passed	
WLJ80S_LWAPP_05	Jumbo frames by Light weight AP	To verify the jumbo frames by default	Passed	
WLJ80S_MFP_01	verification of MFP logs	To verify the corresponding MFP logs	Passed	
WLJ80S_MGTERR_01	Ping loss after upgrading	Check if there is no ping loss after upgrading the WLC	Passed	
WLJ80S_MGTERR_02	Ping loss after upgrading	Check if there is no ping loss after upgrading the WLC	Passed	
WLJ80S_MGTERR_03	Ping loss after upgrading	Check if there is no ping loss after upgrading the WLC	Passed	
WLJ80S_MGTERR_04	WLC don't synchronize to NTP	Check if WLC syncronize with NTP	Passed	

WLJ80S_MGTERR_05	Massive Radius overrides disabled messages are observed	Check if there is no overrides disabled messages appears	Passed	
WLJ80S_MGTERR_06	Massive Radius overrides disabled messages are observed	Check if there is no overrides disabled messages appears	Passed	
WLJ80S_MGTERR_07	Massive Radius overrides disabled messages are observed	Check if there is no overrides disabled messages appears	Passed	
WLJ80S_MGTERR_08	Massive Radius overrides disabled messages are observed	Check if there is no overrides disabled messages appears	Passed	
WLJ80S_MGTERR_09	AP always use UTC, not the controllers timezone	Check if AP and Controller time zone is same	Passed	
WLJ80S_MGTERR_10	AP always use UTC, not the controllers timezone	Check if AP and Controller time zone is same	Passed	
WLJ80S_MGTERR_11	AP always use UTC, not the controllers timezone	Check if AP and Controller time zone is same	Passed	
WLJ80S_MGTERR_12	AP always use UTC, not the controllers timezone	Check if AP and Controller time zone is same	Passed	
WLJ80S_MGTERR_13	WLC: cannot save AP configuration on NCS	Check if AP configuration can be saved in NCS	Passed	
WLJ80S_MGTERR_14	Shutting down 7500	Check if 7500 is able to shutdown using IMM	Passed	
WLJ80S_MGTERR_15	Shutting down 8500	Check if 8500 is able to shutdown using IMM	Passed	
WLJ80S_MGTERR_16	Admin password change in 2500	Check if admin password is changed through cli	Passed	
WLJ80S_MGTERR_17	Admin password change in 5500	Check if admin password is changed through cli	Passed	
WLJ80S_MGTERR_18	Admin password change in 7500	Check if admin password is changed through cli	Passed	

WLJ80S_MGTERR_19	Admin password change in 8500	Check if admin password is changed through cli	Passed	
WLJ80S_MGTERR_20	Assign different VLAN per SSID	To check if different Vlan can ve assigned per SSID	Passed	
WLJ80S_MGTERR_21	CT2504 message about # APF - 1 - ADD _ TO _ BLACKLIST _ FAILED	To check if there is no error message after upgrading	Passed	
WLJ80S_MGTERR_22	CAP2600 pre-download failure	To check if there is no pre-download failure	Passed	
WLJ80S_MGTERR_23	Syslog server error messages	To check if error messages are proper	Passed	
WLJ80S_MOBILITY_01	Check the wireless mobility feature in 2500	To check and verify the clients connectivity in wireless mobility feature.	Passed	
WLJ80S_MSE_01	check the MSE strong root password configuration	To verify whether configuration of MSE strong root password reflected after reboot	Passed	
WLJ80S_MSE_02	check the power supply status of MSE	To verify whether MSE shows the power supply status using specified command	Passed	
WLJ80S_MSE_03	check MSE tracks client with respect to the license limit	To verify whether the MSE tracks the client when increase the AP license or decrease the AP count	Passed	
WLJ80S_MSE_04	check the rogue AP count on both MSE and WLC	To verify whether the MSE and WLC shows the same rogue AP count status	Passed	
WLJ80S_MSE_05	check any license error show after upgrading NCS and MSE	To verify whether the PI and MSE show the wrong license error messages after upgrading	Passed	
WLJ80S_MSE_06	check the Wips exception error occurance when MSE framework forward traps and PI receive any alarm	To verify whether the MSE WIPS exception error occur when MSE forward traps	Passed	

WLJ80S_PIADM_01	Scheduled admin (Enable)status change by PI	To verify the scheduled admin status change ,enable	Passed	
WLJ80S_PIADM_02	Scheduled admin (Disable))status change by PI	To verify the scheduled admin status change disable	Passed	
WLJ80S_PIMSE_01	check the integration of MSE to PI with different names	To verify whether able to add MSE to PI when using the different types of MSE names	Passed	
WLJ80S_PIREP_01	PI reports with client bandwidth	To verify the PI reports with client bandwidth	Passed	
WLJ80S_RCV_01	Check the connectivity of the connected clients	To check the connectivity status of the connected clients with the wireless controller 2500	Passed	
WLJ80S_RCV_02	Check the connectivity of the connected clients	To check the connectivity status of the connected clients with the wireless controller 2500	Passed	
WLJ80S_RCV_03	Upgrading the firmware of the access points	To check the firmware upgrading process for the access points through gui	Passed	
WLJ80S_RCV_04	Upgrading the firmware of the access points	To check the firmware upgrading process for the access points through cli	Passed	
WLJ80S_RRM_01	Setting custom channel in 2600 AP via WLC CLI	To check whether custom channel 52 is able to set or not in 2600 AP via WLC CLI.	Passed	
WLJ80S_RRM_02	Checking the config of dca sensitivity after upload/download the config file in 5508 WLC.	To check whether dca sensitivity configuration(configured via WLC CLI) is present or not in 5508 WLC after upload/download the config file.	Passed	

WLJ80S_RRM_03	Checking the config of dca sensitivity after upload/download the config file in 8500 WLC.	To check whether dca sensitivity configuration(configured via WLC CLI) is present or not in 8500 WLC after upload/download the config file.	Passed	
WLJ80S_RRM_04	Checking the config of dca sensitivity after upload/download the config file in vWLC.	To check whether dca sensitivity configuration(configured via WLC CLI) is present or not in vWLC after upload/download the config file.	Passed	
WLJ80S_RRM_05	Enabling beamforming configuration in WLC via CLI commands	To check whether beamforming configuration can be enabled or not in WLC via CLI commands	Passed	
WLJ80S_RRM_06	Trying to enable custom channels in WLC GUI without disabling network status	To check whether custom channels are configured or not in WLC GUI without disabling network status.	Passed	
WLJ80S_RRM_07	Performing DFS detection event in WLC	To check whether AP radio's getting reset or not in WLC once DFS detection event is performed.	Passed	
WLJ80S_RRM_08	De-auth frames with RRM DCA	To verify the de auth frames with DCA RRM	Passed	
WLJ80S_RRM_09	Setting custom channel in 2600 AP via WLC GUI	To check whether custom channel 52 is able to set or not in 2600 AP via WLC GUI.	Passed	
WLJ80S_SWUPG_01	To upload the config backup to the TFTP server	To check and upload the config backup of the wireless controller to the TFTP server through GUI	Passed	

WLJ80S_SWUPG_02	To upload the config backup to the TFTP server	To check and upload the config backup of the wireless controller to the TFTP server through CLI	Passed	
WLJ80S_SWUPG_03	Verify whether AP is getting image successfully from the controller	To verify whether AP is getting image successfully from the controller after upgrading the WLC image using GUI	Passed	
WLJ80S_SWUPG_04	Verify whether AP is getting image successfully from the controller	To verify whether AP is getting image successfully from the controller after upgrading the WLC image using CLI	Passed	
WLJ80S_SWUPG_05	To upgrade the wireless LAN controller image using tftp	To check and upgrade the wireless LAN controller image for 2500 through GUI	Passed	
WLJ80S_SWUPG_06	To upgrade the wireless LAN controller image using tftp	To check and upgrade the wireless LAN controller image for 2500 through CLI	Passed	
WLJ80S_SWUPG_07	To pre-download AP image from controller	To verify whether the AP is able to pre-download the image from the 2500 controller using GUI	Passed	
WLJ80S_SWUPG_08	To pre-download AP image from controller	To verify whether the AP is able to pre-download the image from the 2500 controller using CLI	Passed	
WLJ80S_SWUPG_09	To Install the AVC protocol pack in the controller	To check and install the avc protocol pack loaded in the controller	Passed	
WLJ80S_SWUPG_10	To upgrade the wireless LAN controller image using ftp	To check and upgrade the wireless LAN controller image for 2500 through GUI	Passed	

WLJ80S_SWUPG_11	To upgrade the wireless LAN controller image using ftp	To check and upgrade the wireless LAN controller image for 2500 through CLI	Passed	
WLJ80S_SWUPG_12	To upgrade the wireless LAN controller image using tftp	To check and upgrade the wireless LAN controller image for 5500 through GUI	Passed	
WLJ80S_SWUPG_13	To upgrade the wireless LAN controller image using tftp	To check and upgrade the wireless LAN controller image for 5500 through CLI	Passed	
WLJ80S_SWUPG_14	To upgrade the wireless LAN controller image using ftp	To check and upgrade the wireless LAN controller image for 5500 through GUI	Passed	
WLJ80S_SWUPG_15	To upgrade the wireless LAN controller image using ftp	To check and upgrade the wireless LAN controller image for 5500 through CLI	Passed	
WLJ80S_TEMP_01	check the PI composite template is applied to the WLC	To verify whether the PI composite template applied successfully without any issue	Passed	
WLJ80S_WEBACL_01	web-auth ACL for LAP -5508,3500	To verify the configuration for Flex ACL for LAP	Passed	
WLJ80S_WEBACL_02	web-auth ACL for LAP -5508 WLC ,3600 AP	To verify the configuration for Flex ACL for LAP	Passed	
WLJ80S_WEBAUTH_01	Web auth redirection with L2 sec as WPA2-PSK-Customized login	To check after web passthrough, the client redirects to the requested url provided L2 security as WPA2-PSK and using customized web login page	Failed	

WLJ80S_WEBAUTH_02	Web auth redirection with L2 sec as WPA2-PSK-internal login	To check after web passthrough, the client redirects to the requested url provided L2 security as WPA2-PSK and using internal web login page	Passed	
WLJ80S_WEBAUTH_03	Customizing the default login page- web auth	To verify the login page with customized settings reflects when client redirects for authentication	Passed	
WLJ80S_WEBAUTH_04	Loading customized webauth bundle	To verify whether the customized login page reflects when client is authenticating via L3 webauth	Passed	
WLJ80S_WEBAUTH_05	Web authentication for iPhone	To verify whether web auth redirection is successful when connecting iPhone with iOS7 and Safari browser	Passed	
WLJ80S_WEBAUTH_06	Web auth bundle extraction in WLC	To verify whether the webauth bundle has been extracted successfully in WLC	Passed	
WLJ80S_WEBAUTH_07	Guest wlan clients' acquiring ip address from external dhcp server	To verify whether the guest wlan clients acquires their ip address from external dhcp server	Passed	
WLJ80S_WIPS_01	restore the MSE WIPS policy	To verify whether the restore of MSE WIPS policy is successful	Passed	
WLJ80S_WIPS_02	check the syncronization of MSE and PI when the WIPS policy enable	To verify the syncronzation loss between MSE and P when the WIPS policy enabled	Passed	
WLJ80S_WIPS_03	check the WIPS profile is applied from the PI to MSE	To verify whether the WIPS profile is applied successfully from the PI to MSE	Passed	

WLJ80S_WLAN_05	Configure a open authentication SSID on both radios in AP1142 GUI and associate a client	To verify whether open authentication SSID is able to create on both radios in 1142AP GUI and client is able to associate with it.	Passed	
WLJ80S_WLAN_06	Configure a open authentication SSID on both radios in AP1142 CLI and associate a client.	To verify whether open authentication SSID is able to create on both radios in 1142AP CLI and client is able to associate with it.	Passed	
WLJ80S_WLAN_07	Upgrade the autonomous AP1262 from GUI	To verify whether the autonomous AP1262 is upgraded from GUI.	Passed	
WLJ80S_WLAN_08	Upgrade the autonomous AP1262 from CLI	To verify whether the autonomous AP1262 is upgraded from CLI.	Passed	
WLJ80S_WLAN_09	Check the status of client link in AP1600	To verify whether the client link is enabled in AP1600.	Passed	
WLJ80S_WLAN_10	Configure a open authentication SSID on both radios in AP1262 GUI and associate two or more clients and ping between them	To verify whether open authentication SSID is able to create on both radios in 1262AP GUI and two or more clients are able to associate with it and able to communicate between them.	Passed	
WLJ80S_WLAN_11	Configure a open authentication SSID on both radios in AP1262 CLI and associate two or more clients and ping between them	To verify whether open authentication SSID is able to create on both radios in 1262AP CLI and two or more clients are able to associate with it and able to communicate between them.	Passed	

WLJ80S_WLAN_14	Configure a Layer2 security WLAN in wlc 5508 GUI and asscoiate 50 clients to it and check.	To verify whether layer 2 security WLAN is able to create in wlc5508 GUI and able to associate 50 clients to it.	Passed	
WLJ80S_WLAN_15	Configure a Layer2 security WLAN in wlc 5508 CLI and asscoiate 50 clients to it and check.	To verify whether layer 2 security WLAN is able to create in wlc5508 CLI and able to associate 50 clients to it.	Passed	
WLJ80S_WLAN_16	Configure a internal DHCP server in WLC and associate a client by getting ip address from dhcp server	To verify whether internal DHCP server is able to create in WLC and associate a client and check whether it getting ip address from DHCP server.	Passed	
WLJ80S_WLAN_17	Configure a DHCP server in AP and associate a client by getting ip address from DHCP server.	To verify whether DHCP server is able to configure in AP and associate a client and check whether it getting ip address from DHCP server.	Passed	
WLJ80S_WLAN_18	Configure a local MAC authentication in AP1042 and associate clients	To verify whether local mac authentication is able to configure and able to associate client in AP1042	Passed	
WLJ80S_WLAN_19	Configure a Mac address authentication in AP1042 with Radius server and associate clients.	To verify whether mac address authentication is able to configure and able to associate client in AP1042 with radius server.	Passed	
WLJ80S_WLAN_20	Confiigure a AP as local radius server with EAP-LEAP security	To verify whether the AP is configured as local radius server with EAP-LEAP and able to associate clients	Passed	

WLJ80S_WLAN_21	Configure a autonomous AP with Radius server for authenticaiton	To verify whether the client is able to authenticate and associate with AP by using radius server	Passed	
WLJ80S_WLAN_22	Configure EAP-TLS authentication with Radius server and associate clients.	To verify whether EAP-TLS authentication with Radius server is able to configure and able to associate client with AP.	Passed	
WLJ80S_WLAN_23	TACACS Authenticaiton for Autonomous AP	To verify whether user can able to login to the Autonoumous AP's GUI successfully or not via ACS Authentication	Passed	
WLJ80S_WLAN_24	Radio Beacons and ACKs from 1142 AP	To verify whether there is any Intermittent disconnection in AP or not	Passed	
WLJ80S_WLAN_25	1142 AP Upgrade	To verify whether 1142 AP can be upgraded from 12.4 image version to 15.2 successfully or not	Passed	
WLJ80S_WLAN_26	Client Roaming from WGB AP1 to AP2	To verify whether clients are associated successfully or not after WGB roaming	Passed	
WLJ80S_WLAN_27	Client Roaming back from WGB AP2 to AP1	To verify whether clients are associated successfully or not after WGB roaming	Passed	
WLJ80S_WLAN_28	WPA2 Security with AES encryption in 1600 Autonomous AP	To verify whether Windows 7 clients can successfully associate to WPA2 Security with AES encryption or not	Passed	

WLJ80S_WLAN_29	WPA2 Security with AES encryption in 1600 Autonomous AP	To verify whether Apple MAC clients can successfully associate to WPA2 Security with AES encryption or not	Passed	
WLJ80S_WLAN_30	Voice in 7921 Series Wireless IP Phones - Intra controller roaming	To verify whether the voice traffic is getting interrupted or not after roaming	Passed	
WLJ80S_WLAN_31	Voice in 7921 Series Wireless IP Phones - Inter controller roaming	To verify whether the voice traffic is getting interrupted or not after roaming	Passed	
WLJ80S_WLAN_32	Multicast traffic to and from wireless client	To verify whether the AP transmission is stopped or not during multicasting	Passed	
WLJ80S_WLAN_33	Downloading via 1602 Series Access Point	To verify whether simultaneously parallel download could be done in 1602 series AP or not	Passed	
WLJ80S_WLAN_34	Uploading via 1602 Series Access Point	To verify whether simultaneously parallel upload could be done in 1602 series AP or not	Passed	
WLJ80S_WLAN_35	AP Buffer size - ACL Config	To verify whether large config is saved to nvram successfully or not	Passed	
WLJ80S_WLAN_36	AP Buffer size - Other large Config changes	To verify whether large config is saved to nvram successfully or not	Passed	
WLJ80S_WLAN_37	Upgrading the autonomous AP software	To verify whether configuration changes or not after upgrading AP software	Passed	
WLJ80S_WLAN_38	Configuring 2600 series Autonomous AP's interface	To verify whether configuration changes or not after rebooting AP	Passed	

WLJ80S_WLAN_39	Configuring 3600 series Autonomous AP's interface	To verify whether configuration changes or not after rebooting AP	Passed	
WLJ80S_WLCHA_01	Incremental config sync between Active and Standby Hot WLCs	To verify whether the incremental config in Active WLC has been synced to Standby Hot WLC	Passed	
WLJ80S_WLCHA_02	Config Check after switchover happens	To verify whether the new Active has all its config restored after switchover happens due to nw/hw failure of previous active	Passed	
WLJ80S_WLCHA_03	AP logs when switchover happens in WLC HA	To verify whether AP doesn't log any error messages(Capwap SN) when switchover happens between the WLC HA	Passed	
WLJ80S_WLCHA_04	AP fallback to primary when AP fallback is enabled globally	To verify whether AP fallback to primary WLC when AP fallback is enabled globally	Passed	
WLJ80S_WLCHA_05	AP fallback to primary when AP fallback is disabled globally	To verify whether AP fallback happens when AP fallback is disabled globally	Passed	
WLJ80S_WLCHA_06	AP fallback when the WLCs in same mobility group	To verify AP fallback happens when the WLCs are in same mobility group	Passed	
WLJ80S_WLCHA_07	AP fallback when primary WLC is configured as Master WLC	To verify AP fallback happens when Primary WLC is configured as Master WLC	Passed	

NEC

Anyconnect VPN

Logical ID	Title	Description	Status	Defects
WLJ80MRS_NEC_01	WPA+WPA2 network (AnyConnect) using LaVie Tab S business	To check whether the Anyconnect VPN is connect or not, using WPA+WPA2 layer2 security in LaVie Tab S business	Passed	
WLJ80MRS_NEC_02	Layer 2 security "None" for open auth network (Anyconnect) in LaVie Tab S business .	To check whether the Anyconnect VPN is connect or not , using "None" Layer 2 security in LaVie Tab S business .	Passed	
WLJ80MRS_NEC_03	Anyconnect VPN - Intra controller roaming within the same subnet in LaVie Tab S business	To verify the intra controller roaming within the same subnet in LaVie Tab S business	Passed	
WLJ80MRS_NEC_04	Anyconnect VPN - Inter controller roaming within the different subnet in LaVie Tab S business	To verify the inter controller roaming using different subnet in LaVie Tab S business	Passed	

L2 Security

Logical ID	Title	Description	Status	Defects
WLJ80MRS_NEC_05	Associating LaVie Tab S business - L2 Security "None"	To check whether the LaVie Tab S business is associated successfully into the network or not.	Passed	
WLJ80MRS_NEC_06	Associating LaVie Tab S business - WPA2+PSK	To check whether the LaVie Tab S business is associated successfully into the network through WPA2+PSK authentication method	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80MRS_NEC_07	Associating LaVie Tab S business - L2 Security "WPA2+Dot1x".	To check whether the LaVie Tab S business is associated successfully into the network or not with L2 Security WPA2+Dot1x	Passed	

L3 Security

Logical ID	Title	Description	Status	Defects
WLJ80MRS_NEC_08	Associating LaVie Tab S business - L3 security "Web-Auth"	To check whether the LaVie Tab S business is associated successfully or not into the network through Web-Auth	Passed	
WLJ80MRS_NEC_09	Associating LaVie Tab S business - L3 security "Web-Auth Passthrough"	To check whether the LaVie Tab S business is associated successfully or not into the network through Web-Auth Passthrough	Passed	

Roaming

Logical ID	Title	Description	Status	Defects
WLJ80MRS_NEC_10	Associating LaVie Tab S business to a WLAN with FT enabled.	To verify whether LaVie Tab S business client is connected or not with FT enabled WLAN in 5760 WLC.	Passed	
WLJ80MRS_NEC_11	Associating LaVie Tab S business to a WLAN without FT enabled.	To verify whether LaVie Tab S business client is connected or not without FT enabled WLAN in 5760 WLC.	Passed	
WLJ80MRS_NEC_12	Roaming LaVie Tab S business client between 2 5760 WLC's with FT enabled & WPA2+PSk security.	To verify whether LaVie Tab S business client is roamed or not between 2 5760 WLC's.	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80MRS_NEC_13	Roaming LaVie Tab S business client between 2 5760 WLC's with FT enabled & WPA2+PSk security.	To verify whether LaVie Tab S business client is roamed or not between 2 5760 WLC's.	Passed	
WLJ80MRS_NEC_14	Roaming LaVie Tab S business client between 2 5760 WLC's with FT enabled & L2 security "None".	To verify whether LaVie Tab S business client is roamed or not between 2 5760 WLC's.	Passed	
WLJ80MRS_NEC_15	Roaming LaVie Tab S business client between 2 5760 WLC's with FT enabled & L2 security "None".	To verify whether LaVie Tab S business client is roamed or not between 2 5760 WLC's.	Passed	

Multiple RADIUS server per SSID

Logical ID	Title	Description	Status	Defects
WLJ80MRS_NEC_16	LaVie Tab S business association through Primary RADIUS server(ISE) at site level with L2 Security WPA2+Dot1x(PEAP)	To verify whether the Client authentication is done via Primary RADIUS server configured in flexconnect group	Passed	
WLJ80MRS_NEC_17	LaVie Tab S business association through Secondary RADIUS server(ISE)at site level with L2 Security WPA2+Dot1x(PEAP)	To verify whether the Client authentication is done via Secondary RADIUS server configured in flexconnect group	Passed	
WLJ80MRS_NEC_18	LaVie Tab S business association through Primary RADIUS server(ACS) at site level with L2 Security WPA2+Dot1x(PEAP)	To verify whether the Client authentication is done via Primary RADIUS server configured in flexconnect group	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80MRS_NEC_19	LaVie Tab S business association through Secondary RADIUS server(ACS) at site level with L2 Security WPA+Dot1x(PEAP)	To verify whether the Client authentication is done via Secondary RADIUS server configured in flexconnect group	Passed	

AAA

Logical ID	Title	Description	Status	Defects
WLJ80MRS_NEC_20	Performing MAC Filtering with LaVie Tab S business registered in ACS server- 7500 Controller	To check whether registered client is successfully authenticated and associated with WLAN enabled MAC Filtering	Passed	
WLJ80MRS_NEC_21	Performing MAC Filtering with LaVie Tab S business registered in ISE server- 7500 Controller	To check whether registered client is successfully authenticated and associated with WLAN enabled MAC Filtering	Passed	

Client SSO

Logical ID	Title	Description	Status	Defects
WLJ80MRS_NEC_22	Client SSO with web authentication L3 Security-LaVie Tab S business	To verify whether the Client SSO is successful with L3 security type web-authentication in WLC 5508	Passed	
WLJ80MRS_NEC_23	Client SSO with web authentication L3 Security after session timeout-LaVie Tab S business	To validate Client SSO with L3 security type web-auth after session timeout	Passed	
WLJ80MRS_NEC_24	Client SSO with L2 Security WPA/WPA2(local switching)-LaVie Tab S business	To validate Client SSO with L2 security WPA/WPA2 (local switching)	Passed	

H-REAP Fault tolerance

Logical ID	Title	Description	Status	Defects
WLJ80MRS_NEC_25	HREAP fault tolerance between connected and standalone AP-2.4 GHz	To verify whether the client associated to flexconnect AP will get reassociated in case of fault tolerance	Passed	
WLJ80MRS_NEC_26	HREAP fault tolerance between standalone and connected AP-5 GHZ	To verify whether the client associated to flexconnect AP will get reassociated in case of fault tolerance	Passed	

Adhoc Test Cases

Logical ID	Title	Description	Status	Defects
WLJ80S_Failed_04	Checking the description of Nas-ID under Controller> general page in OLH page.	To check whether Nas-id under Controller> general tab is present or not in OLH page.	Passed	
WLJ80S_Failed_19	Check the accessibility for analytics and other tab	To Verify the analytics tab take more time compare to the Dashboard and reports Tab for accessing.	Failed	CSCun75576
WLJ80S_Failed_21	check the zone based analytics for the specific zone at specific time	To verify the Zone based analytics for the multiple zone displays wrongly by selecting specific zone on the specific date. And it displays the zone instead selected zone. The selected zone for analysis was not created on the date instead it shows the another zone.	Failed	CSCun78279
WLJ80S_Failed_27	Check whether analytics displays building with corresponding maps after reset	To verify the building with corresponding maps changed after reset analytics.	Passed	
WLJ80S_Failed_20	PI Maps is not synchronized with MSE while copying the exiting Maps	To verify PI Maps is synchronized with MSE while copying the exiting Maps	Failed	CSCun76218

Logical ID	Title	Description	Status	Defects
WLJ80S_Failed_26	Unable to select multiple date option for the Zone analysis	To verify whether able to select multiple date option for the Zone analysis	Failed	CSCun78876
WLJ80S_Failed_25	Deleted real path is displayed in most popular path analysis	To verify Deleted real path is displayed in most popular path analysis	Failed	CSCun78862
WLJ80S_Failed_22	Page gets reset when changing clients max records in HTTPS mode of GUI	To check whether Page doesn't get reset when changing clients max records in HTTPS mode of GUI	Passed	
WLJ80S_Failed_12	Checking the apply button in VLAN mapping page of Flexconnect AP	To verify whether apply button works or not in VLAN mapping page of Flexconnect AP	Failed	CSCun59052
WLJ80S_Failed_15	Clicking save Event notification shows wrong message	To verify whether error message is correct while selecting save Event notification	Passed	
WLJ80S_Failed_36	Station role is shown as "Unknown" in Autonomous AP GUI for spectrum mode	To verify whether Station role is shown as "Unknown" in Autonomous AP GUI for spectrum mode	Passed	
WLJ80S_Failed_38	Add/Update Zone Description is not stored in the Maps tab	To verify Add/Update Zone Description is not stored in the Maps tab	Passed	
WLJ80S_Failed_24	Inheritance level for all WLAN entries changed to AP in Central DHCP page	To verify Inheritance level for all WLAN entries changed to AP in Central DHCP page	Passed	
WLJ80S_Failed_06	GUI : WLAN Profile name mismatch in WLAN VLAN mapping tab of flex group	GUI : To verify WLAN Profile name mismatch in WLAN VLAN mapping tab of flex group	Passed	

Logical ID	Title	Description	Status	Defects
WLJ80S_Failed_10	Unable to change the Access mode in SNMP community from the WLC GUI	To verify whether it is able to change the Access mode in SNMP community from the WLC GUI	Passed	
WLJ80S_Failed_05	HA works fine with untagged management vlan after upgraded to 8.0	To verify HA works fine with untagged management vlan after upgraded to 8.0	Passed	
WLJ80S_Failed_42	AP CLI accepting primary and secondary controller as same server	To verify AP CLI accepts primary and secondary controller as same server	Passed	
WLJ80S_Failed_01	IP address reversed for NTP server in 8500 WLC GUI	To verify IP address reversed for NTP server in 8500 WLC GUI	Passed	
WLJ80S_Failed_51	Unable to login PI CLI after changing hostname/IP upon PI re-setup	To verify PI CLI after changing hostname/IP upon re-setup	Failed	CSCup56865
WLJ80S_Failed_43	Device Port Summary dashlet shows wrong info for controllers	To verify whether Device Port Summary dashlet shows wrong info for controllers	Failed	CSCuo37342
WLJ80S_Failed_46	CLI description is missing for module3G in command "config ap ?"	To verify whether CLI description for module3G is appropriate	Failed	CSCup59088
WLJ80S_Failed_54	Policy Type for Static WEP clients in WLC GUI - (No Config)	To verify Policy Type for Static WEP clients in WLC GUI - (No Config)	Failed	CSCup86941
WLJ80S_Fail_02	System Configuration of AP in AP GUI	To verify the System configuration under Software tab in AP GUI	Failed	CSCuq82767
WLJ80S_Fail_03	LED Flash state description is missing in OLH page for All APs details	To check the LED flash state description in OLH page	Failed	CSCuq89168

Logical ID	Title	Description	Status	Defects
WLJ80S_Fail_06	EAP profile name display as Junk character if created in UTF-8 character	To verify whether WLC accepts EAP profile name as UTF-8 character and display it as it is. To verify whether WLC accepts EAP profile name as UTF-8 character and display it as it is.	Failed	CSCuq94587
WLJ80S_Fail_08	Deleted VLAN is showing in Autonomous AP CLI.	To check the VLAN status in auto AP cli	Failed	CSCur00347
WLJ80S_Fail_10	Custom Webauth and Webauth ACL config in AAP	To verify whether webauth acl could be configured without deactivating Custom webauth in AAP	Failed	CSCuq93760
WLJ80S_Fail_11	AP CLI:show command in non-privileged mode	To verify whether AP cli displays the output for the command show capwap client config	Failed	CSCur08583
WLJ80S_Fail_12	Creating WLAN profile and SSID names as empty gets accepted in CLI	To verify whether the WLC doesn't accept wlan profile and ssid name as empty	Failed	CSCur12267
WLJ80S_Failed_11	NGWC configuration via System config dialog	To verify whether NGWC configuration via System config dialog	Failed	CSCun55413
WLJ80S_Failed_02	Some options missing in WLAN> Advanced> Flexconnect in OLH page	To verify whether no options are missing in WLAN> Advanced> Flexconnect in OLH page	Failed	CSCum84944
WLJ80S_Failed_31	OEAP ACL's & Network lists gets deleted after upload /download the config	To verify whether OEAP ACL's & Network lists gets deleted after upload/download the config	Failed	CSCun96815
WLJ80MRS_Failed_01	Unable to block the Hangouts (Gtalk) messenger in AVC	To verify whether Hangouts (Gtalk) messenger in AVC is blocked	Failed	CSCus60566

Logical ID	Title	Description	Status	Defects
WLJ80MRS_Failed_02	Gmail works in Android Client when Gmail application WLC is blocked in AVC	To verify whether Gmail works in android client when gmail application WLC is blocked in AVC	Failed	CSCus68028

Related Documentation

ACS Installation Guide

http://www.cisco.com/en/US/partner/docs/net_mgmt/cisco_secure_access_control_system/5.3/user/guide/introd.html

ISE User Guide

http://www.cisco.com/en/US/docs/security/ise/1.2/user_guide/ise_overview.html

PI 2.0 User Guide

http://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/2-0/user/guide/prime_infra_ug.pdf

WLC 7.6 Configuration Guide

http://www.cisco.com/c/dam/en/us/td/docs/wireless/controller/7-6/configuration/guide/b_cg76.pdf

MSE Reference Guide

http://www.cisco.com/en/US/docs/wireless/mse/3310/quick/guide/MSE3310_GSG.html

CT5760 Controller Deployment Guide

http://www.cisco.com/en/US/docs/wireless/technology/5760_deploy/Supported_Features.html

Cisco Catalyst 3850 Switch Deployment Guide

http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps12686/deployment_guide_c07-727067.html