



Test Results Summary for Cisco Wireless LAN Controller AireOS 8.7 ,CME 8.7 for Japan (Release Version AireOS 8.7.102.0 ,CME 8.7.102.0)

First Published: 2018-05-14

Last Modified: 2018-05-15

Americas Headquarters

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



CONTENTS

CHAPTER 1	Overview	1
	Cisco Wireless LAN Solution Test	1

CHAPTER 2	Test Topology and Environment Matrix	7
	Test Topology	7
	Component Matrix	8
	What's New ?	10
	Open Caveats	10
	Resolved Caveats	11
	Limitation	12

CHAPTER 3	New Features - Test Summary	13
	WLC AireOS	13
	Limit clients per Radio	13
	CMX 10.4 Support	16
	IPv4 DNS Filtering for BYOD	17
	Enhancement to High Availability Monitoring and Management	19
	Assurance: In Line Monitoring	21
	AP-Group Configuration CLI on APIOS Parity: MFP support	23
	Flexconnect IOS Parity: Ethernet fallback	25
	Flexconnect IOS Parity: AAA Override bi-directional rate limit per client/BSSID	26
	Flexconnect IOS Parity: AAA Override of VLAN Name template	27
	Flexconnect IOS Parity: DHCP Option 60 Support	28
	CME	29
	802.1x support with EAP-TLS and EAP-PEAP	29
	Ethernet Fallback	31

OUI File Upload	32
Software update using SFTP	32
Import EAP certificate	34
PnP for Software Download in Day0	37
Central web authentication (CWA) with change of authorization (CoA)	40
Dynamic OID update	42
Bidirectional rate limit per client	42
RLAN support for APs with multiple Ethernet ports	44
Limit clients per radio	47
AAA Override of VLAN Name and VLAN Name-id template	49
Passive client support	50
ME GUI for P2P Blocking	53
Flexconnect IOS Parity: Passive Client / Wireless Proxy ARP	56
DNS Based ACL Rules	57
WSA Agent for Mobility Express	59

CHAPTER 4
Regression Features - Test Summary 61

WLC AireOS	61
Support vWLC on Amazon Web Services (AWS) (SP WiFi)	61
Private PSK	66
Fabric Enable Wireless	69
MAB Bypass Support	70
Passpoint R2 Flex Mode	73
Passive Client ARP Unicast	77
Selective Re-anchor	79
Network Assurance	80
High Availability & Monitoring HA	82
Default flex group	85
Roaming	86
Multiple RADIUS server per SSID	90
Hyperlocation Module supports for AP 37XX	91
Domain Based URL ACL	92
ATF on Mesh	94
LAG in Transition Restrictions	97

EoGRE Tunnel Priority / Fallback	98
TKIP/ Enabler for Wave 2 - 1800/2800/3800 APs Passpoint	103
Simplifying Cisco ISE Configuration on Cisco WLC - Phase 2	104
Flexconnect VLAN based Central switching	107
TrustSec Enhancements	108
Facebook WIFI	111
Location Analytics	113
Internal DHCP Server	115
Cisco WLC 3504 Support	118
Monitor Mode support in Aps(1810/1815)	121
Mobility Converged access on 5520/8540 WLC	122
HA WLC Auth/Authz	125
DHCP Option 82 - Google	128
Client Auth Failures(AAA Failures/WLC Failures)	131
Intra/Inter WLC Roaming Failures(Ping Pong Issues)	134
MIMO Coverage	137
Dot1x and Web-Auth	139
Autonomous AP	143
Flex Video stream	144
Home Page	147
MFP support	150
Flexconnect IOS Parity: Ethernet fallback	151
Flexconnect IOS Parity: AAA Override bi-directional rate limit per client/BSSID	153
Flexconnect IOS Parity: AAA Override of VLAN Name template	154
Flexconnect IOS Parity: DHCP Option 60 Support	155
AP Support (1815I/1815W/1562)	156
AP 1562 RF Support	159
SSID Filtering	161
EAP Types	162
H-REAP Fault Tolerance	163
Sensor Neighbor Info	164
Flexconnect Mode Feature Parity with IOS APs - 1832/1852/2800/3800 based Aps	164
WLAN Security	168
Config Wireless	169

CME	170
ME support on AP1815I/ 1562I	170
Captive Portal with Email address and Web Consent	176
TACACS	180
Hotspot 2.0	181
Mac filtering (for L2 security)	184
Access Visibility Control	187
Lobby Ambassador	193
Guest Login	195
PI support for ME	196
Syslogs	198
NAT	201
Rogue AP	203
Access Control List	205
Internal DHCP Server	209
Flex Video Streaming	210
DNS Based ACL Rules	214
Open DNS	216
Custom AP Group	217
CME Crashes(DHCP/Troubleshooting)	219
Client Auth Failures(AAA Failures/WLC Failures)	224
Intra/Inter WLC Roaming Failures(Ping Pong Issues)	229
Master AP Fail-over Issues	232
TLS Tunnel	235
Global AP configuration 802.1x	238
OUI File Upload	240
SNMP Trap Receivers	241
Central web authentication (CWA) with change of authorization (CoA)	242
ME GUI for Bidirectional rate limit per client	245
ME GUI with RLAN support for APs with multiple Ethernet ports	246
ME GUI for Limit clients per radio	249
ME GUI for AAA Override of VLAN Name / VLAN Name-id template	251
ME GUI for Passive client support	253
ME GUI for P2P Blocking	255

Flexconnect IOS Parity: Passive Client / Wireless Proxy ARP 258

External Guest Webauth in UI 259

Mobexp 261

CHAPTER 5 **CFD Derived Test cases** 263

CFD derived Test Cases 263

CHAPTER 6 **Related Documents** 297

Related Documentation 297



CHAPTER 1

Overview

- [Cisco Wireless LAN Solution Test](#) , on page 1

Cisco Wireless LAN Solution Test

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

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

- New features in WLC 8.7 & CME 8.7
- High priority scenarios and basic regression features
- Inputs from Cisco SEs/ TAC

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

The following products are covered in the test execution:

- Cisco Wireless LAN Controller 8540
- Cisco Wireless LAN Controller 5520
- Cisco Wireless LAN Controller 3504
- Cisco Mobility Express 1850
- Cisco Mobility Express 1830
- Cisco Mobility Express 1815I
- Cisco Mobility Express 1562
- APIC-EM Controller appliance
- Virtual Controller
- Access Point 1700

- Access Point 3700
- Access Point 1530
- Access Point 1600
- Access Point 2700
- Access Point 1570
- Access Point 702
- Access Point 1850
- Access Point 1830
- Access Point 3800
- Access Point 2800
- Access Point 1810
- Access Point 1815I
- Access Point 1815W
- Access Point 1542
- Cisco Prime Infrastructure (Physical-UCS,VM)

Acronyms

Acronym	Description
AAA	Authentication Authorization and Accounting
ACL	Access Control List
ACS	Access Control Server
AKM	Authentication Key Management
AP	Access Point
API	Application Programming Interface
APIC-EM	Application Policy Infrastructure Controller - Enterprise Module
ATF	Air-Time Fairness
AVC	Application Visibility and Control.
BGN	Bridge Group Network
BLE	Bluetooth Low Energy
BYOD	Bring Your Own Device
CA	Central Authentication
CAC	Call Admissions Control
CAPWAP	Control and Provisioning of Wireless Access Point

Acronym	Description
CCKM	Cisco Centralized Key Management
CCN	Channel Change Notification
CCX	Cisco Compatible Extensions
CDP	Cisco Discovery Protocol
CKIP	Cisco Key Integrity Protocol
CMX	Connected Mobile Experience
CVBF	Cisco Vector Beam Forming
CWA	Central Web Authentication
DCA	Dynamic Channel Assignment
DMZ	Demilitarized Zone
DNS	Domain Name System
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
MAP	Mesh Access Point
MCS	Modulation Coding Scheme
MFP	Management Frame Protection

Acronym	Description
mDNS	multicast Domain Name System
MIC	Message Integrity Check
MSE	Mobility Service Engine
MTU	Maximum Transmission Unit
NAC	Network Admission Control
NAT	Network Address Translation
NBAR	Network Based Application Recognition
NCS	Network Control System
NGWC	Next Generation Wiring closet
NMSP	Network Mobility Services Protocol
OEAP	Office Extended Access Point
PEAP	Protected Extensible Authentication Protocol
PEM	Policy Enforcement Module
PI	Prime Infrastructure
PMF	Protected Management Frame
POI	Point of Interest
PPPoE	Point-to-Point Protocol over Ethernet
PSK	Pre-shared Key
QOS	Quality of service
RADIUS	Remote Authentication Dial-In User Service
RAP	Root Access Point
RP	Redundancy Port
RRM	Radio Resource Management
SDN	Software Defined Networking
SOAP	Simple Object Access Protocol
SFTP	Secure File Transfer Protocol
SNMP	Simple Network Management Protocol
SS	Spatial Stream
SSID	Service Set Identifier
SSO	Single Sign On
SSO	Stateful Switch Over
TACACS	Terminal Access Controller Access Control System

Acronym	Description
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
vWLC	Virtual Wireless LAN Controller
VPC	Virtual port channel
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WGB	Workgroup Bridge
wIPS	Wireless Intrusion Prevention System
WLAN	Wireless LAN
WLC	Wireless LAN Controller
WPA	Wi-Fi Protected Access
WSM	Wireless Security Module



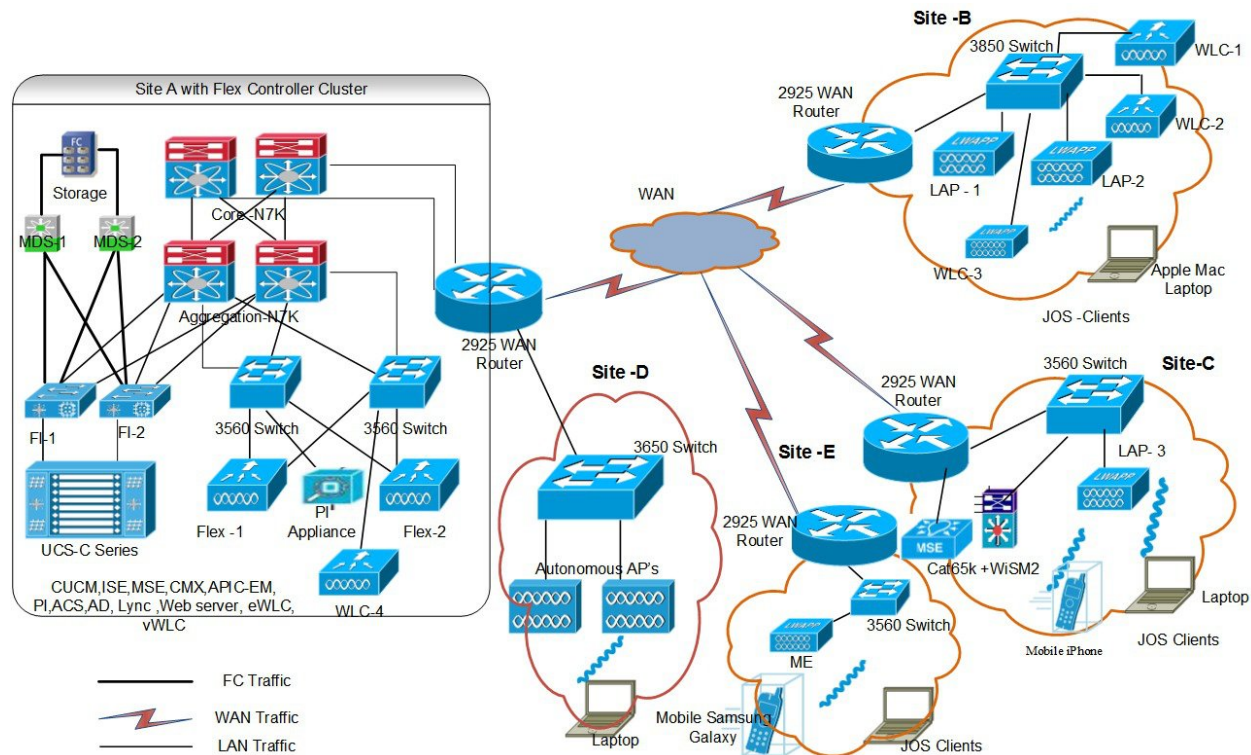
CHAPTER 2

Test Topology and Environment Matrix

- Test Topology, on page 7
- Component Matrix, on page 8
- What's New ?, on page 10
- Open Caveats, on page 10
- Resolved Caveats, on page 11
- Limitation, on page 12

Test Topology

Figure 1: Topology In Use



Component Matrix

Category	Component	Version
Controller	Wireless LAN Controller 5520	8.7.102.0
	CME 1800/2800/3800/1562	8.7.102.0
	Wireless LAN controller 8540	8.7.102.0
	Virtual Controller	8.7.102.0
	APIC-EM Controller appliance	1.6
	Wireless LAN Controller 3504	8.7.102.0
Applications	Prime Infrastructure (Virtual Appliance, UCS based)	3.4.0.0.348
	ISE(VM)	2.4
	Secure ACS(VM)	5.8.1
	CMX(Physical (3365), VM)	10.4.2
	MSE(Physical (3365), VM)	8.0.140.0
	Cisco Jabber for Windows, iPhone	11.8.0
	Cisco Air Provisioning App	1.4
	Cisco Wireless App	1.0.228
Access Point	Cisco AP 3700	15.3
	Cisco AP 3800	15.3
	Cisco AP 2800	15.3
	Cisco AP 2700	15.3
	Cisco AP 1600	15.3
	Cisco AP 1700	15.3
	Cisco AP 1850	15.3
	Cisco AP 1810	15.3
	Cisco AP 1815	15.3
	Cisco AP 1830	15.3
	Cisco AP 702I	15.3
	Cisco AP 1562	15.3
	Cisco AP 1542	15.3
	Cisco AP 1570	15.3

Category	Component	Version
Switch	Cisco 3750V2 switch	15.0(2)SE2
	Cisco Cat 6509-E	15.1(1)SY1
	Cisco Cat 9300	16.8.1
Chipset	5300, 6300 AGN	15.13.0.2
	7265 AC	19.10.0.9
	Airport Extreme	7.7
Client	Operating System(JOS)	Windows 7 Enterprise
		Windows 8 & 8.1 Enterprise
		Windows XP Professional
		Windows 10
	Apple Mac Book Pro, Apple Mac Book Air (JP Locale)	Mac OS 10.13.4
	iPad Pro	iOS 11.3(15E216)
	iPhone 6, 6S & 7 (JP Locale)	iOS 11.3(15E216)
	Samsung Galaxy S4 & S7, Nexus 6P, Sony Xperia XZ	Android 8.0 Oreo
	Wireless IP Phone 8821	11-0-3-221
	End points	Windows 7 Enterprise
		Apple Mac 10.13.4
		Windows 8 & 8.1
		iPhone 6,6S & 7
Windows 10		
Samsung Galaxy S4, S7, Nexus 6P		
Cisco AnyConnect VPN Client	4.5.05030	
Module	Hyper location Module	NA
Active Directory	AD	Windows 2008R2 Enterprise
Call Control	Cisco Unified Communications Manager	10.5.1-10000-7/10.5.1.1000-1(JP)
Browsers	IE	11.0.11
	Mozilla Firefox	57.0
	Safari	11.0.2
	Chrome	63

What's New ?

WLC AireOS

- Limit clients per Radio
- CMX 10.4 Support
- IPv4 DNS Filtering for BYOD
- Assurance: In Line Monitoring
- Enhancement to High Availability Monitoring and Management
- AP-Group Configuration CLI on APIOS Parity: MFP support
- Flexconnect IOS Parity: Ethernet fallback
- Flexconnect IOS Parity: AAA Override bi-directional rate limit per client/BSSID
- Flexconnect IOS Parity: AAA Override of VLAN Name template

CME

- 802.1x support with EAP-TLS and EAP-PEAP
- Ethernet Fallback
- Dynamic OID update
- Software update using SFTP
- Import EAP certificate
- PnP for Software Download in Day0
- Central web authentication (CWA) with change of authorization (CoA)
- Bidirectional rate limit per client
- RLAN support for APs with multiple Ethernet ports
- Limit clients per radio
- AAA Override of VLAN Name and VLAN Name-id template
- Passive client support
- ME GUI for P2P Blocking
- Flexconnect IOS Parity: Passive Client / Wireless Proxy ARP
- DNS Based ACL Rules
- WSA Agent for Mobility Express

Open Caveats

Logical ID	Title
CSCvi90562	User allowed to change MAC Filter WLAN ID as ANY in WLC CLI
CSCvi96766	CCX version for same client shown wrongly in 1810 and 1815 AP
CSCvj08339	2802/1852 AP's not reloading while enable/disable the 802.11g standard in WLC
CSCvj08974	Insufficient access to user when logged with selected privileges as configured in TACACS
CSCvi85683	1852 AP hits Out of range measurement slot 0 rssi 90 snr 90 nf 88 counter 1
CSCvh00117	WLC: Database entries mismatch in both controller and config guide

CSCvh12029	Crash log gets generated in WLC when 1562 AP gets joined
CSCvh12376	AP usage showing zero for 2700 AP while clients connected in WLC
CSCvh31058	Active hours under local policies shows incorrect time in WLC GUI
CSCvh51372	Accepting Same IP address for multiple media stream after displaying error message in CLI
CSCvh53238	WLC not returning MIB values for Lobby Admin account
CSCvi35837	CWA ACL Rule name is not displaying in Vlan & Firewall Tab
CSCvi55283	Admin account displaying error message while creating new user in ME UI
CSCvi65356	Pre Auth ACLs are not displaying when the user is in Read-Only access
CSCvi74109	Adding Pre Auth ACLs IP rules when the user is in Read-only access
CSCvi81672	CWA security policy changing to Open+Macfilter when user deleting and adding the Radius Server in ME
CSCvi90865	Irrelevant error message is displayed during deletion of Guest wlan profile
CSCvi90922	Unable to change security of WLAN profile when hs2 is configured
CSCvi96981	User unable to add Channel 165 for 80 and 160 MHz in ME UI
CSCvj04336	ME is throwing improper error while enabling the sensor Provisioning
CSCvj11216	Global AP configuration details are not showing after Export and Import the configurations
CSCvj13318	Not possible to create the DHCP scope name with combination of "!" symbol
CSCvj03946	ACL rule not possible to create with Upper and lower case rule names from UI
CSCvi79996	3802E coming as CAPWAP with next preferred master after ME to CAPWAP conversion
CSCvi35837	CWA ACL Rule name is not displaying in Vlan & Firewall Tab
CSCvi74109	Adding Pre Auth ACLs IP rules when the user is in Read-only access
CSCvh61417	ME 1562 name is showing as Cisco Wireless Controller in UI
CSCvh61484	Not able to abort the software Image update in CME
CSCvh65773	Radius server cannot be added to the WLAN/RLAN.
CSCvh48115	Rate limit value given with decimal takes 0
CSCvh04962	Need to click two times on ping test Start button after showing error
CSCvg20696	User is not able to remove the radius server

Resolved Caveats

Logical ID	Title
CSCvh24561	SXP Peer IP is accepting network IP through CLI in AP global configuration
CSCvi21178	Error in adding new Syslog server IP while creating the same series in ME UI

Limitation

CSCvi21091	Enabling show password for SSH tab is reflecting in 802.1x tab
CSCvh17309	User is not able to test radius response for wlan with security type CWA via Troubleshooting tools
CSCvh17235	WLAN Profile name length is mismatch between CLI and UI in ME
CSCvi21178	Error in adding new Syslog server IP while creating the same series in ME UI
Logical ID	Enabling show password for SSH tab is reflecting in 802.1x tab
CSCvh65876	Unauthorized access for TACACS User with selected privileges in WLC
CSCvh04887	Configuration file not importing in ME using Japanese browser
CSCvh51157	Not possible to create the Domain and Realm name with special characters in 802.11u
CSCvh51170	Enabling show password for 802.1x tab is reflecting in SSH tab

Limitation

Logical ID	Title
CSCvj11261	Packet capture is shown as started on the device but the files are not getting generated
CSCvh30911	WLAN security changed while deploying WLAN template from PI to CME



CHAPTER 3

New Features - Test Summary

- [WLC AireOS, on page 13](#)
- [CME, on page 29](#)

WLC AireOS

Limit clients per Radio

Logical ID	Title	Description	Status	Defect ID
WLJ87IIS_CPR_01	Configuring maximum Allowed Clients Per AP Radio with radio policy as 2.4 GHz and connecting client with different security policy.	To configure maximum allowed client Per AP radio with radio policy as 2.4GHz and connecting a client.	Passed	
WLJ87IIS_CPR_02	Configuring maximum Allowed Clients Per AP Radio with radio policy as 5 GHz and connecting client with different security policy.	To configure maximum allowed client Per AP radio with radio policy as 5 GHz and connecting a client.	Passed	
WLJ87IIS_CPR_03	Configuring maximum Allowed Clients Per AP Radio with radio policy as 2.4 GHz and connecting client to different AP's.	To connect client to different AP's configuring maximum allowed client per AP radio and check if the configured client alone gets authenticated.	Passed	

Limit clients per Radio

WLJ87IIS_CPR_04	Configuring maximum Allowed Clients Per AP Radio with radio policy as 5 GHz and connecting client to different AP's.	To connect client to different AP's configuring maximum allowed client per AP radio and check if the configured client alone gets authenticated.	Passed	
WLJ87IIS_CPR_05	Configuring maximum allowed client Per AP radio with radio policy as 2.4 GHz with central switching WLAN	To configure maximum allowed client Per AP radio as 2.4 GHZ with central switching and connecting a clients to it.	Passed	
WLJ87IIS_CPR_06	Configuring maximum allowed client Per AP radio with radio policy as 2.4 GHz with local switching WLAN	To configure maximum allowed client Per AP radio as 2.4 GHZ with Local switching and connecting a clients to it.	Passed	
WLJ87IIS_CPR_07	Configuring maximum allowed client Per AP radio with radio policy as 2.4 GHz with local switcing and local authentication	To configure maximum allowed client Per AP radio as 2.4 GHZ with local switching and local authentication and connecting a clients to it.	Passed	
WLJ87IIS_CPR_08	Configuring maximum allowed client Per AP radio with radio policy as 5 GHz with central switching WLAN	To configure maximum allowed client Per AP radio as 5 GHZ with central switching and connecting a clients to it.	Passed	
WLJ87IIS_CPR_09	Configuring maximum allowed client Per AP radio as 5 GHz with local switching WLAN	To configure maximum allowed client Per AP radio as 5 GHZ with Local switching and connecting a clients to it.	Passed	

WLJ87IIS_CPR_10	Configuring maximum allowed client Per AP radio as 5 GHz with local switching and local authentication	To configure maximum allowed client Per AP radio as 5 GHZ with local switching and local authentication and connecting a clients to it.	Passed	
WLJ87IIS_CPR_11	Configuring maximum allowed client Per AP radio as 2.4 GHz and try connecting 5 GHZ client.	To configuring maximum allowed client Per AP radio as 2.4 GHz and try connecting 5 GHZ client . check if only 2.4 GHz clients gets connected and 5 GHz client does not get connected.	Passed	
WLJ87IIS_CPR_12	Configuring maximum allowed client Per AP radio as 5 GHz and try connecting 2.4 GHZ client.	To configuring maximum allowed client Per AP radio as 5 GHz and try connecting 5 GHZ client . check if only 2.4 GHz clients gets connected and 2.4 GHz client does not get connected.	Passed	
WLJ87IIS_CPR_13	Deleting one already existing client in 2.4 GHz when max limit reached and try connecting new client .	To delete one existing client in 2.4 GHz when the client limit is reached to maximum and try connecting a new client and check if the clients gets connected to it .	Passed	
WLJ87IIS_CPR_14	Deleting one already existing client in 5 GHz when max limit reached and try connecting new client .	To delete one existing client in 5 GHz when the client limit is reached to maximum and try connecting a new client and check if the clients gets connected to it .	Passed	

WLJ87IIS_CPR_15	Trying AP failover priority when clients connected to a AP .	To try AP failover priority when clients connected and the HA WLC has the same WLAN with radio as 2.4 GHz .The WLAN is configured with maximum allowed client Per AP	Passed	
WLJ87IIS_CPR_16	Intra roaming of clients configuring maximum allowed client Per AP radio	To try intra roaming of clients on the same WLC in a WLAN configured with maximum allowed client Per AP radio and check if the client roam from one AP to another AP.	Passed	
WLJ87IIS_CPR_17	Inter roaming of clients configuring maximum allowed client Per AP radio	To try inter roaming of clients configuring maximum allowed client per AP radio and check if only the configured limit of clients alone gets connected.	Passed	

CMX 10.4 Support

Logical ID	Title	Description	Status	Defect ID
WLJ87IIS_CMX_01	Adding Cisco WLC to CMX	To add a Cisco WLC to CMX and check if the WLC gets added to the CMX with the WLC status showing	Passed	
WLJ87IIS_CMX_02	Importing maps from prime infrastructure	To import maps from prime infrastructure and check if the maps gets imported to the cmx .	Passed	
WLJ87IIS_CMX_03	Importing the maps with 2 to 3 Access points from PI to CMX	To import the maps from prime infra to CMX with 2 to 3 access point and check if the access point details are shown correctly including clients connected .	Passed	

WLJ87IIS_CMX_04	Connecting the client to the access point on the floor and check if the details of the client.	To connect a client to the access point on the floor and check if the details of the clients are shown correctly or not.	Passed	
WLJ87IIS_CMX_05	Connecting many clients from different place and check the location of the clients	To connect many client from different place to the access points and check if the location of the client are shown in CMX	Passed	
WLJ87IIS_CMX_06	Searching the client by MAC address	To check whether client device can be searched by specifying its MAC address or not	Passed	
WLJ87IIS_CMX_07	Searching the client using its IP address	To check whether client device can be searched by specifying its IP address or not	Passed	
WLJ87IIS_CMX_08	Searching client using its SSID	To verify whether client device can be searched by specifying the SSID or not	Passed	
WLJ87IIS_CMX_09	Check the number of clients visting the building and floor in hourly basic and daily basic	To check the the number of client visiting the building or floor on hourly and daily basic	Passed	
WLJ87IIS_CMX_10	Checking the number of new and repeat visitors to the building or floor.	To check the number of new and repeat clients to the building or floor .	Passed	

IPv4 DNS Filtering for BYOD

Logical ID	Title	Description	Status	Defect ID
WLJ87IIS_BYOD_01	Connecting Android client with single ssid BYOD network	Verify that Android client is getting connected or not with single SSID	Passed	
WLJ87IIS_BYOD_02	Connecting ios client with single ssid BYOD network	Verify that IOS client is getting connected or not with single SSID	Passed	
WLJ87IIS_BYOD_03	Connecting windows client with single ssid BYOD network	Verify that windows client is getting connected or not with single SSID	Passed	

WLJ87IIS_BYOD_04	Connecting android client with dual ssid BYOD network	Verify that android client is getting connected or not with dual SSID	Passed	
WLJ87IIS_BYOD_05	Connecting ios client with dual ssid BYOD network	Verify that IOS client is getting connected or not with dual SSID	Passed	
WLJ87IIS_BYOD_06	Connecting windows client with dual ssid BYOD network	Verify that windows client is getting connected or not with dual SSID	Passed	
WLJ87IIS_BYOD_07	Debugging the BYOD client connection	Verify that user is able to take debug the BYOD Client or not	Passed	
WLJ87IIS_BYOD_08	Connecting JOS client with single ssid BYOD network	Verify that JOS client is connected with single ssid BYOD network or not	Passed	
WLJ87IIS_BYOD_09	Connecting JOS client with dual ssid BYOD network	Verify that JOS client is connected with dual ssid BYOD network or not	Passed	
WLJ87IIS_BYOD_10	Configuring the maximum URL ACL via GUI/CLI/PI	Verify that user is able to configure maximum url acl or not	Passed	
WLJ87S_BYOD_01	Configuring the maximum URL ACL via GUI/CLI/PI	Verify that user is able to configure maximum url acl or not	Passed	
WLJ87S_BYOD_02	Connecting android client with single ssid BYOD network	Verify that android client is getting connected or not with single SSID	Passed	
WLJ87S_BYOD_03	Connecting ios client with single ssid BYOD network	Verify that IOS client is getting connected or not with single SSID	Passed	
WLJ87S_BYOD_04	Connecting windows client with single ssid BYOD network	Verify that windows client is getting connected or not with single SSID	Passed	
WLJ87S_BYOD_05	Connecting android client with single ssid BYOD network	Verify that android client is getting connected or not with dual SSID	Passed	
WLJ87S_BYOD_06	Connecting ios client with single ssid BYOD network	Verify that IOS client is getting connected or not with dual SSID	Passed	

WLJ87S_BYOD_07	Connecting windows client with single ssid BYOD network	Verify that windows client is getting connected or not with dual SSID	Passed	
WLJ87S_BYOD_08	Debugging the BYOD client connection	Verify that user is able to take debug the BYOD Client or not	Passed	
WLJ87S_BYOD_09	Connecting JOS client with single ssid BYOD network	Verify that JOS client is connected with single ssid BYOD network or not	Passed	
WLJ87S_BYOD_10	Connecting JOS client with dual ssid BYOD network	Verify that JOS client is connected with dual ssid BYOD network or not	Passed	

Enhancement to High Availability Monitoring and Management

Logical ID	Title	Description	Status	Defect ID
WLJ87PIIS_BHA_01	Configuring HA pair up- WLC 5520 /8540 by using the cli command	To verify whether the HA pair (ACTIVE:STANDBY) is up successfully by using the cli command	Passed	
WLJ87PIIS_BHA_02	Controller HA pair with different hardware models (3504 and 8540)	To verify the role negotiation between the controllers with different hardware models	Passed	
WLJ87PIIS_BHA_03	Verifying the serial number of the standby controller	To check whether the serial number of the standby controller is getting or not	Passed	
WLJ87PIIS_BHA_04	Verifying the FAN status of the standby controller	To verify whether the FAN status of the standby controller is getting or not	Passed	
WLJ87PIIS_BHA_05	Setting the FAN status of the standby controller to full/low speed and read the FAN status	To check whether full/low speed FAN status of the standby controller is getting or not	Passed	

WLJ87PIIS_BHA_06	Configuring controller HA pair with different software versions	To verify whether controllers HA pair with different software versions	Passed	
WLJ87PIIS_BHA_07	Checking the controller mode when the redundancy port loses connectivity	To verify the HA pair controller mode after disconnecting the redundancy port	Passed	
WLJ87PIIS_BHA_08	Checking the controller modes(HA pair) after power failure	To verify the controller modes after power failure on both the controllers	Passed	
WLJ87PIIS_BHA_09	Checking the HA mode after resetting the peer system from active controller	To verify the HA mode after resetting the peer system from active controller	Passed	
WLJ87PIIS_BHA_10	Checking the JOS client status during AP SSO after active failover-L2 Authentication	To verify whether the client gets disassociated and forced to re-join to the controller after AP SSO	Passed	
WLJ87PIIS_BHA_11	Checking 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	
WLJ87PIIS_BHA_12	Checking the serial number of standby controller after connect the android client	To verify whether the serial number of standby controller is showing or not after connect the android client	Passed	
WLJ87PIIS_BHA_13	Checking the FAN status of standby controller after connect the IOS client	To verify whether the FAN status of standby controller is showing or not after connect the IOS client	Passed	

WLJ87IIS_BHA_14	Checking the windows 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	
-----------------	---	---	--------	--

Assurance: In Line Monitoring

Logical ID	Title	Description	Status	Defect ID
WLJ87IIS_ILM_01	Checking that after PS marked AP is receiving trigger from Windows client or not	Verify that after PS marked AP is receiving trigger from Windows client or not	Passed	
WLJ87IIS_ILM_02	Checking that after PS marked AP is receiving trigger from IOS client or not	Verify that after PS marked AP is receiving trigger from IOS client or not	Passed	
WLJ87IIS_ILM_03	Checking that after PS marked AP is receiving trigger from andriod client or not	Verify that after PS marked AP is receiving trigger from andriod client or not	Passed	
WLJ87IIS_ILM_04	Verify that TIM bit is getting cleared or not after dilvery the buffered data to windows client	Checking that TIM bit is getting cleared or not after dilvery the buffered data to windows client	Passed	
WLJ87IIS_ILM_05	Verify that TIM bit is getting cleared or not after dilvery the buffered data to IOS client	Checking that TIM bit is getting cleared or not after dilvery the buffered data to IOS client	Passed	
WLJ87IIS_ILM_06	Verify that TIM bit is getting cleared or not after dilvery the buffered data to android client	Checking that TIM bit is getting cleared or not after dilvery the buffered data to android client	Passed	
WLJ87IIS_ILM_07	Checking that ap is sending the packet if windows client is in PS state	Verify that ap is sending the packet if windows client is in PS state	Passed	

WLJ87IIS_ILM_08	Checking that ap is sending the packet if IOS client is in PS state	Verify that ap is sending the packet if IOS client is in PS state	Passed	
WLJ87IIS_ILM_09	Checking that ap is sending the packet if android client is in PS state	Verify that ap is sending the packet if android client is in PS state	Passed	
WLJ87IIS_ILM_10	Deauthentication the Windows client with WLC	Verify that deauthentication event logged in ILM or not for windows client	Passed	
WLJ87IIS_ILM_11	Deauthentication the IOS client with WLC	Verify that deauthentication event logged in ILM or not for IOS client	Passed	
WLJ87IIS_ILM_12	Deauthentication the android OS client with WLC	Verify that deauthentication event logged in ILM or not for android client	Passed	
WLJ87S_ILM_01	Checking that after PS marked AP is receiving trigger from Windows client or not	Verify that after PS marked AP is receiving trigger from Windows client or not	Passed	
WLJ87S_ILM_02	Checking that after PS marked AP is receiving trigger from IOS client or not	Verify that after PS marked AP is receiving trigger from IOS client or not	Passed	
WLJ87S_ILM_03	Checking that after PS marked AP is receiving trigger from android client or not	Verify that after PS marked AP is receiving trigger from android client or not	Passed	
WLJ87S_ILM_04	Verify that TIM bit is getting cleared or not after delivery the buffered data to windows client	Checking that TIM bit is getting cleared or not after delivery the buffered data to windows client	Passed	
WLJ87S_ILM_05	Verify that TIM bit is getting cleared or not after delivery the buffered data to IOS client	Checking that TIM bit is getting cleared or not after delivery the buffered data to IOS client	Passed	

WLJ87S_ILM_06	Verify that TIM bit is getting cleared or not after delivery the buffered data to android client	Checking that TIM bit is getting cleared or not after delivery the buffered data to android client	Passed	
WLJ87S_ILM_07	Checking that ap is sending the packet if windows client is in PS state	Verify that ap is sending the packet if windows client is in PS state	Passed	
WLJ87S_ILM_08	Checking that ap is sending the packet if IOS client is in PS state	Verify that ap is sending the packet if IOS client is in PS state	Passed	
WLJ87S_ILM_09	Checking that ap is sending the packet if android client is in PS state	Verify that ap is sending the packet if android client is in PS state	Passed	
WLJ87S_ILM_10	Deauthentication the Windows client with WLC	Verify that deauthentication event logged in ILM or not for windows client	Passed	
WLJ87S_ILM_11	Deauthentication the IOS client with WLC	Verify that deauthentication event logged in ILM or not for IOS client	Passed	
WLJ87S_ILM_12	Deauthentication the android OS client with WLC	Verify that deauthentication event logged in ILM or not for android client	Passed	

AP-Group Configuration CLI on APIOS Parity: MFP support

Logical ID	Title	Description	Status	Defect ID
WLJ87IIS_MFP_01	Verifying if MFP can be enabled and disabled via cli on WLC	To verify if MFP can be enabled ,disabled via WLC CLI and check if the MFP is applied globally or not.	Passed	

WLJ87IIS_MFP_02	Checking if IMIC IE value in MFP is appended in 3800 AP	To check if the IMIC IE value in MFP is appended in 3800 AP or not after enabling MFP globally.	Passed	
WLJ87IIS_MFP_03	Checking if IMIC IE value in MFP is appended in 2800 AP	To check if the IMIC IE value in MFP is appended in 2800 AP or not after enabling MFP globally.	Passed	
WLJ87IIS_MFP_04	Connecting a CCXv5 Window client to a 3800 AP with MFP option as Required .	To connect a window CCxv5 client to a 3800 AP with MFP option as required and check the IMIC IE value in MFP .	Passed	
WLJ87IIS_MFP_05	Connecting a Mac OS CCXv5 client to a 3800 AP with MFP option as Required .	To connect a Mac OS CCxv5 client to a 3800 AP with MFP option as required and check the IMIC IE value in MFP.	Passed	
WLJ87IIS_MFP_06	Connecting a CCXv5 Window client to a 2800 AP with MFP option as Required .	To connect a window CCxv5 client to a 2800 AP with MFP option as required and check the IMIC IE value in MFP .	Passed	
WLJ87IIS_MFP_07	Connecting a Mac OS CCXv5 client to a 2800 AP with MFP option as Required .	To connect a Mac OS CCxv5 client to a 2800 AP with MFP option as required and check the IMIC IE value in MFP .	Passed	
WLJ87IIS_MFP_08	Pushing MFP configuration from PI and connecting a client .	To connect a client to the 2800 AP where the template is pushed from PI and check if the IMIC IE value is appended or not.	Passed	

WLJ87IIS_MFP_09	Exporting and Importing configuration of MFP	To exporting and importing configuration of MFP and check if the configuration remains the same after import and export.	Passed	
-----------------	--	--	--------	--

Flexconnect IOS Parity: Ethernet fallback

Logical ID	Title	Description	Status	Defect ID
WLJ87S_FLEXIOSEthernet_01	Enable/Disable Ethernet fall-back in WLC UI	To verify whether Ethernet fall-back is enable/disable successfully or not from WLC UI	Passed	
WLJ87S_FLEXIOSEthernet_02	Enable/Disable Ethernet fall-back in WLC CLI	To verify whether Ethernet fall-back is enable/disable successfully or not from WLC CLI	Passed	
WLJ87S_FLEXIOSEthernet_03	Disabling the radio 802.11a b after POE remove	To verify whether Radios getting disable or not after removing the POE connection to AP	Passed	
WLJ87S_FLEXIOSEthernet_04	Checking the disabled Radios 'a' & 'b' details after POE connect	To check whether the 802.11 radios comes Up/Down as configured before once POE connected to AP	Passed	
WLJ87S_FLEXIOSEthernet_05	Checking Disabled 802.11a and enable 802.11b details after POE remove	To verify whether Radios getting disable or not after removing the POE connection in AP	Passed	
WLJ87S_FLEXIOSEthernet_06	Checking Disabled 802.11a and enable 802.11b details after POE connect	To check whether the 802.11 radios comes Up/Down as configured before once POE connected to AP	Passed	

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

WLJ87S_ FLEXIOSEthernet _07	Checking enabled 802.11a and disabled 802.11b details after POE remove	To verify whether Radios getting disable or not after removing the POE connection in AP	Passed	
WLJ87S_ FLEXIOSEthernet _08	Checking enabled 802.11a and disabled 802.11b details after POE connect	To check whether the 802.11 radios comes Up/Down as configured before once POE connected to AP	Passed	
WLJ87S_ FLEXIOSEthernet _09	Configuring the fall-back details in Read-only mode from UI	To verify whether Ethernet fall-back details are possible to configure or not for read only users	Passed	
WLJ87S_ FLEXIOSEthernet _10	Configuring the fall-back details in read only mode from Cli	To verify whether Ethernet fall-back details are possible to configure or not from CLI	Passed	
WLJ87S_ FLEXIOSEthernet _11	Verifying the fall back details from CLI for read only	To verify whether Ethernet fall-back details are showing or not	Passed	
WLJ87S_ FLEXIOSEthernet _12	Reloading the AP after Ethernet fall-back configuring	To verify whether Ethernet fall-back details are showing properly or not after reload	Passed	
WLJ87S_ FLEXIOSEthernet _13	Upgrading the Ap after Ethernet fall-back configuring	To verify whether Ethernet fall-back details are showing properly or not after Upgrade the image	Passed	
WLJ87S_ FLEXIOSEthernet _14	Checking the roaming scenarios after client connect	To verify whether roaming happening not after Ethernet fall-back	Passed	

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

Logical ID	Title	Description	Status	Defect ID
WLJ87S_ Bi-DirectiRate _01	Configuring the downstream and upstream value as "0" per User	To verify whether downstream and upstream values are no restrictions for configured values as "0" per User or not	Passed	

WLJ87S_ Bi-DirectiRate _02	Configuring the downstream and upstream value as "0" per SSID	To verify whether downstream and upstream values are no restrictions for configured values as "0" per SSID or not	Passed	
WLJ87S_ Bi-DirectiRate _03	Configuring the downstream and upstream value as certain range per User	To verify whether downstream and upstream values access with restrictions for configured values as per User or not	Passed	
WLJ87S_ Bi-DirectiRate _04	Configuring the downstream and upstream value as certain range per SSID	To verify whether downstream and upstream values access with restrictions for configured values as per SSID	Passed	
WLJ87S_ Bi-DirectiRate _05	Resetting the WLC after configure the Client and SSID values	To verify whether Client and SSID values are proper or not	Passed	
WLJ87S_ Bi-DirectiRate _06	Clearing the values after AAA override enable	To verify whether values are clearing or not	Passed	
WLJ87S_ Bi-DirectiRate _07	Checking the roaming scenario	To verify whether after client roam between controllers client accessing proper bandwidth or not	Passed	
WLJ87S_ Bi-DirectiRate _08	Checking the bandwidth for client and SSID in standalone mode	To verify whether clients are getting proper connection for standalone or nor	Passed	

Flexconnect IOS Parity: AAA Override of VLAN Name template

Logical ID	Title	Description	Status	Defect ID
WLJ87S_VLAN_Temp_01	Creating the VLAN Template	To verify whether VLAN Template is creating or not	Passed	
WLJ87S_VLAN_Temp_02	Assigning the Flexconnect VLAN to Flexconnect group	To verify whether VLAN Template is assigning successfully or not to Flexconnect group	Passed	
WLJ87S_VLAN_Temp_03	Checking the AAA override for VLAN name id	To verify whether AAA overriding happening or not with VLAN name	Passed	

Flexconnect IOS Parity: DHCP Option 60 Support

WLJ87S_VLAN_Temp_04	Configuring VLAN name id for AAA override at the time of VLAN support in disable state	To verify whether AAA override is happening or not when VLAN support is in disable state	Passed	
WLJ87S_VLAN_Temp_05	After configure the WLAN-VLAN support checking the details	To verify whether WLAN-VLAN details are applying or not after configure and disable the VLAN support	Passed	
WLJ87S_VLAN_Temp_06	Checking the details in AP after VLAN name id Exchange	To verify details are showing in AP CLI or not	Passed	
WLJ87S_VLAN_Temp_07	Checking the debug details at the time of VLAN name id details	To verify whether details are showing successfully or not at the time of VLAN name id exchange	Passed	
WLJ87S_VLAN_Temp_08	Rebooting the WLC after AAA override with VLAN name ID	To verify whether Client are getting AAA override details or not after reboot	Passed	
WLJ87S_VLAN_Temp_09	Checking the details in Roaming	To verify whether Roaming is happening with AAA override for VLAN name id	Passed	

Flexconnect IOS Parity: DHCP Option 60 Support

Logical ID	Title	Description	Status	Defect ID
WLJ87S_DHCP60_01	Configuring the DHCP Option 60 in router	To verify whether DHCP Option 60 is configuring successfully or not	Passed	
WLJ87S_DHCP60_02	Checking DHCP option 63 is matching with AP	To verify whether DHCP Option 60 details are matching with AP or not	Passed	
WLJ87S_DHCP60_03	Connecting the android client without adding VCI	To verify whether android is getting the IP address or not	Passed	
WLJ87S_DHCP60_04	Connecting the IOS client without adding VCI	To verify whether IOS client is getting the IP address or not	Passed	
WLJ87S_DHCP60_05	Connecting the Japanese client without adding VCI	To verify whether Japanese is getting the IP address or not	Passed	

CME

802.1x support with EAP-TLS and EAP-PEAP

Logical ID	Title	Description	Status	Defect Id
MEJ87PhIS_dot1x_01	Enabling dot1x auth for AP and joining AP to ME WLC	To check whether AP joins ME or not after dot1x authentication from Switch/ISE	Passed	
MEJ87PhIS_dot1x_02	Associating Windows clients to AP joined via Dot1x authentication	To check whether Windows clients associated successfully or not once AP joined via dot1x authentication from Switch/ISE	Passed	
MEJ87PhIS_dot1x_03	Joining COS AP to ME through Dot1x+PEAP authentication	To check whether COS AP joins ME or not after dot1x authentication from Switch/ISE via EAP method PEAP	Passed	
MEJ87PhIS_dot1x_04	Joining iOS AP to ME through Dot1x+EAP TLS authentication	To check whether iOS AP joins ME or not after dot1x authentication from Switch/ISE via EAP method TLS	Passed	
MEJ87PhIS_dot1x_05	Trying to join AP's through Dot1x authentication with LSC provisioning	To check whether AP's joins ME or not through LSC provisioning & dot1x authentication	Passed	
MEJ87PhIS_dot1x_06	Providing invalid credentials for AP authentication and checking the status of AP in console	To check whether AP throws error message or not when invalid credentials provided during dot1x authentication	Passed	

MEJ87PhIIS_dot1x_07	Disabling dot1x support in Switch and trying to associate AP via Dot1x authentication to ME WLC	To check whether AP joins ME or not even dot1x is disabled in switch	Passed	
MEJ87PhIIS_dot1x_08	Enabling dot1x auth for AP in 3850 Switch	Configuring the 3850 Switch for Dot1x authentication by mapping the identity profiles to a port.	Passed	
MEJ87PhIIS_dot1x_09	Checking the configuration of 802.1x authentication paramaters after export/import the config file	To check whether 802.1x auth parameters restores or not after export/import the config file in ME UI via TFTP	Passed	
MEJ87PhIIS_dot1x_10	Associating Mac OS clients to AP joined via Dot1x authentication	To check whether Mac OS clients associated successfully or not once AP joined via dot1x authentication from Switch/ISE	Passed	
MEJ87PhIIS_dot1x_11	Associating Android clients to AP joined via Dot1x authentication	To check whether Android clients associated successfully or not once AP joined via dot1x authentication from Switch/ISE	Passed	
MEJ87PhIIS_dot1x_12	Associating iOS clients to AP joined via Dot1x authentication	To check whether iOS clients associated successfully or not once AP joined via dot1x authentication from Switch/ISE	Passed	
MEJ87PhIIS_dot1x_13	Trying to configure of 802.1x authentication paramaters via Read-only User	To check whether Read only user can be able to configure or not the 802.1x auth parameters in ME UI	Passed	

Ethernet Fallback

Logical ID	Title	Description	Status	Defect ID
MEJ87PhIIS_Eth_01	Checking the radio status of iOS AP after enabling the Ethernet Fallback	To verify whether Radios getting disable or not after enabling the ethernet Fallback for iOS AP	Passed	
MEJ87PhIIS_Eth_02	Checking the radio status of COS AP after enabling the Ethernet Fallback	To verify whether Radios getting disable or not after enabling the ethernet Fallback for COS AP	Passed	
MEJ87PhIIS_Eth_02	Associating Windows clients to AP and checking the clients network access after removing PoE connection	To verify whether Windows clients access to network remains same or not when AP's PoE connection is removed	Passed	
MEJ87PhIIS_Eth_03	Associating Mac OS clients to AP and checking the clients network access after removing PoE connection	To verify whether Mac OS clients access to network remains same or not when AP's PoE connection is removed	Passed	
MEJ87PhIIS_Eth_04	Associating Android clients to AP and checking the clients network access after removing PoE connection	To verify whether Android clients access to network remains same or not when AP's PoE connection is removed	Passed	
MEJ87PhIIS_Eth_05	Associating iOS clients to AP and checking the clients network access after removing PoE connection	To verify whether iOS clients access to network remains same or not when AP's PoE connection is removed	Passed	
MEJ87PhIIS_Eth_06	Configuring the fall-back details in read only mode from ME CLI	To verify whether Ethernet fall-back details are possible to configure or not from ME CLI by read-only user	Passed	

MEJ87PhIIS_Eth_07	Checking the disabled Radios 'a' & 'b' details after PoE disconnect	To verify whether the 802.11 radios comes Up/Down as configured or not once PoE is disconnected to AP	Passed	
-------------------	---	---	--------	--

OUI File Upload

Logical ID	Title	Description	Status	Defect Id
MEJ87IIS_Reg_190	OUI file uploading through TFTP server	To check whether OUI file is uploading or not through TFTP server	Passed	
MEJ87IIS_Reg_191	Uploading the invalid OUI file through TFTP server	Verify Invalid OUI file is uploading or not through TFTP sever	Passed	
MEJ87IIS_Reg_192	OUI file uploading through HTTP server	To check whether OUI file is uploading through HTTP server or not in ME UI	Passed	
MEJ87IIS_Reg_193	Invalid OUI File uploading through HTTP sever	Validate Invalid OUI file is uploading or not through HTTP server	Passed	
MEJ87IIS_Reg_194	uploading the OUI file through FTP server	To check whether OUI file is uploading or not	Passed	
MEJ87IIS_Reg_195	Invalid OUI File uploading through FTP sever	To check whether Invalid OUI file is uploading or not through FTP sever	Passed	

Software update using SFTP

Logical ID	Title	Description	Status	Defect ID
MEJ87IIS_SUSFTP_01	ME AP1830 Software updating via SFTP server	Verifying AP 1830 ME software updating or not via SFTP server	Passed	

MEJ87IIS_SUSFTP_02	Invalid software updating via SFTP server for ME AP 1830	To check whether Invalid software updating or not via SFTP server	Passed	
MEJ87IIS_SUSFTP_03	Software Schedule Update on ME AP 1830 via SFTP server	Validate the software Schedule Update on ME AP1830 via SFTP server	Passed	
MEJ87IIS_SUSFTP_04	Software Update on ME AP 1850 via SFTP server	Verifying AP 1850 ME software updating or not via SFTP server	Passed	
MEJ87IIS_SUSFTP_05	Invalid software updating via SFTP server on ME AP 1850	Verifying whether Invalid software updating or not on ME AP 1850	Passed	
MEJ87IIS_SUSFTP_06	Schedule the Software update on 1850 ME AP	Verifying on schedule time ME software is updating or not	Passed	
MEJ87IIS_SUSFTP_07	Software updating via SFTP server on ME 2800AP	To check whether software is updating or not via SFTP server on 2800AP	Passed	
MEJ87IIS_SUSFTP_08	Invalid software updating on ME 2800AP via SFTP software	Verifying whether Invalid software updating or not on ME AP2800	Passed	
MEJ87IIS_SUSFTP_09	Software Update Schedule on ME AP2800 via SFTP server	Validate the software Schedule Update on ME AP2800 via SFTP server	Passed	
MEJ87IIS_SUSFTP_10	Software updating via SFTP server on ME 3800AP	To check whether software is updating or not via SFTP server on 3800AP	Passed	
MEJ87IIS_SUSFTP_11	Invalid software updating on ME 3800AP via SFTP software	Verifying whether Invalid software updating or not on ME AP3800	Passed	

Import EAP certificate

MEJ87IIS_SUSFTP_12	Software Update Schedule on ME AP3800 via SFTP server	Validate the software Schedule Update on ME AP3800 via SFTP server	Passed	
			Passed	

Import EAP certificate

Logical ID	Title	Description	Status	Defect ID
MEJ87IIS_EAP_01	Downloading the EAP device certificate through HTTP	To verify whether EAP device certificate is downloading or not through HTTP mode	Passed	
MEJ87IIS_EAP_02	Downloading the EAP device certificate through FTP	To verify whether EAP device certificate is downloading or not through FTP mode	Passed	
MEJ87IIS_EAP_03	Downloading the EAP device certificate through TFTP	To verify whether EAP device certificate is downloading or not through TFTP mode	Passed	
MEJ87IIS_EAP_04	Downloading the EAP CA certificate through HTTP	To verify whether EAP CA certificate is downloading or not through HTTP mode	Passed	
MEJ87IIS_EAP_05	Downloading the EAP CA certificate through FTP	To verify whether EAP CA certificate is downloading or not through FTP mode	Passed	
MEJ87IIS_EAP_06	Downloading the EAP CA certificate through TFTP	To verify whether EAP CA certificate is downloading or not through TFTP mode	Passed	
MEJ87IIS_EAP_07	Downloading the NA SERV CA Certificate through HTTP	To verify whether NA SERV CA Certificate is downloading or not through HTTP mode	Passed	
MEJ87IIS_EAP_08	Downloading the NA SERV CA Certificate through FTP	To verify whether NA SERV CA Certificate is downloading or not through FTP mode	Passed	

MEJ87IIS_EAP_09	Downloading the NAsERV CA Certificate through TFTP	To verify whether NAsERV CA Certificate is downloading or not through TFTP mode	Passed	
MEJ87IIS_EAP_10	Changing the OUI String values	To verify whether OUI string values are changing or not	Passed	
MEJ87IIS_EAP_11	Initiating the download with invalid file name	To verify whether Invalid file name is accepting or not	Passed	
MEJ87IIS_EAP_12	Initiate the download with read-only mode	To verify whether image download initiating or not for read-only user or not	Passed	
MEJ87IIS_EAP_13	Trying to reset the system at the time of certificate download	To verify whether system resetting or not at the time of downloading the certificate	Passed	
MEJ87IIS_EAP_14	Initiating the certificates(EAP,EAP CA,NA SEV) download through HTTP from CLI	To verify whether image is downloading or not from HTTP mode through CLI	Passed	
MEJ87IIS_EAP_15	Initiating the certificates(EAP,EAP CA,NA SEV) download through FTP from CLI	To verify whether image is downloading or not from FTP mode through CLI	Passed	
MEJ87IIS_EAP_16	Initiating the certificates(EAP,EAP CA,NA SEV) download through TFTP from CLI	To verify whether image is downloading or not from TFTP mode through CLI	Passed	
MEJ87IIS_EAP_17	Checking the certification details through CII for read-only users	To verify whether certificate details are showing properly or not for read-only users	Passed	
MEJ87IIS_EAP_18	Initiating the download through read-only mode	To verify whether certificate are downloading or not read-only user	Passed	
MEJ87IIS_EAP_19	Clearing the details after download	To verify whether details are clearing or not	Passed	

Import EAP certificate

MEJ87S_IEC_01	Downloading the EAP device certificate through HTTP	To verify whether EAP device certificate is downloading or not through HTTP mode	Passed	
MEJ87S_IEC_02	Downloading the EAP device certificate through FTP	To verify whether EAP device certificate is downloading or not through FTP mode	Passed	
MEJ87S_IEC_03	Downloading the EAP device certificate through TFTP	To verify whether EAP device certificate is downloading or not through TFTP mode	Passed	
MEJ87S_IEC_04	Downloading the EAP CA certificate through HTTP	To verify whether EAP CA certificate is downloading or not through HTTP mode	Passed	
MEJ87S_IEC_05	Downloading the EAP CA certificate through FTP	To verify whether EAP CA certificate is downloading or not through FTP mode	Passed	
MEJ87S_IEC_06	Downloading the EAP CA certificate through TFTP	To verify whether EAP CA certificate is downloading or not through TFTP mode	Passed	
MEJ87S_IEC_07	Downloading the NA SERV CA Certificate through HTTP	To verify whether NA SERV CA Certificate is downloading or not through HTTP mode	Passed	
MEJ87S_IEC_08	Downloading the NA SERV CA Certificate through FTP	To verify whether NA SERV CA Certificate is downloading or not through FTP mode	Passed	
MEJ87S_IEC_09	Downloading the NA SERV CA Certificate through TFTP	To verify whether NA SERV CA Certificate is downloading or not through TFTP mode	Passed	
MEJ87S_IEC_10	Changing the OUI String values	To verify whether OUI sting values are changing or not	Passed	
MEJ87S_IEC_11	Initiating the download with invalid file name	To verify whether Invalid file name is accepting or not	Passed	

MEJ87S_IEC_12	Initiate the download with read-only mode	To verify whether image download initiating or not for read-only user or not	Passed	
MEJ87S_IEC_13	Trying to reset the system at the time of certificate download	To verify whether system resetting or not at the time of downloading the certificate	Passed	
MEJ87S_IEC_14	Initiating the certificates(EAP,EAP CA,NA SEV) download through HTTP from CLI	To verify whether image is downloading or not from HTTP mode through CLI	Passed	
MEJ87S_IEC_15	Initiating the certificates(EAP,EAP CA,NA SEV) download through FTP from CLI	To verify whether image is downloading or not from FTP mode through CLI	Passed	
MEJ87S_IEC_16	Initiating the certificates(EAP,EAP CA,NA SEV) download through TFTP from CLI	To verify whether image is downloading or not from TFTP mode through CLI	Passed	
MEJ87S_IEC_17	Checking the certification details through CII for read-only users	To verify whether certificate details are showing properly or not for read-only users	Passed	
MEJ87S_IEC_18	Initiating the download through read-only mode	To verify whether certificate are downloading or not read-only user	Passed	
MEJ87S_IEC_19	Clearing the details after download	To verify whether details are clearing or not	Passed	

PnP for Software Download in Day0

Logical ID	Title	Description	Status	Defect ID
MEJ87IIS_PnP_01	Provisioning the 1852/1832 ME in day0 via PnP profile	Verify that user is able to Provisioned the 1852/1832 ME in day0 via PnP profile or not	Passed	

MEJ87IIS_PnP_02	Provisioning the 1815 ME in day0 via PnP profile	Verify that user is able to Provisioned the 1815ME in day0 via PnP profile or not	Passed	
MEJ87IIS_PnP_03	Provisioning the 1852/1832 ME in day0 via claiming the device	Verify that user is able to Provisioned the 1852/1832 ME in day0 via claming the device in day2	Passed	
MEJ87IIS_PnP_04	Provisioning the 1815 ME in day0 via claiming the device	Verify that user is able to Provisioned the 1815 ME in day0 via claming the device in day3	Passed	
MEJ87IIS_PnP_05	Downloading the image in day0 of 1852/1832 ME	Verify that user is able to download the ME image on ap 1852/1832 via PnP or not	Passed	
MEJ87IIS_PnP_06	Downloading the image in day0 of 1815 ME	Verify that user is able to download the ME image on ap 1815 via PnP or not	Passed	
MEJ87IIS_PnP_07	Checking that 1852/1832 ME is rebooting after downloading the image	Verify that ME 1852/1832 is rebooting and coming up with new image or not	Passed	
MEJ87IIS_PnP_08	Checking that 1815 ME is rebooting after downloading the image	Verify that ME 1815 is rebooting and coming up with new image or not	Passed	
MEJ87IIS_PnP_09	Try to download the ME image with invalid CCO credentials	Checking that user is able to download the image with invalid CCO credentials or not	Passed	
MEJ87IIS_PnP_10	Applying the config after image download	Verify that user can apply the config file on provisioned device image download or not	Passed	
MEJ87IIS_PnP_11	Downloading the image via SFTP in day0	Verify that user is able to download the image via SFTP in day0 or not	Passed	

MEJ87S_PnP_01	Provisioning the 3800/2800 ME in day0 via PnP profile	Verify that user is able to Provisioned the 3800/2800 ME in day0 via PnP profile or not	Passed	
MEJ87S_PnP_02	Provisioning the 1852/1832 ME in day0 via PnP profile	Verify that user is able to Provisioned the 1852/1832 ME in day0 via PnP profile or not	Passed	
MEJ87S_PnP_03	Provisioning the 1815 ME in day0 via PnP profile	Verify that user is able to Provisioned the 1815ME in day0 via PnP profile or not	Passed	
MEJ87S_PnP_04	Provisioning the 3800/2800 ME in day0 via claiming the device	Verify that user is able to Provisioned the 3800/2800 ME in day0 via claiming the device in day0	Passed	
MEJ87S_PnP_05	Provisioning the 1852/1832 ME in day0 via claiming the device	Verify that user is able to Provisioned the 1852/1832 ME in day0 via claiming the device in day2	Passed	
MEJ87S_PnP_06	Provisioning the 1815 ME in day0 via claiming the device	Verify that user is able to Provisioned the 1815 ME in day0 via claiming the device in day3	Passed	
MEJ87S_PnP_07	Downloading the image in day0 of 3800/2800 ME	Verify that user is able to download the ME image on ap 3800/2800 via PnP or not	Passed	
MEJ87S_PnP_08	Downloading the image in day0 of 1852/1832 ME	Verify that user is able to download the ME image on ap 1852/1832 via PnP or not	Passed	
MEJ87S_PnP_09	Downloading the image in day0 of 1815 ME	Verify that user is able to download the ME image on ap 1815 via PnP or not	Passed	
MEJ87S_PnP_10	Checking that 3800/2800 ME is rebooting after downloading the image	Verify that ME 3800/2800 is rebooting and coming up with new image or not	Passed	

Central web authentication (CWA) with change of authorization (CoA)

MEJ87S_PnP_11	Checking that 1852/1832 ME is rebooting after downloading the image	Verify that ME 1852/1832 is rebooting and coming up with new image or not	Passed	
MEJ87S_PnP_12	Checking that 1815 ME is rebooting after downloading the image	Verify that ME 1815 is rebooting and coming up with new image or not	Passed	
MEJ87S_PnP_13	Try to download the ME image with invalid CCO credentials	Checking that user is able to download the image with invalid CCO credentials or not	Passed	
MEJ87S_PnP_14	Applying the config after image download	Verify that user can apply the config file on provisioned device image download or not	Passed	
MEJ87S_PnP_15	Downloading the image via SFTP in day0	Verify that user is able to download the image via SFTP in day0 or not	Passed	

Central web authentication (CWA) with change of authorization (CoA)

Logical ID	Title	Description	Status	Defect ID
MEJ87S_CWA_01	Creating a CWA along with ACL Configuration in CME UI	To check Whether CWA along with ACL Configuration in CME UI created or not	Passed	
MEJ87S_CWA_02	Associating a Japanese Windows Client to a SSID which is mapped with ISE	To verify whether Japanese Windows Client which is mapped to ISE is redirected successfully or not	Passed	
MEJ87S_CWA_03	Associating a iOS Client to a SSID which is mapped with ISE	To verify whether iOS Client which is mapped to ISE is redirected successfully or not	Passed	
MEJ87S_CWA_04	Associating a Android Client to a SSID which is mapped with ISE	To verify whether Android Client which is mapped to ISE is redirected successfully or not	Passed	
MEJ87S_CWA_05	Associating a MAC OS Client to a SSID which is mapped with ISE	To verify whether MAC Client which is mapped to ISE is redirected successfully or not	Passed	

MEJ87S_CWA_06	Associating a different Clients to SSID which is mapped with ISE and redirecting to Guest portal page with invalid credentials	To verify whether client connected to SSID redirecting to Guest portal page with invalid credentials	Passed	
MEJ87S_CWA_07	Associating a different Clients to a SSID which is mapped with ISE by creating AVC profile	To verify whether different Clients is redirected successfully and checking that particular application is dropped or not	Passed	
MEJ87S_CWA_08	Associating a different Clients to a SSID which is mapped with ISE by denying the action in ACL	To verify whether Clients gets denied when it is connected to SSID which is mapped with ISE	Passed	
MEJ87S_CWA_09	Associating a different Clients to a SSID which is mapped with ISE by permitting the action in ACL using TCP protocol	To verify whether Clients gets connected to SSID which is mapped with ISE by permitting the action in ACL using TCP protocol	Passed	
MEJ87S_CWA_10	Associating a different Clients to a SSID which is mapped with ISE by permitting the action in ACL using UDP protocol	To verify whether Clients gets connected to SSID which is mapped with ISE by permitting the action in ACL using UDP protocol	Passed	
MEJ87S_CWA_11	Associating a different Clients to a SSID which is mapped with ISE by permitting the action in ACL using ICMP protocol	To verify whether Clients gets connected to SSID which is mapped with ISE by permitting the action in ACL using ICMP protocol	Passed	
MEJ87S_CWA_12	Checking the expired Radius Guest User for proper error message	To verify whether the expired Guest user gets proper Error messages when he logging in	Passed	
MEJ87S_CWA_13	Validate whether CME is switch between configured Radius servers	To verify whether AAA authentication is occurring when one radius server goes down	Passed	
MEJ87S_CWA_14	Reboot the Controller after CWA enabling	To verify whether Configurations are showing same or different after controller reboot	Passed	

MEJ87S_CWA_15	Creating a CWA along with ACL Configuration through CLI	To verify whether ACL rule is created or not through CLI	Passed	
MEJ87S_CWA_16	Checking the configuration of CWA when the user is in Read-only	To verify whether configuration display error message or not when the user is in Read-only	Passed	

Dynamic OID update

Logical ID	Title	Description	Status	Defect Id
MEJ87IIS_OUI_01	OUI file uploading via TFTP server In ME UI	To check whether OUI file is uploading or not via TFTP server	Passed	
MEJ87IIS_OUI_02	OUI file uploading via TFTP server In ME CLI	Validate the OUI file is uploading or not in ME CLI	Passed	
MEJ87IIS_OUI_03	Uploading the invalid OUI file through via TFTP server	Verify Invalid OUI file is uploading or not via TFTP sever	Passed	
MEJ87IIS_OUI_04	OUI file uploading via HTTP server in ME UI	To check whether OUI file is uploading via HTTP server or not in ME UI	Passed	
MEJ87IIS_OUI_05	OUI file uploading via HTTP server in ME CLI	validate via http server OUI file is uploading or not in ME CLI	Passed	
MEJ87IIS_OUI_06	Invalid OUI File uploading via HTTP sever	Validate Invalid OUI file is uploading or not via HTTP server	Passed	
MEJ87IIS_OUI_07	Uploading the OUI file via FTP server in ME UI	To check whether OUI file is uploading or not	Passed	
MEJ87IIS_OUI_08	Uploading the OUI file via FTP server in ME CLI	Validate the OUI file is uploading via ftp server in ME CLI	Passed	
MEJ87IIS_OUI_09	Invalid OUI File uploading via FTP sever	To check whether Invalid OUI file is uploading or not via FTP server	Passed	

Bidirectional rate limit per client

Logical ID	Title	Description	Status	Defect ID
MEJ87S_BRL_01	Configuring rate limit for per client for JOS client with WPA 2 Personal security with QOS as Silver	To configure rate limit for JOS client with open security and QOS as silver and check if the client gets the rate that is been configured or not.	Failed	CSCvh48115

MEJ87S_BRL_02	Configuring rate limit for per client for Android client with WPA 2 Personal security with QOS as Silver	To configure rate limit for Android client with open security and QOS as silver and check if the client gets the rate that is been configured or not.	Passed	
MEJ87S_BRL_03	Configuring rate limit for per client for Mac OS client with WPA 2 Personal security with QOS as Silver	To configure rate limit for Mac OS client with open security and QOS as silver and check if the client gets the rate that is been configured or not.	Passed	
MEJ87S_BRL_04	Configuring rate limit for per client for IOS client with WPA 2 Personal security with QOS as Silver	To configure rate limit for IOS client with open security and QOS as silver and check if the client gets the rate that is been configured or not.	Passed	
MEJ87S_BRL_05	Configuring rate limit for per client with QOS as Gold for JOS client with WPA 2 Enterprise security	To configure rate limit per client with QOS as Gold and connecting a JOS client with WPA 2 Enterprise security and check if the rate limit is applied or not.	Failed	CSCvh48115
MEJ87S_BRL_06	Configuring rate limit for per client with QOS as Gold for Android client with WPA 2 Enterprise security	To configure rate limit per client with QOS as Gold and connecting a Android client with WPA 2 Enterprise security and check if the rate limit is applied or not.	Passed	
MEJ87S_BRL_07	Configuring rate limit for per client with QOS as Gold for IOS client with WPA 2 Enterprise security	To configure rate limit per client with QOS as Gold and connecting a IOS client with WPA 2 Enterprise security and check if the rate limit is applied or not.	Passed	
MEJ87S_BRL_08	Configuring rate limit for per client with QOS as Gold for Mac OS client with WPA 2 Enterprise security	To configure rate limit per client with QOS as Gold and connecting a Mac OS client with WPA 2 Enterprise security and check if the rate limit is applied or not.	Passed	

MEJ87S_BRL_09	Connecting a client to a WLAN configured with rate limit using two different AP	To configure rate limit for client and connecting a client to one AP and check the rate limit and making that AP down and connecting the client to other AP and check if the behavior of the client is same or not	Passed	
MEJ87S_BRL_10	Connecting a client to a WLAN configured with rate limit using one ME capable AP and Non Me capable AP in AP group	To Connecting a client to a WLAN configured with rate limit using one ME capable AP and Non Me capable AP in AP group	Passed	
MEJ87S_BRL_11	Creating a AVC rule for the WLAN for which rate limit is configured .	To configure lesser rate limit in WLAN and configuring higher rate limit in AVC and check if the rate limit for the client	Passed	

RLAN support for APs with multiple Ethernet ports

Logical ID	Title	Description	Status	Defect ID
MEJ87S_RLAN_01	Creating a RLAN with Open security and connecting JOS windows 7 client to the RLAN .	To create a RLAN with Open security and connecting a JOS window 7 client to the RLAN and check if the client gets connected to the RLAN port in th AP and there is flow in traffic	Passed	
MEJ87S_RLAN_02	Creating a RLAN with Open security and connecting windows 10 client to the RLAN .	To create a RLAN with Open security and connecting a window 10 client to the RLAN and check if the client gets connected to the RLAN port in th AP and there is flow in traffic.	Passed	
MEJ87S_RLAN_03	Creating a RLAN with Open security and connecting Mac OS client to the RLAN .	To create a RLAN with Open security and connecting a Mac OS client to the RLAN and check if the client gets connected to the RLAN port in th AP and there is flow in traffic.	Passed	

MEJ87S_RLAN_04	Configuring a RLAN with Open security and Mac filtering with whitelist enabled and connecting JOS windows 7 client to the RLAN .	To configure a RLAN with Open security enabling MAC filtering with whitelist and connecting a JOS window 7 client to the RLAN and check if the client gets connected to the RLAN port in th AP and there is flow in traffic.	Passed	
MEJ87S_RLAN_05	Configuring a RLAN with Open security and Mac filtering with Blacklist enabled and connecting JOS windows 7 client to the RLAN .	To configure a RLAN with Open security enabling MAC filtering with whitelist and connecting a JOS window 7 client to the RLAN and check if the client gets connected to the RLAN port in th AP and there is flow in traffic.	Passed	
MEJ87S_RLAN_06	Creating a RLAN with Type 802.1X security and connecting JOS windows 7 client to the RLAN .	To create a RLAN with 802.1X security and connecting a JOS window 7 client to the RLAN and check if the client gets connected to the RLAN port in th AP and there is flow in traffic.	Failed	CSCvh65773
MEJ87S_RLAN_07	Creating a RLAN with 802.1X security and connecting windows 10 client to the RLAN .	To create a RLAN with 802.1X security and connecting a window 10 client to the RLAN and check if the client gets connected to the RLAN port in th AP and there is flow in traffic.	Failed	CSCvh65773
MEJ87S_RLAN_08	Creating a RLAN with Type 802.1X security and connecting Mac OS client to the RLAN .	To create a RLAN with 802.1X security and connecting a Mac OS client to the RLAN and check if the client gets connected to the RLAN port in th AP and there is flow in traffic.	Failed	CSCvh65773

MEJ87S_RLAN_09	Creating a RLAN with Type 802.1X security with host mode as single and connecting client to the RLAN .	To Create a RLAN with Type 802.1X security with host mode as single and authenticating server as External radius connecting client to the RLAN .	Failed	CSCvh65773
MEJ87S_RLAN_10	Creating a RLAN with Type 802.1X security with host mode as Multi keeping authentication server as External Radius and connecting client to the RLAN .	To Create a RLAN with Type 802.1X security with host mode as Multi keeping authentication server as External Radius and connecting client to the RLAN .	Failed	CSCvh65773
MEJ87S_RLAN_11	Configuring a RLAN with 802.1x security and Mac filtering with whitelist enabled and connecting JOS windows 7 client to the RLAN .	To configure a RLAN with 802.1x security enabling MAC filtering with whitelist and connecting a JOS window 7 client to the RLAN and check if the client gets connected to the RLAN port in th AP and there is flow in traffic.	Failed	CSCvh65773
MEJ87S_RLAN_12	Configuring a RLAN with 802.1x security and Mac filtering with Blacklist enabled and connecting JOS windows 7 client to the RLAN .	To configure a RLAN with 802.1x security enabling MAC filtering with whitelist and connecting a JOS window 7 client to the RLAN and check if the client gets connected to the RLAN port in th AP and there is flow in traffic.	Failed	CSCvh65773
MEJ87S_RLAN_13	Creating a RLAN with Guest network with different access type enabling MAB mode .	To create a RLAN with Guest network using different access type and enabling MAB mode and connecting a client to it.	Passed	
MEJ87S_RLAN_14	Configuring AVC profile for RLAN with 802.1x security and check if AVC profile is applied	To configure AVC profile for RLAN with 802.1x security and check fi the AVC profile gets applied to the client connecting to it or not.	Passed	

MEJ87S_RLAN_15	Enable AAA override and connecting a client to the AAA override enabled RLAN with 802.1x security .	To enable AAA override and connecting a IOS client to the AAA override enabled with 802.1x security RLAN and check if the VLAN from AAA server is overridden to the client	Passed	
----------------	---	--	--------	--

Limit clients per radio

Logical ID	Title	Description	Status	Defect ID
MEJ87S_CPR_01	Configuring maximum Allowed Clients Per AP Radio as 4 and connecting client with WPA 2 Personal security.	To configure maximum allowed client Per AP radio as 4 and connecting 5 different client with radio policy as ALL and check if the number of client that is configured alone gets connected to the WLAN	Passed	
MEJ87S_CPR_02	Configuring maximum Allowed Clients Per AP Radio as 3 and connecting client with WPA 2 Enterprise security .	To configure maximum allowed client Per AP radio as 3 and connecting 4 different client with radio policy as ALL and now after 3 client disconnect one client and check if other client get authenticated to the WLAN	Passed	
MEJ87S_CPR_03	Configuring maximum allowed client per AP radio as 6 setting radio policy as 5 GHz and trying to connect 3 5GHZ client and 3 2.4GHz	To set radio policy as 5 GHz and trying to connect 3 5GHZ client and 3 2.4GHz while applying maximum allowed client per AP radio as 6 and check if only the 3 5 GHZ client get connected to it	Passed	
MEJ87S_CPR_04	Configuring maximum Allowed Clients Per AP Radio in RF profile as 4 and in WLAN as 3 and connecting the client	To configure maximum allowed client Per AP radio in RF profile and also setting the same in WLAN and check which of the configured number of clients gets connected .	Passed	

Limit clients per radio

MEJ87S_CPR_05	Creating open security WLAN with radio policy as 5 GHz and configuring Maximum Allowed Clients Per AP Radio	To configure maximum allowed client per AP radio setting the WLAN security with Open and radio policy as 5 GHz and check if only the defined number of client alone connect to the WLAN.	Passed	
MEJ87S_CPR_06	Creating WPA 2 Personal security WLAN with radio policy as 5 GHz and configuring Maximum Allowed Clients Per AP Radio	To configure maximum allowed client per AP radio setting the WLAN security with WPA 2 Personal and radio policy as 5 GHz and check if only the defined number of client alone connect to the WLAN.	Passed	
MEJ87S_CPR_07	Creating WPA 2 Enterprise security WLAN with radio policy as 5 GHz and configuring Maximum Allowed Clients Per AP Radio	To configure maximum allowed client per AP radio setting the WLAN security with WPA 2 Enterprise and radio policy as 5 GHz and check if only the defined number of client alone connect to the WLAN.	Passed	
MEJ87S_CPR_08	Creating open security WLAN with radio policy as 2.4 GHz and configuring Maximum Allowed Clients Per AP Radio	To create open security WLAN configuring Maximum allowed client per AP radio with radio policy as 2.4 GHz and check if only the defined number of client alone connect to the WLAN.	Passed	
MEJ87S_CPR_09	Creating WPA 2 Personal security WLAN with radio policy as 2.4 GHz and configuring Maximum Allowed Clients Per AP Radio	To create WPA 2 Personal security WLAN configuring Maximum allowed client per AP radio with radio policy as 2.4 GHz and check if only the defined number of client alone connect to the WLAN.	Passed	

MEJ87S_CPR_10	Creating WPA 2 Enterprise security WLAN with radio policy as 2.4 GHz and configuring Maximum Allowed Clients Per AP Radio	To create WPA 2 Enterprise security WLAN configuring Maximum allowed client per AP radio with radio policy as 2.4 GHz and check if only the defined number of client alone connect to the WLAN.	Passed	
---------------	---	---	--------	--

AAA Override of VLAN Name and VLAN Name-id template

Logical ID	Title	Description	Status	Defect ID
ME87S_AAA_VLAN_01	Enable AAA override and connecting a JOS window 7 client to the AAA override enabled WLAN with WPA 2 Personal security .	To enable AAA override and connecting a JOS window 7 client to the AAA override enabled with WPA 2 Personal security WLAN and check if the VLAN from AAA server is overridden to the client	Passed	
ME87S_AAA_VLAN_02	Enable AAA override and connecting a Android client to the AAA override enabled WLAN with WPA 2 Personal security .	To enable AAA override and connecting a Android client to the AAA override enabled with WPA 2 Personal security WLAN and check if the VLAN from AAA server is overridden to the client	Passed	
ME87S_AAA_VLAN_03	Enable AAA override and connecting a IOS client to the AAA override enabled WLAN with WPA 2 Personal security .	To enable AAA override and connecting a IOS client to the AAA override enabled with WPA 2 Personal security WLAN and check if the VLAN from AAA server is overridden to the client	Passed	
ME87S_AAA_VLAN_04	Enable AAA override and connecting a Mac OS client to the AAA override enabled WLAN with WPA 2 Personal security .	To enable AAA override and connecting a Mac OS client to the AAA override enabled with WPA 2 Personal security WLAN and check if the VLAN from AAA server is overridden to the client	Passed	

ME87S_AAA_VLAN_05	Connecting a JOS window 7 client to the AAA override enabled WLAN with WPA 2 Enterprise security enabled with AAA override .	To connect a JOS Window 7 client to AAA override enabled WLAN with WPA 2 Enterprise security and check if the Native VLAN is overridden or not.	Passed	
ME87S_AAA_VLAN_06	Connecting a Android client to the AAA override enabled WLAN with WPA 2 Enterprise security enabled with AAA override .	To connect a Android client to AAA override enabled WLAN with WPA 2 Enterprise security and check if the Native VLAN is overridden or not.	Passed	
ME87S_AAA_VLAN_07	Connecting a Android client to the AAA override enabled WLAN with WPA 2 Enterprise security enabled with AAA override .	To connect a IOS client to AAA override enabled WLAN with WPA 2 Enterprise security and check if the Native VLAN is overridden or not.	Passed	
ME87S_AAA_VLAN_08	Connecting a Android client to the AAA override enabled WLAN with WPA 2 Enterprise security enabled with AAA override .	To connect a Mac OS client to AAA override enabled WLAN with WPA 2 Enterprise security and check if the Native VLAN is overridden or not.	Passed	
ME87S_AAA_VLAN_09	Connecting a client to the WLAN enabled with AAA override but the configuration of VLAN on AAA is not done.	To connect a client to the WLAN enabled with AAA override and the configuration of VLAN is not done in the AAA server.	Passed	

Passive client support

Logical ID	Title	Description	Status	Defect ID
MEJ87S_PC_01	Configuring static IP for a wireless printer and enabling passive clients with security as Open	To configure static IP for Wireless printer and enabling passive client option in the controller with Open security and check if the clients details are shown in the client detail page or not.	Passed	

MEJ87S_PC_02	Configuring static IP for JOS Windows 7 client and enabling passive clients with security as Open	To configure static IP for JOS client and enabling passive client option in the controller with Open security and check if the clients details are shown in the client detail page or not.	Passed	
MEJ87S_PC_03	Configuring static IP for Windows 10 client and enabling passive clients with security as Open	To configure static IP for Windows client and enabling passive client option in the controller with Open security and check if the clients details are shown in the client detail page or not.	Passed	
MEJ87S_PC_04	Configuring static IP for Android client and enabling passive clients with security as Open	To configure static IP for Android client and enabling passive client option in the controller with Open security and check if the clients details are shown in the client detail page or not.	Passed	
MEJ87S_PC_05	Configuring static IP for IOS client and enabling passive clients with security as Open	To configure static IP for IOS client and enabling passive client option in the controller with Open security and check if the clients details are shown in the client detail page or not.	Passed	
MEJ87S_PC_06	Configuring static IP for Mac OS client and enabling passive clients with security as Open	To configure static IP for Mac OS client and enabling passive client option in the controller with Open security and check if the clients details are shown in the client detail page or not.	Passed	
MEJ87S_PC_07	Enabling passive clients with security as WPA 2 personal and configuring Static IP for JOS Windows 7 client	To enabling passive client option in the CME with WPA 2 personal while Configuring static IP for JOS client and check if the clients details are shown in the client detail page or not.	Passed	

MEJ87S_PC_08	Enabling passive clients with security as WPA 2 personal and configuring Static IP for Windows 10 client	To enabling passive client option in the CME with WPA 2 personal while Configuring static IP for Windows client and check if the clients details are shown in the client detail page or not.	Passed	
MEJ87S_PC_09	Enabling passive clients with security as WPA 2 personal and configuring Static IP for Android client	To enabling passive client option in the CME with WPA 2 personal while Configuring static IP for Android client and check if the clients details are shown in the client detail page or not.	Passed	
MEJ87S_PC_10	Enabling passive clients with security as WPA 2 personal and configuring Static IP for IOS client	To enabling passive client option in the CME with WPA 2 personal while Configuring static IP for IOS client and check if the clients details are shown in the client detail page or not.	Passed	
MEJ87S_PC_11	Enabling passive clients with security as WPA 2 personal and configuring Static IP for Mac OS client	To enabling passive client option in the CME with WPA 2 personal while Configuring static IP for Mac OS client and check if the clients details are shown in the client detail page or not.	Passed	
MEJ87S_PC_12	Connecting a JOS Windows 7 client to a WLAN configured with WPA 2 Enterprise security enabled with Passive client .	To connect a JOS client to a WPA 2 Enterprise security WLAN with Passive client option enabled by configuring the client with a static IP.	Passed	
MEJ87S_PC_13	Connecting a Windows 10 client to a WLAN configured with WPA 2 Enterprise security enabled with Passive client .	To connect a Windows client to a WPA 2 Enterprise security WLAN with Passive client option enabled by configuring the client with a static IP.	Passed	
MEJ87S_PC_14	Connecting a Android client to a WLAN configured with WPA 2 Enterprise security enabled with Passive client .	To connect a Android client to a WPA 2 Enterprise security WLAN with Passive client option enabled by configuring the client with a static IP.	Passed	

MEJ87S_PC_15	Connecting a IOS client to a WLAN configured with WPA 2 Enterprise security enabled with Passive client .	To connect a IOS client to a WPA 2 Enterprise security WLAN with Passive client option enabled by configuring the client with a static IP.	Passed	
MEJ87S_PC_16	Connecting a Mac OS client to a WLAN configured with WPA 2 Enterprise security enabled with Passive client .	To connect a Mac OS client to a WPA 2 Enterprise security WLAN with Passive client option enabled by configuring the client with a static IP.	Passed	
MEJ87S_PC_17	Configuring JOS client to Guest network with Internal splash page and access type as Local user account by enabling passive client .	To configuring JOS client to Guest network with Internal splash page and access type as Local user account by enabling passive client .	Passed	
MEJ87S_PC_18	Configuring a AVC rule to a passive client	To configure a AVC rule to a passive client and check if the AVC rule gets applied to the client successfully or not	Passed	
MEJ87S_PC_19	Connecting two passive client and enabling Peer to peer block.	To connect two passive client and enabling Peer to peer blocking for a wlan and check if both there is no traffic flow between the two connected passive clients.	Passed	
MEJ87S_PC_20	Configuring DHCP pool for the client by enabling passive client option.	To configure DHCP pool for the client and enabling passive client option for the WLAN.	Passed	

ME GUI for P2P Blocking

Logical ID	Title	Description	Status	Defect ID
MEJ87S_P2P_01	Connecting two JOS client to a open security WLAN enabling Peer to Peer Block	To connect two JOS client to a open security WLAN enabling Peer to Peer Block and check if there is a traffic flow between two clients or not	Passed	

MEJ87S_P2P_02	Connecting two Windows client to a open security WLAN enabling Peer to Peer Block	To connect two Windows client to a open security WLAN enabling Peer to Peer Block and check if there is a traffic flow between two clients or not	Passed	
MEJ87S_P2P_03	Connecting two Android client to a open security WLAN enabling Peer to Peer Block	To connect two Android client to a open security WLAN enabling Peer to Peer Block and check if there is a traffic flow between two clients or not	Passed	
MEJ87S_P2P_04	Connecting two IOS client to a open security WLAN enabling Peer to Peer Block	To connect two IOS client to a open security WLAN enabling Peer to Peer Block and check if there is a traffic flow between two clients or not	Passed	
MEJ87S_P2P_05	Connecting two Mac OS client to a open security WLAN enabling Peer to Peer Block	To connect two Mac OS client to a open security WLAN enabling Peer to Peer Block and check if there is a traffic flow between two clients or not	Passed	
MEJ87S_P2P_06	Connecting two JOS client to a WPA 2 Personal security WLAN enabling Peer to Peer Block	To connect two JOS client to a WPA 2 Personal security WLAN enabling Peer to Peer Block and check if there is a traffic flow between two clients or not	Passed	
MEJ87S_P2P_07	Connecting two Windows client to a WPA 2 Personal security WLAN enabling Peer to Peer Block	To connect two Windows client to a WPA 2 Personal security WLAN enabling Peer to Peer Block and check if there is a traffic flow between two clients or not	Passed	
MEJ87S_P2P_08	Connecting two Android client to a WPA 2 Personal security WLAN enabling Peer to Peer Block	To connect two Android client to a WPA 2 Personal security WLAN enabling Peer to Peer Block and check if there is a traffic flow between two clients or not	Passed	

MEJ87S_P2P_09	Connecting two IOS client to a WPA 2 Personal security WLAN enabling Peer to Peer Block	To connect two IOS client to a WPA 2 Personal security WLAN enabling Peer to Peer Block and check if there is a traffic flow between two clients or not	Passed	
MEJ87S_P2P_10	Connecting two Mac OS client to a WPA 2 Personal security WLAN enabling Peer to Peer Block	To connect two Mac OS client to a WPA 2 Personal security WLAN enabling Peer to Peer Block and check if there is a traffic flow between two clients or not	Passed	
MEJ87S_P2P_11	Connecting two JOS client to a WPA 2 Enterprise security WLAN enabling Peer to Peer Block	To connect two JOS client to a WPA 2 Enterprise security WLAN enabling Peer to Peer Block and check if there is a traffic flow between two clients or not	Passed	
MEJ87S_P2P_12	Connecting two Windows client to a WPA 2 Enterprise security WLAN enabling Peer to Peer Block	To connect two Windows client to a WPA 2 Enterprise security WLAN enabling Peer to Peer Block and check if there is a traffic flow between two clients or not	Passed	
MEJ87S_P2P_13	Connecting two Android client to a WPA 2 Enterprise security WLAN enabling Peer to Peer Block	To connect two Android client to a WPA 2 Enterprise security WLAN enabling Peer to Peer Block and check if there is a traffic flow between two clients or not	Passed	
MEJ87S_P2P_14	Connecting two IOS client to a WPA 2 Enterprise security WLAN enabling Peer to Peer Block	To connect two IOS client to a WPA 2 Enterprise security WLAN enabling Peer to Peer Block and check if there is a traffic flow between two clients or not	Passed	
MEJ87S_P2P_15	Connecting two Mac OS client to a WPA 2 Enterprise security WLAN enabling Peer to Peer Block	To connect two Mac OS client to a WPA 2 Personal Enterprise WLAN enabling Peer to Peer Block and check if there is a traffic flow between two clients or not	Passed	

Flexconnect IOS Parity: Passive Client / Wireless Proxy ARP

MEJ87S_P2P_16	Connecting four different client to a open security WLAN enabling Peer to Peer Block	To connect four different client to a open security WLAN enabling Peer to Peer Block and check if there is a traffic flow between two clients or not	Passed	
MEJ87S_P2P_17	Connecting four different client to a WPA 2 Personal security WLAN enabling Peer to Peer Block	To connect four different client to a WPA 2 Personal security WLAN enabling Peer to Peer Block and check if there is a traffic flow between two clients or not	Passed	
MEJ87S_P2P_18	Connecting four different client to a WPA 2 Enterprise security WLAN enabling Peer to Peer Block	To connect four different client to a WPA 2 Enterprise security WLAN enabling Peer to Peer Block and check if there is a traffic flow between two clients or not	Passed	
MEJ87S_P2P_19	Connecting two Windows client to WLAN enabling Peer to Peer Block and trying Webex meeting between client	To connect two Windows client to WLAN enabling Peer to Peer Block and trying Webex meeting between client	Passed	

Flexconnect IOS Parity: Passive Client / Wireless Proxy ARP

Logical ID	Title	Description	Status	Defect ID
MEJ87S_ARP_01	Enable/Disable Passive client with multicast IP address	To verify whether Passive client with multicast enable/disable or not	Passed	
MEJ87S_ARP_02	Rebooting Ap after Passive client with multicast IP address	To verify whether Passive client with multicast details are showing properly or not after reboot	Passed	
MEJ87S_ARP_03	Enable/disable the Proxy ARP cache	To verify whether Proxy ARP cache details are enabling or not	Passed	
MEJ87S_ARP_04	Rebooting AP after Proxy ARP cache enable	To verify whether Proxy ARP details are showing properly or not after reboot th AP	Passed	

MEJ87S_ARP_05	Checking ARP with passive client details in standalone mode	To verify whether ARP with passive client details are showing properly or not in standalone	Passed	
MEJ87S_ARP_06	Roaming clients between AP with ARP and passive clients	To verify whether clients are roaming or not with ARP and passive client	Passed	
MEJ87S_ARP_07	Enable proxy and disable the passive client	To verify whether ARP details are transferring to the router or not when proxy is in enable and passive client disable state	Passed	
MEJ87S_ARP_08	Disable proxy and enable passive client	To verify whether ARP details are transferring to the router or not when proxy is in disable and passive client enable state	Passed	
MEJ87S_ARP_09	Enable proxy and enable the passive client	To verify whether ARP details are transferring to the router or not when proxy is in enable and passive client enable state	Passed	
MEJ87S_ARP_10	Disable proxy and disable passive client	To verify whether ARP details are transferring to the router or not when proxy is in disable and passive client disable state	Passed	
MEJ87S_ARP_11	Verifying the debug logs	To verify whether debug logs are showing properly or not	Passed	

DNS Based ACL Rules

Logical ID	Title	Description	Status	Defect ID
MEJ87S_DNSACL_01	Create URL ACL rule with guest network WLAN	To verify that URL ACL created with guest network	Passed	
MEJ87S_DNSACL_02	Configure guest network with captive portal Internal Splash Page - local user account and checking URL ACL rule by connecting Window JOS client	To verify that Window client connect successfully with guest network with captive portal Internal Splash Page , Access type local user account and URL ACL rule deny	Passed	

MEJ87S_DNSACL_03	Configure guest network with captive portal Internal Splash Page-Radius server and checking URL ACL rule by connecting Window JOS client	To verify that Window client connect successfully with guest network with captive portal Internal Splash Page , Access type radius server and URL ACL rule Permit	Passed	
MEJ87S_DNSACL_04	Configure guest network with captive portal Internal Splash Page-Radius server and checking URL ACL rule by connecting iOS client	To verify that iOS client connect successfully with guest network with captive portal Internal Splash Page , Access type radius server and URL ACL rule deny	Passed	
MEJ87S_DNSACL_05	Configure guest network with captive portal Internal Splash Page-local user account and checking URL ACL rule by connecting iOS client	To verify that iOS client connect successfully with guest network with captive portal Internal Splash Page , Access type local user account and URL ACL rule deny	Passed	
MEJ87S_DNSACL_06	Configure guest network with captive portal Internal Splash Page-WPA2 personal and checking URL ACL rule with permit by connecting Android client	To verify that Android client connect successfully with guest network with captive portal Internal Splash Page , Access type WPA2 Per and URL ACL rule deny	Passed	
MEJ87S_DNSACL_07	Configure guest network with captive portal External Splash page-local user account and checking URL ACL rule by connecting Window client	To verify that Window client connect successfully with guest network with captive portal External Splash Page , Access type local user account and URL ACL rule deny	Passed	
MEJ87S_DNSACL_08	Configure guest network with captive portal External Splash page-local user account and checking permit URL ACL rule by connecting Android client	To verify that Android client connect successfully with guest network with captive portal External Splash Page , Access type local user account and URL ACL rule Permit	Passed	
MEJ87S_DNSACL_09	Configure guest network with captive portal External Splash page-Radius sever and checking deny URL ACL rule by connecting iOS client	To verify that iOS client connect successfully with guest network with captive portal External Splash Page , Access type radius Server and URL ACL rule deny	Passed	

MEJ87S_DNSACL_10	Configure guest network with captive portal CMX Connect and checking deny URL ACL rule by connecting Android client	To verify that Android client connect successfully with guest network with captive portal CMX Connect and URL ACL rule deny	Passed	
MEJ87S_DNSACL_11	Configure guest network with captive portal CMX Connect and checking Permit URL ACL rule by connecting iOS client	To verify that iOS client connect successfully with guest network with captive portal CMX Connect and URL ACL rule Permit	Passed	
MEJ87S_DNSACL_12	Configure guest network with captive portal Internal Splash Page-WPA Personal Mac Filtering enabled and checking URL ACL rule by connecting Window JOS client	To verify that Window JOS client connect successfully with guest network with captive portal Internal Splash Page-WPA Personal Mac Filtering enabled and URL ACL rule Permit	Passed	

WSA Agent for Mobility Express

Logical ID	Title	Description	Status	Defect ID
MEJ87S_WSA_01	Setting UP the Network Assurance Server in CME	To check whether Network Assurance server status gets UP or not while adding NA server in CME	Passed	
MEJ87S_WSA_02	Creating the SSID in Sensor tab and connecting the sensor mode AP in CME	To check whether the user is able to connect the sensor mode ap as a client or nor in CME after configuring the SSID under sensor page	Passed	
MEJ87S_WSA_03	Adding 3 to 4 AP's in CME and checking the AP events in NA server	To check whether AP events showing properly or not in NA server when more AP's gets associated to CME	Passed	
MEJ87S_WSA_04	Adding different OS clients to AP in CME and checking the client events in NA server	To check whether clients events showing properly or not in NA server when different OS clients gets associated to AP in CME	Passed	
MEJ87S_WSA_05	Adding Radius servers in CME and checking the Radius events in NA server	To check whether Radius events showing properly or not in NA server when Radius servers added in CME	Passed	
MEJ87S_WSA_06	Rebooting the CME and checking the system events in NA server	To check whether system events showing properly or not in NA server when CME is reloaded	Passed	

MEJ87S_WSA_07	Attempting to associate blacklist client to AP in CME and checking the error events in NA server	To check whether error events showing properly or not in NA server when blacklisted client tries to associate to AP in CME	Passed	
MEJ87S_WSA_08	Checking the configurations of NA server after export/import the config file	To check whether NA server configuration parameters gets retained or not after export/import the config file	Passed	
MEJ87S_WSA_09	Checking the rogue/interferer events in NA server	To check whether rogue/interferer events shown properly or not in NA server when CME detects rogue/interferers in the network	Passed	
MEJ87S_WSA_10	Creating the SSID in Sensor tab and connecting the sensor mode AP via Dot1x in CME	To check whether the user is able to connect the sensor mode ap as a client or nor in CME after configuring the SSID with dot1x security under sensor page	Passed	



CHAPTER 4

Regression Features - Test Summary

- [WLC AireOS, on page 61](#)
- [CME, on page 170](#)

WLC AireOS

Support vWLC on Amazon Web Services (AWS) (SP WiFi)

Logical ID	Title	Description	Status	Defect ID
WLJ87IIS_REG_01	Creating WLANs with different L2 security types and associating Android clients in vWLC	To check whether Android clients associated successfully or not with all different security types in vWLC	Passed	
WLJ87IIS_REG_02	Creating WLANs with different L2 security types and associating JOS clients in vWLC	To check whether Windows JOS clients associated successfully or not with all different security types in vWLC	Passed	
WLJ87IIS_REG_03	Creating WLANs with different L2 security types and associating Apple MacBook clients in vWLC	To check whether Apple MacBook clients associated successfully or not with all different security types in vWLC	Passed	
WLJ87IIS_REG_04	Checking the AP Fallback/failover functionalities between vWLC and 5508 WLC	To check whether AP failover/fallback functionalities works properly or not between vWLC and 5508 WLC	Passed	

WLJ87IIS_REG_05	Checking the SSID broadcast by local mode AP in vWLC	To check whether local mode AP can able to broadcast the SSID or not in vWLC which is installed on AWS	Passed	
WLJ87IIS_REG_06	Creating WLANs with different L3 security types and associating Android clients in vWLC	To check whether Android clients associated successfully or not with all different L3 security types in vWLC	Passed	
WLJ87IIS_REG_07	Creating WLANs with different L3 security types and associating IOS clients in vWLC	To check whether Windows IOS clients associated successfully or not with all different L3 security types in vWLC	Passed	
WLJ87IIS_REG_08	Creating WLANs with different L3 security types and associating Apple MacBook clients in vWLC	To check whether Apple MacBook clients associated successfully or not with all different L3 security types in vWLC	Passed	
WLJ87IIS_REG_09	Checking the management login using TACACS server	To check whether management login gets successful or not via TACACS server	Passed	
WLJ87IIS_REG_10	Verifying the SXP config between vWLC and ISE	To check whether SXP config gets UP or not between vWLC and ISE	Passed	
WLJ87IIS_REG_11	Creating Local policies for different OS and checking the same for diff OS clients by mapping in different WLANs in vWLC	To check whether local policies parameters works properly or not for mapped OS clients in each WLANs	Passed	
WLJ87IIS_REG_12	Verifying the Out-Of-Box functionality in RF-profile	To check whether Out-of-box in RF-profile gets enabled or not with default profiles in AP-group & RF-profile	Passed	
WLJ87IIS_REG_13	Checking the IPv4 EoGRE tunneling configurations in vWLC	To check whether IPv4 EoGRE tunneling works properly or not for all clients in vWLC	Passed	

WLJ87IIS_REG_14	Performing Intra-controller roaming for Android clients in vWLC	To check whether intra-controller roaming is successful or not for Android clients in vWLC	Passed	
WLJ87IIS_REG_15	Performing Intra-controller roaming for IOS clients in vWLC	To check whether intra-controller roaming is successful or not for IOS clients in vWLC	Passed	
WLJ87IIS_REG_16	Performing Intra-controller roaming for MAC OS clients in vWLC	To check whether intra-controller roaming is successful or not for MAC OS clients in vWLC	Passed	
WLJ87IIS_REG_17	Performing Intra-controller roaming for Windows JOS clients in vWLC	To check whether intra-controller roaming is successful or not for Windows JOS clients in vWLC	Passed	
WLJ87IIS_REG_18	Checking the local authentication of clients	To check whether local authentication works properly or not for clients in vWLC	Passed	
WLJ87IIS_REG_19	Checking the AVC functionalities in vWLC	To check whether AVC applications can be dropped or not as configuration in AVC profiles for all OS clients	Passed	
WLJ87IIS_REG_20	Connecting the Clients with different Radio details	To verify whether Clients are getting connecting or not with differenet Radio details	Passed	
WLJ87IIS_REG_21	Adding the vWLC to PI	To verify whether vWLC is adding successfully or not in PI	Passed	
WLJ87S_Reg_01	Creating WLANs with different L2 security types and associating Android clients in vWLC	To check whether Andriod clients associated successfully or not with all different security types in vWLC	Passed	
WLJ87S_Reg_02	Creating WLANs with different L2 security types and associating IOS clients in vWLC	To check whether IOS clients associated successfully or not with all different security types in vWLC	Passed	

WLJ87S_Reg_03	Creating WLANs with different L2 security types and associating JOS clients in vWLC	To check whether Windows JOS clients associated successfully or not with all different security types in vWLC	Passed	
WLJ87S_Reg_04	Creating WLANs with different L2 security types and associating Apple MacBook clients in vWLC	To check whether Apple MacBook clients associated successfully or not with all different security types in vWLC	Passed	
WLJ87S_Reg_05	Installing vWLC on Amazon Web Service	To check whether vWLC can be installed successfully or not on Amazon Web Service cloud using AMI image of WLC	Passed	
WLJ87S_Reg_06	Associating AP's to vWLC which is installed on AWS	To check whether AP's joining successfully or not to vWLC which is installed on AWS	Passed	
WLJ87S_Reg_07	Checking the AP Fallback/failover functionalities between vWLC and 5508 WLC	To check whether AP failover/fallback functionalities works properly or not between vWLC and 5508 WLC	Passed	
WLJ87S_Reg_08	Checking the SSID broadcast by local mode AP in vWLC	To check whether local mode AP can able to broadcast the SSID or not in vWLC which is installed on AWS	Passed	
WLJ87S_Reg_09	Upload/download config file from WLC.	To verify the config retain on upload/download the config file.	Passed	
WLJ87S_Reg_10	Creating WLANs with different L3 security types and associating Android clients in vWLC	To check whether Android clients associated successfully or not with all different L3 security types in vWLC	Passed	
WLJ87S_Reg_11	Creating WLANs with different L3 security types and associating IOS clients in vWLC	To check whether IOS clients associated successfully or not with all different L3 security types in vWLC	Passed	

WLJ87S_Reg_12	Creating WLANs with different L3 security types and associating IOS clients in vWLC	To check whether Windows IOS clients associated successfully or not with all different L3 security types in vWLC	Passed	
WLJ87S_Reg_13	Creating WLANs with different L3 security types and associating Apple MacBook clients in vWLC	To check whether Apple MacBook clients associated successfully or not with all different L3 security types in vWLC	Passed	
WLJ87S_Reg_14	Checking the management login using TACACS server	To check whether management login gets successful or not via TACACS server	Passed	
WLJ87S_Reg_15	Checking the cleanair functionalities in vWLC	To check whether cleanair detection works fine or not for AP's in vWLC	Passed	
WLJ87S_Reg_16	Verifying the SXP config between vWLC and ISE	To check whether SXP config gets UP or not between vWLC and ISE	Passed	
WLJ87S_Reg_17	Creating Local policies for different OS and checking the same for diff OS clients by mapping in different WLANs in vWLC	To check whether local policies parameters works properly or not for mapped OS clients in each WLANs	Passed	
WLJ87S_Reg_18	Verifying the Out-Of-Box functionality in RF-profile	To check whether Out-of-box in RF-profile gets enabled or not with default profiles in AP-group & RF-profile	Passed	
WLJ87S_Reg_19	Checking the IPv4 EoGRE tunneling configurations in vWLC	To check whether IPv4 EoGRE tunneling works properly or not for all clients in vWLC	Passed	
WLJ87S_Reg_20	Performing Intra-controller roaming for Android clients in vWLC	To check whether intra-controller roaming is successful or not for Android clients in vWLC	Passed	
WLJ87S_Reg_21	Performing Intra-controller roaming for IOS clients in vWLC	To check whether intra-controller roaming is successful or not for IOS clients in vWLC	Passed	

WLJ87S_Reg_22	Performing Intra-controller roaming for MAC OS clients in vWLC	To check whether intra-controller roaming is successful or not for MAC OS clients in vWLC	Passed	
WLJ87S_Reg_23	Performing Intra-controller roaming for Windows JOS clients in vWLC	To check whether intra-controller roaming is successful or not for Windows JOS clients in vWLC	Passed	
WLJ87S_Reg_24	Checking the local authentication of clients	To check whether local authentication works properly or not for clients in vWLC	Passed	
WLJ87S_Reg_25	Checking the AVC functionalities in vWLC	To check whether AVC applications can be dropped or not as configuration in AVC profiles for all OS clients	Passed	
WLJ87S_Reg_26	Checking the sleeping clients functionalites in vWLC	To check whether clients moving to sleep mode or not as per configured in vWLC	Passed	
WLJ87S_Reg_27	Checking the ACL fuctionalities after clients connected in vWLC	To verify whether ACL rules are applying to the WLAN or not after client connected	Passed	
WLJ87S_Reg_28	Connecting the Clients with different Radio details	To verify whether Clients are getting connecting or not with differenet Radio details	Passed	
WLJ87S_Reg_29	Adding the vWLC to PI	To verify whether vWLC is adding successfully or not in PI	Passed	
WLJ87S_Reg_30	Chaging the AP from one to other in vWLC after AP joined	To verify whether AP modes are changing successfully or not without any issues	Passed	

Private PSK

Logical ID	Title	Description	Status	Defect ID
WLJ87IIS_REG_22	Connecting different OS client via ascii private psk key	Verify that different OS client is able to connect with ascii private psk key or not	Passed	

WLJ87IIS_REG_23	Connecting different OS client with hex private psk key	Verify that different OS client is able to connect with hex private psk key or not	Passed	
WLJ87IIS_REG_24	Trying to connect client that identity created in radius server,with wlan psk key	Verify that client which is mapped with radius server, is able to connect with wlan psk key or not	Passed	
WLJ87IIS_REG_25	Connecting different OS client that identity not created in radius server	Verify that different OS client that identity not created in radius server,is able to connect via wlan psk or not	Passed	
WLJ87IIS_REG_26	Checking that clients able to reauthenticate with private psk key after session time out	Verify that client is able to reauthenticate with private psk key after session time out or not	Passed	
WLJ87IIS_REG_27	Checking that clients able to reauthenticate with WLAN psk key after session time out	Verify that client is able to reauthenticate with WLAN psk key after session time out or not	Passed	
WLJ87IIS_REG_28	Verify that client is able to connect via private psk after forgetting the network once and try again	Checking that client is able to connect via private psk after forgetting the network once and try again	Passed	
WLJ87IIS_REG_29	Verify that radius fallback working with private psk or not	Checking that radius fallback is working with private psk or not	Passed	
WLJ87IIS_REG_30	On client monitor page verifying that key management is showing "private psk"or not, while connected with private psk	Checking that key management is showing private psk or not	Passed	

WLJ87S_Reg_31	Connecting different OS client via ascii private psk key	Verify that different OS client is able to connect with ascii private psk key or not	Passed	
WLJ87S_Reg_32	Connecting different OS client with hex private psk key	Verify that different OS client is able to connect with hex private psk key or not	Passed	
WLJ87S_Reg_33	Trying to connect client that identity created in radius server,with wlan psk key	Verify that client which is mapped with radius server, is able to connect with wlan psk key or not	Passed	
WLJ87S_Reg_34	Connecting different OS client that identity not created in radius server	Verify that different OS client that identity not created in radius server,is able to connect via wlan psk or not	Passed	
WLJ87S_Reg_35	Checking that clients able to reauthenticate with private psk key after session time out	Verify that client is able to reauthenticate with private psk key after session time out or not	Passed	
WLJ87S_Reg_36	Checking that clients able to reauthenticate with WLAN psk key after session time out	Verify that client is able to reauthenticate with WLAN psk key after session time out or not	Passed	
WLJ87S_Reg_37	Verify that client is able to connect via private psk after forgetting the network once and try again	Checking that client is able to connect via private psk after forgetting the network once and try again	Passed	
WLJ87S_Reg_38	Verify that radius fallback working with private psk or not	Checking that radius fallback is working with private psk or not	Passed	
WLJ87S_Reg_39	Debugging the client connection while connecting with private psk	To debug the client connection and verify the debug log while connecting with private psk	Passed	

WLJ87S_Reg_40	On client monitor page verifying that key management is showing "private psk" or not, while connected with private psk	Checking that key management is showing private psk or not	Passed	
---------------	--	--	--------	--

Fabric Enable Wireless

Logical ID	Title	Description	Status	Defect ID
WLJ87IIS_REG_31	Associating Windows clients to a fabric enabled WLAN and checking the association of the clients	To check whether windows JOS clients gets associated or not to a fabric enabled WLAN in 5520 WLC	Passed	
WLJ87IIS_REG_32	Associating Android clients to a fabric enabled WLAN and checking the association of the clients	To check whether Android clients gets associated or not to a fabric enabled WLAN in 5520 WLC	Passed	
WLJ87IIS_REG_33	Associating IOS clients to a fabric enabled WLAN and checking the association of the clients	To check whether IOS clients gets associated or not to a fabric enabled WLAN in 5520 WLC	Passed	
WLJ87IIS_REG_34	Associating MAC OS clients to a fabric enabled WLAN and checking the association of the clients	To check whether MAC OS clients gets associated or not to a fabric enabled WLAN in 5520 WLC	Passed	
WLJ87IIS_REG_35	Checking the fabric configuration after upload/download the config file in 5520 WLC	To check whether fabric configurations gets retained or not after upload/download the config file in 5520 WLC	Passed	
WLJ87IIS_REG_36	Enabling/Disabling the fabric configuration in 5520 WLC from apic em server	To check whether fabric configuration can be enabled/disabled or not for WLC from apic em server via PNP (plug and play)	Passed	
WLJ87IIS_REG_37	Pushing the configuration template of fabric from apic em server to WLC	To check whether fabric parameters like template, fabric acl, fabric avc can be pushed or not to 5520 WLC from apic em server	Passed	
WLJ87IIS_REG_38	Monitoring the clients connected to a fabric WLAN in PI	To check whether PI can able to monitor or not the clients connected to a fabric WLAN	Passed	

WLJ87S_Reg_41	Associating Windows clients to a fabric enabled WLAN and checking the association of the clients	To check whether windows JOS clients gets associated or not to a fabric enabled WLAN in 5520 WLC	Passed	
WLJ87S_Reg_42	Associating Android clients to a fabric enabled WLAN and checking the association of the clients	To check whether Android clients gets associated or not to a fabric enabled WLAN in 5520 WLC	Passed	
WLJ87S_Reg_43	Associating IOS clients to a fabric enabled WLAN and checking the association of the clients	To check whether IOS clients gets associated or not to a fabric enabled WLAN in 5520 WLC	Passed	
WLJ87S_Reg_44	Associating MAC OS clients to a fabric enabled WLAN and checking the association of the clients	To check whether MAC OS clients gets associated or not to a fabric enabled WLAN in 5520 WLC	Passed	
WLJ87S_Reg_45	Checking the fabric configuration after upload/download the config file in 5520 WLC	To check whether fabric configurations gets retained or not after upload/download the config file in 5520 WLC	Passed	
WLJ87S_Reg_46	Enabling/Disabling the fabric configuration in 5520 WLC from apic em server	To check whether fabric configuration can be enabled/disabled or not for WLC from apic em server via PNP (plug and play)	Passed	
WLJ87S_Reg_47	Pushing the configuration template of fabric from apic em server to WLC	To check whether fabric parameters like template, fabric acl, fabric avc can be pushed or not to 5520 WLC from apic em server	Passed	
WLJ87S_Reg_48	Monitoring the clients connected to a fabric WLAN in PI	To check whether PI can able to monitor or not the clients connected to a fabric WLAN	Passed	

MAB Bypass Support

Logical ID	Title	Description	Status	Defect ID
WLJ87IIS_REG_39	JSSID client with valid MAC address	check whether japanese client connecting or not with MAB	Passed	
WLJ87IIS_REG_40	Invalid MAC address with Japanese client	verify the Japanese client is able connect or not with invalid MAB	Passed	
WLJ87IIS_REG_41	Connecting different OS japanese client with MAB	Check whether japanese client is able connect different OS or not with MAB	Passed	

WLJ87IIS_REG_42	Verifying if the CLI shows the MAC filtering enabled and it shows the status of the mac filtering	To Validate if the CLI show the mac filtering enabled and check if the details of the mac filtering are shown properly or not	Passed	
WLJ87IIS_REG_43	Client Reassociate with mac filtering enabled on wlan with external radius server.	To check if the Client with mac filtering is reassociated with the WLAN and client is able to pass the traffic or not	Passed	
WLJ87IIS_REG_44	Verifying japanese client reassociation with MAC filtering enabled on WLAN with external radius server.	To check if japanese client with MAC filtering is reassociated with the WLAN and client is able to pass the traffic or not	Passed	
WLJ87IIS_REG_45	Configuring specific mac address allowed on wlan by using AAA-attribute list.	To configure specific mac address allowed on wlan by using AAA-attribute list Verify that other mac address are not allowed.	Passed	
WLJ87IIS_REG_46	configure a named authorization list as part of aaa config. Configure this list on wlan.	To check if the named authorization list is configured and the authorization list is mapped on wlan and Verify if client join/disconnect/rejoin.	Passed	
WLJ87IIS_REG_47	verifying japanese client maximum retries failed.	To check whether japanese client after maximum retries failed moved or not in excluded list	Passed	
WLJ87IIS_REG_48	Verifying that client reauthenticated after session timeout or not	Checking that after session timeout client is reauthenticated or not	Passed	
WLJ87IIS_REG_49	Japanese client reauthenticated after session expired	To check whether Japanese client reauthenticated or not after client session expired	Passed	
WLJ87IIS_REG_50	Japanese client status on monitor page	validate the japanese client details on monitor page	Passed	

WLJ87S_Reg_49	Connecting the client with valid MAC address	Verify that client is able to connect with MAB or not	Passed	
WLJ87S_Reg_50	JSSID client with valid MAC address	check whether japanese client connecting or not with MAB	Passed	
WLJ87S_Reg_51	Connecting the client with invalid MAC address	Verify that client is able to connect with invalid MAB or not	Passed	
WLJ87S_Reg_52	Invalid MAC address with Japanese client	verify the Japanese client is able connect or not with invalid MAB	Passed	
WLJ87S_Reg_53	Connecting the different OS client with MAB	Verify that different OS client is able to connect with MAB or not	Passed	
WLJ87S_Reg_54	different OS japanese client with MAB	Check whether japanese client is able connect different OS or not with MAB	Passed	
WLJ87S_Reg_55	Verifying if the CLI shows the MAC filtering enabled and it shows the status of the mac filtering	To Validate if the CLI show the mac filtering enabled and check if the details of the mac filtering are shown properly or not	Passed	
WLJ87S_Reg_56	Client Reassociate with mac filtering enabled on wlan with external radius server.	To check if the Client with mac filtering is reassociated with the WLAN and client is able to pass the traffic or not	Passed	
WLJ87S_Reg_57	Verifying japanese client reassociation with MAC filtering enabled on WLAN with external radius server.	To check if japanese client with MAC filtering is reassociated with the WLAN and client is able to pass the traffic or not	Passed	
WLJ87S_Reg_58	Configuring specific mac address allowed on wlan by using AAA-attribute list.	To configure specific mac address allowed on wlan by using AAA-attribute list Verify that other mac address are not allowed.	Passed	

WLJ87S_Reg_59	configure a named authorization list as part of aaa config. Configure this list on wlan.	To check if the named authorization list is configured and the authorization list is mapped on wlan and Verifyif client join/disconnect/rejoin.	Passed	
WLJ87S_Reg_60	Verifying that client excluded after maximum retries failed.	Checking that after maximum retries failed authentication,client moved to excluded list or not	Passed	
WLJ87S_Reg_61	verifying japanese client maximum retries failed.	To check whether japanese client after maximum retries failed moved or not in excluded list	Passed	
WLJ87S_Reg_62	Verifying that client reauthenticated after session timeout or not	Checking that after session timeout client is reauthenticated or not	Passed	
WLJ87S_Reg_63	Japanese client reauthenticated after session expired	To check whether Japanese client reauthenticated or not after client session expired	Passed	
WLJ87S_Reg_64	Verifying client status on monitor page	Verifying client details on monitor page	Passed	
WLJ87S_Reg_65	Japanese client status on monitor page	validate the japanese client details on monitor page	Passed	

Passpoint R2 Flex Mode

Logical ID	Title	Description	Status	Defect ID
WLJ87IIS_REG_51	Enabling the 802.11u mode on WLAN with WPA	To verify whether 802.11u mode enabled or not on WLAN	Passed	
WLJ87IIS_REG_52	Configuring the Network type	To verify whether client connecting or not with network type changes from one to other	Passed	

WLJ87IIS_REG_53	Configuring the Network Authentication	To verify whether Client is connecting after Network Authentication or not	Passed	
WLJ87IIS_REG_54	Checking with IPv4 type details	To verify whether Client connecting or not after IPv4 type changes from one to another	Passed	
WLJ87IIS_REG_55	Creating OUI with Duplicate name	To verify whether OUI is creating with duplicate name or not	Passed	
WLJ87IIS_REG_56	Checking the Roaming after Relam configurations	To verify whether client will roam between hotspots or not	Passed	
WLJ87IIS_REG_57	Adding cellular network information with duplicate name	To verify whether Cellular network information added successfully	Passed	
WLJ87IIS_REG_58	Configuring domain and OSU ID	To verify whether domain and OSU id are applying or not	Passed	
WLJ87IIS_REG_59	WAN link selection after client connection	To verify whether WAN status is varying or not	Passed	
WLJ87IIS_REG_60	Configure the OSU and Operator name	To verify whether OSU and Operator selection applied successfully or not	Passed	
WLJ87IIS_REG_61	Varying Port configurations	To verify whether Port configurations can vary after client connect	Passed	
WLJ87IIS_REG_62	Downgrading the AP after Hotspot configurations	To verify whether Client connected or not after downgrade with Hotspot	Passed	
WLJ87IIS_REG_63	Checking the Hotspot details through CLI	To verify whether Hotspot details showing properly or not	Passed	
WLJ87IIS_REG_64	Debugging the Hotspot details	To verify the Hotspot details with debug command	Passed	

WLJ87IIS_REG_65	Installing cred.conf file in CLient devices for EAP-SIM method	Verifying that user is able to Install cred.conf file in CLient devices for EAP-SIM or not	Passed	
WLJ87IIS_REG_66	Installing CA certificate on CLient device for EAP-TLS/TTLS	Verifying that user is able to Install CA certificate on CLient device for EAP-TLS/TTLS or not	Passed	
WLJ87IIS_REG_67	Assigning the Venue Group to access points	To verify whether Hotspot enabled access point will comes under venue group or not	Passed	
WLJ87S_Reg_81	Enabling the 802.11u mode on WLAN with WPA	To verify whether 802.11u mode enabled or not on WLAN	Passed	
WLJ87S_Reg_82	Enabling the Internet Access WLAN	To verify whether Internet Access mode is enabled or not	Passed	
WLJ87S_Reg_83	Configuring the Network type	To verify whether client connecting or not with network type changes from one to other	Passed	
WLJ87S_Reg_84	Configuring the Network Authentication	To verify whether Client is connecting after Network Authentication or not	Passed	
WLJ87S_Reg_85	Checking with IPv4 type details	To verify whether Client connecting or not after IPv4 type changes from one to another	Passed	
WLJ87S_Reg_86	Creating OUI with Duplicatate name	To verify whether OUI is creating with duplicate name or not	Passed	
WLJ87S_Reg_87	Checking the Roaming after Relam configurations	To verify whether client will roam between hotspots or not	Passed	
WLJ87S_Reg_88	Adding cellular network information with duplicate name	To verify whether Cellular network information added successfully	Passed	

WLJ87S_Reg_89	Configuring domain and OSU ID	To verify whether domain and OSU id are applying or not	Passed	
WLJ87S_Reg_90	WAN link selection after client connection	To verify whether WAN status is varying or not	Passed	
WLJ87S_Reg_91	Configure the OSU and Operator name	To verify whether OSU and Operator selection applied successfully or not	Passed	
WLJ87S_Reg_92	Varying Port configurations	To verify whether Port configurations can vary after client connect	Passed	
WLJ87S_Reg_93	Downgrading the AP after Hotspot configurations	To verify whether Client connected or not after downgrade with Hotspot	Passed	
WLJ87S_Reg_94	Upgrading the AP after Hotspot configurations	To verify whether all hotspot details are showing properly or not	Passed	
WLJ87S_Reg_95	Changing the AP modes after Client connect to Hotspot	To verify whether client will connect or not after modes changes in AP	Passed	
WLJ87S_Reg_96	Disable the Internet access check the connectivity	To verify whether Internet is accessing the client or not at the time of internet access disable	Passed	
WLJ87S_Reg_97	Checking the Hotspot details through CLI	To verify whether Hotspot details showing properly or not	Passed	
WLJ87S_Reg_98	Debugging the Hotspot details	To verify the Hotspot details with debug command	Passed	
WLJ87S_Reg_99	Installing cred.conf file in Client devices for EAP-SIM method	Verifying that user is able to Install cred.conf file in Client devices for EAP-SIM or not	Passed	

WLJ87S_Reg_100	Installing CA certificate on Client device for EAP-TLS/TTLS	Verifying that user is able to Install CA certificate on Client device for EAP-TLS/TTLS or not	Passed	
WLJ87S_Reg_101	Checking the different client access	To verify whether android, mac and windows will connect properly or not	Passed	
WLJ87S_Reg_102	Assigning the Venue Group to access points	To verify whether Hotspot enabled access point will come under venue group or not	Passed	

Passive Client ARP Unicast

Logical ID	Title	Description	Status	Defect ID
WLJ87IIS_REG_68	Passive Clients is sent to all AP's as unicast packet	To verify whether ARP Unicast packets send to all AP's or not	Passed	
WLJ87IIS_REG_69	Enabling the Passive client data in 2500/5520/8510/8540 controllers	To verify whether Passive client or sending the Unicast data from AP to client or not	Passed	
WLJ87IIS_REG_70	Checking the ARP Packet with Multicast-multicast enable	To verify whether ARP packet is sending or not whether Multicast mode enabled	Passed	
WLJ87IIS_REG_71	Checking the ARP packet when Multicast-unicast enable	To verify whether Packed is sending or not whether Multicast-unicast enable	Passed	
WLJ87IIS_REG_72	Connecting with two WLAN with different client ARP	To verify whether WLAN will support with two different ARP methods in same Interface	Passed	
WLJ87IIS_REG_73	ARP unicast verification when AP's are in AP group	To verify whether ARP unicast enabling and accessing fine or not at the time of AP's are in same AP group	Passed	

WLJ87IIS_REG_74	Checking with ARP unicast behavior when feature is disabled and passive client is enabled	To verify whether Client accessing or not whenever we have disable the feature	Passed	
WLJ87IIS_REG_75	Testing with non-Cisco WGB with wired clients	To verify whether non-cisco WGB with wired clients will connect or not	Passed	
WLJ87IIS_REG_76	Rebootinthe AP after Client ARP unicast enable	To verify whether WLAN showing the information correctly after reboot also	Passed	
WLJ87IIS_REG_77	Checking after Upgrade/Downgrade	To verify whether Client is connecting or not after Upgrade/Downgrade	Passed	
WLJ87IIS_REG_78	Debuging the ARPclient data	To verify whether ARP details are showing properly or not	Passed	
WLJ87IIS_REG_79	Veryfyng Maximum packets per second	To verify whether the Maximum packets per second the AP will send	Passed	
WLJ87S_Reg_103	Passive Clients is sent to all AP's as unicast packet	To verify whether ARP Unicast packets send to all AP's or not	Passed	
WLJ87S_Reg_104	Enabling the Passive client data in 2500/5520/8510/8540 controllers	To verify whether Passive client or sending the Unicast data from AP to client or not	Passed	
WLJ87S_Reg_105	Cheking the ARP Packet with Multicast-multicast enable	To verify whether ARP packet is sending or not whether Multicast mode enabled	Passed	
WLJ87S_Reg_106	Cheking the ARP packet when Multicast-unicast enable	To verify whether Packed is sending or not whether Multicast-unicast enable	Passed	
WLJ87S_Reg_107	Connecting with two WLAN with different client ARP	To verify whether WLAN will support with two different ARP methods in same Interface	Passed	

WLJ87S_Reg_108	ARP unicast verification when AP's are in AP group	To verify whether ARP unicast enabling and accessing fine or not at the time of AP's are in same AP group	Passed	
WLJ87S_Reg_109	Checking with ARP unicast behavior when feature is disabled and passive client is enabled	To verify whether Client accessing or not whenever we have disable the feature	Passed	
WLJ87S_Reg_110	Testing with non-Cisco WGB with wired clients	To verify whether non-cisco WGB with wired clients will connect or not	Passed	
WLJ87S_Reg_111	Rebootinthe AP after Client ARP unicast enable	To verify whether WLAN showing the information correctly after reboot also	Passed	
WLJ87S_Reg_112	Checking after Upgrade/Downgrade	To verify whether Client is connecting or not after Upgrade/Downgrade	Passed	
WLJ87S_Reg_113	Debugging the ARPclient data	To verify whether ARP details are showing properly or not	Passed	
WLJ87S_Reg_114	Veryfying Maximum packets per second	To verify whether the Maximum packets per second the AP will send	Passed	

Selective Re-anchor

Logical ID	Title	Description	Status	Defect ID
WLJ87IIS_REG_80	Roaming the client between 2 controllers	To verify whether client roaming successfully between two controllers	Passed	
WLJ87IIS_REG_81	Checking FT roaming for the client within controller	To verify FT roaming for the client using FT protocols	Passed	
WLJ87IIS_REG_82	Checking the Windows/MAC JOS Client connectivity after enabling Selective reanchor in WLAN	To verify whether windows jos client is connecting properly or not	Passed	

WLJ87IIS_REG_83	Checking the android/iOS Client connectivity after enabling Selective reanchor in WLAN	To verify whether android/iOS client is connecting properly or not	Passed	
WLJ87S_Reg_115	Reboot the Controller after Re-anchor enabling	To verify whether Configurations are showing same or different after controller reboot	Passed	
WLJ87S_Reg_116	Downgrade/upgrade the controller with Re-anchor enable	To verify whether Downgrade/upgrade the controller with Re-anchor enable	Passed	
WLJ87S_Reg_117	Checking the Windows JOS Client connectivity after enabling Selective reanchor in WLAN	To verify whether windows jos client is connecting properly or not	Passed	
WLJ87S_Reg_118	Checking the android Client connectivity after enabling Selective reanchor in WLAN	To verify whether android client is connecting properly or not	Passed	
WLJ87S_Reg_119	Checking the IOS Client connectivity after enabling Selective reanchor in WLAN	To verify whether IOS client is connecting properly or not	Passed	
WLJ87S_Reg_120	Roaming the client between 2 controllers	To verify whether client roaming successfully between two controllers	Passed	
WLJ87S_Reg_121	Checking FT roaming for the client	To verify FT roaming for the client using FT protocols	Passed	

Network Assurance

Logical ID	Title	Description	Status	Defect ID
WLJ87IIS_REG_84	Adding the NA server	Verify that user is able to add NA server in WLC or not	Passed	
WLJ87IIS_REG_85	Creating the SSID and connecting the sensor mode AP	Verify that user is able to connect the sensor mode ap as a client	Passed	

WLJ87IIS_REG_86	Radius server up/down event data to Network Assurance	Verify that Radius server up/down event data is sending to Network Assurance server or not	Passed	
WLJ87IIS_REG_87	Verify that user is able to disabled NAC via CLI	Checking that user is able to disable NAC via CLI or not	Passed	
WLJ87IIS_REG_88	Verify that JSON data is sending out from WLC	Checking that JSON data is sending out from WLC to NA server or not	Passed	
WLJ87IIS_REG_89	WLC CLI allowing XOR radio as sensor even when WSA is disabled	Checking that user is able to XOR radio as a sensor while WSA disabled	Passed	
WLJ87IIS_REG_90	Verify that WLC sends nearestAP neighbors data to NA server correctly or not	Checking that WLC sends nearestAP neighbors data to NA server correctly or not	Passed	
WLJ87IIS_REG_91	Verify that wlan changes are reflecting in client event reason type for retries or not	Checking that WLAN changes are refelecting in NA server or not	Passed	
WLJ87IIS_REG_92	Verify that wsa server url config is syncing to standby wlc or not	Checking that wsa config syncing with standby in HA mode	Passed	
WLJ87IIS_REG_93	Verify that WLC able to resolve url if dns server ip is updated of NA server	Checking that wlc able to resolve the url of NA server if NA server ip address changes	Passed	
WLJ87IIS_REG_94	Configuring PSK key for wsa backhaul ssid	Verify that user is able to config psk key in backhaul ssid as normal WLAN or not	Passed	
WLJ87IIS_REG_95	Verifying that mac filtering working properly for sensor mode ap debug	Checking that mac-filtering working properly for sensor mode ap debug or not	Passed	
WLJ87S_Reg_122	Adding the NA server	Verify that user is able to add NA server in WLC or not	Passed	
WLJ87S_Reg_123	Creating the SSID and connecting the sensor mode AP	Verify that user is able to connect the sensor mode ap as a client	Passed	
WLJ87S_Reg_124	Radius server up/down event data to Network Assurance	Verify that Radius server up/down event data is sending to Network Assurance server or not	Passed	
WLJ87S_Reg_125	Verify that user is able to disabled NAC via CLI	Checking that user is able to disable NAC via CLI or not	Passed	
WLJ87S_Reg_126	Verify that JSON data is sending out from WLC	Checking that JSON data is sending out from WLC to NA server or not	Passed	
WLJ87S_Reg_127	WLC CLI allowing XOR radio as sensor even when WSA is disabled	Checking that user is able to XOR radio as a sensor while WSA disabled	Passed	
WLJ87S_Reg_128	Verify that WLC sends nearestAP neighbors data to NA server correctly or not	Checking that WLC sends nearestAP neighbors data to NA server correctly or not	Passed	

WLJ87S_Reg_129	Verify that wlan changes are reflecting in client event reason type for retries or not	Checking that WLAN changes are refelecting in NA server or not	Passed	
WLJ87S_Reg_130	Verify that wsa server url config is syncing to standby wlc or not	Checking that wsa config syncing with standby in HA mode	Passed	
WLJ87S_Reg_131	Verify that WLC able to resolve url if dns server ip is updated of NA server	Checking that wlc able to resolve the url of NA server if NA server ip address changes	Passed	
WLJ87S_Reg_132	Configuring PSK key for wsa backhaul ssid	Verify that user is able to config psk key in backhaul ssid as normal WLAN or not	Passed	
WLJ87S_Reg_133	Verifying that mac filltering working properly for sensor mode ap debug	Checking that mac-filtering working properly for sensor mode ap debug or not	Passed	

High Availability & Monitoring HA

Logical ID	Title	Description	Status	Defect ID
WLJ87IIS_REG_96	Controller HA pair with different hardware models	To verify the role negotiation between the controllers with different hardware models	Passed	
WLJ87IIS_REG_97	Controller HA pair with different software versions	To verify the role negotiation between the controllers with different software versions	Passed	
WLJ87IIS_REG_98	Controller mode when the redundancy port loses connectivity	To verify the HA pair controller modes after disconnecting the redundancy port	Passed	
WLJ87IIS_REG_99	Controller mode when the Gateway is not reachable to the both controller	To verify the HA pair controller modes when the Gateway is not reachable to both the controllers	Passed	
WLJ87IIS_REG_100	Controller modes(HA pair) after power failure	To verify the controller modes after power failure on both the controllers	Passed	
WLJ87IIS_REG_101	HA mode after resetting the peer system from ACTIVE	To verify the HA mode after resetting the peer system from ACTIVE controller	Passed	

WLJ87IIS_REG_102	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	
WLJ87IIS_REG_103	Client status during AP SSO after active failover-L2 Authentication	To check whether the Client gets disassociated and forced to re-join to the controller after AP SSO	Passed	
WLJ87IIS_REG_104	Controller mode when the Gateway is not reachable to the STANDBY controller ID	To verify the HA pair controller modes when the Gateway is not reachable from the STANDBY controller	Passed	
WLJ87IIS_REG_105	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	
WLJ87IIS_REG_106	Controller modes(HA pair) after power failure	To verify the controller modes after power failure on both the controllers	Passed	
WLJ87IIS_REG_107	HA mode after resetting the peer system from ACTIVE	To verify the HA mode after resetting the peer system from ACTIVE controller	Passed	
WLJ87IIS_REG_108	Transfer Upload of config, crashfile, debug-file on the ACTIVE controller and STANDBY controller-WLC 5508	To verify the successful upload of config, crashfile, debug-file on the ACTIVE controller and STANDBY controller	Passed	
WLJ87IIS_REG_109	Bulk Config sync between ACTIVE and STANDBY	To check the bulk config sync between ACTIVE and STANDBY controller in case of different configuration	Passed	
WLJ87S_Reg_172	Bringing HA pair up- WLC 5508 /7500	To verify whether the HA pair(ACTIVE:STANDBY) is up successfully	Passed	

WLJ87S_Reg_173	Controller HA pair with different hardware models	To verify the role negotiation between the controllers with different hardware models	Passed	
WLJ87S_Reg_174	Controller HA pair with different software versions	To verify the role negotiation between the controllers with different software versions	Passed	
WLJ87S_Reg_175	Controller mode when the redundancy port loses connectivity	To verify the HA pair controller modes after disconnecting the redundancy port	Passed	
WLJ87S_Reg_176	Controller mode when the Gateway is not reachable to the both controller	To verify the HA pair controller modes when the Gateway is not reachable to both the controllers	Passed	
WLJ87S_Reg_177	Controller modes(HA pair) after power failure	To verify the controller modes after power failure on both the controllers	Passed	
WLJ87S_Reg_178	HA mode after resetting the peer system from ACTIVE	To verify the HA mode after resetting the peer system from ACTIVE controller	Passed	
WLJ87S_Reg_179	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	
WLJ87S_Reg_180	Client status during AP SSO after active failover-L2 Authentication	To check whether the Client gets disassociated and forced to re-join to the controller after AP SSO	Passed	
WLJ87S_Reg_181	Controller mode when the Gateway is not reachable to the STANDBY controller ID	To verify the HA pair controller modes when the Gateway is not reachable from the STANDBY controller	Passed	
WLJ87S_Reg_182	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	

WLJ87S_Reg_183	Controller modes(HA pair) after power failure	To verify the controller modes after power failure on both the controllers	Passed	
WLJ87S_Reg_184	HA mode after resetting the peer system from ACTIVE	To verify the HA mode after resetting the peer system from ACTIVE controller	Passed	
WLJ87S_Reg_185	Transfer Upload of config, crashfile, debug-file on the ACTIVE controller and STANDBY controller-WLC 5508	To verify the successful upload of config, crashfile, debug-file on the ACTIVE controller and STANDBY controller	Passed	
WLJ87S_Reg_186	Bulk Config sync between ACTIVE and STANDBY	To check the bulk config sync between ACTIVE and STANDBY controller in case of different configuration	Passed	
WLJ87S_Reg_187	AP-count check after HA pair-up	To verify the AP-Count after HA pair up	Passed	

Default flex group

Logical ID	Title	Description	Status	Defect ID
WLJ87IIS_REG_110	Configuring the Flex connect AP's in default flex group	To verify whether the flex connect AP's added in default flex group or not	Passed	
WLJ87IIS_REG_111	Flex AP's move from default flex group to user created group with client.	To check whether client is disconnecting or not when Aps move to user group from default flex group	Passed	
WLJ87IIS_REG_112	Configure the flexconnect to Local mode AP's in WLC	AP's should removed from default flex group and client should disconnect	Passed	
WLJ87IIS_REG_113	Delete the user created flex group	Aps should move to default flex group and client should connect after remove the user flex group	Passed	

WLJ87IIS_REG_114	Configure the AVC Mapping in default flex group	To verify the WLAN AVC mapping configuration in default flex group	Passed	
WLJ87IIS_REG_115	Configuring Local authentication for WLAN with flex group	To verify the local authentication with flex group	Passed	
WLJ87IIS_REG_116	Upgrades FlexConnect APs via CLI	To Upgrades FlexConnect AP via CLI	Passed	
WLJ87S_Reg_188	Configuring the Flex connect AP's in default flex group	To verify whether the flex connect AP's added in default flex group or not	Passed	
WLJ87S_Reg_189	Flex AP's move from default flex group to user created group with client.	To check whether client is disconnecting or not when Aps move to user group from default flex group	Passed	
WLJ87S_Reg_190	Configure the flexconnect to Local mode AP's in WLC	AP's should removed from default flex group and client should disconnect	Passed	
WLJ87S_Reg_191	Delete the user created flex group	Aps should move to default flex group and client should connect after remove the user flex group	Passed	
WLJ87S_Reg_192	Configure the AVC Mapping in default flex group	To verify the WLAN AVC mapping configuration in default flex group	Passed	
WLJ87S_Reg_193	Configuring Local authentication for WLAN with flex group	To verify the local authentication with flex group	Passed	
WLJ87S_Reg_194	Upgrades FlexConnect APs via CLI	To Upgrades FlexConnect AP via CLI	Passed	

Roaming

Logical ID	Title	Description	Status	Defect ID
------------	-------	-------------	--------	-----------

WLJ87IIS_REG_117	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	
WLJ87IIS_REG_118	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	
WLJ87IIS_REG_119	Roaming of wireless clients within APs of one Flex connect group when controller is Down.	To check for the successful and seamless roaming of wireless clients between APs of same Flex connect group when controller is “Down”.	Passed	
WLJ87IIS_REG_120	Roaming of data clients between APs in different Flex connect group.	To check for the seamless roaming from one AP to another from the different Flex Connect group.	Passed	
WLJ87S_Reg_195	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	
WLJ87S_Reg_196	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	
WLJ87S_Reg_197	Roaming of wireless clients within APs of one Flex connect group when controller is Down.	To check for the successful and seamless roaming of wireless clients between APs of same Flex connect group when controller is “Down”.	Passed	

WLJ87S_Reg_198	Roaming of data clients between APs in different Flex connect group.	To check for the seamless roaming from one AP to another from the different Flex Connect group.	Passed	
WLJ87S_Reg_554	Mobility Management configuration	To verify whether Mobility Management can be successfully configured between two controllers or not	Passed	
WLJ87S_Reg_555	L2 Security Roaming between WLANs with differenet security	To verify whether Mobility Management can be successfully configured between two controllers or not	Passed	
WLJ87S_Reg_556	L2 Security Roaming between WLANs with same security	To verify whether Client is moving between two WLANs with same security or not in with L2 Roaming	Passed	
WLJ87S_Reg_557	L2 Security Roaming between Controllers with Differenet Radio types	To verify whether Client is Moving between Controllers with differenet Radio type or not with L2 Roaming	Passed	
WLJ87S_Reg_558	L2 Security Roaming between Controllers with same Radio types	To verify whether Client is Moving between Controllers with same Radio type or not with L2 Roaming	Passed	
WLJ87S_Reg_559	Monitoring the Client details before/after Roaming	To verify whether Client details are showing properly or not in Monitoring page	Passed	
WLJ87S_Reg_560	L3 Roaming between WLANs with Differenet security	To verify whether Client is Moving between Controllers with Different security or not with L3 Roaming	Passed	
WLJ87S_Reg_561	L3 Roaming between WLANs with same security	To verify whether Client is Moving between Controllers with same security type or not with L3 Roaming	Passed	

WLJ87S_Reg_562	L3 Roaming between Controllers with Different Radio type	To verify whether Client is Roaming between the Controllers with different Radio type or not	Passed	
WLJ87S_Reg_563	Intra Controller Roaming between same AP-Group	To verify whether Intra Controller Roaming is performing or not without any issues in same AP-Groups	Passed	
WLJ87S_Reg_564	Intra Controller Roaming between Different AP-Groups	To verify whether Intra Controller Roaming is performing or not without any issues in different AP-Groups	Passed	
WLJ87S_Reg_565	Debugging the Client details	To verify whether Client details are showing or not at the time of Roaming	Passed	
WLJ87S_Reg_566	Enabling the New Converged Access	To verify whether New Converged Access and Mobility parameters are enabling or not	Passed	
WLJ87S_Reg_567	Roaming the Client with Different QOS details	To verify whether Client is roaming or not with different QOS details	Passed	
WLJ87S_Reg_568	Roaming the Client with AVC rules	To verify whether after client Roaming the AVC rules will apply or not	Passed	
WLJ87S_Reg_569	Roaming the Client with ACL rules	To verify whether after Client Roam the ACL rules are applying or not	Passed	
WLJ87S_Reg_570	Roaming the Client with HA mode	To verify whether Client is connecting or not after Active controller is down	Passed	
WLJ87S_Reg_571	Roaming the Client when the AP is in Flexconnect group	To verify whether Client is Roaming or not when the AP is in Flexconnect Group	Passed	
WLJ87S_Reg_572	Roaming between two Aps with in the controller	To verify whether Roaming is working fine or not with in the same Controller between different Aps	Passed	

Multiple RADIUS server per SSID

WLJ87S_Reg_573	Roaming between two AP-Groups with in the controller	To verify whether Roaming is working fine or not between two AP-Groups	Passed	
----------------	--	--	--------	--

Multiple RADIUS server per SSID

Logical ID	Title	Description	Status	Defect ID
WLJ87IIS_REG_121	Performing Dot1x authentication over flexconnectAP with RADIUS servers configured(Secondary)	To verify whether Dot1x authentication can be performed successfully to the clients associated via the secondary RADIUS server over the flexconnectconnection with the Vlan mapped \u0007	Passed	
WLJ87IIS_REG_122	Performing Dot1x authentication over flexconnectAP with RADIUS servers configured(Primary failover)	To verify whether Dot1x authentication can be performed successfully to the clients associated via the secondary RADIUS server over the flexconnectconnection with the Vlan mapped \u0007	Passed	
WLJ87IIS_REG_123	Performing Dot1x authentication over FlexConnect AP with RADIUS servers configured(Primary)	To verify whether Dot1x authentication can be performed successfully to the clients associated via the Primary RADIUS server over the Flex AP connection with the Vlan mapped \u0007	Passed	
WLJ87IIS_REG_124	Performing Dot1x authentication over FlexConnect AP with RADIUS servers configured(Secondary)	To verify whether Dot1x authentication can be performed successfully to the clients associated via the secondary RADIUS server over the Flex AP connection with the Vlan mapped \u0007	Passed	

WLJ87S_Reg_199	Performing Dot1x authentication over flexconnectAP with RADIUS servers configured(Secondary)	To verify whether Dot1x authentication can be performed successfully to the clients associated via the secondary RADIUS server over the flexconnectconnection with the Vlan mapped \u0007	Passed	
WLJ87S_Reg_200	Performing Dot1x authentication over flexconnectAP with RADIUS servers configured(Primary failover)	To verify whether Dot1x authentication can be performed successfully to the clients associated via the secondary RADIUS server over the flexconnectconnection with the Vlan mapped \u0007	Passed	
WLJ87S_Reg_201	Performing Dot1x authentication over FlexConnect AP with RADIUS servers configured(Primary)	To verify whether Dot1x authentication can be performed successfully to the clients associated via the Primary RADIUS server over the Flex AP connection with the Vlan mapped \u0007	Passed	
WLJ87S_Reg_202	Performing Dot1x authentication over FlexConnect AP with RADIUS servers configured(Secondary)	To verify whether Dot1x authentication can be performed successfully to the clients associated via the secondary RADIUS server over the Flex AP connection with the Vlan mapped \u0007	Passed	

Hyperlocation Module supports for AP 37XX

Logical ID	Title	Description	Status	Defect ID
WLJ87IIS_REG_178	Importing maps to CMX through Japanese PI	To check whether the maps can be imported in CMX from PI	Passed	
WLJ87IIS_REG_179	Sync the WLC in to CMX	To check whether the WLC and CMX gets synced up	Passed	

Domain Based URL ACL

WLJ87IIS_REG_180	Tracking the Window,iPhone client devices in CMX	To check the tracking of Window ,iphone devices using CMX	Passed	
WLJ87IIS_REG_181	Android,iOS Client Locate in CMX	To verify the Location of the clients	Passed	
WLJ87IIS_REG_182	Location Accuracy Test in CMX of Window client	To verify the location accuracy of the clients	Passed	
WLJ87IIS_REG_183	History of client location(Client Playback)	To verify the client location history	Passed	
WLJ87S_Reg_302	Importing maps to CMX through PI	To check whether the maps can be imported in CMX from PI	Passed	
WLJ87S_Reg_303	Sync the WLC in to CMX	To check whether the WLC and CMX gets synced up	Passed	
WLJ87S_Reg_304	Tracking the Window,iPhone client devices in CMX	To check the tracking of Window ,iphone devices using CMX	Passed	
WLJ87S_Reg_305	Android,iOs Client Locate in CMX	To verify the Location of the clients	Passed	
WLJ87S_Reg_306	Location Accuracy Test in CMX of Window client	To verify the location accuracy of the clients	Passed	
WLJ87S_Reg_307	History of client location(Client Playback)	To verify the client location history	Passed	

Domain Based URL ACL

Logical ID	Title	Description	Status	Defect ID
WLJ87IIS_REG_184	Create new URL ACL , Add new URL on ACL on 5520 WLC	To verify that new ACL created , rule added or not using UI	Passed	
WLJ87IIS_REG_185	Add new URL domain on created url acl	To verify that new URL domain (www.cisco.com,www.yahoo.com) added or not	Passed	

WLJ87IIS_REG_186	Configure URL ACL as blacklist on WLAN and connect one Window client , open URL that configured in acl	To verify that URL is blocking that configured in URL-ACL profile and showing hit count in UI of WLC	Passed	
WLJ87IIS_REG_187	Configure URL ACL on interface using CLI and connect iOS client	To verify that URL ACL configured on interface or not and iOS client connectivity with URL blocked	Passed	
WLJ87IIS_REG_188	Delete URL ACL rule after applied	To verify that URL ACL rule delete successfully or not	Passed	
WLJ87IIS_REG_189	Modified rule of URL ACL and connect Android client	To verify that rule action modified or not and Android client connectivity	Passed	
WLJ87IIS_REG_190	Clear counter of URL ACL profile after open url in client web browser	To verify that counter is clear or not of URL ACL profile	Passed	
WLJ87IIS_REG_191	Show URL ACL status on WLAN using CLI	To verify that URL ACL status showing configured on WLAN	Passed	
WLJ87S_Reg_308	Create new URL ACL , Add new URL on ACL on 5520 WLC	To verify that new ACL created , rule added or not using UI	Passed	
WLJ87S_Reg_309	Add new URL domain on created url acl	To verify that new URL domain (www.cisco.com, www.yahoo.com) added or not	Passed	
WLJ87S_Reg_310	Configure URL ACL as blacklist on WLAN and connect one Window client , open URL that configured in acl	To verify that URL is blocking that configured in URL-ACL profile and showing hit count in UI of WLC	Passed	
WLJ87S_Reg_311	Configure URL ACL on interface using CLI and connect iOS client	To verify that URL ACL configured on interface or not and iOS client connectivity with URL blocked	Passed	

WLJ87S_Reg_312	Delete URL ACL rule after applied	To verify that URL ACL rule delete successfully or not	Passed	
WLJ87S_Reg_313	Modified rule of URL ACL and connect Android client	To verify that rule action modified or not and Android client connectivity	Passed	
WLJ87S_Reg_314	Clear counter of URL ACL profile after open url in client web browser	To verify that counter is clear or not of URL ACL profile	Passed	
WLJ87S_Reg_315	Show URL ACL status on WLAN using CLI	To verify that URL ACL status showing configured on WLAN	Passed	

ATF on Mesh

Logical ID	Title	Description	Status	Defect ID
WLJ87IIS_REG_192	Config Mesh setup and apply config on Mesh Aps	To verify that Mesh setup configured and ATF applied on Mesh Aps	Passed	
WLJ87IIS_REG_193	Apply ATF Enforcement mode on MESH AP	To verify that ATF Enforcement mode applied on MESH AP or not	Passed	
WLJ87IIS_REG_194	Apply ATF policy on wlan and connect Android client	To verify that policy applied on WLAN or not and client connected successfully	Passed	
WLJ87IIS_REG_195	Monitoring ATF statistics of root AP after Window and iPhone client connectivity	To verify that ATF statistics for root AP showing showing correct or not	Passed	
WLJ87IIS_REG_196	Monitoring ATF statistics of MESH AP after Window and iPhone client connectivity	To verify that ATF statistics for Mesh APs showing showing correct or not	Passed	

WLJ87IIS_REG_197	Mac OS client connectivity with 12 security WLAN which having different Policy weight	To verify the client connectivity with two SSID having different weight	Passed	
WLJ87IIS_REG_198	Apply ATF Enforcement mode on AP group	To verify that ATF Enforcement mode applied on AP group or not	Passed	
WLJ87IIS_REG_199	Airtime allocation override on universal client access radio 802.11a	To verify that ATF override on universal client access radio 802.11a is enable or not	Passed	
WLJ87IIS_REG_200	Monitoring ATF statistics after atf allocation on universal client access radio	To verify the ATF statistics after allocation on universal client access radio is showing properly or not	Passed	
WLJ87IIS_REG_201	Airtime allocation override on universal client access radio 802.11b	To verify that ATF override on universal client access radio 802.11b is enable or not	Passed	
WLJ87IIS_REG_202	Monitoring the CLI and GUI values of ATF statistics	To verify that ATF statistics values are showing same on CLI and GUI of MESH AP	Passed	
WLJ87IIS_REG_203	Monitoring the ATF statistics of client using CLI	To verify that ATF statistics of client is showing properly in CLI	Passed	
WLJ87IIS_REG_204	Disable Enforced mode of network for 802.11a radio on GUI	To verify that optimization is disable for network , 802.11 a radio	Passed	
WLJ87S_Reg_316	Config Mesh setup and apply config on Mesh Aps	To verify that Mesh setup configured and ATF applied on Mesh Aps	Passed	
WLJ87S_Reg_317	Apply ATF Enforcement mode on MESH AP	To verify that ATF Enforcement mode applied on MESH AP or not	Passed	

WLJ87S_Reg_318	Apply ATF policy on wlan and connect Android client	To verify that policy applied on WLAN or not and client connected successfully	Passed	
WLJ87S_Reg_319	Monitoring ATF statistics of root AP after Window and iPhone client connectivity	To verify that ATF statistics for root AP showing showing correct or not	Passed	
WLJ87S_Reg_320	Monitoring ATF statistics of MESH AP after Window and iPhone client connectivity	To verify that ATF statistics for Mesh APs showing showing correct or not	Passed	
WLJ87S_Reg_321	Mac OS client connectivity with 12 security WLAN which having different Policy weight	To verify the client connectivity with two SSID having different weight	Passed	
WLJ87S_Reg_322	Apply ATF Enforcement mode on AP group	To verify that ATF Enforcement mode applied on AP group or not	Passed	
WLJ87S_Reg_323	Airtime allocation override on universal client access radio 802.11a	To verify that ATF override on universal client access radio 802.11a is enable or not	Passed	
WLJ87S_Reg_324	Monitoring ATF statistics after atf allocation on universal client access radio	To verify the ATF statistics after allocation on universal client access radio is showing properly or not	Passed	
WLJ87S_Reg_325	Airtime allocation override on universal client access radio 802.11b	To verify that ATF override on universal client access radio 802.11b is enable or not	Passed	
WLJ87S_Reg_326	Monitoring the CLI and GUI values of ATF statistics	To verify that ATF statistics values are showing same on CLI and GUI of MESH AP	Passed	
WLJ87S_Reg_327	Monitoring the ATF statistics of client using CLI	To verify that ATF statistics of client is showing properly in CLI	Passed	

WLJ87S_Reg_328	Disable Enforced mode of network for 802.11a radio on GUI	To verify that optimization is disable for network , 802.11 a radio	Passed	
----------------	---	---	--------	--

LAG in Transition Restrictions

Logical ID	Title	Description	Status	Defect ID
WLJ87IIS_REG_205	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	
WLJ87IIS_REG_206	Active controller ports status when it is in Link Aggregation (LAG) failover	To check active controller ports status in Link Aggregation failover	Passed	
WLJ87IIS_REG_207	Checking the DHCP information in Lag-in-Transition (LAT) before WLC reboot in WLC GUI	To check whether the DHCP information changes in Lag-in-Transition state before the WLC is rebooted	Passed	
WLJ87IIS_REG_208	Checking the Interface address in Enable Lag-in-Transition (LAT) state	To verify whether the interface address changes during the WLC is in Lag-in-Transition state	Passed	
WLJ87IIS_REG_209	Checking the enhanced warnings for LAT state config changes	To check whether the warning are raised when the user reverts the LAG state	Passed	
WLJ87IIS_REG_210	Configuring neighbor port to which the controller is connected to support LAG	verifying the neighbor port configuration which controller is connected to support LAG	Passed	
WLJ87IIS_REG_211	configure the port channel on the neighbor switch to support LAG	validate the port channel on the neighbor switch to support LAG.	Passed	
WLJ87IIS_REG_212	LAG Port status Trap Log with SNMP Manager	To verify the successful LAG port status message in SNMP manager	Passed	

WLJ87S_Reg_364	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	
WLJ87S_Reg_365	Active controller ports status when it is in Link Aggregation (LAG) failover	To check active controller ports status in Link Aggregation failover	Passed	
WLJ87S_Reg_366	Checking the DHCP information in Lag-in-Transition (LAT) before WLC reboot in WLC GUI	To check whether the DHCP information changes in Lag-in-Transition state before the WLC is rebooted	Passed	
WLJ87S_Reg_367	Checking the Interface address in Enable Lag-in-Transition (LAT) state	To verify whether the interface address changes during the WLC is in Lag-in-Transition state	Passed	
WLJ87S_Reg_368	Checking the enhanced warnings for LAT state config changes	To check whether the warning are raised when the user reverts the LAG state	Passed	
WLJ87S_Reg_369	Configuring neighbor port to which the controller is connected to support LAG	verifying the neighbor port configuration which controller is connected to support LAG	Passed	
WLJ87S_Reg_370	configure the port channel on the neighbor switch to support LAG	validate the port channel on the neighbor switch to support LAG.	Passed	
WLJ87S_Reg_371	LAG Port status Trap Log with SNMP Manager	To verify the successful LAG port status message in SNMP manager	Passed	

EoGRE Tunnel Priority / Fallback

Logical ID	Title	Description	Status	Defect ID
------------	-------	-------------	--------	-----------

WLJ87IIS_REG_213	Associating Android clients to a local switching enabled WLAN with Tunnel profile mapped	To check whether Android clients gets associated or not to 2800/3800 AP's with local switching enabled WLAN with EoGRE tunnel mapped in it	Passed	
WLJ87IIS_REG_214	Associating IOS clients to a local switching enabled WLAN with Tunnel profile mapped	To check whether IOS clients gets associated or not to 2800/3800 AP's with local switching enabled WLAN with EoGRE tunnel mapped in it	Passed	
WLJ87IIS_REG_215	Associating Windows clients to a local switching enabled WLAN with Tunnel profile mapped	To check whether windows clients gets associated or not to 2800/3800 AP's with local switching enabled WLAN with EoGRE tunnel mapped in it	Passed	
WLJ87IIS_REG_216	Associating Apple MacBook clients to a local switching enabled WLAN with Tunnel profile mapped	To check whether Apple MacBook clients gets associated or not to 2800/3800 AP's with local switching enabled WLAN with EoGRE tunnel mapped in it	Passed	
WLJ87IIS_REG_217	Checking the tunnel gateway fallback works properly for Android clients	To check whether Android clients fallback to secondary tunnel or not when primary tunnel gateway goes down	Passed	
WLJ87IIS_REG_218	Checking the tunnel gateway fallback works properly for IOS clients	To check whether IOS clients fallback to secondary tunnel or not when primary tunnel gateway goes down	Passed	

WLJ87IIS_REG_219	Checking the tunnel gateway fallback works properly for Windows clients	To check whether Windows clients fallback to secondary tunnel or not when primary tunnel gateway goes down	Passed	
WLJ87IIS_REG_220	Checking the tunnel gateway fallback works properly for Apple MacBook clients	To check whether Apple MacBook clients fallback to secondary tunnel or not when primary tunnel gateway goes down	Passed	
WLJ87IIS_REG_221	Checking the tunnel configuration in HA WLCs	To check whether config sync occurs or not for tunnel gateway/domain configuration between Active and Standby WLC's	Passed	
WLJ87IIS_REG_222	Creating a tunnel gateway with invalid ipv4 address	To check whether proper error message thrown or not while creating tunnel gateway with invalid ipv4 address	Passed	
WLJ87IIS_REG_223	Changing the role for created tunnel domain in WLC GUI/CLI	To check whether role can be changed or not for created tunnel domain via WLC GUI and CLI	Passed	
WLJ87IIS_REG_224	Configuring the tunnel domain for WLC from PI	To check whether tunnel configurations can be done or not for WLC via PI and vice versa	Passed	
WLJ87IIS_REG_225	Associating Client to a local switching enabled and dot1X security WLAN with Tunnel profile mapped in AP standalone mode	To check whether clients gets associated or not to 2800/3800 AP's with local switching enabled WLAN with EoGRE tunnel mapped in it in AP standalone mode	Passed	

WLJ87IIS_REG_226	Associating Client to a local switching enabled and open security WLAN with Tunnel profile mapped in AP standalone mode	To check whether clients gets associated or not to 2800/3800 AP's with local switching enabled WLAN with EoGRE tunnel mapped in it in AP standalone mode	Passed	
WLJ87S_Reg_383	Associating Android clients to a local switching enabled WLAN with Tunnel profile mapped	To check whether Android clients gets associated or not to 2800/3800 AP's with local switching enabled WLAN with EoGRE tunnel mapped in it	Passed	
WLJ87S_Reg_384	Associating IOS clients to a local switching enabled WLAN with Tunnel profile mapped	To check whether IOS clients gets associated or not to 2800/3800 AP's with local switching enabled WLAN with EoGRE tunnel mapped in it	Passed	
WLJ87S_Reg_385	Associating Windows clients to a local switching enabled WLAN with Tunnel profile mapped	To check whether windows clients gets associated or not to 2800/3800 AP's with local switching enabled WLAN with EoGRE tunnel mapped in it	Passed	
WLJ87S_Reg_386	Associating Apple MacBook clients to a local switching enabled WLAN with Tunnel profile mapped	To check whether Apple MacBook clients gets associated or not to 2800/3800 AP's with local switching enabled WLAN with EoGRE tunnel mapped in it	Passed	
WLJ87S_Reg_387	Checking the tunnel gateway fallback works properly for Android clients	To check whether Android clients fallback to secondary tunnel or not when primary tunnel gateway goes down	Passed	

WLJ87S_Reg_388	Checking the tunnel gateway fallback works properly for IOS clients	To check whether IOS clients fallback to secondary tunnel or not when primary tunnel gateway goes down	Passed	
WLJ87S_Reg_389	Checking the tunnel gateway fallback works properly for Windows clients	To check whether Windows clients fallback to secondary tunnel or not when primary tunnel gateway goes down	Passed	
WLJ87S_Reg_390	Checking the tunnel gateway fallback works properly for Apple MacBook clients	To check whether Apple MacBook clients fallback to secondary tunnel or not when primary tunnel gateway goes down	Passed	
WLJ87S_Reg_391	Checking the tunnel configuration in HA WLCs	To check whether config sync occurs or not for tunnel gateway/domain configuration between Active and Standby WLC's	Passed	
WLJ87S_Reg_392	Creating a tunnel gateway with invalid ipv4 address	To check whether proper error message thrown or not while creating tunnel gateway with invalid ipv4 address	Passed	
WLJ87S_Reg_393	Changing the role for created tunnel domain in WLC GUI/CLI	To check whether role can be changed or not for created tunnel domain via WLC GUI and CLI	Passed	
WLJ87S_Reg_394	Configuring the tunnel domain for WLC from PI	To check whether tunnel configurations can be done or not for WLC via PI and vice versa	Passed	

WLJ87S_Reg_395	Associating Client to a local switching enabled and dot1X security WLAN with Tunnel profile mapped in AP standalone mode	To check whether clients gets associated or not to 2800/3800 AP's with local switching enabled WLAN with EoGRE tunnel mapped in it in AP standalone mode	Passed	
WLJ87S_Reg_396	Associating Client to a local switching enabled and open security WLAN with Tunnel profile mapped in AP standalone mode	To check whether clients gets associated or not to 2800/3800 AP's with local switching enabled WLAN with EoGRE tunnel mapped in it in AP standalone mode	Passed	

TKIP/ Enabler for Wave 2 - 1800/2800/3800 APs Passpoint

Logical ID	Title	Description	Status	Defect ID
WLJ87IIS_REG_227	Windows client connectivity with WPA1-TKIP + WPA2-AES	To validate the The client connectivity with WPA1-TKIP + WPA2-AES whether able to connect or not.	Passed	
WLJ87IIS_REG_228	Android client Connectivity with WPA1-TKIP + WPA2-AES support 1800/2800/3800 AP	To validate the android client connectivity whether able to connect or not with WPA1-TKIP + WPA2-AES support 2800/3800 AP	Passed	
WLJ87IIS_REG_229	IOS client connectivity with WPA1-TKIP + WPA2-AES support 1800/2800/3800 AP	To validate the IOS client Connectivity	Passed	
WLJ87IIS_REG_230	Mac OS client connectivity with WPA1-TKIP + WPA2-AES support 1800/2800/3800 AP	To validate the WPA1-TKIP + WPA2-AES support 2800/3800 AP able to connect or not Mac client.	Passed	
WLJ87IIS_REG_231	Monitoring the 1800/2800/3800 AP join Statistics	Monitoring the TKIP support 1800/2800/3800 AP	Passed	

WLJ87IIS_REG_232	Client connectivity to 802.11a radio TKIP support 1800/2800/3800 AP	To validate the client connectivity to 802.11a radio	Passed	
WLJ87IIS_REG_233	Client connectivity to 802.11b radio with 1800/2800/3800 AP	To validate the client connectivity to 802.11b radio with 1800/2800/3800 AP.	Passed	
WLJ87S_Reg_397	Windows client connectivity with WPA1-TKIP + WPA2-AES	To validate the The client connectivity with WPA1-TKIP + WPA2-AES whether able to connect or not.	Passed	
WLJ87S_Reg_398	Android client Connectivity with WPA1-TKIP + WPA2-AES support 1800/2800/3800 AP	To validate the android client connectivity whether able to connect or not with WPA1-TKIP + WPA2-AES support 2800/3800 AP	Passed	
WLJ87S_Reg_399	IOS client connectivity with WPA1-TKIP + WPA2-AES support 1800/2800/3800 AP	To validate the IOS client Connectivity	Passed	
WLJ87S_Reg_400	Mac OS client connectivity with WPA1-TKIP + WPA2-AES support 1800/2800/3800 AP	To validate the WPA1-TKIP + WPA2-AES support 2800/3800 AP able to connect or not Mac client.	Passed	
WLJ87S_Reg_401	Monitoring the 1800/2800/3800 AP join Statistics	Monitoring the TKIP support 1800/2800/3800 AP	Passed	
WLJ87S_Reg_402	client connectivity to 802.11a radio TKIP support 1800/2800/3800 AP	To validate the client connectivity to 802.11a radio	Passed	
WLJ87S_Reg_403	Client connectivity to 802.11b radio with 1800/2800/3800 AP	To validate the client connectivity to 802.11b radio with 1800/2800/3800 AP.	Passed	

Simplifying Cisco ISE Configuration on Cisco WLC - Phase 2

Logical ID	Title	Description	Status	Defect ID
------------	-------	-------------	--------	-----------

WLJ87IIS_REG_234	Create WLAN with L2 security 'none' enable mac filtering and connect Android/Windows/iOS client	To check the WLAN create or not with none and Android/Windows/iOS client connect succesfully	Passed	
WLJ87IIS_REG_235	Create WLAN with L2 security 'WPA+WPA2' , enable 802.1x and connect with Windows/Android/iOS client	To check that WLAN create or not with 'WPA+WPA2' , 802.1x enabled and iOSWindows/Android client connect succesfully	Passed	
WLJ87IIS_REG_236	Create WLAN with L2 security 'none' , enabled Local EAP Authentication	To check that WLAN create or not with L2 security 'none' , enabled Local EAP Authentication	Passed	
WLJ87IIS_REG_237	Create WLAN with L2 security 'WPA+WPA2' enabled Local EAP Authentication	To check that WLAN create or not with L2 security 'WPA+WPA2' , enabled Local EAP Authentication	Passed	
WLJ87IIS_REG_238	Create WLAN with L2 security 'none' , select LDAP server	To check that WLAN create or not with L2 security 'none' , select LDAP server	Passed	
WLJ87IIS_REG_239	Create WLAN with L2 security 'WPA+WPA2' ,select LDAP server	To check that WLAN create or not with L2 security 'WPA+WPA2' ,select LDAP server	Passed	
WLJ87IIS_REG_240	Create WLAN with L2 security 'none' , select Authentication priority order	To check that WLAN create or not with L2 security 'none' ,select Authentication priority order for web auth user	Passed	
WLJ87IIS_REG_241	Create WLAN with L2 security 'WPA+WPA2' , select Authentication priority order	To check that WLAN create or not with L2 security 'WPA+WPA2' ,select Authentication priority order for web auth user	Passed	
WLJ87S_Reg_405	Create WLAN with L2 security 'none' , enable mac filtering and connect iOS client	To check the WLAN create or not with none and iOS client connect succesfully	Passed	

WLJ87S_Reg_406	Create WLAN with L2 security 'none' , enable mac filtering and connect android client	To check the WLAN create or not with none and window client connect successfully	Passed	
WLJ87S_Reg_407	Create WLAN with L2 security 'WPA+WPA2' , enable 802.1x and connect with iOS client	To check that WLAN create or not with 'WPA+WPA2' , 802.1x enabled and iOS client connect successfully	Passed	
WLJ87S_Reg_408	Create WLAN with L2 security 'WPA+WPA2' , enable 802.1x and connect with window client	To check that WLAN create or not with 'WPA+WPA2' , 802.1x enabled and window client connect successfully	Passed	
WLJ87S_Reg_409	Create WLAN with L2 security 'WPA+WPA2' , enable 802.1x and connect with Android client	To check that WLAN create or not with 'WPA+WPA2' , 802.1x enabled and Android client connect successfully	Passed	
WLJ87S_Reg_410	Create WLAN with L2 security 'none' , enabled Local EAP Authentication	To check that WLAN create or not with L2 security 'none' , enabled Local EAP Authentication	Passed	
WLJ87S_Reg_411	Create WLAN with L2 security 'WPA+WPA2' enabled Local EAP Authentication	To check that WLAN create or not with L2 security 'WPA+WPA2' , enabled Local EAP Authentication	Passed	
WLJ87S_Reg_412	Create WLAN with L2 security 'none' , select LDAP server	To check that WLAN create or not with L2 security 'none' , select LDAP server	Passed	
WLJ87S_Reg_413	Create WLAN with L2 security 'WPA+WPA2' ,select LDAP server	To check that WLAN create or not with L2 security 'WPA+WPA2' ,select LDAP server	Passed	
WLJ87S_Reg_414	Create WLAN with L2 security 'none' , select Authentication priority order	To check that WLAN create or not with L2 security 'none' ,select Authentication priority order for web auth user	Passed	

WLJ87S_Reg_415	Create WLAN with L2 security 'WPA+WPA2' , select Authentication priority order	To check that WLAN create or not with L2 security 'WPA+WPA2' ,select Authentication priority order for web auth user	Passed	
----------------	--	--	--------	--

Flexconnect VLAN based Central switching

Logical ID	Title	Description	Status	Defect ID
WLJ87IIS_REG_242	Creating a WLAN with Flexconnect vlan based central switching enabled and associating Android client to this WLAN	To check whether Andriod client gets associated or not to a WLAN in which Flexconnect based central switching is enabled.	Passed	
WLJ87IIS_REG_243	Creating a WLAN with Flexconnect vlan based central switching enabled and associating MAC/Windows/IOS client to this WLAN	To check whether MAC client gets associated or not to a WLAN in which Flexconnect based central switching is enabled.	Passed	
WLJ87IIS_REG_244	Checking the flexconnect VLAN based central switching by mapping a different interface	To check whether the fexconnect is working with the different interface	Passed	
WLJ87S_Reg_416	Creating a WLAN with Flexconnect vlan based central switching enabled and associating Android client to this WLAN	To check whether Andriod client gets associated or not to a WLAN in which Flexconnect based central switching is enabled.	Passed	
WLJ87S_Reg_417	Creating a WLAN with Flexconnect vlan based central switching enabled and associating MAC client to this WLAN	To check whether MAC client gets associated or not to a WLAN in which Flexconnect based central switching is enabled.	Passed	

WLJ87S_Reg_418	Creating a WLAN with Flexconnect vlan based central switching enabled and associating windows client to this WLAN	To check whether Windows client gets associated or not to a WLAN in which Flexconnect based central switching is enabled.	Passed	
WLJ87S_Reg_419	Creating a WLAN with Flexconnect vlan based central switching enabled and associating IOS client to this WLAN	To check whether IOS client gets associated or not to a WLAN in which Flexconnect based central switching is enabled.	Passed	
WLJ87S_Reg_420	Checking the flexconnect VLAN based centrl switching by mapping a different interface	To check whether the fexconnect is working with the different interface	Passed	

TrustSec Enhancements

Logical ID	Title	Description	Status	Defect ID
WLJ87IIS_REG_245	Associating Android clients to TrustSec configured AP and checking the policy hit statistics in WLC UI	To verify the policy hit for Android client after Trustsec configured on AP	Passed	
WLJ87IIS_REG_246	Performing Inter controller roaming of Windows client in TrustSec enabled WLC's with Dot1x security.	To check whether inter controller roaming of windows clients works properly or not between WLC's with Dot1x security.	Passed	
WLJ87IIS_REG_247	Performing Inter controller roaming of Android client in TrustSec enabled WLC's with Dot1x security.	To check whether inter controller roaming of Android clients works properly or not between WLC's with Dot1x security.	Passed	
WLJ87IIS_REG_248	Performing Inter controller roaming of IOS client in TrustSec enabled WLC's with Dot1x security.	To check whether inter controller roaming of IOS clients works properly or not between WLC's with Dot1x security.	Passed	

WLJ87IIS_REG_249	Performing Inter controller roaming of MacOS client in TrustSec enabled WLC's with Dot1x security.	To check whether inter controller roaming of windows clients works properly or not between WLC's with Dot1x security.	Passed	
WLJ87IIS_REG_250	Performing Inter controller roaming of Windows client in TrustSec enabled WLC's with WPA2-dot1x security.	To check whether inter controller roaming of windows clients works properly or not between WLC's with WPA2-dot1x security.	Passed	
WLJ87IIS_REG_251	Performing Inter controller roaming of Android client in TrustSec enabled WLC's with WPA2-dot1x security.	To check whether inter controller roaming of Android clients works properly or not between WLC's with WPA2-dot1x security.	Passed	
WLJ87IIS_REG_252	Performing Inter controller roaming of IOS client in TrustSec enabled WLC's with WPA2-dot1x security.	To check whether inter controller roaming of IOS clients works properly or not between WLC's with WPA2-dot1x security.	Passed	
WLJ87IIS_REG_253	Performing Inter controller roaming of MacOS client in TrustSec enabled WLC's with WPA2-dot1x security.	To check whether inter controller roaming of MacOS clients works properly or not between WLC's with WPA2-dot1x security.	Passed	
WLJ87IIS_REG_254	Enabling CTS override in 2800/3800 AP's which is joined in 5520 WLC UI/CLI	To check that CTS override is enabled or not for 2800/3800 AP's	Passed	
WLJ87IIS_REG_255	Checking the trustsec configuration sync in HA WLC's	To check that trustsec configuration sync or not in HA WLC's	Passed	
WLJ87S_Reg_421	Associating Android clients to TrustSec configured AP and checking the policy hit statistics in WLC UI	To verify the policy hit for Android client after Trustsec configured on AP	Passed	

WLJ87S_Reg_422	Performing Inter controller roaming of Windows client in TrustSec enabled WLC's with Dot1x security.	To check whether inter controller roaming of windows clients works properly or not between WLC's with Dot1x security.	Passed	
WLJ87S_Reg_423	Performing Inter controller roaming of Android client in TrustSec enabled WLC's with Dot1x security.	To check whether inter controller roaming of Android clients works properly or not between WLC's with Dot1x security.	Passed	
WLJ87S_Reg_424	Performing Inter controller roaming of IOS client in TrustSec enabled WLC's with Dot1x security.	To check whether inter controller roaming of IOS clients works properly or not between WLC's with Dot1x security.	Passed	
WLJ87S_Reg_425	Performing Inter controller roaming of MacOS client in TrustSec enabled WLC's with Dot1x security.	To check whether inter controller roaming of windows clients works properly or not between WLC's with Dot1x security.	Passed	
WLJ87S_Reg_426	Performing Inter controller roaming of Windows client in TrustSec enabled WLC's with WPA2-dot1x security.	To check whether inter controller roaming of windows clients works properly or not between WLC's with WPA2-dot1x security.	Passed	
WLJ87S_Reg_427	Performing Inter controller roaming of Android client in TrustSec enabled WLC's with WPA2-dot1x security.	To check whether inter controller roaming of Android clients works properly or not between WLC's with WPA2-dot1x security.	Passed	
WLJ87S_Reg_428	Performing Inter controller roaming of IOS client in TrustSec enabled WLC's with WPA2-dot1x security.	To check whether inter controller roaming of IOS clients works properly or not between WLC's with WPA2-dot1x security.	Passed	

WLJ87S_Reg_429	Performing Inter controller roaming of MacOS client in TrustSec enabled WLC's with WPA2-dot1x security.	To check whether inter controller roaming of MacOS clients works properly or not between WLC's with WPA2-dot1x security.	Passed	
WLJ87S_Reg_430	Enabling CTS override in 2800/3800 AP's which is joined in 5520 WLC UI/CLI	To check that CTS override is enabled or not for 2800/3800 AP's	Passed	
WLJ87S_Reg_431	Checking the trustsec configuration sync in HA WLC's	To check that trustsec configuration sync or not in HA WLC's	Passed	

Facebook WIFI

Logical ID	Title	Description	Status	Defect ID
WLJ87IIS_REG_256	Redirection to Facebook Page	To verify redirection to facebook page for logging in is successful or not	Passed	
WLJ87IIS_REG_257	Restricting free internet access for unauthenticated Windows client	To verify denial of internet access for unauthenticated Windows users is successful or not	Passed	
WLJ87IIS_REG_258	Http Redirection for Continuing Browsing in Android Phone	To Verify Redirection to the Http page initially requested by the Android user is successful or not	Passed	
WLJ87IIS_REG_259	Https Redirection for Continuing Browsing in Windows Laptop	To Verify Redirection to the Https page initially requested by the Windows Laptop user is successful or not	Passed	
WLJ87IIS_REG_260	Show Logs tab	To Verify successful download of each individual log file listed in the show logs tab	Passed	
WLJ87IIS_REG_261	User data statistics	To verify whether the user's data statistics are displayed correctly or not	Passed	

WLJ87IIS_REG_262	KNOWN Users	To verify whether authenticated users are listed in the user data tab or not	Passed	
WLJ87IIS_REG_263	UNKNOWN Users	To verify whether users not authenticated are listed in the user data tab or not	Passed	
WLJ87IIS_REG_264	IN-AUTH Users	To verify whether users attempting to get authenticated are listed in the user data tab or not	Passed	
WLJ87S_Reg_432	Redirection to Facebook Page	To verify redirection to facebook page for logging in is successful or not	Passed	
WLJ87S_Reg_433	Authentication using facebook credentials	To verify successful authentication using facebook credentials	Passed	
WLJ87S_Reg_434	Authentication using WiFi Code	To verify successful authentication using WiFi Code	Passed	
WLJ87S_Reg_435	Get WiFi access using Skip-check-in	To verify whether user getting free wifi access using Skip check-in	Passed	
WLJ87S_Reg_436	Restricting free internet access for unauthenticated Windows client	To verify denial of internet access for unauthenticated Windows users is successful or not	Passed	
WLJ87S_Reg_437	Restricting free internet access for unauthenticated Android clients	To verify denial of internet access for unauthenticated Android users is successful or not	Passed	
WLJ87S_Reg_438	Restricting free internet access for unauthenticated IOS clients	To verify denial of internet access for unauthenticated IOS users is successful or not	Passed	
WLJ87S_Reg_439	Http Redirection for Continuing Browsing in IOS	To Verify Redirection to the Http page initially requested by the IOS user is successful or not	Passed	

WLJ87S_Reg_440	Http Redirection for Continuing Browsing in Android Phone	To Verify Redirection to the Http page initially requested by the Android user is successful or not	Passed	
WLJ87S_Reg_441	Https Redirection for Continuing Browsing in Windows Laptop	To Verify Redirection to the Https page initially requested by the Windows Laptop user is successful or not	Passed	
WLJ87S_Reg_442	Setup the WiFi session length and check using Windows user	To verify whether the windows user not getting wifi access after session length time expires	Passed	
WLJ87S_Reg_443	Setup the WiFi session length and check using Android user	To verify whether the Android user not getting wifi access after session length time expires	Passed	
WLJ87S_Reg_444	Setup the WiFi session length and check using IOS user	To verify whether the IOS user not getting wifi access after session length time expires	Passed	
WLJ87S_Reg_445	Show Logs tab	To Verify successful download of each individual log file listed in the show logs tab	Passed	
WLJ87S_Reg_446	User data statistics	To verify whether the user's data statistics are displayed correctly or not	Passed	
WLJ87S_Reg_447	KNOWN Users	To verify whether authenticated users are listed in the user data tab or not	Passed	
WLJ87S_Reg_448	UNKNOWN Users	To verify whether users not authenticated are listed in the user data tab or not	Passed	
WLJ87S_Reg_449	IN-AUTH Users	To verify whether users attempting to get authenticated are listed in the user data tab or not	Passed	

Location Analytics

Logical ID	Title	Description	Status	Defect ID
------------	-------	-------------	--------	-----------

WLJ87IIS_REG_265	Access points in the Floor map	To verify whether client devices are displayed in the floor map or not	Passed	
WLJ87IIS_REG_266	Wireless Laptop Client Location in Floor map	To verify whether laptop client devices are displayed in the floor map or not	Passed	
WLJ87IIS_REG_267	Wireless mobile Client Location in Floor map	To verify whether mobile client devices are displayed in the floor map or not	Passed	
WLJ87IIS_REG_268	Search client by MAC address	To verify whether client device can be searched by specifying its MAC address or not	Passed	
WLJ87IIS_REG_269	Search client by IP	To verify whether client device can be searched by specifying its IP address or not	Passed	
WLJ87IIS_REG_270	Search client by SSID	To verify whether client device can be searched by specifying the SSID or not	Passed	
WLJ87IIS_REG_271	Interferers in Floor map	To verify whether interferers are displayed in the floor map or not	Passed	
WLJ87IIS_REG_272	Rogue Devices in Floor map	To verify whether rogues are displayed in the floor map or not	Passed	
WLJ87IIS_REG_273	Client movement history playback	To verify whether client's movement history is shown or not	Passed	
WLJ87IIS_REG_274	Creating New Report	To verify whether new report can be created or not	Passed	
WLJ87S_Reg_450	Access points in the Floor map	To verify whether client devices are displayed in the floor map or not	Passed	
WLJ87S_Reg_451	Wireless Laptop Client Location in Floor map	To verify whether laptop client devices are displayed in the floor map or not	Passed	

WLJ87S_Reg_452	Wireless mobile Client Location in Floor map	To verify whether mobile client devices are displayed in the floor map or not	Passed	
WLJ87S_Reg_453	Search client by MAC address	To verify whether client device can be searched by specifying its MAC address or not	Passed	
WLJ87S_Reg_454	Search client by IP	To verify whether client device can be searched by specifying its IP address or not	Passed	
WLJ87S_Reg_455	Search client by SSID	To verify whether client device can be searched by specifying the SSID or not	Passed	
WLJ87S_Reg_456	Interferers in Floor map	To verify whether interferers are displayed in the floor map or not	Passed	
WLJ87S_Reg_457	Rogue Devices in Floor map	To verify whether rogues are displayed in the floor map or not	Passed	
WLJ87S_Reg_458	Client movement history playback	To verify whether client's movement history is shown or not	Passed	
WLJ87S_Reg_459	Creating New Report	To verify whether new report can be created or not	Passed	

Internal DHCP Server

Logical ID	Title	Description	Status	Defect ID
WLJ87IIS_REG_275	Assigning the Internal DHCP server to WLAN	To verify whether Internal DHCP server assigned successfully to WLAN or not	Passed	
WLJ87IIS_REG_276	configure the internal DHCP server to JSSID WLAN	To check Internal DHCP server assigned successfully or not to JSSID WLAN	Passed	

WLJ87IIS_REG_277	Disabling the DHCP Proxy server	To verify whether without DHCP proxy server enable client will get IP address or not	Passed	
WLJ87IIS_REG_278	Configuring the DHCP option 82 with binary format	To verify whether DHCP option 82 configured client is showing binary format or not	Passed	
WLJ87IIS_REG_279	Configuring the DHCP option 82 with ascii format	To verify whether DHCP option 82 configured client is showing ASCII format or not	Passed	
WLJ87IIS_REG_280	DHCP option 82 with AP-MAC & AP-MAC-SSID format	To verify whether AP-MAC & AP-MAC-SSID details are showing or not at the time of debug	Passed	
WLJ87IIS_REG_281	DHCP option 82 with AP-ETHMAC & AP-NAME-SSID format	To verify whether AP-ETHMAC & AP-NAME-SSID details are showing or not at the time of debug	Passed	
WLJ87IIS_REG_282	DHCP option 82 with AP-Group-Name & Flex-Group-Name format	To verify whether AP-Group-Name & Flex-Group-Name details are showing or not at the time of debug	Passed	
WLJ87IIS_REG_283	DHCP option 82 with AP-Location & AP-Mac-Vlan-ID format	To verify whether AP-Location & AP-Mac-Vlan-ID details are showing or not at the time of debug	Passed	
WLJ87IIS_REG_284	Configuring the DHCP with maximum & minimum timeout	To verify whether DHCP maximum & minimum values are configured successfully	Passed	
WLJ87S_Reg_460	Assigning the Internal DHCP server to WLAN	To verify whether Internal DHCP server assigned successfully to WLAN or not	Passed	

WLJ87S_Reg_461	configure the internal DHCP server to JSSID WLAN	To check Internal DHCP server assigned successfully or not to JSSID WLAN	Passed	
WLJ87S_Reg_462	Disabling the DHCP Proxy server	To verify whether without DHCP proxy server enable client will get IP address or not	Passed	
WLJ87S_Reg_463	Configuring the DHCP option 82 with binary format	To verify whether DHCP option 82 configured client is showing binary format or not	Passed	
WLJ87S_Reg_464	Configuring the DHCP option 82 with ascii format	To verify whether DHCP option 82 configured client is showing ASCII format or not	Passed	
WLJ87S_Reg_465	DHCP option 82 with AP-MAC & AP-MAC-SSID format	To verify whether AP-MAC & AP-MAC-SSID details are showing or not at the time of debug	Passed	
WLJ87S_Reg_466	DHCP option 82 with AP-ETHMAC & AP-NAME-SSID format	To verify whether AP-ETHMAC & AP-NAME-SSID details are showing or not at the time of debug	Passed	
WLJ87S_Reg_467	DHCP option 82 with AP-Group-Name & Flex-Group-Name format	To verify whether AP-Group-Name & Flex-Group-Name details are showing or not at the time of debug	Passed	
WLJ87S_Reg_468	DHCP option 82 with AP-Location & AP-Mac-Vlan-ID format	To verify whether AP-Location & AP-Mac-Vlan-ID details are showing or not at the time of debug	Passed	
WLJ87S_Reg_469	Configuring the DHCP with maximum & minimum timeout	To verify whether DHCP maximum & minimum values are configured successfully	Passed	

Cisco WLC 3504 Support

Logical ID	Title	Description	Status	Defect ID
WLJ87IIS_REG_285	Configuring WLC3504 in Day0 mode with wired client	To verify the Day0 configuration of WLC3504 through wired client.	Passed	
WLJ87IIS_REG_286	Converting AP mode from local to flexconnect In WLC3504	To verify the AP mode conversion from local to flexconnect.	Passed	
WLJ87IIS_REG_287	Converting AP mode from flexconnect to local mode.	To verify the AP mode conversion from flexconnect to local.	Passed	
WLJ87IIS_REG_288	Connecting wireless clients to the WLAN configured in WLC3504.	To verify the client connectivity to the WLAN configured in WLC.	Passed	
WLJ87IIS_REG_289	Configuring Internal dhcp server and connecting clients.	To verify the internal dhcp configuration and client connectivity through internal dhcp.	Passed	
WLJ87IIS_REG_290	Connecting client with L2 security Static WEP.	to verify the client connectivity with L2 Security WEP.	Passed	
WLJ87IIS_REG_291	Connecting client with L2 Security - WPA/WPA2 + PSK	To verify the client connectivity with L2 Security WPA/WPA2 + PSK	Passed	
WLJ87IIS_REG_292	Connecting client with L2 Security - WPA/WPA2 + dot1x	To verify the client connectivity with L2 security WPA/WPA2+dot1x	Passed	
WLJ87IIS_REG_293	Connecting client with L3 security - WebAuth Internal	To verify the client connectivity with L3 security internal web authentication.	Passed	
WLJ87IIS_REG_294	Connecting client with L3 security - WebAuth Customized	To verify the client connectivity with customized webauth	Passed	

WLJ87IIS_REG_295	Connecting client with L3 security - WebAuth external	To verify the client connectivity with L3 security External web authentication.	Passed	
WLJ87IIS_REG_296	Client connectivity with Flex central auth and local switching.	To verify whether client connects successfully with central auth and local switching.	Passed	
WLJ87IIS_REG_297	Client connectivity with Flex local auth and local switching.	To verify client connectivity with local auth and local switching.	Passed	
WLJ87IIS_REG_298	Config migration check between 5500 and 3504.	To verify the config migration check between 5500 and WLC3504.	Passed	
WLJ87S_Reg_470	Configuring WLC3504 into the network	To check whether CT3504 can be configured without any issues.	Passed	
WLJ87S_Reg_471	Configuring WLC3504 in Day0 mode with wired client	To verify the Day0 configuration of WLC3504 through wired client.	Passed	
WLJ87S_Reg_472	Configuring WLC3504 in Day0 mode by connecting wireless client.	To verify the Day0 configuration of WLC3504 through wireless client.	Passed	
WLJ87S_Reg_473	AP joining to WLC3504	To verify the supported Aps are joining the WLC without any issues.	Passed	
WLJ87S_Reg_474	Converting AP mode from local to flexconnect In WLC3504	To verify the AP mode conversion from local to flexconnect.	Passed	
WLJ87S_Reg_475	Converting AP mode from flexconnect to local mode.	To verify the AP mode conversion from flexconnect to local.	Passed	
WLJ87S_Reg_476	Connecting wireless clients to the WLAN configured in WLC3504.	To verify the client connectivity to the WLAN configured in WLC.	Passed	

WLJ87S_Reg_477	Upgrading the WLC3504 to the latest build.	To verify the upgrading of WLC3504 to the latest build without any issues.	Passed	
WLJ87S_Reg_478	Upload/download config file from WLC.	To verify the config retain on upload/download the config file.	Passed	
WLJ87S_Reg_479	Configuring Internal dhcp server and connecting clients.	To verify the internal dhcp configuration and client connectivity through internal dhcp.	Passed	
WLJ87S_Reg_480	Connecting client with L2 security Static WEP.	to verify the client connectivity with L2 Security WEP.	Passed	
WLJ87S_Reg_481	Connecting client with L2 Security - WPA/WPA2 + PSK	To verify the client connectivity with L2 Security WPA/WPA2 + PSK	Passed	
WLJ87S_Reg_482	Connecting client with L2 Security - WPA/WPA2 + dot1x	To verify the client connectivity with L2 security WPA/WPA2+dot1x	Passed	
WLJ87S_Reg_483	Connecting client with L3 security - WebAuth Internal	To verify the client connectivity with L3 security internal web authentication.	Passed	
WLJ87S_Reg_484	Connecting client with L3 security - WebAuth Customized	To verify the client connectivity with customized webauth	Passed	
WLJ87S_Reg_485	Connecting client with L3 security - WebAuth external	To verify the client connectivity with L3 security External web authentication.	Passed	
WLJ87S_Reg_486	Client connectivity with Flex central auth and central switching.	To verify whether client connects successfully with central auth and central switching.	Passed	
WLJ87S_Reg_487	Client connectivity with Flex central auth and local switching.	To verify whether client connects successfully with central auth and local switching.	Passed	

WLJ87S_Reg_488	Client connectivity with Flex local auth and local switching.	To verify client connectivity with local auth and local switching.	Passed	
WLJ87S_Reg_489	Config migration check between 5500 and 3504.	To verify the config migration check between 5500 and WLC3504.	Passed	

Monitor Mode support in Aps(1810/1815)

Logical ID	Title	Description	Status	Defect ID
WLJ87IIS_REG_302	Making the AP mode of 1815/1810 to monitor mode	To verify that user is able to change the AP mode to monitor mode or not	Passed	
WLJ87IIS_REG_303	Checking that in monitor mode AP 1815/1810 broadcasting the SSID or not	To check wheather AP in monitor mode broadcasting the SSID or not	Passed	
WLJ87IIS_REG_304	Checking that AP 1815/1810 after mode changes from monitor to local or flexconnect serving the client or not	Verifying that AP 1815/1810 after mode changes from monitor to local or flexconnect serving the client or not	Passed	
WLJ87IIS_REG_305	Detecting the interfering devices via 5GHZ band	Verifying that AP 1815/1810 able to detect interfering device via 5GHZ band or not	Passed	
WLJ87IIS_REG_306	Detecting the interfering devices via 2.4 ghz band	Verifying that AP 1815/1810 able to detect interfering device via 2.4 ghz band or not	Passed	
WLJ87IIS_REG_307	Configuring the channel for tarking optimization via CLI and GUI	To check wheather user is able to config channel for tarking optimization or not via GUI/CLI	Passed	
WLJ87IIS_REG_308	Enabling submode wips with monitor mode and intergerating with MSE and PI	Verifying that user is able to enable submode wips with monitor mode and intgrate with MSE and PI or not	Passed	
WLJ87IIS_REG_309	Checking that monitor mode AP(1815/1810) with wIPS enabled detecting wips Local AP clients as ROGUE	Verify that whether monitor AP with wIPS enabled detecting wips Local AP clients as ROGUE or not	Passed	
WLJ87IIS_REG_310	Verifying the Monitor mode ap is scanning all the DCA and country channel for 5ghz or not	Checking that user is able to scan all the DCA and country channel for 5ghz or not	Passed	
WLJ87IIS_REG_311	Verifying the Monitor mode ap is scanning all the DCA and country channel for 2.4 ghz or not	Checking that user is able to scan all the DCA and country channel for 2.4ghz or not	Passed	

Mobility Converged access on 5520/8540 WLC

WLJ87S_Reg_497	Making the AP mode of 1815/1810 to monitor mode	To verify that user is able to change the AP mode to monitor mode or not	Passed	
WLJ87S_Reg_498	Checking that in monitor mode AP 1815/1810 broadcasting the SSID or not	To check whether AP in monitor mode broadcasting the SSID or not	Passed	
WLJ87S_Reg_499	Checking that AP 1815/1810 after mode changes from monitor to local or flexconnect serving the client or not	Verifying that AP 1815/1810 after mode changes from monitor to local or flexconnect serving the client or not	Passed	
WLJ87S_Reg_500	Detecting the interfering devices via 5GHZ band	Verifying that AP 1815/1810 able to detect interfering device via 5GHZ band or not	Passed	
WLJ87S_Reg_501	Detecting the interfering devices via 2.4 ghz band	Verifying that AP 1815/1810 able to detect interfering device via 2.4 ghz band or not	Passed	
WLJ87S_Reg_502	Configuring the channel for tracking optimization via CLI and GUI	To check whether user is able to config channel for tracking optimization or not via GUI/CLI	Passed	
WLJ87S_Reg_503	Enabling submode wips with monitor mode and intergerating with MSE and PI	Verifying that user is able to enable submode wips with monitor mode and integrate with MSE and PI or not	Passed	
WLJ87S_Reg_504	Checking that monitor mode AP(1815/1810) with wIPS enabled detecting wips Local AP clients as ROGUE	Verify that whether monitor AP with wIPS enabled detecting wips Local AP clients as ROGUE or not	Passed	
WLJ87S_Reg_505	Verifying the Monitor mode ap is scanning all the DCA and country channel for 5ghz or not	Checking that user is able to scan all the DCA and country channel for 5ghz or not	Passed	
WLJ87S_Reg_506	Verifying the Monitor mode ap is scanning all the DCA and country channel for 2.4 ghz or not	Checking that user is able to scan all the DCA and country channel for 2.4ghz or not	Passed	

Mobility Converged access on 5520/8540 WLC

Logical ID	Title	Description	Status	Defect ID
WLJ87IIS_REG_302	Making the AP mode of 1815/1810 to monitor mode	To verify that user is able to change the AP mode to monitor mode or not	Passed	
WLJ87IIS_REG_303	Checking that in monitor mode AP 1815/1810 broadcasting the SSID or not	To check whether AP in monitor mode broadcasting the SSID or not	Passed	

WLJ87IIS_REG_304	Checking that AP 1815/1810 after mode changes from monitor to local or flexconnect serving the client or not	Verifying that AP 1815/1810 after mode changes from monitor to local or flexconnect serving the client or not	Passed	
WLJ87IIS_REG_305	Detecting the interfering devices via 5GHZ band	Verifying that AP 1815/1810 able to detect interfering device via 5GHZ band or not	Passed	
WLJ87IIS_REG_306	Detecting the interfering devices via 2.4 ghz band	Verifying that AP 1815/1810 able to detect interfering device via 2.4 ghz band or not	Passed	
WLJ87IIS_REG_307	Configuring the channel for tracking optimization via CLI and GUI	To check whether user is able to config channel for tracking optimization or not via GUI/CLI	Passed	
WLJ87IIS_REG_308	Enabling submode wips with monitor mode and intergerating with MSE and PI	Verifying that user is able to enable submode wips with monitor mode and integrate with MSE and PI or not	Passed	
WLJ87IIS_REG_309	Checking that monitor mode AP(1815/1810) with wIPS enabled detecting wips Local AP clients as ROGUE	Verify that whether monitor AP with wIPS enabled detecting wips Local AP clients as ROGUE or not	Passed	
WLJ87IIS_REG_310	Verifying the Monitor mode ap is scanning all the DCA and country channel for 5ghz or not	Checking that user is able to scan all the DCA and country channel for 5ghz or not	Passed	
WLJ87IIS_REG_311	Verifying the Monitor mode ap is scanning all the DCA and country channel for 2.4 ghz or not	Checking that user is able to scan all the DCA and country channel for 2.4ghz or not	Passed	
WLJ87S_Reg_497	Making the AP mode of 1815/1810 to monitor mode	To verify that user is able to change the AP mode to monitor mode or not	Passed	

WLJ87S_Reg_498	Checking that in monitor mode AP 1815/1810 broadcasting the SSID or not	To check wheather AP in monitor mode broadcasting the SSID or not	Passed	
WLJ87S_Reg_499	Checking that AP 1815/1810 after mode changes from monitor to local or flexconnect serving the client or not	Verifying that AP 1815/1810 after mode changes from monitor to local or flexconnect serving the client or not	Passed	
WLJ87S_Reg_500	Detecting the interfering devices via 5GHZ band	Verifying that AP 1815/1810 able to detect interfering device via 5GHZ band or not	Passed	
WLJ87S_Reg_501	Detecting the interfering devices via 2.4 ghz band	Verifying that AP 1815/1810 able to detect interfering device via 2.4 ghz band or not	Passed	
WLJ87S_Reg_502	Configuring the channel for tarcking optimization via CLI and GUI	To check wheather user is able to config channel for tarcking optimization or not via GUI/CLI	Passed	
WLJ87S_Reg_503	Enabling submode wips with monitor mode and intergerating with MSE and PI	Verifying that user is able to enable submode wips with monitor mode and intgrate with MSE and PI or not	Passed	
WLJ87S_Reg_504	Checking that monitor mode AP(1815/1810) with wIPS enabled detecting wips Local AP clients as ROGUE	Verify that whether monitor AP with wIPS enabled detecting wips Local AP clients as ROGUE or not	Passed	
WLJ87S_Reg_505	Verifying the Monitor mode ap is scanning all the DCA and country channel for 5ghz or not	Checking that user is able to scan all the DCA and country channel for 5ghz or not	Passed	
WLJ87S_Reg_506	Verifying the Monitor mode ap is scanning all the DCA and country channel for 2.4 ghz or not	Checking that user is able to scan all the DCA and country channel for 2.4ghz or not	Passed	

HA WLC Auth/Authz

Logical ID	Title	Description	Status	Defect ID
WLJ87IIS_REG_326	Allowing the user for complete access to WLC network via TACACS and connecting a client to it.	To check whether user can able to read-write access the primary controller of WLC network or not via TACACS	Passed	
WLJ87IIS_REG_327	Providing the user for monitoring access to the Primary Controller of WLC via TACACS	To check whether user can able to have monitoring access read-only or not to WLC via TACACS and check if any configuration changes can be made or not.	Passed	
WLJ87IIS_REG_328	Providing the user for lobby admin access to the Primary WLC via TACACS	To check whether user can able to have lobby admin access or not to Primary WLC via TACACS	Passed	
WLJ87IIS_REG_329	Allowing the user for complete access to Secondary WLC after Bringing the Primary WLC down via TACACS and connecting a JOS client to it.	To check whether user can able to read-write access the Secondary controller of WLC network after the primary controller goes down via TACACS or not and connecting a JOS Client to the Secondary WLC.	Passed	
WLJ87IIS_REG_330	Allowing the user for complete access to Secondary WLC after Bringing the Primary WLC down via TACACS and connecting a Window client to it.	To check whether user can able to read-write access the Secondary controller of WLC network after the primary controller goes down via TACACS or not and connecting a Window Client to the Secondary WLC.	Passed	
WLJ87IIS_REG_331	Allowing the user for complete access to Secondary WLC after Bringing the Primary WLC down via TACACS and connecting a IOS client to it.	To check whether user can able to read-write access the Secondary controller of WLC network after the primary controller goes down via TACACS or not and connecting a IOS Client to the Secondary WLC.	Passed	

WLJ87IIS_REG_332	Allowing the user for complete access to Secondary WLC after Bringing the Primary WLC down via TACACS and connecting a Mac OS client to it.	To check whether user can able to read-write access the Secondary controller of WLC network after the primary controller goes down via TACACS or not and connecting a Mac OS Client to the Secondary WLC.	Passed	
WLJ87IIS_REG_333	Providing the user for monitoring access to the Secondary Controller via TACACS if the primary controller goes down.	To check whether user can able to have monitoring access read-only or not to Secondary WLC via TACACS if Primary Controller link is down and check if any configuration changes can be made or not.	Passed	
WLJ87IIS_REG_334	Providing the user for lobby admin access to the Secondary WLC via TACACS when the link of the Primary WLC goes down.	To check whether user can able to have lobby admin access or not with Secondary WLC via TACACS when the link of the Primary WLC goes down.	Passed	
WLJ87S_Reg_521	Allowing the user for complete access to WLC network via TACACS and connecting a client to it.	To check whether user can able to read-write access the primary controller of WLC network or not via TACACS	Passed	
WLJ87S_Reg_522	Providing the user for monitoring access to the Primary Controller of WLC via TACACS	To check whether user can able to have monitoring access read-only or not to WLC via TACACS and check if any configuration changes can be made or not.	Passed	
WLJ87S_Reg_523	Providing the user for lobby admin access to the Primary WLC via TACACS	To check whether user can able to have lobby admin access or not to Primary WLC via TACACS	Passed	

WLJ87S_Reg_524	Allowing the user for complete access to Secondary WLC after Bringing the Primary WLC down via TACACS and connecting a JOS client to it.	To check whether user can able to read-write access the Secondary controller of WLC network after the primary controller goes down via TACACS or not and connecting a JOS Client to the Secondary WLC.	Passed	
WLJ87S_Reg_525	Allowing the user for complete access to Secondary WLC after Bringing the Primary WLC down via TACACS and connecting a Window client to it.	To check whether user can able to read-write access the Secondary controller of WLC network after the primary controller goes down via TACACS or not and connecting a Window Client to the Secondary WLC.	Passed	
WLJ87S_Reg_526	Allowing the user for complete access to Secondary WLC after Bringing the Primary WLC down via TACACS and connecting a IOS client to it.	To check whether user can able to read-write access the Secondary controller of WLC network after the primary controller goes down via TACACS or not and connecting a IOS Client to the Secondary WLC.	Passed	
WLJ87S_Reg_527	Allowing the user for complete access to Secondary WLC after Bringing the Primary WLC down via TACACS and connecting a Mac OS client to it.	To check whether user can able to read-write access the Secondary controller of WLC network after the primary controller goes down via TACACS or not and connecting a Mac OS Client to the Secondary WLC.	Passed	
WLJ87S_Reg_528	Providing the user for monitoring access to the Secondary Controller via TACACS if the primary controller goes down.	To check whether user can able to have monitoring access read-only or not to Secondary WLC via TACACS if Primary Controller link is down and check if any configuration changes can be made or not.	Passed	

WLJ87S_Reg_529	Providing the user for lobby admin access to the Secondary WLC via TACACS when the link of the Primary WLC goes down.	To check whether user can able to have lobby admin access or not with Secondary WLC via TACACS when the link of the Primary WLC goes down.	Passed	
----------------	---	--	--------	--

DHCP Option 82 - Google

Logical ID	Title	Description	Status	Defect ID
WLJ87IIS_REG_335	Connecting the android/IOS/MAC clients without enabling DHCP proxy	To verify whether android/IOS/MAC Clients are getting the internal DHCP IP address or not when DHCP Proxy is in disabled state	Passed	
WLJ87IIS_REG_336	Connecting the android/IOS/MAC clients after enable DHCP proxy	To verify whether android/IOS/MAC Clients are getting IP address or not when Proxy is in enable state	Passed	
WLJ87IIS_REG_337	Enable/disable the DHCP Proxy through CLI	To verify whether DHCP proxy server enable/disable through CLI or not	Passed	
WLJ87IIS_REG_338	Configuring the DHCP Option 82 Remote Id field format with AP-MAC	To verify whether DHCP option 82 with AP-MAC is sending the client association/disassociation requests or not	Passed	
WLJ87IIS_REG_339	Configuring the DHCP Option 82 Remote Id field format with AP-MAC-SSID	To verify whether DHCP option 82 with AP-MAC-SSID is sending the client association/disassociation requests or not	Passed	
WLJ87IIS_REG_340	Configuring the DHCP Option 82 Remote Id field format with AP-ETHMAC	To verify whether DHCP option 82 with AP-ETHMAC is sending the client association/disassociation requests or not	Passed	

WLJ87IIS_REG_341	Configuring the DHCP Option 82 Remote Id field format with AP-Name-SSID	To verify whether DHCP option 82 with AP-Name-SSID is sending the client association/disassociation requests or not	Passed	
WLJ87IIS_REG_342	Configuring the DHCP Option 82 Remote Id field format with Flex-Group-Name	To verify whether DHCP option 82 with Flex-Group-Name is sending the client association/disassociation requests or not	Passed	
WLJ87IIS_REG_343	Configuring the DHCP Option 82 Remote Id field format with AP-Location	To verify whether DHCP option 82 with AP-Location is sending the client association/disassociation requests or not	Passed	
WLJ87IIS_REG_344	Configuring the DHCP Option 82 Remote Id field format with AP-MAC-VLAN-ID	To verify whether DHCP option 82 with AP-MAC-VLAN-ID is sending the client association/disassociation requests or not	Passed	
WLJ87IIS_REG_345	Configuring the DHCP Option 82 Remote Id field format with AP-NAME-VLAN-ID	To verify whether DHCP option 82 with AP-NAME-VLAN-ID is sending the client association/disassociation requests or not	Passed	
WLJ87IIS_REG_346	Configuring the DHCP Option 82 Remote Id field format with AP-ETHMAC-SSID	To verify whether DHCP option 82 with AP-ETHMAC-SSID is sending the client association/disassociation requests or not	Passed	
WLJ87IIS_REG_347	Configuring the DHCP option 82 through PI	To verify whether DHCP option 82 is enabling through PI or not	Passed	
WLJ87S_Reg_530	Connecting the android/IOS/MAC clients without enabling DHCP proxy	To verify whether android/IOS/MAC Clients are getting the internal DHCP IP address or not when DHCP Proxy is in disabled state	Passed	

WLJ87S_Reg_531	Connecting the android/IOS/MAC clients after enable DHCP proxy	To verify whether android/IOS/MAC Clients are getting IP address or not when Proxy is in enable state	Passed	
WLJ87S_Reg_532	Enable/disable the DHCP Proxy through CLI	To verify whether DHCP proxy server enable/disable through CLI or not	Passed	
WLJ87S_Reg_533	Configuring the DHCP Option 82 Remote Id field format with AP-MAC	To verify whether DHCP option 82 with AP-MAC is sending the client association/disassociation requests or not	Passed	
WLJ87S_Reg_534	Configuring the DHCP Option 82 Remote Id field format with AP-MAC-SSID	To verify whether DHCP option 82 with AP-MAC-SSID is sending the client association/disassociation requests or not	Passed	
WLJ87S_Reg_535	Configuring the DHCP Option 82 Remote Id field format with AP-ETHMAC	To verify whether DHCP option 82 with AP-ETHMAC is sending the client association/disassociation requests or not	Passed	
WLJ87S_Reg_536	Configuring the DHCP Option 82 Remote Id field format with AP-Name-SSID	To verify whether DHCP option 82 with AP-Name-SSID is sending the client association/disassociation requests or not	Passed	
WLJ87S_Reg_537	Configuring the DHCP Option 82 Remote Id field format with Flex-Group-Name	To verify whether DHCP option 82 with Flex-Group-Name is sending the client association/disassociation requests or not	Passed	
WLJ87S_Reg_538	Configuring the DHCP Option 82 Remote Id field format with AP-Location	To verify whether DHCP option 82 with AP-Location is sending the client association/disassociation requests or not	Passed	

WLJ87S_Reg_539	Configuring the DHCP Option 82 Remote Id field format with AP-MAC-VLAN-ID	To verify whether DHCP option 82 with AP-MAC-VLAN-ID is sending the client association/disassociation requests or not	Passed	
WLJ87S_Reg_540	Configuring the DHCP Option 82 Remote Id field format with AP-NAME-VLAN-ID	To verify whether DHCP option 82 with AP-NAME-VLAN-ID is sending the client association/disassociation requests or not	Passed	
WLJ87S_Reg_541	Configuring the DHCP Option 82 Remote Id field format with AP-ETHMAC-SSID	To verify whether DHCP option 82 with AP-ETHMAC-SSID is sending the client association/disassociation requests or not	Passed	
WLJ87S_Reg_542	Configuring the DHCP option 82 through PI	To verify whether DHCP option 82 is enabling through PI or not	Passed	
WLJ87S_Reg_543	Monitoring the Client details	To verify whether Client details are showing properly or not in Monitoring page	Passed	

Client Auth Failures(AAA Failures/WLC Failures)

Logical ID	Title	Description	Status	Defect ID
WLJ87IIS_REG_348	Configure maximum allowed clients per AP radio	To configure maximum allowed clients per AP radio and check if the number of clients given alone gets connected or not	Passed	
WLJ87IIS_REG_349	Applying access control list to the WLAN and check if the ACL rule works to deny the client .	To check whether the ACL applied to WLAN works and check if the client get denied or not.	Passed	
WLJ87IIS_REG_350	Configuring maximum allowed clients for the WLAN and check if the specified clients alone gets connected	To connect a specified number of clients to a specific WLAN and check if client more than the specified value does not authenticated or not	Passed	

WLJ87IIS_REG_351	Creating a local policy adding device type as Android and Sleeping client Timeout and check if client move into sleeping client after Timeout.	To create a local policy with device type as Android and configuring Sleeping Client Timeout and check if the sleeping timeout	Passed	
WLJ87IIS_REG_352	Creating a local policy adding device type as Apple and Sleeping client Timeout and check if client move into sleeping client after timeout.	To create a local policy with device type as Apple and configuring Sleeping Client Timeout and check the sleeping timeout	Passed	
WLJ87IIS_REG_353	Creating a local policy adding device type as Windows and Sleeping Client Timeout and check if client move into sleeping client after Timeout.	To create a local policy with device type as Windows and configuring Sleeping Client Timeout and check the sleeping timeout	Passed	
WLJ87IIS_REG_354	Configuring Identity Request Timeout and Identity Request Retries .	To configure Identity Request Timeout and Identity Request Retries and check if the request is send to client to the limited number of times within the limeted time or not.	Passed	
WLJ87IIS_REG_355	Configuring Session timeout for WLAN and check if the client re-auth when the timer gets expired.	To Enable and configure session timeout for WLAN and check if the session timeout interval works fine or not	Passed	
WLJ87IIS_REG_356	Creating a DHCP scope and check if the IP address given in the scope is given to client.	To Configure DHCP scope and check if the Ip address is given to the client and check if the ip address allocated is shown in the DHCP Allocates leases.	Passed	

WLJ87IIS_REG_357	Checking the client status if the security of the WLAN changes when a client connected to WLAN .	To Check the status of the client if the security of the WLAN changes when the client is connected to the WLAN.	Passed	
WLJ87S_Reg_544	Configure maximum allowed clients per AP radio	To configure maximum allowed clients per AP radio and check if the number of clients given alone gets connected or not	Passed	
WLJ87S_Reg_545	Applying access control list to the WLAN and check if the ACL rule works to deny the client .	To check whether the ACL applied to WLAN works and check if the client get denied or not.	Passed	
WLJ87S_Reg_546	Configuring maximum allowed clients for the WLAN and check if the specified clients alone gets connected	To connect a specified number of clients to a specific WLAN and check if client more than the specified value does not authenticated or not	Passed	
WLJ87S_Reg_547	Creating a local policy adding device type as Android and Sleeping client Timeout and check if client move into sleeping client after Timeout.	To create a local policy with device type as Android and configuring Sleeping Client Timeout and check if the sleeping timeout	Passed	
WLJ87S_Reg_548	Creating a local policy adding device type as Apple and Sleeping client Timeout and check if client move into sleeping client after timeout.	To create a local policy with device type as Apple and configuring Sleeping Client Timeout and check the sleeping timeout	Passed	
WLJ87S_Reg_549	Creating a local policy adding device type as Windows and Sleeping Client Timeout and check if client move into sleeping client after Timeout.	To create a local policy with device type as Windows and configuring Sleeping Client Timeout and check the sleeping timeout	Passed	

Intra/Inter WLC Roaming Failures(Ping Pong Issues)

WLJ87S_Reg_550	Configuring Identity Request Timeout and Identity Request Retries .	To configure Identity Request Timeout and Identity Request Retries and check if the request is send to client to the limited number of times within the limeted time or not.	Passed	
WLJ87S_Reg_551	Configuring Session timeout for WLAN and check if the client re-auth when the timer gets expired.	To Enable and configure session timeout for WLAN and check if the session timeout interval works fine or not	Passed	
WLJ87S_Reg_552	Creating a DHCP scope and check if the IP address given in the scope is given to client.	To Configure DHCP scope and check if the Ip address is given to the client and check if the ip address allocated is shown in the DHCP Allocates leases.	Passed	
WLJ87S_Reg_553	Checking the client status if the security of the WLAN changes when a client connected to WLAN .	To Check the status of the client if the security of the WLAN changes when the client is connected to the WLAN.	Passed	

Intra/Inter WLC Roaming Failures(Ping Pong Issues)

Logical ID	Title	Description	Status	Defect ID
WLJ87IIS_REG_358	L2 Security Roaming between WLANs with differenet security	To verify whether Mobility Management can be successfully configured between two controllers or not	Passed	
WLJ87IIS_REG_359	L2 Security Roaming between WLANs with same security	To verify whether Client is moving between two WLANs with same security or not in with L2 Roaming	Passed	

WLJ87IIS_REG_360	L2 Security Roaming between Controllers with Different Radio types	To verify whether Client is Moving between Controllers with different Radio type or not with L2 Roaming.	Passed	
WLJ87IIS_REG_361	L2 Security Roaming between Controllers with same Radio types	To verify whether Client is Moving between Controllers with same Radio type or not with L2 Roaming	Passed	
WLJ87IIS_REG_362	Monitoring the Client details before/after Roaming	To verify whether Client details are showing properly or not in Monitoring page	Passed	
WLJ87IIS_REG_363	L3 Roaming between WLANs with Different security	To verify whether Client is Moving between Controllers with Different security or not with L3 Roaming	Passed	
WLJ87IIS_REG_364	L3 Roaming between WLANs with same security	To verify whether Client is Moving between Controllers with same security type or not with L3 Roaming	Passed	
WLJ87IIS_REG_365	L3 Roaming between Controllers with Different Radio type	To verify whether Client is Roaming between the Controllers with different Radio type or not	Passed	
WLJ87IIS_REG_366	Intra Controller Roaming between same AP-Group	To verify whether Intra Controller Roaming is performing or not without any issues in same AP-Groups	Passed	

Intra/Inter WLC Roaming Failures(Ping Pong Issues)

WLJ87IIS_REG_367	Intra Controller Roaming between Different AP-Groups	To verify whether Intra Controller Roaming is performing or not without any issues in different AP-Groups	Passed	
WLJ87IIS_REG_368	debuging the Client details	To verify whether Client details are shoing or not at the time of Roaming	Passed	
WLJ87IIS_REG_369	Enabling the New Converged Access	To verify whether New Converged Access and Mobility parameters are enabling or not	Passed	
WLJ87IIS_REG_370	Roaming the Client with Different QOS details	To verify whether Client is roaming or not with different QOS details	Passed	
WLJ87IIS_REG_371	Roaming the Client with AVC rules	To verify whether after client Roaming the AVC rules will apply or not	Passed	
WLJ87IIS_REG_372	Roaming the Client with ACL rules	To verify whether after Client Roam the ACL rules are applying or not	Passed	
WLJ87IIS_REG_373	Roaming the Client with HA mode	To verify whether Client is connecting or not after Active controller is down	Passed	
WLJ87IIS_REG_374	Roaming the Client when the AP is in Flexconnect group	To verify whether Client is Roaming or not when the AP is in Flexconnect Group	Passed	
WLJ87IIS_REG_375	Roaming between two Aps with in the controller	To verify whether Roaming is working fine or not with in the same Controller between differenet Aps	Passed	

WLJ87IIS_REG_376	Roaming between two AP-Groups with in the controller	To verify whether Roaming is working fine or not between two AP-Groups	Passed	
------------------	--	--	--------	--

MIMO Coverage

Logical ID	Title	Description	Status	Defect ID
WLJ87IIS_REG_377	Enabling HT either in in 802.11b/g/n or 802.11a/n/ac and checking the clients association & their throughput	To check whether clients data rates are getting at maximum output or not as configured in 802.11b/g/n or 802.11a/n/ac	Passed	
WLJ87IIS_REG_378	Enabling VHT alone in 802.11a/n/ac and checking the clients association & their throughput	To check whether clients data rates are getting at maximum output or not as per their spatial streams configured in 802.11a/n/ac	Passed	
WLJ87IIS_REG_379	Setting the channel width to 40MHz/80MHz and checking the clients association	To check whether clients data rates are getting at maximum output or not as per their spatial streams configured in 802.11a/n/ac when it is configured with 40MHz	Passed	
WLJ87IIS_REG_380	Capturing the beacon packets and checking the HT & VHT parameters	To check whether HT & VHT parameters displays the configurations properly or not in beacon packets.	Passed	
WLJ87IIS_REG_381	Setting the AP channel to extended UNII-2 channels and checking the clients association	To check whether clients associated successfully or not to AP when AP configured in UNII-2 channels	Passed	
WLJ87IIS_REG_382	Setting the channel width to best and checking the clients association	To check whether clients data rates are getting at maximum output or not as per their spatial streams configured in 802.11a/n/ac when it is configured with best channel width	Passed	

WLJ87IIS_REG_383	Setting the AP channel to India extended channels and checking the clients association	To check whether clients associated successfully or not to AP when AP configured in India extended channels	Passed	
WLJ87IIS_REG_384	Setting the maximum allowed clients range in 802.11a global parameters	To check whether more numbers of clients allowed or not than the range set in 802.11a global parameters	Passed	
WLJ87S_Reg_574	Enabling HT in 802.11b/g/n alone and checking the clients association & their throughput	To check whether clients data rates are getting at maximum output or not as configured in 802.11b/g/n	Passed	
WLJ87S_Reg_575	Enabling HT alone in 802.11a/n/ac and checking the clients association & their throughput	To check whether clients data rates are getting at maximum output or not as per their spatial streams configured in 802.11a/n/ac	Passed	
WLJ87S_Reg_576	Enabling VHT alone in 802.11a/n/ac and checking the clients association & their throughput	To check whether clients data rates are getting at maximum output or not as per their spatial streams configured in 802.11a/n/ac	Passed	
WLJ87S_Reg_577	Setting the channel width to 40MHz and checking the clients association	To check whether clients data rates are getting at maximum output or not as per their spatial streams configured in 802.11a/n/ac when it is configured with 40MHz	Passed	
WLJ87S_Reg_578	Setting the channel width to 80MHz and checking the clients association	To check whether clients data rates are getting at maximum output or not as per their spatial streams configured in 802.11a/n/ac when it is configured with 80MHz	Passed	
WLJ87S_Reg_579	Capturing the beacon packets and checking the HT & VHT parameters	To check whether HT & VHT parameters displays the configurations properly or not in beacon packets.	Passed	

WLJ87S_Reg_580	Setting the AP channel to extended UNII-2 channels and checking the clients association	To check whether clients associated successfully or not to AP when AP configured in UNII-2 channels	Passed	
WLJ87S_Reg_581	Setting the channel width to best and checking the clients association	To check whether clients data rates are getting at maximum output or not as per their spatial streams configured in 802.11a/n/ac when it is configured with best channel width	Passed	
WLJ87S_Reg_582	Setting the AP channel to India extended channels and checking the clients association	To check whether clients associated successfully or not to AP when AP configured in India extended channels	Passed	
WLJ87S_Reg_583	Setting the maximum allowed clients range in 802.11a global parameters	To check whether more numbers of clients allowed or not than the range set in 802.11a global parameters	Passed	

Dot1x and Web-Auth

Logical ID	Title	Description	Status	Defect ID
WLJ87IIS_REG_125	Authentication of Android client with Security Dot1x and Web-Auth	Checking for the Authentication of the client when connected to a WLAN in which Dot1x and Web-Auth is enabled	Passed	
WLJ87IIS_REG_126	Authentication of window 10 client with Security Dot1x and Web-Auth	Checking for the Authentication of the client when connected to a WLAN in which Dot1x and Web-Auth is enabled	Passed	
WLJ87IIS_REG_127	Authentication of Android client with Security Static WEP and Web-Auth	Checking for the Authentication of the client when connected to a WLAN in which Static WEP and Web-Auth is enabled	Passed	
WLJ87IIS_REG_128	Authentication of Window 10 client with Security Static WEP and Web-Auth	Checking for the Authentication of the client when connected to a WLAN in which Static WEP and Web-Auth is enabled	Passed	

WLJ87IIS_REG_129	Authentication of clients Win 7 laptop with Security Static WEP and Web-Auth	Checking for the Authentication of the clients when connected to a WLAN in which Static WEP and Web-Auth is enabled. \u0007	Passed	
WLJ87IIS_REG_130	Authentication of clients iOS with Security Static WEP and Web-Auth	Checking for the Authentication of the clients when connected to a WLAN in which Static WEP and Web-Auth is enabled. \u0007	Passed	
WLJ87IIS_REG_131	Authentication of Win 7 laptop with Security Dot1x and Web-Auth	Checking for the Authentication of the clients when connected to a WLAN in which Static WEP and Web-Auth is enabled. \u0007	Passed	
WLJ87IIS_REG_132	Authentication of Android client with Security Static WEP+DOT1X and Web-Auth	Checking for the Authentication of the client when connected to a WLAN in which Static WEP+Dot1x and Web-Auth is enabled. \u0007	Passed	
WLJ87IIS_REG_133	Authentication of Window 10 client with Security Static WEP+DOT1X and Web-Auth	Checking for the Authentication of the client when connected to a WLAN in which Static WEP+Dot1x and Web-Auth is enabled. \u0007	Passed	
WLJ87IIS_REG_134	Authentication of client(Apple Mac Book) with Security Static WEP+DOT1X and Web-Auth	Checking for the Authentication of the client when connected to a WLAN in which Static WEP+Dot1x and Web-Auth is enabled. \u0007	Passed	
WLJ87IIS_REG_135	Authentication of client(Apple Mac Book) with Security Static WEP and Web-Auth	Checking for the Authentication of the client when connected to a WLAN in which Static WEP and Web-Auth is enabled. \u0007	Passed	
WLJ87IIS_REG_136	Authentication of client(Apple Mac Book) with Security Dot1x and Web-Auth	Checking for the Authentication of the client when connected to a WLAN in which Dot1x and Web-Auth is enabled. \u0007	Passed	
WLJ87IIS_REG_137	Authentication of clients(Apple Mac Book & Win 7) with Security Dot1x and Web-Auth(Same SSID) .	Checking for the Authentication of the clients when connected to a WLAN in which Dot1x and Web-Auth is enabled. \u0007	Passed	
WLJ87IIS_REG_138	Authentication of clients(Apple Mac Book & Win 10) with Security Dot1x and Web-Auth(Same SSID)	Checking for the Authentication of the clients when connected to a WLAN in which Dot1x and Web-Auth is enabled. \u0007	Passed	
WLJ87IIS_REG_139	Authentication of clients(Apple Mac Book & Win 7) with Security Static WEP+Dot1x and Web-Authusing ISE	Checking for the Authentication of the clients when connected to a WLAN in which Static WEP+Dot1x and Web-Auth is enabled. \u0007	Passed	

WLJ87IIS_REG_140	Authentication of clients(Apple Mac Book & Win 10) with Security Static WEP+Dot1x and Web-Auth using ISE	Checking for the Authentication of the clients when connected to a WLAN in which Static WEP+Dot1x and Web-Auth is enabled. \u0007	Passed	
WLJ87IIS_REG_141	Authentication of clients(Apple Mac Book & Win 7) with Security Static WEP+Dot1x and Web-Auth using ISE	Checking for the Authentication of the clients when connected to a WLAN in which Static WEP+Dot1x and Web-Auth is enabled. \u0007	Passed	
WLJ87IIS_REG_142	Authentication of clients(Apple Mac Book & Win 10) with Security Dot1x using ISE and WebAuth	Checking for the Authentication of the clients when connected to a WLAN in which Dot1x and Web-Auth is enabled. \u0007	Passed	
WLJ87IIS_REG_143	Authentication of clients(Apple Mac Book & Win 7) with Security Dot1x using ISE and WebAuth	Checking for the Authentication of the clients when connected to a WLAN in which Dot1x and Web-Auth is enabled. \u0007	Passed	
WLJ87IIS_REG_144	Authentication of clients(Apple Mac Book & Win 10) with Security Dot1x using ISE and WebAuth	Checking for the Authentication of the clients when connected to a WLAN in which Dot1x and Web-Auth is enabled. \u0007	Passed	
WLJ87S_Reg_203	Authentication of Android client with Security Dot1x and Web-Auth	Checking for the Authentication of the client when connected to a WLAN in which Dot1x and Web-Auth is enabled	Passed	
WLJ87S_Reg_204	Authentication of window 10 client with Security Dot1x and Web-Auth	Checking for the Authentication of the client when connected to a WLAN in which Dot1x and Web-Auth is enabled	Passed	
WLJ87S_Reg_205	Authentication of Android client with Security Static WEP and Web-Auth	Checking for the Authentication of the client when connected to a WLAN in which Static WEP and Web-Auth is enabled	Passed	
WLJ87S_Reg_206	Authentication of Window 10 client with Security Static WEP and Web-Auth	Checking for the Authentication of the client when connected to a WLAN in which Static WEP and Web-Auth is enabled	Passed	
WLJ87S_Reg_207	Authentication of clients Win 7 laptop with Security Static WEP and Web-Auth	Checking for the Authentication of the clients when connected to a WLAN in which Static WEP and Web-Auth is enabled. \u0007	Passed	
WLJ87S_Reg_208	Authentication of clients iOS with Security Static WEP and Web-Auth	Checking for the Authentication of the clients when connected to a WLAN in which Static WEP and Web-Auth is enabled. \u0007	Passed	

WLJ87S_Reg_209	Authentication of Win 7 laptop with Security Dot1x and Web-Auth	Checking for the Authentication of the clients when connected to a WLAN in which Static WEP and Web-Auth is enabled. \u0007	Passed	
WLJ87S_Reg_210	Authentication of Android client with Security Static WEP+DOT1X and Web-Auth	Checking for the Authentication of the client when connected to a WLAN in which Static WEP+Dot1x and Web-Auth is enabled. \u0007	Passed	
WLJ87S_Reg_211	Authentication of Window 10 client with Security Static WEP+DOT1X and Web-Auth	Checking for the Authentication of the client when connected to a WLAN in which Static WEP+Dot1x and Web-Auth is enabled. \u0007	Passed	
WLJ87S_Reg_212	Authentication of client(Apple Mac Book) with Security Static WEP+DOT1X and Web-Auth	Checking for the Authentication of the client when connected to a WLAN in which Static WEP+Dot1x and Web-Auth is enabled. \u0007	Passed	
WLJ87S_Reg_213	Authentication of client(Apple Mac Book) with Security Static WEP and Web-Auth	Checking for the Authentication of the client when connected to a WLAN in which Static WEP and Web-Auth is enabled. \u0007	Passed	
WLJ87S_Reg_214	Authentication of client(Apple Mac Book) with Security Dot1x and Web-Auth	Checking for the Authentication of the client when connected to a WLAN in which Dot1x and Web-Auth is enabled. \u0007	Passed	
WLJ87S_Reg_215	Authentication of clients(Apple Mac Book & Win 7) with Security Dot1x and Web-Auth(Same SSID) .	Checking for the Authentication of the clients when connected to a WLAN in which Dot1x and Web-Auth is enabled. \u0007	Passed	
WLJ87S_Reg_216	Authentication of clients(Apple Mac Book & Win 10) with Security Dot1x and Web-Auth(Same SSID)	Checking for the Authentication of the clients when connected to a WLAN in which Dot1x and Web-Auth is enabled. \u0007	Passed	
WLJ87S_Reg_217	Authentication of clients(Apple Mac Book & Win 7) with Security Static WEP+Dot1x and Web-Authusing ISE	Checking for the Authentication of the clients when connected to a WLAN in which Static WEP+Dot1x and Web-Auth is enabled. \u0007	Passed	
WLJ87S_Reg_218	Authentication of clients(Apple Mac Book & Win 10) with Security Static WEP+Dot1x and Web-Authusing ISE	Checking for the Authentication of the clients when connected to a WLAN in which Static WEP+Dot1x and Web-Auth is enabled. \u0007	Passed	
WLJ87S_Reg_219	Authentication of clients(Apple Mac Book & Win 7) with Security Static WEP+Dot1x and Web-Authusing ISE	Checking for the Authentication of the clients when connected to a WLAN in which Static WEP+Dot1x and Web-Auth is enabled. \u0007	Passed	

WLJ87S_Reg_220	Authentication of clients(Apple Mac Book & Win 10) with Security Dot1x using ISE and WebAuth	Checking for the Authentication of the clients when connected to a WLAN in which Dot1x and Web-Auth is enabled. \u0007	Passed	
WLJ87S_Reg_221	Authentication of clients(Apple Mac Book & Win 7) with Security Dot1x using ISE and WebAuth	Checking for the Authentication of the clients when connected to a WLAN in which Dot1x and Web-Auth is enabled. \u0007	Passed	
WLJ87S_Reg_222	Authentication of clients(Apple Mac Book & Win 10) with Security Dot1x using ISE and WebAuth	Checking for the Authentication of the clients when connected to a WLAN in which Dot1x and Web-Auth is enabled. \u0007	Passed	

Autonomous AP

Logical ID	Title	Description	Status	Defect ID
WLJ87IIS_REG_145	Client association with no security	To check whether clients gets associated or not Autonomous AP with Open security.	Passed	
WLJ87IIS_REG_146	Client association with WEP security	To check whether clients gets associated or not Autonomous AP with WEP security.	Passed	
WLJ87IIS_REG_147	Client association with WPA2+PSK	To check whether clients gets associated or not Autonomous AP with WPA2+PSK security.	Passed	
WLJ87IIS_REG_148	Client association with 802.11x	To check whether clients gets associated or not Autonomous AP with 802.11x security.	Passed	
WLJ87IIS_REG_149	Checking the traffic flow between two wireless clients	To Traffic flow between two wireless clients	Passed	
WLJ87IIS_REG_150	Checking the Trap logs for connected client	To verify the Trap Logs for connected client	Passed	
WLJ87S_Reg_223	Client association with no security	To check whether clients gets associated or not Autonomous AP with Open security.	Passed	

WLJ87S_Reg_224	Client association with WEP security	To check whether clients gets associated or not Autonomous AP with WEP security.	Passed	
WLJ87S_Reg_225	Client association with WPA2+PSK	To check whether clients gets associated or not Autonomous AP with WPA2+PSK security.	Passed	
WLJ87S_Reg_226	Client association with 802.11x	To check whether clients gets associated or not Autonomous AP with 802.11x security.	Passed	
WLJ87S_Reg_227	Checking the traffic flow between two wireless clients	To Traffic flow between two wireless clients	Passed	
WLJ87S_Reg_228	Checking the Trap logs for connected client	To verify the Trap Logs for connected client	Passed	

Flex Video stream

Logical ID	Title	Description	Status	Defect ID
WLJ87IIS_REG_151	MC2UC traffic to local-switching client	To verify that the local-switching client subscribed to videostreaming receives MC2UC traffic	Passed	
WLJ87IIS_REG_152	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	
WLJ87IIS_REG_153	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	
WLJ87IIS_REG_154	Multiple LS clients in same vlan, same wlan, receiving MC2UC traffic	To verify whether the multiple local-switching clients receives MC2UC traffic when subscribed to videostream	Passed	

WLJ87IIS_REG_155	Client disassociates when receiving MC2UC traffic	To verify whether AP stops sending traffic when client disassociates	Passed	
WLJ87IIS_REG_156	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	
WLJ87IIS_REG_157	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	
WLJ87IIS_REG_158	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	
WLJ87IIS_REG_159	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	
WLJ87IIS_REG_160	Flex AP reboot in connected mode when Flex LS client receiving MC2UC traffic	To verify whether client reassociates and receives MC2UC traffic when flex AP is rebooted in connected mode.	Passed	
WLJ87IIS_REG_161	Videstream config sync for LS WLAN in HA setup	To verify whether the videostreaming config for LS WLAN has been synced between the Active and Standby in HA setup	Passed	
WLJ87IIS_REG_162	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	

WLJ87S_Reg_229	MC2UC traffic to local-switching client	To verify that the local-switching client subscribed to videostreaming receives MC2UC traffic	Passed	
WLJ87S_Reg_230	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	
WLJ87S_Reg_231	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	
WLJ87S_Reg_232	Multiple LS clients in same vlan, same wlan, receiving MC2UC traffic	To verify whether the multiple local-switching clients receives MC2UC traffic when subscribed to videostream	Passed	
WLJ87S_Reg_233	Client disassociates when receiving MC2UC traffic	To verify whether AP stops sending traffic when client disassociates	Passed	
WLJ87S_Reg_234	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	
WLJ87S_Reg_235	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	
WLJ87S_Reg_236	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	

WLJ87S_Reg_237	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	
WLJ87S_Reg_238	Flex AP reboot in connected mode when Flex LS client receiving MC2UC traffic	To verify whether client reassociates and receives MC2UC traffic when flex AP is rebooted in connected mode.	Passed	
WLJ87S_Reg_239	Videstream config sync for LS WLAN in HA setup	To verify whether the videostreaming config for LS WLAN has been synced between the Active and Standby in HA setup	Passed	
WLJ87S_Reg_240	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	

Home Page

Logical ID	Title	Description	Status	Defect ID
WLJ87IIS_REG_163	Android/MAC/Windows/iOS client connectivity with Japanese SSID and L2 None security.	Verify Android/ MAC/ Windows/iOS client connectivity with japanese SSID.	Passed	
WLJ87IIS_REG_164	Android/MAC/Windows/iOS client connectivity with Japanese SSID and L2 WPA+WPA2 security.	Validate theAndroid/ MAC/ Windows/iOS client connectivity with japanese SSID and L2 WPA+WPA2 security.	Passed	
WLJ87IIS_REG_165	Android/MAC/Windows/iOS client connectivity with Japanese SSID and L2 802.1x security.	Validate the Android/ MAC/ Windows/iOS client connectivity with japanese SSID and L2 802.1X security.	Passed	
WLJ87IIS_REG_166	AP Capability connection rates and channel bandwidth	To check whether the AP Capability and bandwidth showing correctly or no	Passed	
WLJ87IIS_REG_167	Client Capability by max protocol and spatial streams	To verify the client max protocol and spatial streams	Passed	

WLJ87IIS_REG_168	Client distribution on top neighbor Aps	To check the whether client distribution on top neighbor Aps showing properly or not	Passed	
WLJ87IIS_REG_169	Checking the functions of all dashlets in AP performance page for AP's (1850 & 1830)	To check whether all dashlets shows details correctly or not in AP performace page for AP's (1850 & 1830).	Passed	
WLJ87IIS_REG_170	Checking the AP's (1850 & 1830) in Access point page of WLC's (5520, 7500 & vWLC) and checking the client association count in respective band.	To check whether AP's details are shown or not in Access point page of WLC's and also check whether client association count is shown properly in respective radios.	Passed	
WLJ87IIS_REG_171	Checking the AP's (1850 & 1830) in Access point page of WLC's (2500, 8500, 5500 & WiSM2) and checking the client association count in respective band.	To check whether AP's details are shown or not in Access point page of WLC's and also check whether client association count is shown properly in respective radios.	Passed	
WLJ87IIS_REG_172	Checking the Access point view page for each AP's(1850 & 1830) in Access point page of RF Dashboard in 5520 WLC.	To check whether Access point view page is displayed or not when clicking the AP name in Access point page of RF Dashboard.	Passed	
WLJ87IIS_REG_173	Performing AP's(1850 & 1830) reboot in Access point page of RF dashboard in 5520 WLC.	To check whether restart function works or not in Access point page for AP's (1850 & 1830).	Passed	
WLJ87IIS_REG_174	Configuring the rogue Details in WLC if Multiple Clients is been associated with AP	To find the rogue details in a controller	Passed	
WLJ87IIS_REG_175	Checking AP rogue entry for difference classification	To Manually classify the rogue AP Details in WLC	Passed	
WLJ87IIS_REG_176	Manually Removing the Rogue Entry from the rogue list if Multiple Clients is connected with an AP.	To manually remove the rogue Entry from the rogue list.	Passed	
WLJ87IIS_REG_177	Checking the rule defined for identifying the Rogue AP	To Verify the rogue AP rules are configured Properly or not	Passed	
WLJ87S_Reg_251	Android client connectivity with Japanese SSID and L2 None security.	Verify Android client connectivity with japanese SSID.	Passed	
WLJ87S_Reg_252	Mac client connectivity with Japanese SSID and L2 None security.	Verify Mac client connectivity with japanese SSID.	Passed	
WLJ87S_Reg_253	Windows client connectivity with Japanese SSID and L2 None security.	Validate the Mac client connectivity with japanese SSID.	Passed	

WLJ87S_Reg_254	IOS client connectivity with Japanese SSID and L2 None security.	Verify the IOS client connectivity with japanese SSID.	Passed	
WLJ87S_Reg_255	Android client connectivity with Japanese SSID and L2 WPA+WPA2 security.	Validate the Android client connectivity with japanese SSID and L2 WPA+WPA2 security.	Passed	
WLJ87S_Reg_256	Mac client connectivity with Japanese SSID and L2 WPA+WPA2 security.	Validate the Mac client connectivity with japanese SSID and L2 WPA+WPA2 security.	Passed	
WLJ87S_Reg_257	IOS client connectivity with Japanese SSID and L2 WPA+WPA2 security.	Verify the IOS client connectivity with japanese SSID and L2 WPA+WPA2 security.	Passed	
WLJ87S_Reg_258	Windows client connectivity with Japanese SSID and L2 WPA+WPA2 security.	Verify the Windows client connectivity with japanese SSID and L2 WPA+WPA2 security.	Passed	
WLJ87S_Reg_259	Android client connectivity with Japanese SSID and L2 802.1x security.	Validate the Android client connectivity with japanese SSID and L2 802.1X security.	Passed	
WLJ87S_Reg_260	IOS client connectivity with Japanese SSID and L2 802.1x security.	Validate the IOS client connectivity with japanese SSID and L2 802.1X security.	Passed	
WLJ87S_Reg_261	Mac client connectivity with Japanese SSID and L2 802.1x security.	Validate the Mac client connectivity with japanese SSID and L2 802.1X security.	Passed	
WLJ87S_Reg_262	Windows client connectivity with Japanese SSID and L2 802.1x security.	Validate the Windows client connectivity with japanese SSID and L2 802.1X security.	Passed	
WLJ87S_Reg_263	AP Capability connection rates and channel bandwidth	To check whether the AP Capability and bandwidth showing correctly or no	Passed	
WLJ87S_Reg_264	Client Capability by max protocol and spatial streams	To verify the client max protocol and spatial streams	Passed	
WLJ87S_Reg_265	Client distribution on top neighbor Aps	To check the whether client distribution on top neighbor Aps showing properly or not	Passed	
WLJ87S_Reg_266	Checking the functions of all dashlets in AP performance page for AP's (1850 & 1830)	To check whether all dashlets shows details correctly or not in AP performance page for AP's (1850 & 1830).	Passed	
WLJ87S_Reg_267	Checking the AP's (1850 & 1830) in Access point page of WLC's (5520, 7500 & vWLC) and checking the client association count in respective band.	To check whether AP's details are shown or not in Access point page of WLC's and also check whether client association count is shown properly in respective radios.	Passed	

WLJ87S_Reg_268	Checking the AP's (1850 & 1830) in Access point page of WLC's (2500, 8500, 5500 & WiSM2) and checking the client association count in respective band.	To check whether AP's details are shown or not in Access point page of WLC's and also check whether client association count is shown properly in respective radios.	Passed	
WLJ87S_Reg_269	Checking the Access point view page for each AP's(1850 & 1830) in Access point page of RF Dashboard in 5520 WLC.	To check whether Access point view page is displayed or not when clicking the AP name in Access point page of RF Dashboard.	Passed	
WLJ87S_Reg_270	Performing AP's(1850 & 1830) reboot in Access point page of RF dashboard in 5520 WLC.	To check whether restart function works or not in Access point page for AP's (1850 & 1830).	Passed	
WLJ87S_Reg_271	Configuring the rogue Details in WLC if Multiple Clients is been associated with AP	To find the rogue details in a controller	Passed	
WLJ87S_Reg_272	Checking AP rogue entry for difference classification	To Manually classify the rogue AP Details in WLC	Passed	
WLJ87S_Reg_273	Manually Removing the Rogue Entry from the rogue list if Multiple Clients is connected with an AP.	To manually remove the rogue Entry from the rogue list.	Passed	
WLJ87S_Reg_274	Checking the rule defined for identifying the Rogue AP	To Verify the rogue AP rules are configured Properly or not	Passed	

MFP support

Logical ID	Title	Description	Status	Defect ID
WLJ87IIS_MFP_01	Verifying if MFP can be enabled and disabled via cli on WLC	To verify if MFP can be enabled ,disabled via WLC CLI and check if the MFP is applied globally or not.	Passed	
WLJ87IIS_MFP_02	Checking if IMIC IE value in MFP is appended in 3800 AP	To check if the IMIC IE value in MFP is appended in 3800 AP or not after enabling MFP globally.	Passed	
WLJ87IIS_MFP_03	Checking if IMIC IE value in MFP is appended in 2800 AP	To check if the IMIC IE value in MFP is appended in 2800 AP or not after enabling MFP globally.	Passed	

WLJ87IIS_MFP_04	Connecting a CCXv5 Window client to a 3800 AP with MFP option as Required .	To connect a window CCxv5 client to a 3800 AP with MFP option as required and check the IMIC IE value in MFP .	Passed	
WLJ87IIS_MFP_05	Connecting a Mac OS CCXv5 client to a 3800 AP with MFP option as Required .	To connect a Mac OS CCxv5 client to a 3800 AP with MFP option as required and check the IMIC IE value in MFP.	Passed	
WLJ87IIS_MFP_06	Connecting a CCXv5 Window client to a 2800 AP with MFP option as Required .	To connect a window CCxv5 client to a 2800 AP with MFP option as required and check the IMIC IE value in MFP .	Passed	
WLJ87IIS_MFP_07	Connecting a Mac OS CCXv5 client to a 2800 AP with MFP option as Required .	To connect a Mac OS CCxv5 client to a 2800 AP with MFP option as required and check the IMIC IE value in MFP .	Passed	
WLJ87IIS_MFP_08	Pushing MFP configuration from PI and connecting a client .	To connect a client to the 2800 AP where the template is pushed from PI and check if the IMIC IE value is appened or not.	Passed	
WLJ87IIS_MFP_09	Exporting and Importing configuration of MFP	To exporting and importing configuration of MFP and check if the configuration remains the same after import and export.	Passed	

Flexconnect IOS Parity: Ethernet fallback

Logical ID	Title	Description	Status	Defect ID
------------	-------	-------------	--------	-----------

WLJ87IIS_REG_396	Enable/Disable Ethernet fall-back in WLC UI	To verify whether Ethernet fall-back is enable/disable successfully or not from WLC UI	Passed	
WLJ87IIS_REG_397	Enable/Disable Ethernet fall-back in WLC CLI	To verify whether Ethernet fall-back is enable/disable successfully or not from WLC CLI	Passed	
WLJ87IIS_REG_398	Disabling the radio 802.11a b after POE remove	To verify whether Radios getting disable or not after removing the POE connection to AP	Passed	
WLJ87IIS_REG_399	Checking the disabled Radios 'a' & 'b' details after POE connect	To check whether the 802.11 radios comes Up/Down as configured before once POE connected to AP	Passed	
WLJ87IIS_REG_400	Checking Disabled 802.11a and enable 802.11b details after POE remove	To verify whether Radios getting disable or not after removing the POE connection in AP	Passed	
WLJ87IIS_REG_401	Checking Disabled 802.11a and enable 802.11b details after POE connect	To check whether the 802.11 radios comes Up/Down as configured before once POE connected to AP	Passed	
WLJ87IIS_REG_402	Checking enabled 802.11a and disabled 802.11b details after POE remove	To verify whether Radios getting disable or not after removing the POE connection in AP	Passed	
WLJ87IIS_REG_403	Checking enabled 802.11a and disabled 802.11b details after POE connect	To check whether the 802.11 radios comes Up/Down as configured before once POE connected to AP	Passed	

WLJ87IIS_REG_404	Configuring the fall-back details in Read-only mode from UI	To verify whether Ethernet fall-back details are possible to configure or not for read only users	Passed	
WLJ87IIS_REG_405	Configuring the fall-back details in read only mode from Cli	To verify whether Ethernet fall-back details are possible to configure or not from CLI	Passed	
WLJ87IIS_REG_406	Verifying the fall back details from CLI for read only	To verify whether Ethernet fall-back details are showing or not	Passed	
WLJ87IIS_REG_407	Reloading the AP after Ethernet fall-back configuring	To verify whether Ethernet fall-back details are showing properly or not after reload.	Passed	
WLJ87IIS_REG_408	Upgrading the Ap after Ethernet fall-back configuring	To verify whether Ethernet fall-back details are showing properly or not after Upgrade the image	Passed	
WLJ87IIS_REG_409	Checking the roaming scenarios after client connect	To verify whether roaming happening not after Ethernet fall-back	Passed	

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

Logical ID	Title	Description	Status	Defect Id
WLJ87IIS_REG_410	Configuring the downstream and upstream value as "0" per User	To verify whether downstream and upstream values are no restrictions for configured values as "0" per User or not	Passed	
WLJ87IIS_REG_411	Configuring the downstream and upstream value as "0" per SSID.	To verify whether downstream and upstream values are no restrictions for configured values as "0" per SSID or not	Passed	

Flexconnect IOS Parity: AAA Override of VLAN Name template

WLJ87IIS_REG_412	Configuring the downstream and upstream value as certain range per User	To verify whether downstream and upstream values access with restrictions for configured values as per User or not	Passed	
WLJ87IIS_REG_413	Configuring the downstream and upstream value as certain range per SSID	To verify whether downstream and upstream values access with restrictions for configured values as per SSID	Passed	
WLJ87IIS_REG_414	Resetting the WLC after configure the Client and SSID values	To verify whether Client and SSID values are proper or not	Passed	
WLJ87IIS_REG_415	Clearing the values after AAA override enable	To verify whether values are clearing or not	Passed	
WLJ87IIS_REG_416	Checking the roaming scenario	To verify whether after client roam between controllers client accessing proper bandwidth or not	Passed	
WLJ87IIS_REG_417	Checking the bandwidth for client and SSID in standalone mode	To verify whether clients are getting proper connection for standalone or nor	Passed	

Flexconnect IOS Parity: AAA Override of VLAN Name template

Logical ID	Title	Description	Status	Defect Id
WLJ87IIS_REG_418	Creating the VLAN Template	To verify whether VLAN Template is creating or not	Passed	
WLJ87IIS_REG_419	Assigning the flexconnect VLAN to Flexconnect group	To verify whether VLAN Template is assigning successfully or not to Flexconnect group	Passed	

WLJ87IIS_REG_420	Checking the AAA override for VLAN name id	To verify whether AAA overriding happening or not with VLAN name	Passed	
WLJ87IIS_REG_421	Configuring VLAN name id for AAA override at the time of VLAN support in disable state	To verify whether AAA override is happening or not when VLAN support is in disable state	Passed	
WLJ87IIS_REG_422	After configure the WLAN-VLAN support checking the details	To verify whether WLAN-VLAN details are applying or not after configure and disable the VLAN support	Passed	
WLJ87IIS_REG_423	Checking the details in AP after VLAN name id Exchange	To verify details are showing in AP cli or not	Passed	
WLJ87IIS_REG_424	Checking the debug details at the time of VLAN name id details	To verify whether details are showing successfully or not at the time of VLAN name id exchange	Passed	
WLJ87IIS_REG_425	Rebooting the WLC after AAA override with VLAN name ID	To verify whether Client are getting AAA override details or not after reboot	Passed	
WLJ87IIS_REG_426	Checking the client details at the time of standalone mode	To verify whether clients are serving or not in standalone mode	Passed	
WLJ87IIS_REG_427	Checking the details in Roaming.	To verify whether Roaming is happening with AAA override for VLAN name id	Passed	

Flexconnect IOS Parity: DHCP Option 60 Support

Logical ID	Title	Description	Status	Defect ID
------------	-------	-------------	--------	-----------

WLJ87IIS_REG_428	Configuring the DHCP Option 60 in router	To verify whether DHCP Option 60 is configuring successfully or not	Passed	
WLJ87IIS_REG_429	Checking DHCP option 63 is matching with AP	To verify whether DHCP Option 60 details are matching with AP or not	Passed	
WLJ87IIS_REG_430	Connecting the android client without adding VCI	To verify whether android is getting the IP address or not	Passed	
WLJ87IIS_REG_431	Connecting the IOS client without adding VCI	To verify whether IOS client is getting the IP address or not	Passed	
WLJ87IIS_REG_432	Connecting the Japanese client without adding VCI	To verify whether Japanese is getting the IP address or not	Passed	

AP Support (1815I/1815W/1562)

Logical ID	Title	Description	Status	Defect ID
WLJ87S_Reg_134	Rebooting the AP with primary controller given in High Availability	To reboot the AP by giving the primary controller IP using high availability and check if the AP joins the primary controller	Passed	
WLJ87S_Reg_135	Connecting a Window iOS client to the 1815I & 1815W AP	To Connect a window client to the AP and check if the client gets connected to the AP without any errors.	Passed	
WLJ87S_Reg_136	Connecting a Android client to the 1815I & 1815W AP	To Connect a Android client to the AP and check if the client gets connected to the AP without any errors.	Passed	
WLJ87S_Reg_137	Connecting a IOS client to the 1815I & 1815W AP	To Connect a IOS client to the AP and check if the client gets connected to the AP without any errors.	Passed	
WLJ87S_Reg_138	Connecting a MAC client to the 1815I & 1815W AP	To Connect a MAC client to the AP and check if the client gets connected to the AP without any errors.	Passed	

WLJ87S_Reg_139	AP fail-over priority with critical	To check AP fail-over priority with critical and check if the AP gets connected to the next controller .	Passed	
WLJ87S_Reg_140	Re-association of client to the AP after reboot	To verify if the client gets re-associated to the to the AP .	Passed	
WLJ87S_Reg_141	Performing Intra controller roaming of Windows J OS client	To check whether intra controller roaming of windows clients works properly or not in WLC	Passed	
WLJ87S_Reg_142	Performing Intra controller roaming of Android client	To check whether intra controller roaming of Android clients works properly or not	Passed	
WLJ87S_Reg_143	Performing Intra controller roaming of IOS client	To check whether intra controller roaming of IOS clients works properly or not in WLC	Passed	
WLJ87S_Reg_144	Performing Intra controller roaming of Mac OS client	To check whether intra controller roaming of MacOS clients works properly or not	Passed	
WLJ87S_Reg_145	Performing Inter controller roaming of Windows J OS client	To check whether inter controller roaming of windows clients works properly or not	Passed	
WLJ87S_Reg_146	Performing Inter controller roaming of Android client	To check whether inter controller roaming of Android clients works properly or not	Passed	
WLJ87S_Reg_147	Performing Inter controller roaming of IOS client	To check whether inter controller roaming of IOS clients works properly or not	Passed	
WLJ87S_Reg_148	Performing Inter controller roaming of Mac OS client	To check whether inter controller roaming of Mac OS clients works properly or not	Passed	
WLJ87S_Reg_149	Adding two 1815 AP in the AP group and connecting a client to the AP with specific WLAN	To Add two 1815 AP in AP group and map a WLAN to group and connect a client to the WLAN and check the client connectivity	Passed	
WLJ87S_Reg_150	Adding 1815I & 1815W AP in the FlexConnect group and connecting a client to the AP with specific WLAN	To Add 1815 Ap to FlexConnect group and check if the AP gets added to the AP group	Passed	

WLJ87S_Reg_151	Checking if FlexConnect Local Switching and Local Auth works properly	To Check if FlexConnect Local Switching and Local Auth works in 1815 Ap and check if the clients gets locally authenticated and switched locally	Passed	
WLJ87S_Reg_152	Checking Local Authentication done by another AP in case of AP fail-over	To verify whether Local Authentication is done by another AP in flex group in case of AP fail-over	Passed	
WLJ87S_Reg_153	Checking the AP fallback once primary controller comes Up	To verify AP is joining to primary controller once it come UP	Passed	
WLJ87S_Reg_154	Rebooting the AP with primary controller given in High Availability	To reboot the AP by giving the primary controller IP using high availability and check if the AP joins the primary controller	Passed	
WLJ87S_Reg_155	Connecting a Window iOS client to the 1562 AP	To Connect a window client to the AP and check if the client gets connected to the AP without any errors.	Passed	
WLJ87S_Reg_156	Connecting a Android client to the 1562 AP	To Connect a Android client to the AP and check if the client gets connected to the AP without any errors.	Passed	
WLJ87S_Reg_157	Connecting a IOS client to the 1562 AP	To Connect a IOS client to the AP and check if the client gets connected to the AP without any errors.	Passed	
WLJ87S_Reg_158	Connecting a MAC client to the 1562 AP	To Connect a MAC client to the AP and check if the client gets connected to the AP without any errors.	Passed	
WLJ87S_Reg_159	AP fail-over priority with critical	To check AP fail-over priority with critical and check if the AP gets connected to the next controller .	Passed	
WLJ87S_Reg_160	Re-association of client to the AP after reboot	To verify if the client gets re-associated to the to the AP .	Passed	
WLJ87S_Reg_161	Performing Intra controller roaming of Windows J OS client	To check whether intra controller roaming of windows clients works properly or not in WLC	Passed	

WLJ87S_Reg_162	Performing Intra controller roaming of Android client	To check whether intra controller roaming of Android clients works properly or not	Passed	
WLJ87S_Reg_163	Performing Intra controller roaming of IOS client	To check whether intra controller roaming of IOS clients works properly or not in WLC	Passed	
WLJ87S_Reg_164	Performing Intra controller roaming of Mac OS client	To check whether intra controller roaming of MacOS clients works properly or not	Passed	
WLJ87S_Reg_165	Performing Inter controller roaming of Windows J OS client	To check whether inter controller roaming of windows clients works properly or not	Passed	
WLJ87S_Reg_166	Performing Inter controller roaming of Android client	To check whether inter controller roaming of Android clients works properly or not	Passed	
WLJ87S_Reg_167	Performing Inter controller roaming of IOS client	To check whether inter controller roaming of IOS clients works properly or not	Passed	
WLJ87S_Reg_168	Performing Inter controller roaming of Mac OS client	To check whether inter controller roaming of Mac OS clients works properly or not	Passed	
WLJ87S_Reg_169	Adding two 1562 AP in the AP group and connecting a client to the AP with specific WLAN	To Add two 1562 AP in AP group and map a WLAN to group and connect a client to the WLAN and check the client connectivity	Passed	
WLJ87S_Reg_170	Adding 1562 AP in the FlexConnect group and connecting a client to the AP with specific WLAN	To Add 1562 Ap to FlexConnect group and check if the AP gets added to the AP group	Passed	
WLJ87S_Reg_171	Checking if FlexConnect Local Switching and Local Auth works properly	To Check if FlexConnect Local Switching and Local Auth works in 1562 Ap and check if the clients gets locally authenticated and switched locally	Passed	

AP 1562 RF Support

Logical ID	Title	Description	Status	Defect ID
------------	-------	-------------	--------	-----------

WLJ87S_Reg_66	Connecting a Japanese OS client to 5GHz radio policy and check the client connectivity	To connect a Japanese OS client to 5GHz radio policy and check if the clients gets connected or not	Passed	
WLJ87S_Reg_67	Connecting a Android client to 5GHz radio policy and check the client connectivity	To connect a Android client to 5GHz radio policy and check if the clients gets connected	Passed	
WLJ87S_Reg_68	Connecting a IOS client to 5GHz radio policy and check the client connectivity	To connect a IOS client to 5GHz radio policy and check if the clients gets connected or not	Passed	
WLJ87S_Reg_69	Connecting a Mac OS client to 5GHz radio policy and check the client connectivity	To connect a Mac OS client to 5GHz radio policy and check if the clients gets connected or not	Passed	
WLJ87S_Reg_70	Connecting a Japanese OS client to 2.4 GHz radio policy and check the client connectivity	To connect a Japanese OS client to 2.4 GHz radio policy and check if the clients gets connected or not	Passed	
WLJ87S_Reg_71	Connecting a Android client to 2.4 GHz radio policy and check the client connectivity	To connect a Android client to 2.4 GHz radio policy and check if the clients gets connected or not	Passed	
WLJ87S_Reg_72	Connecting a IOS client to 2.4 GHz radio policy and check the client connectivity	To connect a IOS client to 2.4 GHz radio policy and check if the clients gets connected or not	Passed	
WLJ87S_Reg_73	Connecting a Mac OS client to 2.4 GHz radio policy and check the client connectivity	To connect a Mac OS client to 2.4 GHz radio policy and check if the clients gets connected or not	Passed	
WLJ87S_Reg_74	Configuring DCA Channel globally and AP specific and connecting a client to it.	To configure DCA Channel globally and AP specific and connecting a client to it and check the details of the client.	Passed	
WLJ87S_Reg_75	Enabling Out Of Box in Rf profile	To enable Out Of Box in RF profile and check if the newly added 1562 AP gets added to the Out-Of-Box AP group	Passed	
WLJ87S_Reg_76	Checking the Client traps and check if the Traps available for the particular number of client given .	To Check if the traps for the given number of client are alone shown and remaining traps are not shown	Passed	

WLJ87S_Reg_77	Performing Client connectivity check giving Maximum Client as 3 and Connecting 5 client	To perform Maximum client check by giving maximum client as 3 and connecting 5 client	Passed	
WLJ87S_Reg_78	Performing upload and download configuration after making RF configuration in 1562 AP	To perform upload and download configuration and check if the RF configuration made on the AP remains the same	Passed	
WLJ87S_Reg_79	Performing HA after configuring RF profile in the primary and check if the profile gets mapped to secondary.	To Perform HA after configuring RF profile in the primary and check if the configuration is reflected in the secondary	Passed	
WLJ87S_Reg_80	Creating a 802.11b/g profile RF profile and giving the data rates to minimum and check the speed of the client	To create a 802.11b/g profile and give data rate to minimum and check the client speed .	Passed	

SSID Filtering

Logical ID	Title	Description	Status	Defect ID
WLJ87S_Reg_275	Configure Maximum SSID on WLC and check if all show up for selection on SSID list	To verify whether Maximum set SSID on WLC which is displayed on the SSID exclusion list.	Passed	
WLJ87S_Reg_276	Deleting some SSID on WLC and check if it is also show up for selection on SSID list	To Delete some SSID on WLC and check if it is also show up for selection on SSID list	Passed	
WLJ87S_Reg_277	Exclusion list for SSID from multiple WLC	To verify whether Multiple WLC SSID Filtering Parameters is configurable	Passed	
WLJ87S_Reg_278	Disabling "Enable SSID filtering" check box and verify that MAC filtering stopped or not	To Disable "Enable SSID filtering check" box and verify that MAC filtering stopped or not	Passed	
WLJ87S_Reg_279	Client MAC on allowed list but SSID excluded	To verify whether Client MAC allowed but SSID excluded will enable client tracking	Passed	

EAP Types

Logical ID	Title	Description	Status	Defect ID
WLJ87S_Reg_280	Verifying client connectivity with LEAP option with WPA2+dot1x security	Validate the client connectivity WPA2-dot1x security with LEAP	Passed	
WLJ87S_Reg_281	Verifying client connectivity with LEAP option with dot1x security	Validate the client connectivity dot1x security with LEAP	Passed	
WLJ87S_Reg_282	Verifying client connectivity with PEAP option with WPA2 dot1x security	Validate the client connectivity WPA2-dot1x security with PEAP	Passed	
WLJ87S_Reg_283	Verifying client connectivity with PEAP option with dot1x security	Validate the client connectivity dot1x security with PEAP	Passed	
WLJ87S_Reg_284	Verifying client connectivity with EAP-FAST option with WPA2 dot1x security	Validate the client connectivity WPA2-dot1x security with EAP-FAST	Passed	
WLJ87S_Reg_285	Verifying client connectivity with EAP-FAST option with dot1x security	Validate the client connectivity dot1x security with EAP-FAST	Passed	
WLJ87S_Reg_286	Verifying client connectivity with EAP-TLS option with WPA2 dot1x security	Validate the client connectivity WPA2-dot1x security with EAP-TLS	Passed	
WLJ87S_Reg_287	Verifying client connectivity with EAP-TLS option with dot1x security	Validate the client connectivity dot1x security with EAP-TLS	Passed	
WLJ87S_Reg_288	Verifying client is able to connect LEAP option with WPA2+dot1x security and able to perform web authentication	Validate the client connectivity WPA2-dot1x security with LEAP	Passed	
WLJ87S_Reg_289	Verifying client is able to connect LEAP option with dot1x security and able to perform web authentication	Validate the client connectivity dot1x security with LEAP	Passed	

WLJ87S_Reg_290	Verifying client is able to connect PEAP option with WPA2+dot1x security and able to perform web authentication	Validate the client connectivity WPA2-dot1x security with PEAP	Passed	
WLJ87S_Reg_291	Verifying client is able to connect PEAP option with dot1x security and able to perform web authentication	Validate the client connectivity dot1x security with PEAP	Passed	
WLJ87S_Reg_292	Checking Local EAP profile template is pushing from PI to WLC	Verifying whether PI is able to push Local EAP profile template to WLC or not	Passed	
WLJ87S_Reg_293	Checking General-Local EAP template is pushing from PI to WLC	Verifying whether PI is able to push General-Local EAP template to WLC or not	Passed	
WLJ87S_Reg_294	Verifying WLC EAP configuration is reflecting same in PI	Verifying whether WLC is synchronizing in PI successfully and EAP configuration is reflection same in PI	Passed	

H-REAP Fault Tolerance

Logical ID	Title	Description	Status	Defect ID
WLJ87S_Reg_241	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	
WLJ87S_Reg_242	HREAP fault tolerance between connected and standalone AP-5 GHz	To verify whether the client associated to Flexconnect AP will get re-associated in case of fault tolerance	Passed	
WLJ87S_Reg_248	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	

WLJ87S_Reg_249	HREAP fault tolerance between connected and standalone AP-5 GHz	To verify whether the client associated to Flexconnect AP will get re-associated in case of fault tolerance	Passed	
WLJ87S_Reg_250	Verifying that radio status of ap in standalone	To Verify that radio status of ap in standalone	Passed	

Sensor Neighbor Info

Logical ID	Title	Description	Status	Defect ID
WLJ87S_Reg_295	Verifying AP neighbor count in WLC	To Verify whether AP neighbor count details shown properly or not in WLC after enabling sensor mode	Passed	
WLJ87S_Reg_296	Verifying AP in a particular AP group	To Verify AP Count Present In a particular group	Passed	
WLJ87S_Reg_297	Verifying sensor AP neighbor information	To verify sensor AP neighbor information	Passed	
WLJ87S_Reg_298	Verifying AP information in all AP group	To verify AP information in AP group	Passed	
WLJ87S_Reg_299	Verifying the neighbor AP information by reboot the AP.	To Verify the neighbor AP information by reboot the AP.	Passed	
WLJ87S_Reg_300	Verifying client is able to connect to AP in sensor mode	To verify whether client is able to connect to AP in sensor mode or not	Passed	
WLJ87S_Reg_301	Verifying client is able to connect to AP after changing from sensor mode to other mode	To Verify whether client is able to connect to AP after changing from sensor mode to other mode	Passed	

Flexconnect Mode Feature Parity with IOS APs - 1832/1852/2800/3800 based Aps

Logical ID	Title	Description	Status	Defect ID
WLJ87S_Reg_329	2802/3802I/3802E APs Connected to Standalone mode transition	To verify the 2802/3802I/3802E APs in flex mode moves to standalone mode when no WLC is detected.	Passed	

WLJ87S_Reg_330	Client connectivity to the flex AP - central switching	To verify the client connectivity with Central Switching in Connected mode.	Passed	
WLJ87S_Reg_331	Client connectivity to the flex AP - local switching	To verify the client connectivity with local Switching in Connected mode.	Passed	
WLJ87S_Reg_332	Central auth Client status when AP moves to standalone mode.	To verify whether central auth clients are retained after AP moves to standalone mode.	Passed	
WLJ87S_Reg_333	Central auth Client status when AP moves back to connected mode.	To verify the central auth client connectivity when AP moves back to connected mode.	Passed	
WLJ87S_Reg_334	Local auth Client status when AP moves to standalone mode.	To verify whether local auth clients are retained after AP moves to standalone mode.	Passed	
WLJ87S_Reg_335	Local auth Client status when AP moves back to connected mode.	To verify the local auth client connectivity when AP moves back to connected mode.	Passed	
WLJ87S_Reg_336	Client connectivity in standalone mode	To verify the client connectivity in Standalone mode.	Passed	
WLJ87S_Reg_337	Client connectivity to 802.11a radio	To verify the client connectivity to 802.11a radio	Passed	
WLJ87S_Reg_338	Client connectivity to 802.11b radio	To verify the client connectivity to 802.11b radio.	Passed	
WLJ87S_Reg_339	Client connectivity test with all wireless clients	To verify the client connectivity	Passed	
WLJ87S_Reg_340	Client statistics in AP and WLC.	To verify the client status in WLC and AP.	Passed	
WLJ87S_Reg_341	WLAN deletion in standalone mode.	To verify WLAN deletion in Standalone mode is not showing up when moves to connected mode.	Passed	

WLJ87S_Reg_342	Pre-image download check on Master AP.	To verify whether pre-image download is successful on the selected Master AP.	Passed	
WLJ87S_Reg_343	Efficient image upgrade for AP1852.	To verify the smart image upgrade for AP1852 in the Flexconnect group.	Passed	
WLJ87S_Reg_344	Pre-image download check by selecting two Master Aps	To verify pre-image download for two Master APs within the same Flexconnect group.	Passed	
WLJ87S_Reg_345	Debug command check for efficient image Upgrade.	To check the debug commands related to efficient image upgrade.	Passed	
WLJ87S_Reg_346	Slave AP image download from WLC when no pre-image download is triggered.	To verify whether Slave Aps are downloading image from WLC when there is no pre-image download.	Passed	
WLJ87S_Reg_347	Slave AP image download from Master AP when pre-image is triggered.	To verify the image download for Slave when pre-image download is triggered.	Passed	
WLJ87S_Reg_348	Image Upgrade configuration persistent across reboot.	To verify the image upgrade configuration such as Master, Slave, retry count are persistent across reboot of WLC.	Passed	
WLJ87S_Reg_349	Pre-image download to slave when slave is in standalone mode.	To verify whether pre-image download on Slave is triggered when Slave goes to Standalone mode.	Passed	
WLJ87S_Reg_350	Connected-Central auth local switching: non-native VLAN mapping to clients.	To verify whether Client acquires the ip address from the configured non-native VLAN for the WLAN	Passed	
WLJ87S_Reg_351	Connected-local auth local switching: non-native VLAN mapping to clients.	To verify whether Client acquires the ip address from the configured non-native VLAN for the WLAN	Passed	
WLJ87S_Reg_352	Connected-Local auth local switching: native VLAN mapping to clients.	To verify whether Client acquires the ip address from the configured native VLAN mapped for the WLAN	Passed	

WLJ87S_Reg_353	Connected mode- WLAN VLAN config and client connectivity	To verify whether client gets the ip address from the VLANs mapped to the WLANs	Passed	
WLJ87S_Reg_354	Standalone- central auth local switching: non-native VLAN map	To verify whether Client acquires the ip address from the configured non-native VLAN for the WLAN	Passed	
WLJ87S_Reg_355	Standalone-local auth local switching: non-native VLAN map	To verify whether Client acquires the ip address from the configured non-native VLAN for the WLAN	Passed	
WLJ87S_Reg_356	Standalone - central auth local switching : native VLAN map	To verify whether Client acquires the ip address from the configured native VLAN for the WLAN	Passed	
WLJ87S_Reg_357	Standalone- local auth local switching: native VLAN map	To verify whether Client acquires the ip address from the configured native VLAN mapped for the WLAN	Passed	
WLJ87S_Reg_358	Multiple WLAN-VLAN mapping and client connectivity in standalone mode.	To verify whether the clients get appropriate ip address from the VLAN mapped.	Passed	
WLJ87S_Reg_359	Standalone to connected mode with no config change	To verify the config when AP moves from standalone to connected mode with no config change.	Passed	
WLJ87S_Reg_360	Standalone to connected mode with WLAN specific config mismatch	To verify the config when AP moves from standalone to connected mode with WLAN specific config mismatch	Passed	
WLJ87S_Reg_361	HA: Standalone to connected mode with no config change	To verify the config in case of WLA HA	Passed	
WLJ87S_Reg_362	Standalone to connected with WLAN removed	To verify the AP status when WLAN removed in standalone mode.	Passed	
WLJ87S_Reg_363	Standalone to connected when VLAN is removed	To verify whether client gets ip address from new VLAN	Passed	

WLAN Security

Logical ID	Title	Description	Status	Defect ID
WLJ87S_Reg_372	Configuring with NONE security	To verify whether client with NONE security is configured in WLAN or not	Passed	
WLJ87S_Reg_373	Configuring with WPA+WPA2 security	To verify whether client with WPA+WPA2 security is connected or not	Passed	
WLJ87S_Reg_374	Configuring with 802.1X security	To verify whether client with 802.1x security is connecting or not	Passed	
WLJ87S_Reg_375	Configuring with Static WEP security	To verify whether client with Static WEP security is connecting or not	Passed	
WLJ87S_Reg_376	Configuring with Static WEP+802.1x security	To verify whether Client with Static WEP+802.1x security is connecting or not	Passed	
WLJ87S_Reg_377	Configuring with EAP+pass through security	To verify whether client with EAP+Pass through security is connecting or not	Passed	
WLJ87S_Reg_378	Configuring with CKIP security	To verify whether client with CKIP security is connecting or not	Passed	
WLJ87S_Reg_379	Configuring with WPA+WPA2 security and authentication key management as PSK	To verify whether client with WPA+WPA2 security is connected or not	Passed	
WLJ87S_Reg_380	Configuring with L2 security 'none' , enable mac filtering and connect Android client	To verify whether WLAN is created with none and Android client connect successfully or not	Passed	
WLJ87S_Reg_381	Configuring with L2 security 'WPA+WPA2' , enable mac filtering and connect iOS client	To verify whether WLAN is created with WPA+WPA2 and Android client connect successfully or not	Passed	
WLJ87S_Reg_382	Configuring with L2 security 'WEP' , enable mac filtering and connect Windows client	To verify whether WLAN is created with none and WEP client connect successfully or not	Passed	

Config Wireless

Logical ID	Title	Description	Status	Defect ID
WLJ87IIS_config_01	Trying to map MAC filter to WLAN in WLC CLI	To check whether MAC Filter can be mapped or not from specific WLAN to all in WLC CLI	Failed	CSCvi90562
WLJ87IIS_config_02	Checking the CCX version of clients with different AP's	To check whether clients CCX version shown correctly or not in all AP's	Failed	CSCvi96766
WLJ87IIS_config_03	Enabling/disabling the 802.11g standard in WLC	To check whether AP's gets reloaded or not while enabling/disabling the 802.11g standard in WLC	Failed	CSCvj08339
WLJ87IIS_config_04	Checking the access of TACACS-Wireless user in WLC UI	To check whether TACACS-Wireless user can access the Flexconnect VLAN templated or not in WLC	Failed	CSCvj08974
WLJ87IIS_config_05	Associating iPhone client to 1852 AP and checking the logs	To check whether any error log thrown or not in AP console while associating iPhone clients	Failed	CSCvi85683
WLJ87IIS_config_06	Checking the AP packet capture command in WLC CLI	To check whether AP packet capture command works properly or not in WLC CLI	Failed	CSCvj11261
WLJ87S_config_01	Verifying Max database entry compare to configuration guide	To check whether WLC is accepting the database entry as per the document guide or not	Failed	CSCvh00117
WLJ87S_config_02	Verifying joining process of AP 1562 to WLC	To check whether AP 1562 AP is getting joined to WLC or not	Failed	CSCvh12029
WLJ87S_config_03	Verifying AP usage statistics for AP 2700 in WLC GUI	To check whether AP usage is showing correct statistics or not when client is served by AP	Failed	CSCvh12376
WLJ87S_config_04	Verifying Local Policy statistics in WLC GUI	To check whether the local policies statistics are correct to not for connected client in WLC GUI	Failed	CSCvh31058
WLJ87S_config_05	Verifying configuration of media stream profile through CLI	To check whether media stream profile can be created or not through WLC CLI	Failed	CSCvh51372
WLJ87S_config_06	Verifying return value for MIB database for local Management user	To check whether correct OID value is returned to MIB database or not for local Management user	Failed	CSCvh53238
WLJ87S_config_07	Verifying selected privileges of TACAS user in WLC	To check whether WLC login via TACAS+ server with selected privileges is possible or not	Passed	

WLJ87S_config_08	Verify SXP Peer IP address config in CLI in AP global configuration	To check SXP Peer Ip is accepting network IP through CLI in AP global configuration	Passed	
------------------	---	---	--------	--

CME

ME support on AP1815I/ 1562I

Logical ID	Title	Description	Status	Defect ID
MEJ87IIS_Reg_01	Verifying the different OS client connectivity with WLAN name with japanese character on CME	To check the different OS client is able to connect or not to JSSID	Passed	
MEJ87IIS_Reg_02	Connecting the client with wlan security mac filtering + WPA personal	To check whether able to connect the client with wan security mac filtering + WPA personal	Passed	
MEJ87IIS_Reg_03	Clearing controller configuration	To check whether configuration can be cleared or not from CME GUI	Passed	
MEJ87IIS_Reg_04	Converting a CAWAP AP into a ME AP	To check whether able to convert the CAWAP AP into a Mobility express AP	Passed	
MEJ87IIS_Reg_05	Converting a ME AP into a CAPWAP AP	To check whether able to convert the ME AP into a CAPWAP AP	Passed	
MEJ87IIS_Reg_06	Verifying that all the ap that associated Master ap and master ap itself converting into capwap after clicking on convert to capwap or not	To check whether able to associate all the ap into Master ap and master ap itself converting into capwap after clicking on convert to capwap or not	Passed	
MEJ87IIS_Reg_07	Verifying to join ME ap to controller that name is in japanese character	To check whether able to join ME ap to controller that name is in japanese character	Passed	
MEJ87IIS_Reg_08	Verifying import config file into CME GUI page.	To check whether able to import the config file into the mobility express.	Passed	

MEJ87IIS_Reg_09	Connecting the clients with DCA channels (5 GHZ) and (2.4 GHZ)	To verify whether windows clients are connected with DCA channels (5 GHZ) and (2.4 GHZ) successfully	Passed	
MEJ87IIS_Reg_10	Associating the MAC client to a non-broadcasting SSID	To check whether the MAC clients are associating with a non-broadcasting SSID and check the association of the same	Passed	
MEJ87IIS_Reg_11	Importing/Exporting configuration file to controller through CLI	To check whether configuration file can be exported.imported or not to the controller in CME CLI	Passed	
MEJ87IIS_Reg_12	Verifying that AVC rule that are applied on a deleted wlan is applying automatically on same name WLAN or not	To check whether AVC rule that are applied on a deleted wlan is applying automatically on same name WLAN or not	Passed	
MEJ87IIS_Reg_13	Verifying that AVC rule of first WLAN automatically applying on second WLAN also with second AVC profile name or not	To check whether AVC rule of first WLAN automatically applying on second WLAN also with second AVC profile name or not	Passed	
MEJ87S_Reg_01	Connecting the Android client with wlan security mac filtering + WPA personal	To check whether the client is connect or not.	Passed	
MEJ87S_Reg_02	Verifying the Android client connectivity with WLAN name japanese character on CME	To check the android client is connect or not	Passed	
MEJ87S_Reg_03	Verifying the iOS client Connectivity with WLAN name as japanese character on CME	To check whether able to connect the iOS client with WLAN name as japanese character on CME	Passed	
MEJ87S_Reg_04	Verifying windows client connectivity with WLAN name as japanese character on CME	To check whether able to connect the windows client with WLAN name as japanese character on CME	Passed	

MEJ87S_Reg_05	Verifying MAC client connectivity with WLAN name as japanese character CME	To check whether able to connect MAC client Connectivity with WLAN name as japanese character on CME	Passed	
MEJ87S_Reg_06	Connecting the client with wlan security mac filtering + WPA personal	To check whether able to connect the client with wan security mac filtering + WPA personal	Passed	
MEJ87S_Reg_07	Clearing controller configuration	To check whether configuration can be cleared or not from CME GUI	Passed	
MEJ87S_Reg_08	Verifying the client to a WLAN in which security web-auth is enabled in ME	To check whether able to connect client connectivity with WLAN in which guest network+captive portal mapped to Radius is enabled.	Passed	
MEJ87S_Reg_09	Converting a CAWAP AP into a ME AP	To check whether able to convert the CAWAP AP into a Mobility express AP	Passed	
MEJ87S_Reg_10	Converting a ME AP into a CAPWAP AP	To check whether able to convert the ME AP into a CAPWAP AP	Passed	
MEJ87S_Reg_11	Verifying that all the ap that associated Master ap and master ap itself converting into capwap after clicking on convert to capwap or not	To check whether able to associate all the ap into Master ap and master ap itself converting into capwap after clicking on convert to capwap or not	Passed	
MEJ87S_Reg_12	Verifying to join ME ap to controller that name is in japanese character	To check whether able to join ME ap to controller that name is in japanese character	Passed	
MEJ87S_Reg_13	Verifying import config file into CME GUI page.	To check whether able to import the config file into the mobility express.	Passed	
MEJ87S_Reg_14	Connecting the windows clients with DCA channels (5 GHZ) and (2.4 GHZ)	To verify whether windows clients are connected with DCA channels (5 GHZ) and (2.4 GHZ) successfully	Passed	

MEJ87S_Reg_15	Connecting the android clients with DCA channels (5 GHZ) and (2.4 GHZ)	To verify whether android clients are connected with DCA channels (5 GHZ) and (2.4 GHZ) successfully	Passed	
MEJ87S_Reg_16	Connecting the MAC clients with DCA channels (2.4 GHZ) and (5 GHZ)	To verify whether windows clients are connected with DCA channels (5 GHZ) and (2.4 GHZ) successfully	Passed	
MEJ87S_Reg_17	Connecting the IOS clients with DCA channels (2.4 GHZ) and (5 GHZ)	To verify whether IOS clients are connected with DCA channels (2.4 GHZ) and (5 GHZ) successfully	Passed	
MEJ87S_Reg_18	Associating the MAC client to a non-broadcasting SSID	To check whether the MAC clients are associating with a non-broadcasting SSID and check the association of the same	Passed	
MEJ87S_Reg_19	Exporting configuration file to controller through CLI	To check whether configuration file can be exported or not to the controller in CME CLI	Passed	
MEJ87S_Reg_20	Importing configuration file from controller through CLI	To check whether configuration file can be imported or not from the controller	Passed	
MEJ87S_Reg_21	Verifying that AVC rule that are applied on a deleted wlan is applying automatically on same name WLAN or not	To check whether AVC rule that are applied on a deleted wlan is applying automatically on same name WLAN or not	Passed	
MEJ87S_Reg_22	Verifying that AVC rule of first WLAN automatically applying on second WLAN also with second AVC profile name or not	To check whether AVC rule of first WLAN automatically applying on second WLAN also with second AVC profile name or not	Passed	
MEJ87S_Reg_23	Verifying CME deployment on AP1815I	To check whether the AP 1815I AP is able to convert into CME	Passed	

MEJ87S_Reg_24	Connecting the client with wlan security mac filtering + WPA personal	To check whether the client is connect or not.	Passed	
MEJ87S_Reg_25	Verifying the Android client connectivity with WLAN name japanese character on CME	To check the android client is connect or not	Passed	
MEJ87S_Reg_26	Verifying the mac os client Connectivity with WLAN name as japanese character on CME	To check whather able to connect the mac os client with WLAN name as japanese character on CME	Passed	
MEJ87S_Reg_27	Verifying windows client connectivity with WLAN name as japanese character on CME	To check whether able to connect the windows client with WLAN name as japanese character on CME	Passed	
MEJ87S_Reg_28	Verifying MAC client connectivity with WLAN name as japanese character CME	To check whether able to connect MAC client Connectivity with WLAN name as japanese character on CME	Passed	
MEJ87S_Reg_29	Connecting the client with wlan security mac filtering + WPA personal	To check whether able to connect the client with wlan security mac filtering + WPA personal	Passed	
MEJ87S_Reg_30	Verifying to clear the controller configuration	To check whether configuration can be cleared or not from CME GUI	Passed	
MEJ87S_Reg_31	Connecting the windows clients with DCA channels (2.4 GHZ) and (5 GHZ)	To verify whether windows clients are connected with DCA channels (2.4 GHZ) and (5 GHZ) successfully	Passed	
MEJ87S_Reg_32	Connecting the IOS clients with DCA channels (2.4 GHZ) and (5 GHZ)	To verify whether IOS clients are connected with DCA channels (2.4 GHZ) and (5 GHZ)) successfully	Passed	
MEJ87S_Reg_33	Connecting the MAC clients with DCA channels (2.4 GHZ) and (5 GHZ)	To verify whether MAC clients are connected with DCA channels (2.4 GHZ) and (5 GHZ) successfully	Passed	

MEJ87S_Reg_34	Connecting the IOS clients with DCA channels (2.4 GHZ) and (5 GHZ)	To verify whether IOS clients are connected with DCA channels (2.4 GHZ) and (5 GHZ) successfully	Passed	
MEJ87S_Reg_35	Verifying to create snmp communities and traps	To check whether able to create the snmp communities and traps or not through CLI	Passed	
MEJ87S_Reg_36	Verifying to enable and disable the snmp versions in CME through CLI	To check whether able to configure the snmp versions or not	Passed	
MEJ87S_Reg_37	Exporting configuration file to controller through CLI	To check whether configuration file can be exported or not to the controller in CME CLI	Passed	
MEJ87S_Reg_38	Importing configuration file from controller through CLI	To check whether configuration file can be imported or not from the controller	Passed	
MEJ87S_Reg_39	Verifying that AVC rule that are applied on a deleted wlan is applying automatically on same name WLAN or not	To check whether AVC rule that are applied on a deleted wlan is applying automatically on same name WLAN or not	Passed	
MEJ87S_Reg_40	Verifying that AVC rule of first WLAN automatically applying on second WLAN also with second AVC profile name or not	To check whether AVC rule of first WLAN automatically applying on second WLAN also with second AVC profile name or not	Passed	
MEJ87S_Reg_41	Verifying the client to get correct video or audio format after applying the AVC rule.	To check whether able to connect client to get correct video or audio format after applying the AVC rule.	Passed	
MEJ87S_Reg_42	Verifying the client to a WLAN in which security web-auth is enabled in ME	To check client connectivity with WLAN in which guest network+captive portal mapped to Radius is enabled.	Passed	

MEJ87S_Reg_43	Verifying the clients status in Monitor dashboard in ME GUI page	To check whether able to connect the different client in CME and shown properly in Monitor Dashboard page.	Passed	
MEJ87S_Reg_44	Verifying to add multiple client mac address in CME and checking the connection of all clients.	To check whether able to connect multiple clients mac address in mac filtering and checking the clients gets associated or not.	Passed	
MEJ87S_Reg_45	Converting a ME AP into a CAPWAP AP	To check whether able to convert the ME AP into a CAPWAP AP	Passed	
MEJ87S_Reg_46	Verifying that all the ap that associated Master ap and master ap itself converting into capwap after clicking on convert to capwap or not	To check whether able to associate all the ap into Master ap and master ap itself converting into capwap after clicking on convert to capwap or not	Passed	
MEJ87S_Reg_47	Verifying to join ME ap to controller that name is in japanese character	To check whether ME ap join to controller that name is in japanese character	Passed	
MEJ87S_Reg_48	Associating the MAC client to a non-broadcasting SSID	To check wheather the MAC clients are associating with a non-broadcasting SSID and check the association of the same	Passed	
MEJ87S_Reg_49	Verifying the CME name as the japanese character	To check whether the CME name with the japanese character is accepted or not.	Passed	
MEJ87S_Reg_50	Reboot 1562I CME AP	To check whether able to reboot 1562I CME or not	Passed	
MEJ87S_Reg_51	Verifying the WLAN name as the japanese character	To check whether the WLAN name with the japanese character is accepted or not.	Passed	

Captive Portal with Email address and Web Consent

Logical ID	Title	Description	Status	Defect ID
------------	-------	-------------	--------	-----------

MEJ87IIS_Reg_14	Configuring the Email address in Internal /External splash page and associating different types clients to a WLAN	To check whether JOS client gets associated successfully or not to a WLAN in which captive portal enabled as Internal splash page with mapping username as Email address	Passed	
MEJ87IIS_Reg_15	Configuring the Web Consent in Internal/External splash page and associating JOS clients to a WLAN	To check whether JOS client gets associated successfully or not to a WLAN in which captive portal enabled as Internal splash page with mapping access type as Web consent	Passed	
MEJ87IIS_Reg_16	Associating MacOS clients to a WLAN with captive portal and mac filtering enabled	To check whether MacOS clients get associated successfully or not to a WLAN in which captive portal mapped to Internal/external splash page with access type Email address	Passed	
MEJ87IIS_Reg_17	Making all clients as blacklist and checking the association of the clients to a WLAN	To check whether blacklisted clients associating or not to a WLAN in which captive portal enabled with access type as Email address.	Passed	
MEJ87IIS_Reg_18	Associating MacOS clients to a WLAN created with UTF-8 Char with providing invalid email address as username	To check whether MacOS clients get associated successfully or not to a WLAN by providing invalid email address as username during captive portal mapped to internal/external splash page	Passed	
MEJ87S_Reg_52	Configuring the Email address in Internal splash page and associating JOS clients to a WLAN	To check whether JOS client gets associated successfully or not to a WLAN in which captive portal enabled as Internal splash page with mapping username as Email address	Passed	

MEJ87S_Reg_53	Configuring the Email address in External splash page and associating JOS clients to a WLAN	To check whether JOS client gets associated successfully or not to a WLAN in which captive portal enabled as external splash page with mapping username as Email address	Passed	
MEJ87S_Reg_54	Configuring the Web Consent in Internal splash page and associating JOS clients to a WLAN	To check whether JOS client gets associated successfully or not to a WLAN in which captive portal enabled as Internal splash page with mapping access type as Web consent	Passed	
MEJ87S_Reg_55	Configuring the Web Consent in External splash page and associating JOS clients to a WLAN	To check whether JOS client gets associated successfully or not to a WLAN in which captive portal enabled as external splash page with mapping access type as web consent	Passed	
MEJ87S_Reg_56	Associating MacOS clients to a WLAN with captive portal and mac filtering enabled	To check whether MacOS clients get associated successfully or not to a WLAN in which captive portal mapped to Internal/external splash page with access type Email address	Passed	
MEJ87S_Reg_57	Associating Android clients to a WLAN with captive portal and mac filtering enabled	To check whether Android clients get associated successfully or not to a WLAN in which captive portal mapped to Internal/external splash page with access type Email address	Passed	
MEJ87S_Reg_58	Associating IOS clients to a WLAN with captive portal and mac filtering enabled	To check whether IOS clients get associated successfully or not to a WLAN in which captive portal mapped to Internal/external splash page with access type Email address	Passed	

MEJ87S_Reg_59	Making all clients as blacklist and checking the association of the clients to a WLAN	To check whether blacklisted clients associating or not to a WLAN in which captive portal enabled with access type as Email address.	Passed	
MEJ87S_Reg_60	Creating a WLAN in UTF-8 character with captive portal enabled and associating all clients to this WLAN	To check whether all clients gets associated or not successfully to a WLAN which is created in UTF-8 characters.	Passed	
MEJ87S_Reg_61	Checking the Local profiling functions in a WLAN and associating multiple clients to this WLAN	To check whether clients details shown correctly or not when they are connected to a WLAN with Captive portal mapped to Internal splash page.	Passed	
MEJ87S_Reg_62	Associating MacOS clients to a WLAN with providing invalid email address as username	To check whether MacOS clients get associated successfully or not to a WLAN by providing invalid email address as username during captive portal mapped to internal/external splash page	Passed	
MEJ87S_Reg_63	Associating Android clients to a WLAN with providing invalid email address as username	To check whether Android clients get associated successfully or not to a WLAN by providing invalid email address as username during captive portal mapped to internal/external splash page	Passed	
MEJ87S_Reg_64	Associating JOS clients to a WLAN with providing invalid email address as username	To check whether JOS clients get associated successfully or not to a WLAN by providing invalid email address as username during captive portal mapped to internal/external splash page	Passed	

MEJ87S_Reg_65	Configuring the Web Consent in Internal/external splash page and associating all different clients	To check whether all clients gets associated successfully or not to a WLAN in which captive portal enabled as Internal/external splash page with mapping access type as Web consent	Passed	
---------------	--	---	--------	--

TACACS

Logical ID	Title	Description	Status	Defect ID
MEJ87IIS_Reg_19	Allowing the user for complete access to CME network via TACACS	To check whether user can able to read-write access the complete CME network or not via TACACS	Passed	
MEJ87IIS_Reg_20	Providing the user for lobby admin access to the CME via TACACS	To check whether user can able to have lobby admin access or not to CME via TACACS	Passed	
MEJ87IIS_Reg_21	Providing the user for monitoring access to the CME via TACACS	To check whether user can able to have monitoring access (which is read-only) or not to CME via TACACS	Passed	
MEJ87IIS_Reg_22	Trying to login CME via TACACS with invalid credentials	To check whether user can able to login or not in CME via TACACS with invalid credentials	Passed	
MEJ87S_Reg_66	Allowing the user for complete access to CME network via TACACS	To check whether user can able to read-write access the complete CME network or not via TACACS	Passed	
MEJ87S_Reg_67	Providing the user for lobby admin access to the CME via TACACS	To check whether user can able to have lobby admin access or not to CME via TACACS	Passed	
MEJ87S_Reg_68	Providing the user for monitoring access to the CME via TACACS	To check whether user can able to have monitoring access (which is read-only) or not to CME via TACACS	Passed	

MEJ87S_Reg_69	Checking the debug commands in CME CLI	To check whether debug logs displayed properly or not while user Login into CME UI with Japanese option and in parallel enable the debug in CLI with 'debug emweb web enable". via TACACS authentication	Passed	
MEJ87S_Reg_70	Trying to login CME via TACACS with invalid credentials	To check whether user can able to login or not in CME via TACACS with invalid credentials	Passed	

Hotspot 2.0

Logical ID	Title	Description	Status	Defect ID
MEJ87IIS_Reg_23	Configuring WLAN with WPA, 802.1x authentication policy in ME 1852/1832 AP	Verifying that user is able to configure WLAN with WPA, 802.1x authentication policy or not	Passed	
MEJ87IIS_Reg_24	Connecting IOS client via hotspot 2.0	Verifying that user is able to connect IOS client via hotspot 2.0 or not	Passed	
MEJ87IIS_Reg_25	Verifying that client is connecting automatically without asking credentials even when client come under coverage area of WLAN	To check whether the client comes under coverage area or not without asking credentials	Passed	
MEJ87IIS_Reg_26	Verifying that hotspot 2.0 config same after uploading the exported config file	To check hotspot 2.0 config same after uploading the exported config file	Passed	
MEJ87IIS_Reg_27	Try to disable WPA on Hotspot enabled WLAN	Verifying that user is able to disable WPA on Hotspot enabled WLAN or not	Passed	
MEJ87IIS_Reg_28	Trying to config passpoint on guset-lan	Verifying that user is able to config Passpoint on guest-lan or not	Passed	

MEJ87IIS_Reg_29	Verifying that user is able to edit or delete the 802.11u and HS 2.0 parameter via CLI and GUI or not	Checking that user is able to edit or delete the 802.11u and HS 2.0 parameter via CLI and GUI or not	Passed	
MEJ87IIS_Reg_30	Try to enable hotspot on open/Guest network	Verifying that user is able to enable hotspot on open network or not	Passed	
MEJ87IIS_Reg_31	Validating the client using WAN and client Downlink Load by enabling Hotspot 2.0	Verifying the client using WAN Downlink Load by enabling Hotspot 2.0	Passed	
MEJ87IIS_Reg_32	Validating the client using WAN and client Uplink Load by enabling Hotspot 2.0	Verifying the client using WAN Uplink Load by enabling Hotspot 2.0	Passed	
MEJ87IIS_Reg_33	Assigning the venue group and venue type for the specific AP on 802.11u	Providing the venue group and venue type for the specific AP on 802.11u	Passed	
MEJ87S_Reg_71	Configuring WLAN with WPA, 802.1x authentication policy in ME 1852/1832 AP	Verifying that user is able to configure WLAN with WPA, 802.1x authentication policy or not	Passed	
MEJ87S_Reg_72	Enabling hotspot 2.0 on WLAN in ME	Verifying that user is able to enable hotspot 2.0 on WLAN or not	Passed	
MEJ87S_Reg_73	Connecting passpoint certified android client via hotspot 2.0	Verifying that user is able to connect android client via hotspot 2.0 or not	Passed	
MEJ87S_Reg_74	Connecting IOS client via hotspot 2.0	Verifying that user is able to connect IOS client via hotspot 2.0 or not	Passed	
MEJ87S_Reg_75	Verifying that client is connecting automatically without asking credentials even when client come under coverage area of WLAN	To check whether the client comes under coverage area or not without asking credentials	Passed	

MEJ87S_Reg_76	Verifying that hotspot 2.0 config same after uploading the exported config file	To check hotspot 2.0 config same after uploading the exported config file	Passed	
MEJ87S_Reg_77	Debugging hotspot event in CME	Verifying that user is able to debug hotspot event in CME or not	Passed	
MEJ87S_Reg_78	Try to disable WPA on Hotspot enabled WLAN	Verifying that user is able to disable WPA on Hotspot enabled WLAN or not	Passed	
MEJ87S_Reg_79	Trying to config passpoint on guset-lan	Verifying that user is able to config Passpoint on guest-lan or not	Passed	
MEJ87S_Reg_80	Verifying that user is able to edit or delete the 802.11u and HS 2.0 parameter via CLI and GUI or not	Checking that user is able to edit or delete the 802.11u and HS 2.0 parameter via CLI and GUI or not	Passed	
MEJ87S_Reg_81	Try to enable hotspot on open network	Verifying that user is able to enable hotspot on open network or not	Passed	
MEJ87S_Reg_82	Verifying that user is able to add EAP method on realm list	To check that the user is able to add EAP method on realm list or not	Passed	
MEJ87S_Reg_83	Validating the client using WAN Downlink Speed by enabling Hotspot 2.0	To check the client downlink speed by enabling hotspot 2.0	Passed	
MEJ87S_Reg_84	Validating the client using WAN Uplink Speed by enabling Hotspot 2.0	Verifying the client using WAN Uplink Speed by enabling Hotspot 2.0	Passed	
MEJ87S_Reg_85	Validating the client using WAN Downlink Load by enabling Hotspot 2.0	Verifying the client using WAN Downlink Load by enabling Hotspot 2.0	Passed	
MEJ87S_Reg_86	Validating the client using WAN Uplink Load by enabling Hotspot 2.0	Verifying the client using WAN Uplink Load by enabling Hotspot 2.0	Passed	

Mac filtering (for L2 security)

MEJ87S_Reg_87	Validating the client using WAN Load Measurement Duration by enabling Hotspot 2.0	Verifying the client using WAN Load Measurement Duration by enabling Hotspot 2.0	Passed	
MEJ87S_Reg_88	Assigning the venue group and venue type for the specific AP on 802.11u	Providing the venue group and venue type for the specific AP on 802.11u	Passed	
MEJ87S_Reg_89	Capturing the debug information for connected clients with hotspot enabled	To verify the debug information for connected clients with hotspot enabled	Passed	

Mac filtering (for L2 security)

Logical ID	Title	Description	Status	Defect ID
MEJ87IIS_Reg_34	Adding Windows (7,8,10) Client mac address in CME and checking the connection of Clients in 1800 Series ME	To add the windows Client mac address in mac filtering in CME and checking whether Clients gets associated or not successfully in 1800 Series ME	Passed	
MEJ87IIS_Reg_35	Uploading the empty CSV file in ME UI	To check whether an blank CSV file could be uploaded in ME UI	Passed	
MEJ87IIS_Reg_36	Importing the .CSV file with modifications in ME	To check whether .CSV file gets imported or not after importing the updated file with some changes in it	Passed	
MEJ87IIS_Reg_37	Connecting the Client with wlan security mac filtering + WPA personal	To Connect the Client with wlan security mac filtering + WPA personal	Passed	
MEJ87IIS_Reg_38	Connecting the Client with wlan security mac filtering + WPA enterprise	To Connect the Client with wlan security mac filtering + WPA enterprise	Passed	

MEJ87IIS_Reg_39	Connecting the Client with WLAN as MAC Filtering+WPA Enterprise Choosing Authentication Server as AP	To Connect the Client with MAC Filtering using WPA Enterprise as security type choosing Authentication Server as AP	Passed	
MEJ87IIS_Reg_40	Connecting the Client with Wlan Security Type as WPA Enterprise enabling MAC Filtering option Choosing Authentication Server as External Radius and RADIUS Compatibility as other	To Connect the Client with MAC Filtering using WPA Enterprise as security type choosing Authentication Server as External Radius and RADIUS Compatibility as other	Passed	
MEJ87IIS_Reg_41	Connecting the client after client identity account expired in ISE	To Connect the Client after client identity account expired in ISE	Passed	
MEJ87S_Reg_90	Adding Windows (7,8,10) Client mac address in CME and checking the connection of Clients in 1800 Series ME	To add the windows Client mac address in mac filtering in CME and checking whether Clients gets associated or not successfully in 1800 Series ME	Passed	
MEJ87S_Reg_91	Adding IOS Client mac address to blacklist and checking the connection of Clients in 1800 Series ME	To add the IOS Client mac address in mac filtering in CME and checking whether Clients gets associated or not successfully in 1800 Series ME	Passed	
MEJ87S_Reg_92	Verifying the Clients status in Monitor dashboard in ME GUI page	To check whether able to connect Client in CME and shown properly in Monitor Dashboard page.	Passed	
MEJ87S_Reg_93	Checking the filter option of local MAC filtering	To check whether the added MAC address is filtered while searching according to the user's choice	Passed	
MEJ87S_Reg_94	Adding a invalid mac address in local database	To add a invalid mac address in mac filter in CME	Passed	

Mac filtering (for L2 security)

MEJ87S_Reg_95	Uploading the empty CSV file in ME UI	To check whether an blank CSV file could be uploaded in ME UI	Passed	
MEJ87S_Reg_96	Importing the .CSV file with modifications in ME	To check whether .CSV file gets imported or not after importing the updated file with some changes in it	Passed	
MEJ87S_Reg_97	Connecting the Client with wlan security mac filtering + WPA personal	To Connect the Client with wlan security mac filtering + WPA personal	Passed	
MEJ87S_Reg_98	Connecting the Client with wlan security mac filtering + WPA enterprise	To Connect the Client with wlan security mac filtering + WPA enterprise	Passed	
MEJ87S_Reg_99	Connecting the Client with WLAN as MAC Filtering+WPA Enterprise Choosing Authentication Server as AP	To Connect the Client with MAC Filtering using WPA Enterprise as security type choosing Authentication Server as AP	Passed	
MEJ87S_Reg_100	Connecting the Client with Wlan Security Type as WPA Enterprise enabling MAC Filtering option Choosing Authentication Server as External Radius and RADIUS Compatibility as Cisco ACS	To Connect the Client with MAC Filtering using WPA Enterprise as security type choosing Authentication Server as External Radius and RADIUS Compatibility as Free RADIUS	Passed	
MEJ87S_Reg_101	Connecting the Client with Wlan Security Type as WPA Enterprise enabling MAC Filtering option Choosing Authentication Server as External Radius and RADIUS Compatibility as Cisco ACS	To Connect the Client with MAC Filtering using WPA Enterprise as security type choosing Authentication Server as External Radius and RADIUS Compatibility as Cisco ACS	Passed	

MEJ87S_Reg_102	Connecting the Client with Wlan Security Type as WPA Enterprise enabling MAC Filtering option Choosing Authentication Server as External Radius and RADIUS Compatibility as other	To Connect the Client with MAC Filtering using WPA Enterprise as security type choosing Authentication Server as External Radius and RADIUS Compatibility as other	Passed	
MEJ87S_Reg_103	Connecting the client after client identity account expired in ISE	To Connect the Client after client identity account expired in ISE	Passed	

Access Visibility Control

Logical ID	Title	Description	Status	Defect ID
MEJ87IIS_Reg_42	Drop/mark the different types of scoail application for the connected clients to the created AVC profile	To confirm whether the particular facebook application is been dropped/marked	Passed	
MEJ87IIS_Reg_43	Gmail Application and Drop/mark action to the created AVC for JSSID MAC OS	Verifying the gmail application is dropped/marked or not after created JSSID client connecting	Passed	
MEJ87IIS_Reg_44	Mark the gmail application for the MAC OS to the created AVC profile by specifying Custom value	To check for the gmail application DSCP values can be changed or not	Passed	
MEJ87IIS_Reg_45	Configuring the custom value for gmail application with JSSID MAC OS	verify whether custom value is assigned or not for gmail application	Passed	
MEJ87IIS_Reg_46	Drop/mark the cisco-jabber-im application for the MAC OS to the created AVC profile	To confirm whether the particular cisco-jabber-im application is been dropped/marked	Passed	

MEJ87IIS_Reg_47	Drop/Mark the apple-ios-updates for the MAC OS clients to the created AVC profile	To confirm whether the particular apple-ios-updates application is been dropped/Marked.	Passed	
MEJ87IIS_Reg_48	apple-ios-updates application with Drop/mark action for JSSID to the created AVC	Verify whether Drop/Mark action is configured or not for apple-ios-updates Application	Passed	
MEJ87IIS_Reg_49	configure the custom value with mark action for apple-services with JSSID	Verify whether custome value is configured or not for apple-services	Passed	
MEJ87IIS_Reg_50	configure the Drop/mark action for amazon-instant-video application to the created AVC profile	To confirm whether the particular amazon-instant-video application is been dropped/marked	Passed	
MEJ87IIS_Reg_51	Drop/mark the amazon-instant-video application for JSSID to the created AVC profile	Validating the amazon-instant-vidio application is dropped/marked or not after connecting JSSID with different OS clients	Passed	
MEJ87IIS_Reg_52	Drop/mark the google-services application for JSSID to the created AVC profile	Validating the google-services application is dropped/marked or not after connecting JSSID with different OS clients	Passed	
MEJ87IIS_Reg_53	Drop/mark the instagram application for JSSID to the created AVC profile	Validating the instagram application is dropped/marked or not after connecting JSSID with different OS clients	Passed	
MEJ87IIS_Reg_54	Configure the Drop/mark action for monster-com application to the created AVC profile	To confirm whether the particular monster-com application is been dropped/marked	Passed	

MEJ87IIS_Reg_55	Drop/mark the monster-com application for JSSID to the created AVC profile	Validating the monster-com application is dropped/marked or not after connecting JSSID with different OS clients	Passed	
MEJ87IIS_Reg_56	Drop/mark theny-daily-news application for JSSID to the created AVC profile	Validating the ny-daily-news application is dropped/marked or not after connecting JSSID with different OS clients	Passed	
MEJ87IIS_Reg_57	DHCP failover rule is dropping from MAC client	To verify whether DHCP Failover rule is dropping or not from MAC client	Passed	
MEJ87IIS_Reg_58	Dropping the Secure File transfer protocol	To verify whether Secure File transfer protocol is dropping or not	Passed	
MEJ87IIS_Reg_59	Dropping the Secure HTTP protocol	To verify whether Secure HTTP protocol is dropping or not	Passed	
MEJ87S_Reg_104	Drop/mark the facebook application for the connected clients to the created AVC profile	To confirm whether the particular facebook application is been dropped/marked	Passed	
MEJ87S_Reg_105	JSSID with facebook application checking the Drop/Mark action after connecting the different os clients	Validating the facebook application is dropped & marked or not after connecting JSSID with different OS clients	Passed	
MEJ87S_Reg_106	Custom value with Facebook application for connected JSSID client to the created AVC	Verifying the Facebook application after custom DSCP value assigned.	Passed	
MEJ87S_Reg_107	Drop/Mark the gmail application for the MAC OS to the created AVC profile	To confirm whether the particular gmail application is been dropped & marked	Passed	

MEJ87S_Reg_108	Gmail Application and Drop/mark action to the created AVC for JSSID MAC OS	Verifying the gmail application is dropped/marked or not after created JSSID client connecting	Passed	
MEJ87S_Reg_109	Mark the gmail application for the MAC OS to the created AVC profile by specifying Custom value	To check for the gmail application DSCP values can be changed or not	Passed	
MEJ87S_Reg_110	Configuring the custom value for gmail application with JSSID MAC OS	verify whether custom value is assigned or not for gmail application	Passed	
MEJ87S_Reg_111	Drop/Mark the LinkedIn application for different client to the created AVC profile	To confirm whether the particular linkedin application is been dropped/marked.	Passed	
MEJ87S_Reg_112	LinkedIn application with Drop/mark action for JSSID to the created AVC	Verify whether Drop/Mark action configured or not for LinkedIn Application	Passed	
MEJ87S_Reg_113	Drop/mark the cisco-jabber-im application for the MAC OS to the created AVC profile	To confirm whether the particular cisco-jabber-im application is been dropped/marked	Passed	
MEJ87S_Reg_114	Cisco-jabber-im application with Drop/mark action for JSSID to the created AVC	Verify whether Drop/Mark action is configured or not for LinkedIn Application	Passed	
MEJ87S_Reg_115	Drop/Mark the apple-ios-updates for the MAC OS clients to the created AVC profile	To confirm whether the particular apple-ios-updates application is been dropped/Marked.	Passed	
MEJ87S_Reg_116	apple-ios-updates application with Drop/mark action for JSSID to the created AVC	Verify whether Drop/Mark action is configured or not for apple-ios-updates Application	Passed	

MEJ87S_Reg_117	Mark the apple-services for the MAC OS clients to the created AVC profile by specifying custom value	To check whether the apple-services application is been marked or not	Passed	
MEJ87S_Reg_118	configure the custom value with mark action for apple-services with JSSID	Verify whether custome value is configured or not for apple-services	Passed	
MEJ87S_Reg_119	configure the Drop/mark action for amazon-instant-video application to the created AVC profile	To confirm whether the particular amazon-instant-video application is been dropped/marked	Passed	
MEJ87S_Reg_120	Drop/mark the amazon-instant-video application for JSSID to the created AVC profile	Validating the amazon-instant-vidio application is dropped/marked or not after connecting JSSID with different OS clients	Passed	
MEJ87S_Reg_121	Configure the Drop/mark action for google-services application to the created AVC profile	To confirm whether the particular google-services application is been dropped/marked	Passed	
MEJ87S_Reg_122	Drop/mark the google-services application for JSSID to the created AVC profile	Validating the google-services application is dropped/marked or not after connecting JSSID with different OS clients	Passed	
MEJ87S_Reg_123	Configure the Drop/mark action for instagram application to the created AVC profile	To confirm whether the particular instagram application is been dropped/marked	Passed	
MEJ87S_Reg_124	Drop/mark the instagram application for JSSID to the created AVC profile	Validating the instagram application is dropped/marked or not after connecting JSSID with different OS clients	Passed	

MEJ87S_Reg_125	Configure the Drop/mark action for linkedin application to the created AVC profile	To confirm whether the particular linkedin application is been dropped/marked	Passed	
MEJ87S_Reg_126	Drop/mark the instagram application for JSSID to the created AVC profile	Validating the linkedin application is dropped/marked or not after connecting JSSID with different OS clients	Passed	
MEJ87S_Reg_127	Configure the Drop/mark action for monster-com application to the created AVC profile	To confirm whether the particular monster-com application is been dropped/marked	Passed	
MEJ87S_Reg_128	Drop/mark the monster-com application for JSSID to the created AVC profile	Validating the monster-com application is dropped/marked or not after connecting JSSID with different OS clients	Passed	
MEJ87S_Reg_129	Configure the Drop/mark action for ny-daily-news application to the created AVC profile	To confirm whether the particular ny-daily-news application is been dropped/marked	Passed	
MEJ87S_Reg_130	Drop/mark theny-daily-news application for JSSID to the created AVC profile	Validating the ny-daily-news application is dropped/marked or not after connecting JSSID with different OS clients	Passed	
MEJ87S_Reg_131	Checking the clients performance in dashboard	To monitor the performance of the clients	Passed	
MEJ87S_Reg_132	Creating the duplicate AVC profile name	To construct the duplicate AVC profile name	Passed	
MEJ87S_Reg_133	Creating the duplicate application name through CLI	To construct the duplicate application name through CLI	Passed	

MEJ87S_Reg_134	DHCP failover rule is dropping from Windows client	To verify whether DHCP Failover rule is dropping or not from Windows client	Passed	
MEJ87S_Reg_135	DHCP failover rule is dropping from MAC client	To verify whether DHCP Failover rule is dropping or not from MAC client	Passed	
MEJ87S_Reg_136	Dropping the File transfer protocol	To verify whether File transfer protocol is dropping or not	Passed	
MEJ87S_Reg_137	Dropping the HTTP protocol	To verify whether HTTP protocol is dropping or not	Passed	
MEJ87S_Reg_138	Dropping the Secure File transfer protocol	To verify whether Secure File transfer protocol is dropping or not	Passed	
MEJ87S_Reg_139	Dropping the Secure HTTP protocol	To verify whether Secure HTTP protocol is dropping or not	Passed	
MEJ87S_Reg_140	Dropping the TFTP data transfer	To verify whether TFTP data transferring or not	Passed	

Lobby Ambassador

Logical ID	Title	Description	Status	Defect ID
MEJ87IIS_Reg_68	Creating a Lobby Admin in CME GUI/CLI	To check whether lobby admin user is created or not in CME GUI/CLI	Passed	
MEJ87IIS_Reg_69	Creating a management guest User	To check whether a guest user can be added or not in CME guest management GUI	Passed	
MEJ87IIS_Reg_70	Deleting a management guest user	To check whether guest user can be deleted or not in CME GUI	Passed	
MEJ87IIS_Reg_71	Generating auto password for management guest user	To check whether password is generated or not for management guest user	Passed	

MEJ87IIS_Reg_72	Generating password manually for management guest user	To check whether manually password is generating or not for management guest user	Passed	
MEJ87IIS_Reg_73	Creating a guest user from admin local account	To check whether a guest user can be added or not from local account in CME GUI	Passed	
MEJ87IIS_Reg_74	Configuring Guest Wlan with default login Page	To check whether a default page can be configured or not for guest login	Passed	
MEJ87IIS_Reg_75	Configuring Guest Wlan with customized login Page	To check whether a customized page can be configured or not for guest login	Passed	
MEJ87S_Reg_149	Creating a Lobby Admin in CME GUI/CLI	To check whether lobby admin user is created or not in CME GUI/CLI	Passed	
MEJ87S_Reg_150	Creating a management guest User	To check whether a guest user can be added or not in CME guest management GUI	Passed	
MEJ87S_Reg_151	Deleting a management guest user	To check whether guest user can be deleted or not in CME GUI	Passed	
MEJ87S_Reg_152	Generating auto password for management guest user	To check whether password is generated or not for management guest user	Passed	
MEJ87S_Reg_153	Generating password manually for management guest user	To check whether manually password is generating or not for management guest user	Passed	
MEJ87S_Reg_154	Creating a guest user from admin local account	To check whether a guest user can be added or not from local account in CME GUI	Passed	
MEJ87S_Reg_155	Configuring Guest Wlan with default login Page	To check whether a default page can be configured or not for guest login	Passed	

MEJ87S_Reg_156	Configuring Guest Wlan with customized login Page	To check whether a customized page can be configured or not for guest login	Passed	
----------------	---	---	--------	--

Guest Login

Logical ID	Title	Description	Status	Defect ID
MEJ87IIS_Reg_60	Creating a WLAN with enabling Guest network and security Web-auth in ME UI	To check whether WLAN is created or not with security L3 Web-auth in ME UI	Passed	
MEJ87IIS_Reg_61	Checking the WLAN configurations after import/export the config file in ME	To check whether WLAN configurations gets retained or not after import/export the config file in CME	Passed	
MEJ87IIS_Reg_62	Associating Windows client to a WLAN in which security web-auth is enabled in ME	To check whether windows client able to connect successfully or not to a WLAN in which guest network+captive portal mapped to Radius is enabled.	Passed	
MEJ87IIS_Reg_63	Associating Apple IOS client to a WLAN in which security web-auth is enabled in ME	To check whether Apple IOS client able to connect successfully or not to a WLAN in which guest network+captive portal mapped to Radius is enabled.	Passed	
MEJ87IIS_Reg_64	Associating MAC OS client to a WLAN in which security web-auth is enabled in ME	To check whether MAC OS client able to connect successfully or not to a WLAN in which guest network+captive portal mapped to Radius is enabled.	Passed	
MEJ87IIS_Reg_65	Associating Android client to a WLAN in which security web-auth is enabled in ME	To check whether Android client able to connect successfully or not to a WLAN in which guest network+captive portal mapped to Radius is enabled.	Passed	

MEJ87IIS_Reg_66	Associating four clients to a WLAN in which security web-auth is enabled in ME	To check whether different OS clients are able to connect successfully or not to a WLAN in which guest network+captive portal mapped to Radius is enabled.	Passed	
MEJ87IIS_Reg_67	Checking the clients stats in Monitor dashboard in ME UI	To check whether different OS clients connected in ME are shown properly or not in Monitor Dashboard.	Passed	
MEJ87IIS_Reg_76	Creating a default login page for guest wlangs after client connect to SSID	To verify whether the default login page is created or not for guest wlangs	Passed	
MEJ87IIS_Reg_77	Creating a customized login page for guest wlangs after associate the SSID	To verify whether the customized login page is created or not for guest wlangs	Passed	
MEJ87IIS_Reg_78	Creating lobby admin account through CLI	To verify whether lobby admin account is created successfully or not through CLI	Passed	
MEJ87S_Reg_157	Creating a default login page for guest wlangs after client connect to SSID	To verify whether the default login page is created or not for guest wlangs	Passed	
MEJ87S_Reg_158	Creating a customized login page for guest wlangs after associate the SSID	To verify whether the customized login page is created or not for guest wlangs	Passed	
MEJ87S_Reg_159	Creating lobby admin account through CLI	To verify whether lobby admin account is created successfully or not through CLI	Passed	

PI support for ME

Logical ID	Features Tested	Title	Description	Status	Defect Id
------------	-----------------	-------	-------------	--------	-----------

MEJ87IIS_Reg_330	PI support for ME	Adding Mobility Express of general parameters into Prime Infrastructure.	To check whether Mobility Express of general parameters added into Prime.	Passed	
MEJ87IIS_Reg_331	PI support for ME	Adding Mobility Express of SNMP parameters into Prime Infrastructure.	To check whether Mobility Express of SNMP parameters added into Prime.	Passed	
MEJ87IIS_Reg_332	PI support for ME	Adding Mobility Express into Prime Infrastructure.	To check whether Mobility Express added into Prime.	Passed	
MEJ87IIS_Reg_333	PI support for ME	Adding into group Mobility Express into Prime Infrastructure.	To check whether Mobility Express added into Prime Infrastructure group.	Passed	
MEJ87IIS_Reg_334	PI support for ME	Sync Mobility Express into Prime Infrastructure.	To check whether Mobility Express sync or not in Prime Infrastructure.	Passed	
MEJ87IIS_Reg_335	PI support for ME	Viewing the list of CME device of WLANs from Prime Infrastructure.	To check whether CME device of WLANs from Prime Infrastructure viewed or not.	Passed	
MEJ87IIS_Reg_336	PI support for ME	Viewing the list of CME device of APs from Prime Infrastructure.	To check whether CME device of APs from Prime Infrastructure viewed or not.	Passed	

MEJ87IIS_Reg_337	PI support for ME	Creating WLANs from Prime on CME	To check whether WLANs from Prime on CME created or not.	Passed	
MEJ87IIS_Reg_338	PI support for ME	Configuring WLANs template from Prime on CME	To check whether WLAN template from Prime on CME configured or not.	Passed	
MEJ87IIS_Reg_339	PI support for ME	Deploying the WLAN template to CME	To check whether WLAN template to CME deployed or not	Passed	
MEJ87IIS_Reg_340	PI support for ME	Viewing the job status to CME	To check whether job status to CME deployed or not	Passed	
MEJ87IIS_Reg_341	PI support for ME	Validating the CME device details from PI	To check the CME device details details from PI	Passed	
MEJ87IIS_Reg_342	PI support for ME	Verifying the client details in PI	To check the client details shown or not in PI	Passed	

Syslogs

Logical ID	Title	Description	Status	Defect ID
MEJ87IIS_Reg_79	Enabling logging for Errors in CME	To check whether log can be generatred or not for Error Message in CME GUI	Passed	
MEJ87IIS_Reg_80	Disabling logging for Errors in CME	To check whether logging for Errors disabled or not in CME	Passed	
MEJ87IIS_Reg_81	Enabling logging for Debugging in CME	To check whether log can be generatred or not for Debug Message in CME GUI	Passed	
MEJ87IIS_Reg_82	Enabling logging server for Emergencies	To check whether log can be generatred or not for Emergncies in CME GUI	Passed	

MEJ87IIS_Reg_83	Enabling logging for Alerts	To check whether log can be generated or not for alerts in CME GUI	Passed	
MEJ87IIS_Reg_84	Enabling logging for Warning	To check whether log can be generated or not for warning in CME GUI	Passed	
MEJ87IIS_Reg_85	Enabling logging for Critical	To check whether log can be generated or not for critical events in CME GUI	Passed	
MEJ87IIS_Reg_86	Enabling logging for Notification	To check whether log can be generated or not for notification in CME GUI	Passed	
MEJ87IIS_Reg_87	Enabling logging for Information message	To check whether log can be generated or not for Informational message in CME GUI	Passed	
MEJ87IIS_Reg_88	Checking the validation of syslog errors in PI	To check whether the syslog errors are displayed in PI	Passed	
MEJ87IIS_Reg_89	Checking the validation of syslog information in PI	To check whether the syslog information are displayed in PI	Passed	
MEJ87IIS_Reg_90	Checking the historic information about syslog in PI	To check whether the historic information about syslog in PI	Passed	
MEJ87IIS_Reg_91	Validating the syslog warning message in PI	To check whether the syslog warning message in PI	Passed	
MEJ87IIS_Reg_92	Validating the syslog notification in PI	To check whether syslog notification in PI	Passed	
MEJ87IIS_Reg_93	Verifying the severity filtering for syslog in PI	To verify the severity filtering for syslog in PI	Passed	
MEJ87IIS_Reg_94	Verifying the Device IP address filtering for syslog in PI	To verify the Device IP address filtering for syslog in PI	Passed	
MEJ87S_Reg_160	Enabling logging for Errors in CME	To check whether log can be generated or not for Error Message in CME GUI	Passed	

MEJ87S_Reg_161	Disabling logging for Errors in CME	To check whether logging for Errors disabled or not in CME	Passed	
MEJ87S_Reg_162	Enabling logging for Debugging in CME	To check whether log can be generatred or not for Debug Message in CME GUI	Passed	
MEJ87S_Reg_163	Enabling logging server for Emergencies	To check whether log can be generatred or not for Emergncies in CME GUI	Passed	
MEJ87S_Reg_164	Enabling logging for Alerts	To check whether log can be generatred or not for alerts in CME GUI	Passed	
MEJ87S_Reg_165	Enabling logging for Warning	To check whether log can be generatred or not for warning in CME GUI	Passed	
MEJ87S_Reg_166	Enabling logging for Criitical	To check whether log can be generatred or not for critical events in CME GUI	Passed	
MEJ87S_Reg_167	Enabling logging for Notification	To check whether log can be generatred or not for notification in CME GUI	Passed	
MEJ87S_Reg_168	Enabling logging for Information message	To check whether log can be generatred or not for Informational message in CME GUI	Passed	
MEJ87S_Reg_169	Checking the validation of syslog errors in PI	To check whether the syslog errors are displayed in PI	Passed	
MEJ87S_Reg_170	Checking the validation of syslog information in PI	To check whether the syslog information are displayed in PI	Passed	
MEJ87S_Reg_171	Checking the hitoric information about syslog in PI	To check whether the hitoric information about syslog in PI	Passed	
MEJ87S_Reg_172	Validating the syslog warning message in PI	To check whether the syslog warning message in PI	Passed	
MEJ87S_Reg_173	Validating the syslog notification in PI	To check whether syslog notification in PI	Passed	

MEJ87S_Reg_174	Verifying the severity filtering for syslog in PI	To verify the severity filtering for syslog in PI	Passed	
MEJ87S_Reg_175	Verifying the Device IP address filtering for syslog in PI	To verify the Device IP address filtering for syslog in PI	Passed	

NAT

Logical ID	Title	Description	Status	Defect ID
MEJ87IIS_Reg_202	Creating the Internal DHCP Pool with IP with Network	To verify whether DHCP Pool is creating or not with valid IP address in Network	Passed	
MEJ87IIS_Reg_203	Client IP Management with Mobility express controller	To verify whether Client IP Management creating or not with mobility express controller	Passed	
MEJ87IIS_Reg_204	Changing the DHCP scope in Client IP management with mobility express controller	To verify whether DHCP scope is changing or not from one to other in Mobility express controller	Passed	
MEJ87IIS_Reg_205	Configuring the Central-NAT configuration at DHCP Scope level	To verify whether Centra-NAT Configuration applied successfully or not	Passed	
MEJ87IIS_Reg_206	NATing enabling in Client	To verify whether NATing applying to the client or not	Passed	
MEJ87IIS_Reg_207	Associating the DHCP Scope to WLAN	To verify whether DHCP Scope is associate the WLAN or not	Passed	
MEJ87IIS_Reg_208	Peer-to-peer blocking the configuration on DHCP through CLI	To verify whether Peer-to-peer blocking applied successfully or not	Passed	
MEJ87IIS_Reg_209	Cheking the lease period after Client connect	To verify whether lease period is showing properly or not after Client connect	Passed	

MEJ87IIS_Reg_210	Configuring the NAT functionality in radio 2.4GHZ band for AP	To verify whether NATing working or not in 2.4 GHZ radio band	Passed	
MEJ87IIS_Reg_211	Configuring the NAT functionality in radio 5GHZ band AP	To verify whether NATing working or not in 5 GHZ radio band	Passed	
MEJ87IIS_Reg_212	Cheking Client performance in Monitoring page after client connect	To verify whether Client performance is showing or not in monitoring page	Passed	
MEJ87IIS_Reg_213	Performing the PING test for Client	To verify whether PING perfoming successfully or not	Passed	
MEJ87IIS_Reg_214	Checking the Connection and event log after client connect	To verify whether Connection showing properly or not	Passed	
MEJ87S_Reg_291	Creating the Internal DHCP Pool with IP with Network	To verify whether DHCP Poll is creating or not with valid IP address in Network	Passed	
MEJ87S_Reg_292	Client IP Management with Mobility express controller	To verify whether Client IP Management creating or not with mobility express controller	Passed	
MEJ87S_Reg_293	Changing the DHCP scope in Client IP management with mobility express controller	To verify whether DHCP scope is changing or not from one to other in Mobility express controller	Passed	
MEJ87S_Reg_294	Configuring the Central-NAT configuration at DHCP Scope level	To verify whether Centra-NAT Configuration applied successfully or not	Passed	
MEJ87S_Reg_295	NATing enabling in Client	To verify whether NATing applying to the client or not	Passed	
MEJ87S_Reg_296	Associating the DHCP Scope to WLAN	To verify whether DHCP Scope is associate the WLAN or not	Passed	
MEJ87S_Reg_297	Peer-to-peer blocking the configuration on DHCP through CLI	To verify whether Peer-to-peer blocking applied successfully or not	Passed	

MEJ87S_Reg_298	Checking the lease period after Client connect	To verify whether lease period is showing properly or not after Client connect	Passed	
MEJ87S_Reg_299	Configuring the NAT functionality in radio 2.4GHZ band for AP	To verify whether NATing working or not in 2.4 GHZ radio band	Passed	
MEJ87S_Reg_300	Configuring the NAT functionality in radio 5GHZ band AP	To verify whether NATing working or not in 5 GHZ radio band	Passed	
MEJ87S_Reg_301	Checking Client performance in Monitoring page after client connect	To verify whether Client performance is showing or not in monitoring page	Passed	
MEJ87S_Reg_302	Performing the PING test for Client	To verify whether PING performing successfully or not	Passed	
MEJ87S_Reg_303	Checking the Connection and event log after client connect	To verify whether Connection showing properly or not	Passed	

Rogue AP

Logical ID	Title	Description	Status	Defect ID
MEJ87IIS_Reg_215	Configuring the rogue AP rule in CME via CLI	To verify that user is able to configure the rogue AP rule in CME via CLI or not	Passed	
MEJ87IIS_Reg_216	Enabling/disabling rogue detection on CME CLI	To verify that user is able to enable/disable rogue detection on CME or not	Passed	
MEJ87IIS_Reg_217	Classifying the rogue Client on CME after client connect	To verify that user is able to classify rogue Client on CME or not	Passed	
MEJ87IIS_Reg_218	Verifying that on the basis of rogue AP rule	To verify that user is able to classify rogue AP on the basis of rogue rule or not	Passed	

MEJ87IIS_Reg_219	Verifying the Japanese character names rogue devices	To verifying that japanese character names rogue devices are Appearing under rogue AP in CME or not	Passed	
MEJ87IIS_Reg_220	Verifying the special character names rogue devices	To verifying that special character names rogue devices are Appearing under rogue AP or not	Passed	
MEJ87IIS_Reg_221	After Appearing the rogue AP in CME ,Updating the their class	To verifying that user is able to update the rogue AP's class or not	Passed	
MEJ87IIS_Reg_222	Manual mitigation of rogue device	Verify that user is able to manually mitigate the rogue AP or not	Passed	
MEJ87IIS_Reg_223	Auto mitigation of rogue device	Verify that user is able to auto mitigate the rogue AP or not	Passed	
MEJ87IIS_Reg_224	Classifying the rogue adhoc on CME	Verify that user is able to classify rogue adhoc on CME or not	Passed	
MEJ87IIS_Reg_225	Deleting the specific rogue AP or all rogue from CME	Verify that user is able to delete the rogue specific rogue AP or all rogue AP from CME or not	Passed	
MEJ87IIS_Reg_226	Verifying the CME is detecting the differnet OS rogue devices	To verifying that CME is able to detect the differnet OS rogue devices or not	Passed	
MEJ87S_Reg_304	Configuring the rogue AP rule in CME via CLI	To verify that user is able to configure the rogue AP rule in CME via CLI or not	Passed	
MEJ87S_Reg_305	Enablng/disabling rogue detection on CME CLI	To verify that user is able to enable/disable rogue detection on CME or not	Passed	
MEJ87S_Reg_306	Classifying the rogue Client on CME after client connect	To verify that user is able to classify rogue Client on CME or not	Passed	

MEJ87S_Reg_307	Verifying that on the basis of rogue AP rule	To verify that user is able to classify rogue AP on the basis of rogue rule or not	Passed	
MEJ87S_Reg_308	Verifying the Japanese character names rogue devices	To verifying that japanese character names rogue devices are Appearing under rogue AP in CME or not	Passed	
MEJ87S_Reg_309	Verifying the special character names rogue devices	To verifying that special character names rogue devices are Appearing under rogue AP or not	Passed	
MEJ87S_Reg_310	After Appearing the rogue AP in CME ,Updating the their class	To verifying that user is able to update the rogoue AP's class or not	Passed	
MEJ87S_Reg_311	Manual mitigation of rogue device	Verify that user is able to manually mitigate the rogue AP or not	Passed	
MEJ87S_Reg_312	Auto mitigation of rogue device	Verify that user is able to auto mitigate the rogue AP or not	Passed	
MEJ87S_Reg_313	Classifying the rogue adhoc on CME	Verify that user is able to classify rogue adhoc on CME or not	Passed	
MEJ87S_Reg_314	Deleting the specific rogue AP or all rogue from CME	Verify that user is able to delete the rogue specific rogue AP or all rogue AP from CME or not	Passed	
MEJ87S_Reg_315	Verifying the CME is detecting the differnet OS rogue devices	To verifying that CME is able to detect the differnet OS rogue devices or not	Passed	

Access Control List

Logical ID	Title	Description	Status	Defect ID
------------	-------	-------------	--------	-----------

MEJ87IIS_Reg_227	Creating the ACL name with Duplicate name	To verify whether ACL name is created with existing name or not	Passed with exception	CSCvj03946
MEJ87IIS_Reg_228	Applying the ACL rule with Egress values	To verify whether Egress rule is applied to ACL or not	Passed	
MEJ87IIS_Reg_229	Applying the ACL rule with Ingress values	To verify whether Ingress rule is applied to ACL or not	Passed	
MEJ87IIS_Reg_230	Applying the ACL rule with Ingress and egress values	To verify whether ingress and Egress rule is applied to ACL or not	Passed	
MEJ87IIS_Reg_231	Creating the ACL rule for Specified source address with Deny action	To verify whether ACL rule is applied to the specified source address with Deny action or not	Passed	
MEJ87IIS_Reg_232	Creating the ACL rule for Specified source address with Permit action	To verify whether ACL rule is applied to the specified source address with Permit action or not	Passed	
MEJ87IIS_Reg_233	Creating the ACL rule for Specified destination address with Deny action	To verify whether ACL rule is applied to the specified destination address with Deny action or not	Passed	
MEJ87IIS_Reg_234	Creating the ACL rule for Specified destination address with Permit action	To verify whether ACL rule is applied to the specified destination address with Permit action or not	Passed	
MEJ87IIS_Reg_235	Creating ACL rule with specific Protocol for Permit rule	To verify whether ACL rule with specific Protocol for Permit rule is applied successfully or not	Passed	

MEJ87IIS_Reg_236	Creating ACL rule with specific DSCP for Deny rule	To verify whether ACL rule is creating with specific DSCP for Deny rule or not	Passed	
MEJ87IIS_Reg_237	Creating ACL rule with specific DSCP for Permit rule	To verify whether ACL rule is creating with specific DSCP for Permit rule or not	Passed	
MEJ87IIS_Reg_238	Creating the ACL name with special characters through CLI	To verify whether ACL name is creating with special characters or not	Passed	
MEJ87IIS_Reg_239	Adding the action to the ACL rule through CLI	To verify whether ACL action is applied successfully or not through CLI	Passed	
MEJ87IIS_Reg_240	Changing the Protocol from one to another	To verify whether Proctocls are changing from one to another or not	Passed	
MEJ87IIS_Reg_241	Applying the ACL rule with Protocol TCP/UDP enabled in source	To verify whether ACL rule with protocol TCP/UDP is applying at the source filed or not	Passed	
MEJ87IIS_Reg_242	Applying the ACL rule with Protocol TCP/UDP enabled in destination	To verify whether ACL rule with protocol TCP/UDP is applying at the Destination filed or not	Passed	
MEJ87S_Reg_316	Creating the ACL name with Duplicate name	To verify whether ACL name is created with existing name or not	Passed	
MEJ87S_Reg_317	Applying the ACL rule with Egress values	To verify whether Egress rule is applied to ACL or not	Passed	
MEJ87S_Reg_318	Applying the ACL rule with Ingress values	To verify whether Ingress rule is applied to ACL or not	Passed	

MEJ87S_Reg_319	Applying the ACL rule with Ingress and egress values	To verify whether ingress and Egress rule is applied to ACL or not	Passed	
MEJ87S_Reg_320	Creating the ACL rule for Specified source address with Deny action	To verify whether ACL rule is applied to the specified source address with Deny action or not	Passed	
MEJ87S_Reg_321	Creating the ACL rule for Specified source address with Permit action	To verify whether ACL rule is applied to the specified source address with Permit action or not	Passed	
MEJ87S_Reg_322	Creating the ACL rule for Specified destination address with Deny action	To verify whether ACL rule is applied to the specified destination address with Deny action or not	Passed	
MEJ87S_Reg_323	Creating the ACL rule for Specified destination address with Permit action	To verify whether ACL rule is applied to the specified destination address with Permit action or not	Passed	
MEJ87S_Reg_324	Creating ACL rule with specific Protocol for Permit rule	To verify whether ACL rule with specific Protocol for Permit rule is applied successfully or not	Passed	
MEJ87S_Reg_325	Creating ACL rule with specific DSCP for Deny rule	To verify whether ACL rule is creating with specific DSCP for Deny rule or not	Passed	
MEJ87S_Reg_326	Creating ACL rule with specific DSCP for Permit rule	To verify whether ACL rule is creating with specific DSCP for Permit rule or not	Passed	
MEJ87S_Reg_327	Creating the ACL name with special characters through CLI	To verify whether ACL name is creating with special characters or not	Passed	

MEJ87S_Reg_328	Adding the action to the ACL rule through CLI	To verify whether ACL action is applied successfully or not through CLI	Passed	
MEJ87S_Reg_329	Changing the Protocol from one to another	To verify whether Proctocls are changing from one to another or not	Passed	
MEJ87S_Reg_330	Applying the ACL rule with Protocol TCP/UDP enabled in source	To verify whether ACL rule with protocol TCP/UDP is applying at the source filed or not	Passed	
MEJ87S_Reg_331	Applying the ACL rule with Protocol TCP/UDP enabled in destination	To verify whether ACL rule with protocol TCP/UDP is applying at the Destination filed or not	Passed	

Internal DHCP Server

Logical ID	Title	Description	Status	Defect ID
MEJ87IIS_Reg_95	Mapping a Internal DHCP pool to WLAN and verifying Windows Client IP Address and vlan id	To verify whether a window client get Ip address and vlan id from a specified DHCP pool or not	Passed	
MEJ87IIS_Reg_96	Mapping a Internal DHCP pool to WLAN and verifying Android Client IP Address and vlan id	To verify whether a Android client get Ip address and vlan id from a specified DHCP pool or not	Passed	
MEJ87IIS_Reg_97	Mapping a Internal DHCP pool to WLAN and verifying MAC Client IP Address and vlan id	To verify whether a MAC Os client get Ip address and vlan id from a specified DHCP pool or not	Passed	

MEJ87IIS_Reg_98	Mapping a Internal DHCP pool to WLAN and verifying iOS Client IP Address and vlan id	To verify whether a iOS client get Ip address and vlan id from a specified DHCP pool or not	Passed	
MEJ87IIS_Reg_99	Checking lease period for connected Client through a DHCP pool	To verify whether DHCP release a particular IP address or not after a certain lease period for client	Passed	
MEJ87S_Reg_176	Mapping a Internal DHCP pool to WLAN and verifying Windows Client IP Address and vlan id	To verify whether a window client get Ip address and vlan id from a specified DHCP pool or not	Passed	
MEJ87S_Reg_177	Mapping a Internal DHCP pool to WLAN and verifying Android Client IP Address and vlan id	To verify whether a Android client get Ip address and vlan id from a specified DHCP pool or not	Passed	
MEJ87S_Reg_178	Mapping a Internal DHCP pool to WLAN and verifying MAC Client IP Address and vlan id	To verify whether a MAC Os client get Ip address and vlan id from a specified DHCP pool or not	Passed	
MEJ87S_Reg_179	Mapping a Internal DHCP pool to WLAN and verifying iOS Client IP Address and vlan id	To verify whether a iOS client get Ip address and vlan id from a specified DHCP pool or not	Passed	
MEJ87S_Reg_180	Checking lease period for connected Client through a DHCP pool	To verify whether DHCP release a particular IP address or not after a certain lease period for client	Passed	

Flex Video Streaming

Logical ID	Title	Description	Status	Defect ID
------------	-------	-------------	--------	-----------

MEJ87IIS_Reg_100	Checking the MC2UC traffic for the JOS clients in CME	To verify whether JOS clients subscribed to videostreaming receives MC2UC traffic or not in CME	Passed	
MEJ87IIS_Reg_101	Checking the MC2UC traffic for the iOS clients in CME	To verify whether iOS clients subscribed to videostreaming receives MC2UC traffic or not in CME	Passed	
MEJ87IIS_Reg_102	Checking the MC2UC traffic for the MacOS clients in CME	To verify whether MacOS clients subscribed to videostreaming receives MC2UC traffic or not in CME	Passed	
MEJ87IIS_Reg_103	Checking the MC2UC traffic for the Android clients in CME	To verify whether Android clients subscribed to videostreaming receives MC2UC traffic or not in CME	Passed	
MEJ87IIS_Reg_104	Associating different OS clients to a WLAN with QoS level platinum and checking the MC2UC traffic in CME	To verify whether all clients subscribed to videostreaming receives MC2UC traffic or not in CME with QoS level mapped to Platinum	Passed	
MEJ87IIS_Reg_105	Changing the bands of clients and checking the Multicast traffic	To verify whether clients receives Multicat traffic or not while changing the bands of clients	Passed	
MEJ87IIS_Reg_106	Checking the Multicast traffic in predefined templates - low resolution by associating different OS clients	To verify whether clients receives Multicat traffic or not in predefined templates- low resolution	Passed	

MEJ87IIS_Reg_107	Checking the Multicast traffic in predefined templates - medium resolution by associating different OS clients	To verify whether clients receives Multicat traffic or not in predefined templates- medium resolution	Passed	
MEJ87IIS_Reg_108	Checking the Multicast traffic in predefined templates - coarse/very coarse by associating different OS clients	To verify whether clients receives Multicat traffic or not in predefined templates- coarse/very coarse resolution	Passed	
MEJ87IIS_Reg_109	Creating media-stream name in all possible combinations	To check whether media-stream name can be created or not in different combinations in ME CLI	Passed	
MEJ87IIS_Reg_110	Setting the packet size in media-stream and checking the same during MC2UC traffic by capturing the packets	To check whether packet size is displayed or not as configured by capturing the packets	Passed	
MEJ87IIS_Reg_111	Setting the maximum bandwidth in a media-stream and checking the same by associating different clients	To check whether clients gets max bandwidth as configured or not in a media-stream	Passed	
MEJ87S_Reg_181	Checking the MC2UC traffic for the JOS clients in CME	To verify whether JOS clients subscribed to videostreaming receives MC2UC traffic or not in CME	Passed	
MEJ87S_Reg_182	Checking the MC2UC traffic for the iOS clients in CME	To verify whether iOS clients subscribed to videostreaming receives MC2UC traffic or not in CME	Passed	

MEJ87S_Reg_183	Checking the MC2UC traffic for the MacOS clients in CME	To verify whether MacOS clients subscribed to videostreaming receives MC2UC traffic or not in CME	Passed	
MEJ87S_Reg_184	Checking the MC2UC traffic for the Android clients in CME	To verify whether Android clients subscribed to videostreaming receives MC2UC traffic or not in CME	Passed	
MEJ87S_Reg_185	Associating different OS clients to a WLAN with QoS level platinum and checking the MC2UC traffic in CME	To verify whether all clients subscribed to videostreaming receives MC2UC traffic or not in CME with QoS level mapped to Platinum	Passed	
MEJ87S_Reg_186	Changing the bands of clients and checking the Multicast traffic	To verify whether clients receives Multicat traffic or not while changing the bands of clients	Passed	
MEJ87S_Reg_187	Checking the Multicast traffic in predefined templates - low resolution by associating different OS clients	To verify whether clients receives Multicat traffic or not in predefined templates- low resolution	Passed	
MEJ87S_Reg_188	Checking the Multicast traffic in predefined templates - medium resolution by associating different OS clients	To verify whether clients receives Multicat traffic or not in predefined templates- medium resolution	Passed	
MEJ87S_Reg_189	Checking the Multicast traffic in predefined templates - coarse/very coarse by associating different OS clients	To verify whether clients receives Multicat traffic or not in predefined templates- coarse/very coarse resolution	Passed	

MEJ87S_Reg_190	Creating media-stream name in all possible combinations	To check whether media-stream name can be created or not in different combinations in ME CLI	Passed	
MEJ87S_Reg_191	Setting the packet size in media-stream and checking the same during MC2UC traffic by capturing the packets	To check whether packet size is displayed or not as configured by capturing the packets	Passed	
MEJ87S_Reg_192	Setting the maximum bandwidth in a media-stream and checking the same by associating different clients	To check whether clients gets max bandwidth as configured or not in a media-stream	Passed	

DNS Based ACL Rules

Logical ID	Title	Description	Status	Defect Id
MEJ87IIS_Reg_343	Configure guest network with captive portal Internal Splash Page - local user account and checking URL ACL rule by connecting Window JOS client	To verify that Window client connect successfully with guest network with captive portal Internal Splash Page , Access type local user account and URL ACL rule deny	Passed	
MEJ87IIS_Reg_344	Configure guest network with captive portal Internal Splash Page-Radius server and checking URL ACL rule by connecting iOS client	To verify that iOS client connect successfully with guest network with captive portal Internal Splash Page , Access type radius server and URL ACL rule deny	Passed	

MEJ87IIS_Reg_345	Configure guest network with captive portal Internal Splash Page-WPA2 personal and checking URL ACL rule with permit by connecting Android client	To verify that Android client connect successfully with guest network with captive portal Internal Splash Page , Access type WPA2 Per and URL Acl rule deny	Passed	
MEJ87IIS_Reg_346	Configure guest network with captive portal External Splash page-local user account and checking URL ACL rule by connecting Window client	To verify that Window client connect successfully with guest network with captive portal External Splash Page , Access type local user account and URL Acl rule deny	Passed	
MEJ87IIS_Reg_347	Configure guest network with captive portal External Splash page-local user account and checking permit URL ACL rule by connecting Android client	To verify that Android client connect successfully with guest network with captive portal External Splash Page , Access type local user account and URL Acl rule Permit	Passed	
MEJ87IIS_Reg_348	Configure guest network with captive portal External Splash page-Radius sever and checking deny URL ACL rule by connecting iOS client	To verify that iOS client connect successfully with guest network with captive portal External Splash Page , Acces type radius Server and URL Acl rule deny	Passed	
MEJ87IIS_Reg_349	Configure guest network with captive portal CMX Connect and checking deny URL ACL rule by connecting Android client	To verify that Android client connect successfully with guest network with captive portal CMX Connect and URL ACL rule deny	Passed	

MEJ87IIS_Reg_350	Configure guest network with captive portal CMX Connect and checking Permit URL ACL rule by connecting iOS client	To verify that iOS client connect successfully with guest network with captive portal CMX Connect and URL ACL rule Permit	Passed	
MEJ87IIS_Reg_351	Configure guest network with captive portal Internal Splash Page-WPA Personal Mac Filtering enabled and checking URL ACL rule by connecting Window JOS client	To verify that Window JOS client connect successfully with guest network with captive portal Internal Splash Page-WPA Personal Mac Filtering enabled and URL ACL rule Permit	Passed	

Open DNS

Logical ID	Title	Description	Status	Defect ID
MEJ87IIS_Reg_252	Configuring Open DNS in DHCP pool and associating Windows JOS clients to a WLAN in CME	To check whether Windows JOS clients gets associated or not to a WLAN in which DHCP pool with Open DNS configured is mapped	Passed	
MEJ87IIS_Reg_253	Configuring Open DNS in DHCP pool and associating Mac OS clients to a WLAN in CME	To check whether Mac OS clients gets associated or not to a WLAN in which DHCP pool with Open DNS configured is mapped	Passed	
MEJ87IIS_Reg_254	Configuring Open DNS in DHCP pool and associating Apple iOS clients to a WLAN in CME	To check whether Apple iOS clients gets associated or not to a WLAN in which DHCP pool with Open DNS configured is mapped	Passed	
MEJ87IIS_Reg_255	Configuring Open DNS in DHCP pool and associating Android clients to a WLAN in CME	To check whether Android clients gets associated or not to a WLAN in which DHCP pool with Open DNS configured is mapped	Passed	

MEJ87S_Reg_341	Configuring Open DNS in DHCP pool and associating Windows JOS clients to a WLAN in CME	To check whether Windows JOS clients gets associated or not to a WLAN in which DHCP pool with Open DNS configured is mapped	Passed	
MEJ87S_Reg_342	Configuring Open DNS in DHCP pool and associating Mac OS clients to a WLAN in CME	To check whether Mac OS clients gets associated or not to a WLAN in which DHCP pool with Open DNS configured is mapped	Passed	
MEJ87S_Reg_343	Configuring Open DNS in DHCP pool and associating Apple iOS clients to a WLAN in CME	To check whether Apple iOS clients gets associated or not to a WLAN in which DHCP pool with Open DNS configured is mapped	Passed	
MEJ87S_Reg_344	Configuring Open DNS in DHCP pool and associating Android clients to a WLAN in CME	To check whether Android clients gets associated or not to a WLAN in which DHCP pool with Open DNS configured is mapped	Passed	

Custom AP Group

Logical ID	Title	Description	Status	Defect ID
MEJ87IIS_Reg_112	Adding the wlan in AP group and connecting the different type of client	To verify that user is able to connecting the different OS client with ap group or not	Passed	
MEJ87IIS_Reg_113	Apply 802.11 a RF -Profile on the ap group and connecting the client	Verify that user is to apply 802.11 a RF -Profile on the ap group or not	Passed	
MEJ87IIS_Reg_114	Apply the 802.11 b RF -Profile on ap group and connecting the client	Verify that user is able to apply 802.11 b RF -Profile on the ap group or not	Passed	
MEJ87IIS_Reg_115	Verify that ap-group and rf -profile config remain the same after performing the forced failover on master ap	To check that ap-group and rf -profile config remain the same after performing the forced failover on master ap	Passed	

MEJ87IIS_Reg_116	Checking that user is able to delete AP -group when ap is associated with ap-group	Verifying that whether user is able to delete ap-group or not when ap is associated with ap group	Passed	
MEJ87IIS_Reg_117	Checking that user is able to delete RF -PROFILE when RF-Profile applied on ap-group	Verifying that user is able to delete RF -PROFILE when RF-Profile applied on ap-group	Passed	
MEJ87IIS_Reg_118	Verify that ap-group and rf -profile config remain the same after performing upgrade/downgrade the controller	To check that ap-group and rf -profile config remain the same after performing upgrade/downgrade the controller	Passed	
MEJ87IIS_Reg_119	Apply the RF-profile on internal AP group	Verify that user is able to apply RF profile on internal AP's ap group or not	Passed	
MEJ87S_Reg_193	Adding the ap in AP group	Verify that user is able to add ap in ap group or not	Passed	
MEJ87S_Reg_194	Adding the wlan in AP group and connecting the JOS client	To verify that user is able to connecting the different OS client with ap group or not	Passed	
MEJ87S_Reg_195	Adding the wlan in AP group and connecting the android client	To verify that user is able to connecting the different OS client with ap group or not	Passed	
MEJ87S_Reg_196	Adding the wlan in AP group and connecting the IOS client	To verify that user is able to connecting the different OS client with ap group or not	Passed	
MEJ87S_Reg_197	Apply 802.11 a RF -Profile on the ap group and connecting the client	Verify that user is to apply 802.11 a RF -Profile on the ap group or not	Passed	
MEJ87S_Reg_198	Apply the 802.11 b RF -Profile on ap group and connecting the client	Verify that user is able to apply 802.11 b RF -Profile on the ap group or not	Passed	

MEJ87S_Reg_199	Verify that ap-group and rf -profile config remain the same after performing the forced failover on master ap	To check that ap-group and rf -profile config remain the same after performing the forced failover on master ap	Passed	
MEJ87S_Reg_200	Checking that user is able to delete AP -group when ap is associated with ap-group	Verifying that whether user is able to delete ap-group or not when ap is associated with ap group	Passed	
MEJ87S_Reg_201	Checking that user is able to delete RF -PROFILE when RF-Profile applied on ap-group	Verifying that user is able to delete RF -PROFILE when RF-Profile applied on ap-group	Passed	
MEJ87S_Reg_202	Verify that ap-group and rf -profile config remain the same after performing upgrade/downgrade the controller	To check that ap-group and rf -profile config remain the same after performing upgrade/downgrade the controller	Passed	
MEJ87S_Reg_203	Checking that client limit per radio basis in high density	Verify that user is able to limit client count on the basis of rf-profile or not	Passed	
MEJ87S_Reg_204	Verify the data rate of client after apply the rf-profile	Checking that client is getting the data rate(if client supported) as config in rf-profile	Passed	
MEJ87S_Reg_205	Apply the RF-profile on internal AP group	Verify that user is able to apply RF profile on internal AP's ap group or not	Passed	
MEJ87S_Reg_206	Changing the internal AP group	Verify that user is able to change internal ap group or not	Passed	
MEJ87S_Reg_207	Viewing the ap group via read-only user	Verify that user is able to view the ap-group in read-onlyusers	Passed	

CME Crashes(DHCP/Troubleshooting)

Logical ID	Title	Description	Status	Defect ID
------------	-------	-------------	--------	-----------

MEJ87IIS_Reg_120	Creating the DHCP Scope with valid IP address	To verify whether DHCP scope is creating or not with valid details	Failed	CSCvj13318
MEJ87IIS_Reg_121	Creating the DHCP scope form CLI with valid IP address	To verify whether DHCP scope is created or not with valid IP address form CLI	Passed	
MEJ87IIS_Reg_122	Creating the DHCP scope form CLI with invalid IP address	To verify whether DHCP scope is created or not with invalid IP address form CLI	Passed	
MEJ87IIS_Reg_123	Changing the DHCP scope default gateway from Network to Mobility Express	To verify whether DHCP scope default gateway changing from Network to Mobility Express or not	Passed	
MEJ87IIS_Reg_124	Changing the RRM details after client connected to WLAN	To verify whether DHCP going to Crash or not after changing the RRM details	Passed	
MEJ87IIS_Reg_125	Enabling/Disabling the Central NAT	To verify whether Central NAT enabling/Disabling without any issues or not	Passed	
MEJ87IIS_Reg_126	Creating more than 10 DHCP scopes and assign to different WLANs	To verify whether more than 10 DHCP scopes are created and assigned to WLAN without any issues or not	Passed	
MEJ87IIS_Reg_127	Checking the DHCP Leases after client connected to the DHCP	To verify whether DHCP leases are showing or not after client connected to DHCP	Passed	
MEJ87IIS_Reg_128	Assigning the DHCP scope to WLAN with network	To verify whether DHCP scope assigned to the WLAN or not with Network DHCP	Passed	
MEJ87IIS_Reg_129	Assigning the DHCP scope to WLAN with Mobility Express	To verify whether DHCP scope assigned to the WLAN or not with mobility capable DHCP	Passed	

MEJ87IIS_Reg_130	Restarting the Controller	To verify whether Controller is restarting or not	Passed	
MEJ87IIS_Reg_131	Clearing the Controller Configurations	To verify whether Controller Configurations are clearing or not	Passed	
MEJ87IIS_Reg_132	Export the Controller Configurations	To verify whether Controller Configurations are Exporting or not	Passed with exception	CSCvj11216
MEJ87IIS_Reg_133	Import the Controller Configurations	To verify whether Controller Configurations are importing or not	Passed with exception	CSCvj11216
MEJ87IIS_Reg_134	Migrate the Cisco Mobility express deployment	To verify whether AP can be migrating to new controller or not	Passed	
MEJ87IIS_Reg_135	Downloading the support bundle from Controller	To verify whether Support bundle downloading successfully or not	Passed	
MEJ87IIS_Reg_136	Invalid DNS server IP address configuration	To verify whether DNS ip address field accepting the Invalid IP address or not	Passed	
MEJ87IIS_Reg_137	Performing the PING test with valid/invalid IP	To verify whether PING test is performing with valid/invalid IP address successfully or not	Passed	
MEJ87IIS_Reg_138	Performing the DNS test without DNS server IP config	To verify whether DNS test is performing or not without DNS server IP address config	Passed	
MEJ87IIS_Reg_139	Checking the Radius response	To verify whether Radius response is applying successfully or not	Passed	
MEJ87IIS_Reg_140	Performing the all tests	To verify whether all tests are performing or not	Passed	

MEJ87IIS_Reg_141	Invalid Calea details	To verify whether invalid CALEA details are configuring successfully or not	Passed	
MEJ87S_Reg_208	Creating the DHCP Scope with valid IP address	To verify whether DHCP scope is creating or not with valid details	Passed	
MEJ87S_Reg_209	Creating the DHCP scope form CLI with valid IP address	To verify whether DHCP scope is created or not with valid IP address form CLI	Passed	
MEJ87S_Reg_210	Creating the DHCP scope form CLI with invalid IP address	To verify whether DHCP scope is created or not with invalid IP address form CLI	Passed	
MEJ87S_Reg_211	Changing the DHCP scope default gateway from Network to Mobility Express	To verify whether DHCP scope default gateway changing from Network to Mobility Express or not	Passed	
MEJ87S_Reg_212	Changing the RRM details after client connected to WLAN	To verify whether DHCP going to Crash or not after changing the RRM details	Passed	
MEJ87S_Reg_213	Enabling/Disabling the P2P blocking through CLI	To verify whether P2P blocking enabling/disabling through CLI or not	Passed	
MEJ87S_Reg_214	Enabling/Disabling the Central NAT	To verify whether Central NAT enabling/Disabling without any issues or not	Passed	
MEJ87S_Reg_215	Creating more than 10 DHCP scopes and assign to different WLANs	To verify whether more than 10 DHCP scopes are created and assigned to WLAN without any issues or not	Passed	
MEJ87S_Reg_216	Checking the DHCP Leases after client connected to the DHCP	To verify whether DHCP leases are showing or not after client connected to DHCP	Passed	

MEJ87S_Reg_217	Assigning the DHCP scope to WLAN with network	To verify whether DHCP scope assigned to the WLAN or not with Network DHCP	Passed	
MEJ87S_Reg_218	Assigning the DHCP scope to WLAN with Mobility Express	To verify whether DHCP scope assigned to the WLAN or not with mobility capable DHCP	Passed	
MEJ87S_Reg_219	Restarting the Controller	To verify whether Controller is restarting or not	Passed	
MEJ87S_Reg_220	Clearing the Controller Configurations	To verify whether Controller Configurations are clearing or not	Passed	
MEJ87S_Reg_221	Export the Controller Configurations	To verify whether Controller Configurations are Exporting or not	Passed	
MEJ87S_Reg_222	Import the Controller Configurations	To verify whether Controller Configurations are importing or not	Passed	
MEJ87S_Reg_223	Migrate the Cisco Mobility express deployment	To verify whether AP can be migrating to new controller or not	Passed	
MEJ87S_Reg_224	Downloading the support bundle from Controller	To verify whether Support bundle downloading successfully or not	Passed	
MEJ87S_Reg_225	Invalid DNS server IP address configuration	To verify whether DNS ip address field accepting the Invalid IP address or not	Passed	
MEJ87S_Reg_226	Performing the PING test with valid/invalid IP	To verify whether PING test is performing with valid/invalid IP address successfully or not	Passed	
MEJ87S_Reg_227	Performing the DNS test without DNS server IP config	To verify whether DNS test is performing or not without DNS server IP address config	Passed	

MEJ87S_Reg_228	Checking the Radius response	To verify whether Radius response is applying successfully or not	Passed	
MEJ87S_Reg_229	Performing the all tests	To verify whether all tests are performing or not	Passed	
MEJ87S_Reg_230	Invalid Calea details	To verify whether invalid CALEA details are configuring successfully or not	Passed	

Client Auth Failures(AAA Failures/WLC Failures)

Logical ID	Title	Description	Status	Defect ID
MEJ87IIS_Reg_142	Client connectivity with WPA2 personal security with correct credentials .	To verify if the client connects to WLAN with WPA2 personal security or not with the correct credentials.	Passed	
MEJ87IIS_Reg_143	Client connectivity with WPA2 personal security with Wrong credentials .	To verify if the client connects to WLAN with WPA2 personal security or not with theWrong credentials.	Passed	
MEJ87IIS_Reg_144	Configuring Client Idle timeout for a particular WLAN and check if the timeout works properly.	To configure Client ideal Timeout and check if the timeout for the client works .	Passed	
MEJ87IIS_Reg_145	Configuring Maximum no. of client connections to be accepted for a particular WLAN.	To configure maximum number of clients to a particular WLAN and check if only the configured number of clients gets connected to the WLAN	Passed	
MEJ87IIS_Reg_146	Configuring Session timeout for WLAN and check if the client de-auth when the timer gets expired.	To Enable and configure session timeout for WLAN and check if the session timeout interval works fine or not	Passed	

MEJ87IIS_Reg_147	Configuring Maximum 802.1x session initiation per AP at a time	To configure Maximum 802.1x session per AP and connecting a client to it and check if the only the particular clients with 802.1x auth gets connected.	Passed	
MEJ87IIS_Reg_148	Connecting a client with WPA2 enterprises security with incorrect credentials and debugging the client for errors .	To provide wrong credentials for the client and check if the clients gets connected or not.	Passed	
MEJ87IIS_Reg_149	Connecting a JOS Client with WPA2 enterprises security and debugging the client for errors .	To verify that JOS client connect succesfully with WPA2 enterprises or not	Passed	
MEJ87IIS_Reg_150	Connecting 3 Window Client with WPA2 enterprises security and debugging the client for errors .	To verify that Window client connect succesfully with WPA2 enterprises or not	Passed	
MEJ87IIS_Reg_151	Connecting 2 different Android Client with WPA2 enterprises security and debugging the client for errors .	To verify that 2 different Android client with different android versions connect succesfully with WPA2 enterprises or not	Passed	
MEJ87IIS_Reg_152	Connecting a IOS Client with WPA2 enterprises security and debugging the client for errors .	To verify that IOS client connect succesfully with WPA2 enterprises or not	Passed	
MEJ87IIS_Reg_153	Connecting a MAC os Client with WPA2 enterprises security and debugging the client for errors .	To verify that MAC os client connect succesfully with WPA2 enterprises or not	Passed	

MEJ87IIS_Reg_154	Connecting a Client with WPA2 enterprises with Local Authentication (AP) and debugging the client for errors .	To verify that client connect successfully to WLAN with WPA2 enterprises and Local Authentication or not	Passed	
MEJ87IIS_Reg_155	Client connectivity with WPA2 personal security with Mac Filtering	To Connect a client with WPA2 personal with MAC filtering enabled and Whitelisting the clients MAC address.	Passed	
MEJ87IIS_Reg_156	Client connectivity with WPA2 personal security with Mac Filtering with Black list	To Connect a client with WPA2 personal with MAC filtering enabled and Black listing the clients MAC address.	Passed	
MEJ87IIS_Reg_157	Connecting a client through Guest with Internal Splash page Network through AAA server.	To Connect a client to a Guest Network using a AAA server and check if the client gets connected to it	Passed	
MEJ87IIS_Reg_158	Connecting a client through Guest with External Splash page Network through AAA server.	To Connect a client to a Guest Network using a AAA server and check if the client gets connected to it	Passed	
MEJ87IIS_Reg_159	Creating a DHCP scope and check if the IP address given in the scope is given to client.	To Configure DHCP scope and check if the Ip address is given to the client and check if the ip address allocated is shown in the DHCP Allocates leases.	Passed	
MEJ87S_Reg_231	Client connectivity with WPA2 personal security with correct credentials .	To verify if the client connects to WLAN with WPA2 personal security or not with the correct credentials.	Passed	
MEJ87S_Reg_232	Client connectivity with WPA2 personal security with Wrong credentials .	To verify if the client connects to WLAN with WPA2 personal security or not with theWrong credentials.	Passed	

MEJ87S_Reg_233	Configuring Client Idle timeout for a particular WLAN and check if the timeout works properly.	To configure Client ideal Timeout and check if the timeout for the client works .	Passed	
MEJ87S_Reg_234	Configuring Maximum no. of client connections to be accepted for a particular WLAN.	To configure maximum number of clients to a particular WLAN and check if only the configured number of clients gets connected to the WLAN	Passed	
MEJ87S_Reg_235	Configuring Session timeout for WLAN and check if the client de-auth when the timer gets expired.	To Enable and configure session timeout for WLAN and check if the session timeout interval works fine or not	Passed	
MEJ87S_Reg_236	Configuring Maximum 802.1x session initiation per AP at a time	To configure Maximum 802.1x session per AP and connecting a client to it and check if the only the particular clients with 802.1x auth gets connected.	Passed	
MEJ87S_Reg_237	Connecting a client with WPA2 enterprises security with incorrect credentials and debugging the client for errors .	To provide wrong credentials for the client and check if the clients gets connected or not.	Passed	
MEJ87S_Reg_238	Connecting a JOS Client with WPA2 enterprises security and debugging the client for errors .	To verify that JOS client connect succesfully with WPA2 enterprises or not	Passed	
MEJ87S_Reg_239	Connecting 3 Window Client with WPA2 enterprises security and debugging the client for errors .	To verify that Window client connect succesfully with WPA2 enterprises or not	Passed	

MEJ87S_Reg_240	Connecting 2 different Android Client with WPA2 enterprises security and debugging the client for errors .	To verify that 2 different Android client with different android versions connect succesfully with WPA2 enterprises or not	Passed	
MEJ87S_Reg_241	Connecting a IOS Client with WPA2 enterprises security and debugging the client for errors .	To verify that IOS client connect succesfully with WPA2 enterprises or not	Passed	
MEJ87S_Reg_242	Connecting a MAC os Client with WPA2 enterprises security and debugging the client for errors .	To verify that MAC os client connect succesfully with WPA2 enterprises or not	Passed	
MEJ87S_Reg_243	Connecting a Client with WPA2 enterprises with Local Authentication (AP) and debugging the client for errors .	To verify that client connect succesfully to WLAN with WPA2 enterprises and Local Authentication or not	Passed	
MEJ87S_Reg_244	Client connectivity with WPA2 personal security with Mac Filtering	To Connect a client with WPA2 personal with MAC filtering enabled and Whitelisting the clients MAC address.	Passed	
MEJ87S_Reg_245	Client connectivity with WPA2 personal security with Mac Filtering with Black list	To Connect a client with WPA2 personal with MAC filtering enabled and Black listing the clients MAC address.	Passed	
MEJ87S_Reg_246	Connecting a client through Guest with Internal Splash page Network through AAA server.	To Connect a client to a Guest Network using a AAA server and check if the client gets connected to it	Passed	
MEJ87S_Reg_247	Connecting a client through Guest with External Splash page Network through AAA server.	To Connect a client to a Guest Network using a AAA server and check if the client gets connected to it	Passed	

MEJ87S_Reg_248	Creating a DHCP scope and check if the IP address given in the scope is given to client.	To Configure DHCP scope and check if the Ip address is given to the client and check if the ip address allocated is shown in the DHCP Allocates leases.	Passed	
----------------	--	---	--------	--

Intra/Inter WLC Roaming Failures(Ping Pong Issues)

Logical ID	Title	Description	Status	Defect ID
MEJ87IIS_Reg_160	Intra Controller Roaming with Open Security	To verify whether Client is Roaming with Open Security or not between Aps	Passed	
MEJ87IIS_Reg_161	Intra Controller Roaming with WPA2 Security	To verify whether Client is Roaming with WPA2 Security or not between Aps	Passed	
MEJ87IIS_Reg_162	Intra Controller Roaming with WPA Enterprise + Radius server Security	To verify whether Client is Roaming with WPA Enterprise + Radios Security or not between Aps	Passed	
MEJ87IIS_Reg_163	Intra Controller Roaming with WPA Enterprise + AP Security	To verify whether Client is Roaming with WPA Enterprise + AP Security or not between Aps	Passed	
MEJ87IIS_Reg_164	Intra Controller Roaming with WPA2+Mac-filtering	To verify whether Client is Roaming with WPA2+ Mac-filtering security or not between Aps	Passed	
MEJ87IIS_Reg_165	Intra Controller Roaming with Guest Network+Mac-filtering	To verify whether Client is Roaming with Guest Network+Mac-filtering security or not between Aps	Passed	
MEJ87IIS_Reg_166	Intra Controller Roaming with Guest Network in Internal splash page+Local user account	To verify whether Client is Roaming in Guest Network with Internal splash page+Local user account or not	Passed	

Intra/Inter WLC Roaming Failures(Ping Pong Issues)

MEJ87IIS_Reg_167	Intra Controller Roaming with Guest Network in Internal splash page+Web consent	To verify whether Client is Roaming in Guest Network with Internal splash page+Web consent	Passed	
MEJ87IIS_Reg_168	Intra Controller Roaming with Guest Network in Internal splash page+Email address	To verify whether Client is Roaming in Guest Network with Internal splash page+Email address	Passed	
MEJ87IIS_Reg_169	Intra Controller Roaming with Guest Network in Internal splash page+Radius server	To verify whether Client is Roaming in Guest Network with Internal splash page+Radius server	Passed	
MEJ87IIS_Reg_170	Intra Controller Roaming with Guest Network in Internal splash page+WPA2 personal	To verify whether Client is Roaming in Guest Network with Internal splash page+WPA2 personal	Passed	
MEJ87IIS_Reg_171	Intra Controller Roaming with Guest Network in CMX Connect	To verify whether Client is Roaming in Guest Network with CMX Connect or not	Passed	
MEJ87IIS_Reg_172	Intra Controller Roaming with Guest Network in External splash page+Local user account	To verify whether Client is Roaming in Guest Network with External splash page+Local user account	Passed	
MEJ87IIS_Reg_173	Intra Controller Roaming with Guest Network in External splash page+Web consent	To verify whether Client is Roaming in Guest Network with External splash page+Web consent	Passed	
MEJ87IIS_Reg_174	Intra Controller Roaming with Guest Network in External splash page+Email address	To verify whether Client is Roaming in Guest Network with External splash page+Email address	Passed	
MEJ87IIS_Reg_175	Intra Controller Roaming with Guest Network in External splash page+Radius server	To verify whether Client is Roaming in Guest Network with External splash page+Radius server	Passed	

MEJ87IIS_Reg_176	Intra Controller Roaming with Guest Network in External splash page+WPA personal	To verify whether Client is Roaming in Guest Network with External splash page+WPA2 personal	Passed	
MEJ87S_Reg_249	Intra Controller Roaming with Open Security	To verify whether Client is Roaming with Open Security or not between Aps	Passed	
MEJ87S_Reg_250	Intra Controller Roaming with WPA2 Security	To verify whether Client is Roaming with WPA2 Security or not between Aps	Passed	
MEJ87S_Reg_251	Intra Controller Roaming with WPA Enterprise + Radius server Security	To verify whether Client is Roaming with WPA Enterprise + Radios Security or not between Aps	Passed	
MEJ87S_Reg_252	Intra Controller Roaming with WPA Enterprise + AP Security	To verify whether Client is Roaming with WPA Enterprise + AP Security or not between Aps	Passed	
MEJ87S_Reg_253	Intra Controller Roaming with WPA2+Mac-filtering	To verify whether Client is Roaming with WPA2+ Mac-filtering security or not between Aps	Passed	
MEJ87S_Reg_254	Intra Controller Roaming with Guest Network+Mac-filtering	To verify whether Client is Roaming with Guest Network+Mac-filtering security or not between Aps	Passed	
MEJ87S_Reg_255	Intra Controller Roaming with Guest Network in Internal splash page+Local user account	To verify whether Client is Roaming in Guest Network with Internal splash page+Local user account or not	Passed	
MEJ87S_Reg_256	Intra Controller Roaming with Guest Network in Internal splash page+Web consent	To verify whether Client is Roaming in Guest Network with Internal splash page+Web consent	Passed	
MEJ87S_Reg_257	Intra Controller Roaming with Guest Network in Internal splash page+Email address	To verify whether Client is Roaming in Guest Network with Internal splash page+Email address	Passed	

MEJ87S_Reg_258	Intra Controller Roaming with Guest Network in Internal splash page+Radius server	To verify whether Client is Roaming in Guest Network with Internal splash page+Radius server	Passed	
MEJ87S_Reg_259	Intra Controller Roaming with Guest Network in Internal splash page+WPA2 personal	To verify whether Client is Roaming in Guest Network with Internal splash page+WPA2 personal	Passed	
MEJ87S_Reg_260	Intra Controller Roaming with Guest Network in CMX Connect	To verify whether Client is Roaming in Guest Network with CMX Connect or not	Passed	
MEJ87S_Reg_261	Intra Controller Roaming with Guest Network in External splash page+Local user account	To verify whether Client is Roaming in Guest Network with External splash page+Local user account	Passed	
MEJ87S_Reg_262	Intra Controller Roaming with Guest Network in External splash page+Web consent	To verify whether Client is Roaming in Guest Network with External splash page+Web consent	Passed	
MEJ87S_Reg_263	Intra Controller Roaming with Guest Network in External splash page+Email address	To verify whether Client is Roaming in Guest Network with External splash page+Email address	Passed	
MEJ87S_Reg_264	Intra Controller Roaming with Guest Network in External splash page+Radius server	To verify whether Client is Roaming in Guest Network with External splash page+Radius server	Passed	
MEJ87S_Reg_265	Intra Controller Roaming with Guest Network in External splash page+WPA personal	To verify whether Client is Roaming in Guest Network with External splash page+WPA2 personal	Passed	

Master AP Fail-over Issues

Logical ID	Title	Description	Status	Defect ID
------------	-------	-------------	--------	-----------

MEJ87IIS_Reg_177	CAPWAP AP to ME Capable AP	To verify whether CAPWAP can be changed to ME capable AP or not	Passed with exception	CSCvi79996
MEJ87IIS_Reg_178	Making the ME Capable AP to Preferred master AP	To verify whether ME AP is changing the Preferred Master AP or not	Passed	
MEJ87IIS_Reg_179	Changing the next preferred ME capable AP to Controller from UI	To verify whether Next preferred Master AP can changing the ME or not by using the UI	Passed	
MEJ87IIS_Reg_180	Changing the next preferred ME capable AP to Controller from CLI	To verify whether Next preferred Master AP can changing the ME or not by using the CLI	Passed	
MEJ87IIS_Reg_181	Making the More than 5 Aps to ME capable	To verify whether more than 5 Aps are changing the state to ME capable or not	Passed	
MEJ87IIS_Reg_182	Deleting the Master Prepared AP from CLI	To verify whether Master preferred AP is deleting from CLI or not	Passed	
MEJ87IIS_Reg_183	Configuring the Controller IP address with DHCP server	To verify whether DHCP server IP address is assign to the Controller and come up with same IP address or not	Passed	
MEJ87IIS_Reg_184	Changing the CAPWAP to CAPWAP	To verify whether proper error showing or not at the time of CAPWAP changing to CAPWAP	Passed	
MEJ87IIS_Reg_185	Assigning the Global AP Configurations	To verify whether Global AP Configurations authenticate to the AP or not	Passed	
MEJ87IIS_Reg_186	Exporting the Configurations after Next master AP Configurations	To verify whether Export Configurations are showing properly or not after next master ap select	Passed	

MEJ87IIS_Reg_187	Importing the Configurations after Next master AP Configurations	To verify whether Import Configurations are showing properly or not after next master ap select	Passed	
MEJ87IIS_Reg_188	802.1x Configurations to AP in CME	To verify whether 802.1x Configurations are applying to the AP in CME or not	Passed	
MEJ87IIS_Reg_189	clearing the 802.1x Configurations to AP in CME	To verify whether 802.1x credentials are deleting or not	Passed	
MEJ87S_Reg_266	CAPWAP AP to ME Capable AP	To verify whether CAPWAP can be changed to ME capable AP or not	Passed	
MEJ87S_Reg_267	Making the ME Capable AP to Preferred master AP	To verify whether ME AP is changing the Preferred Master AP or not	Passed	
MEJ87S_Reg_268	Changing the next preferred ME capable AP to Controller from UI	To verify whether Next preferred Master AP can changing the ME or not by using the UI	Passed	
MEJ87S_Reg_269	Changing the next preferred ME capable AP to Controller from CLI	To verify whether Next preferred Master AP can changing the ME or not by using the CLI	Passed	
MEJ87S_Reg_270	Making the More than 5 Aps to ME capable	To verify whether more than 5 Aps are changing the state to ME capable or not	Passed	
MEJ87S_Reg_271	Deleting the Master Prepared AP from CLI	To verify whether Master preferred AP is deleting from CLI or not	Passed	
MEJ87S_Reg_272	Configuring the Controller IP address with DHCP server	To verify whether DHCP server IP address is assign to the Controller and come up with same IP address or not	Passed	

MEJ87S_Reg_273	Changing the CAPWAP to CAPWAP	To verify whether proper error showing or not at the time of CAPWAP changing to CAPWAP	Passed	
MEJ87S_Reg_274	Assigning the Global AP Configurations	To verify whether Global AP Configurations authenticate to the AP or not	Passed	
MEJ87S_Reg_275	Exporting the Configurations after Next master AP Configurations	To verify whether Export Configurations are showing properly or not after next master ap select	Passed	
MEJ87S_Reg_276	Importing the Configurations after Next master AP Configurations	To verify whether Import Configurations are showing properly or not after next master ap select	Passed	
MEJ87S_Reg_277	802.1x Configurations to AP in CME	To verify whether 802.1x Configurations are applying to the AP in CME or not	Passed	
MEJ87S_Reg_278	clearing the 802.1x Configurations to AP in CME	To verify whether 802.1x credentials are deleting or not	Passed	

TLS Tunnel

Logical ID	Title	Description	Status	Defect ID
MEJ87IIS_Reg_256	Associating Windows JOS Client with WPA2-dot1x using ISE server in cloud	To verify whether Windows JOS client associated successfully or not with WPA2-dot1x via ISE server configured in cloud	Passed	
MEJ87IIS_Reg_257	Associating Apple iOS Client with WPA2-dot1x using ISE server in cloud	To verify whether Apple iOS client associated successfully or not with WPA2-dot1x via ISE server configured in cloud	Passed	

MEJ87IIS_Reg_258	Associating MAC OS Client with WPA2-dot1x using ISE server in cloud	To verify whether MAC OS client associated successfully or not with WPA2-dot1x via ISE server configured in cloud	Passed	
MEJ87IIS_Reg_259	Associating Android Client with WPA2-dot1x using ISE server in cloud	To verify whether Android client associated successfully or not with WPA2-dot1x via ISE server configured in cloud	Passed	
MEJ87IIS_Reg_260	Allowing the user for complete access to CME network via TACACS (ISE server configured in cloud)	To check whether user can able to read-write access the complete CME network or not via TACACS (ISE server configured in cloud)	Passed	
MEJ87IIS_Reg_261	Associating all OS clients to CME with Security MAC filtering via Cloud ISE server	To check whether all OS clients associated successfully or not to CME with Mac filtering via Cloud ISE server	Passed	
MEJ87IIS_Reg_262	Setting up the tunnel configurations in CME	To check whether tunnel status get UP or not after configuring in CME	Passed	
MEJ87IIS_Reg_263	Checking the ME association with PI	To check whether ME is getting synchronized or not with PI	Passed	
MEJ87IIS_Reg_264	Checking the TLS Tunnel configurations after export/import the config file via TFTP	To check whether TLS Tunnel configurations gets retained or not while export/import the config file via TFTP	Passed	
MEJ87IIS_Reg_265	Checking the RADIUS server's reachability from CME	To check whether cloud RADIUS server is reachable or not from CME using Ping functionality/username in troubleshooting tools page	Passed	
MEJ87S_Reg_345	Associating Windows JOS Client with WPA2-dot1x using ISE server in cloud	To verify whether Windows JOS client associated successfully or not with WPA2-dot1x via ISE server configured in cloud	Passed	

MEJ87S_Reg_346	Associating Apple iOS Client with WPA2-dot1x using ISE server in cloud	To verify whether Apple iOS client associated successfully or not with WPA2-dot1x via ISE server configured in cloud	Passed	
MEJ87S_Reg_347	Associating MAC OS Client with WPA2-dot1x using ISE server in cloud	To verify whether MAC OS client associated successfully or not with WPA2-dot1x via ISE server configured in cloud	Passed	
MEJ87S_Reg_348	Associating Android Client with WPA2-dot1x using ISE server in cloud	To verify whether Android client associated successfully or not with WPA2-dot1x via ISE server configured in cloud	Passed	
MEJ87S_Reg_349	Allowing the user for complete access to CME network via TACACS (ISE server configured in cloud)	To check whether user can able to read-write access the complete CME network or not via TACACS (ISE server configured in cloud)	Passed	
MEJ87S_Reg_350	Associating all OS clients to CME with Security MAC filtering via Cloud ISE server	To check whether all OS clients associated successfully or not to CME with Mac filtering via Cloud ISE server	Passed	
MEJ87S_Reg_351	Setting up the tunnel configurations in CME	To check whether tunnel status get UP or not after configuring in CME	Passed	
MEJ87S_Reg_352	Checking the ME association with PI	To check whether ME is getting synchronized or not with PI	Passed	
MEJ87S_Reg_353	Checking the TLS Tunnel configurations after export/import the config file via TFTP	To check whether TLS Tunnel configurations gets retained or not while export/import the config file via TFTP	Passed	
MEJ87S_Reg_354	Checking the RADIUS server's reachability from CME	To check whether cloud RADIUS server is reachable or not from CME using Ping functionality/username in troubleshooting tools page	Passed	

Global AP configuration 802.1x

Logical ID	Title	Description	Status	Defect ID
MEJ87IIS_Reg_243	Adding Network devices in ISE with configuring 802.1x profile.	To check whether Network devices (AireOS & IOS controllers) are added in ISE or not with enabling the TrustSec settings.	Passed	
MEJ87IIS_Reg_244	Validating the 802.1x Global AP configuration GUI.	To Validate the GUI of the Global AP credential and check if the UI is works fine or not.	Passed	
MEJ87IIS_Reg_245	Connecting a JOS client to a AP with Global 802.1x Authentication.	To check if the JOS client gets connected to the the AP configured with 802.1x	Passed	
MEJ87IIS_Reg_246	Connecting a Windows client to a AP with Global 802.1x Authentication.	To check if the Windows client gets connected to the the AP configured with 802.1x	Passed	
MEJ87IIS_Reg_247	Connecting a Android client to a AP with Global 802.1x Authentication.	To check if the Android client gets connected to the the AP configured with 802.1x	Passed	
MEJ87IIS_Reg_248	Connecting a IOS client to a AP with Global 802.1x Authentication.	To check if the IOS client gets connected to the the AP configured with 802.1x	Passed	
MEJ87IIS_Reg_249	Connecting a MAC OS client to a AP with Global 802.1x Authentication.	To check if the MAC OS client gets connected to the the AP configured with 802.1x	Passed	
MEJ87IIS_Reg_250	Applying Global 802.1x Authentication for non ME capable AP and connecting a client to that AP	To check if the Global 802.1x authentication is applied for Non ME capable AP and check if a client is able to connect to it or not.	Passed	
MEJ87IIS_Reg_251	Applying Global 802.1x Authentication for ME capable AP and connecting a client to that AP	To check if the Global 802.1x authentication is applied for ME capable AP and check if a client is able to connect to it or not.	Passed	

MEJ87S_Reg_285	Create the SNMP trap receiver name with invalid IP address.	To check whether the SNMP trap receiver is created with invalid IP address or not in CME GUI	Passed	
MEJ87S_Reg_286	Create the SNMP trap receiver name is the more than 31 characters in CME ui.	To check whether the SNMP trap receiver is created with more than 31 characters or not in CME GUI	Passed	
MEJ87S_Reg_287	Checking the validation of SNMP trap receiver information.	To check whether the SNMP trap receiver is received the information or not.	Passed	
MEJ87S_Reg_288	Verifying the severity filtering for SNMP trap receiver information.	To verify the severity filtering for SNMP trap receiver information.	Passed	
MEJ87S_Reg_289	Verifying the Device IP address filtering for SNMP trap receiver in PI	To verify the Device IP address filtering for SNMP trap receiver in PI	Passed	
MEJ87S_Reg_290	Create the SNMP trap receiver by using the invalid IP address in CME CLI.	To check whether the SNMP trap receiver is created or not in CME CLI	Passed	
MEJ87S_Reg_332	Adding Network devices in ISE with configuring 802.1x profile.	To check whether Network devices (AireOS & IOS controllers) are added in ISE or not with enabling the TrustSec settings.	Passed	
MEJ87S_Reg_333	Validating the 802.1x Global AP configuration GUI.	To Validate the GUI of the Global AP credential and check if the UI is works fine or not.	Passed	
MEJ87S_Reg_334	Connecting a JOS client to a AP with Global 802.1x Authentication.	To check if the JOS client gets connected to the the AP configured with 802.1x	Passed	
MEJ87S_Reg_335	Connecting a Windows client to a AP with Global 802.1x Authentication.	To check if the Windows client gets connected to the the AP configured with 802.1x	Passed	

MEJ87S_Reg_336	Connecting a Android client to a AP with Global 802.1x Authentication.	To check if the Android client gets connected to the the AP configured with 802.1x	Passed	
MEJ87S_Reg_337	Connecting a IOS client to a AP with Global 802.1x Authentication.	To check if the IOS client gets connected to the the AP configured with 802.1x	Passed	
MEJ87S_Reg_338	Connecting a MAC OS client to a AP with Global 802.1x Authentication.	To check if the MAC OS client gets connected to the the AP configured with 802.1x	Passed	
MEJ87S_Reg_339	Applying Global 802.1x Authentication for non ME cabale AP and connecting a client to that AP	To check if the Global 802.1x authentication is applied for Non ME capable AP and check if a client is able to connect to it or not.	Passed	
MEJ87S_Reg_340	Applying Global 802.1x Authentication for ME cabale AP and connecting a client to that AP	To check if the Global 802.1x authentication is applied for ME capable AP and check if a client is able to connect to it or not.	Passed	

OUI File Upload

Logical ID	Title	Description	Status	Defect ID
MEJ87IIS_Reg_190	OUI file uploading through TFTP server	To check whether OUI file is uploading or not through TFTP server	Passed	
MEJ87IIS_Reg_191	Uploading the invalid OUI file through TFTP server	Verify Invalid OUI file is uploading or not through TFTP sever	Passed	
MEJ87IIS_Reg_192	OUI file uploading through HTTP server	To check whether OUI file is uploading through HTTP server or not in ME UI	Passed	
MEJ87IIS_Reg_193	Invalid OUI File uploading through HTTP sever	Validate Invalid OUI file is uploading or not through HTTP server	Passed	
MEJ87IIS_Reg_194	uploading the OUI file through FTP server	To check whether OUI file is uploading or not	Passed	

MEJ87IIS_Reg_195	Invalid OUI File uploading through FTP sever	To check whether Invalid OUI file is uploading or not through FTP sever	Passed	
MEJ87S_Reg_279	OUI file uploading through TFTP server	To check whether OUI file is uploading or not through TFTP server	Passed	
MEJ87S_Reg_280	Uploading the invalid OUI file through TFTP server	Verify Invalid OUI file is uploading or not through TFTP sever	Passed	
MEJ87S_Reg_281	OUI file uploading through HTTP server	To check whether OUI file is uploading through HTTP server or not in ME UI	Passed	
MEJ87S_Reg_282	Invalid OUI File uploading through HTTP sever	Validate Invalid OUI file is uploading or not through HTTP server	Passed	
MEJ87S_Reg_283	uploading the OUI file through FTP server	To check whether OUI file is uploading or not	Passed	
MEJ87S_Reg_284	Invalid OUI File uploading through FTP sever	To check whether Invalid OUI file is uploading or not through FTP sever	Passed	

SNMP Trap Receivers

Logical ID	Title	Description	Status	Defect ID
MEJ87IIS_Reg_196	Create the SNMP trap receiver name with invalid IP address.	To check whether the SNMP trap receiver is created with invalid IP address or not in CME GUI	Passed	
MEJ87IIS_Reg_197	Create the SNMP trap receiver name is the more than 31 characters in CME ui.	To check whether the SNMP trap receiver is created with more than 31 characters or not in CME GUI	Passed	
MEJ87IIS_Reg_198	Checking the validation of SNMP trap receiver information.	To check whether the SNMP trap receiver is received the information or not.	Passed	

Central web authentication (CWA) with change of authorization (CoA)

MEJ87IIS_Reg_199	Verifying the severity filtering for SNMP trap receiver information.	To verify the severity filtering for SNMP trap receiver information.	Passed	
MEJ87IIS_Reg_200	Verifying the Device IP address filtering for SNMP trap receiver in PI	To verify the Device IP address filtering for SNMP trap receiver in PI	Passed	
MEJ87IIS_Reg_201	Create the SNMP trap receiver by using the invalid IP address in CME CLI.	To check whether the SNMP trap receiver is created or not in CME CLI	Passed	
MEJ87S_Reg_285	Create the SNMP trap receiver name with invalid IP address.	To check whether the SNMP trap receiver is created with invalid IP address or not in CME GUI	Passed	
MEJ87S_Reg_286	Create the SNMP trap receiver name is the more than 31 characters in CME ui.	To check whether the SNMP trap receiver is created with more than 31 characters or not in CME GUI	Passed	
MEJ87S_Reg_287	Checking the validation of SNMP trap receiver information.	To check whether the SNMP trap receiver is received the information or not.	Passed	
MEJ87S_Reg_288	Verifying the severity filtering for SNMP trap receiver information.	To verify the severity filtering for SNMP trap receiver information.	Passed	
MEJ87S_Reg_289	Verifying the Device IP address filtering for SNMP trap receiver in PI	To verify the Device IP address filtering for SNMP trap receiver in PI	Passed	
MEJ87S_Reg_290	Create the SNMP trap receiver by using the invalid IP address in CME CLI.	To check whether the SNMP trap receiver is created or not in CME CLI	Passed	

Central web authentication (CWA) with change of authorization (CoA)

Logical ID	Title	Description	Status	Defect Id
------------	-------	-------------	--------	-----------

MEJ87IIS_Reg_274	Creating a CWA along with ACL Configuration in CME UI	To check Whether CWA along with ACL Configuration in CME UI created or not	Failed	CSCvi35837
MEJ87IIS_Reg_275	Associating a Japanese Windows Client to a SSID which is mapped with ISE	To verify whether Japanese Windows Client which is mapped to ISE is redirected successfully or not.	Passed	
MEJ87IIS_Reg_276	Associating a iOS Client to a SSID which is mapped with ISE	To verify whether iOS Client which is mapped to ISE is redirected successfully or not	Passed	
MEJ87IIS_Reg_277	Associating a Android Client to a SSID which is mapped with ISE	To verify whether Android Client which is mapped to ISE is redirected successfully or not	Passed	
MEJ87IIS_Reg_278	Associating a MAC OS Client to a SSID which is mapped with ISE	To verify whether MAC Client which is mapped to ISE is redirected successfully or not	Passed	
MEJ87IIS_Reg_279	Associating a different Clients to SSID which is mapped with ISE and redirecting to Guest portal page with invalid credentials	To verify whether client connected to ssid redirecting to Guest portal page with invalid credentials	Passed	
MEJ87IIS_Reg_280	Associating a different Clients to a SSID which is mapped with ISE by creating AVC profile	To verify whether different Clients is redirected successfully and checking that particular application is dropped or not	Passed	

Central web authentication (CWA) with change of authorization (CoA)

MEJ87IIS_Reg_281	Associating a different Clients to a SSID which is mapped with ISE by denying the action in ACL	To verify whether Clients gets denied when it is connected to SSID which is mapped with ISE	Passed	
MEJ87IIS_Reg_282	Associating a different Clients to a SSID which is mapped with ISE by permitting the action in ACL using TCP protocol	To verify whether Clients gets connected to SSID which is mapped with ISE by permitting the action in ACL using TCP protocol	Passed	
MEJ87IIS_Reg_283	Associating a different Clients to a SSID which is mapped with ISE by permitting the action in ACL using UDP protocol	To verify whether Clients gets connected to SSID which is mapped with ISE by permitting the action in ACL using UDP protocol	Passed	
MEJ87IIS_Reg_284	Associating a different Clients to a SSID which is mapped with ISE by permitting the action in ACL using ICMP protocol	To verify whether Clients gets connected to SSID which is mapped with ISE by permitting the action in ACL using ICMP protocol	Passed	
MEJ87IIS_Reg_285	Checking the expired Radius Guest User for proper error message	To verify whether the expired Guest user gets proper Error messages when he logging in	Passed	
MEJ87IIS_Reg_286	Validate whether CME is switch between configured Radius servers	To verify whether AAA authentication is occurring when one radius server goes down	Passed	
MEJ87IIS_Reg_287	Reboot the Controller after CWA enabling	To verify whether Configurations are showing same or different after controller reboot	Passed	

MEJ87IIS_Reg_288	Creating a CWA along with ACL Configuration through CLI	To verify whether ACL rule is created or not through CLI	Passed	
MEJ87IIS_Reg_289	Checking the configuration of CWA when the user is in Read-only	To verify whether configuration display error message or not when the user is in Read-only	Failed	CSCvi74109

ME GUI for Bidirectional rate limit per client

Logical ID	Title	Description	Status	Defect ID
MEJ87S_BRL_01	Configuring rate limit for per client for JOS client with WPA 2 Personal security with QOS as Silver	To configure rate limit for JOS client with open security and QOS as silver and check if the client gets the rate that is been configured or not.	Failed	CSCvh48115
MEJ87S_BRL_02	Configuring rate limit for per client for Android client with WPA 2 Personal security with QOS as Silver	To configure rate limit for Android client with open security and QOS as silver and check if the client gets the rate that is been configured or not.	Passed	
MEJ87S_BRL_03	Configuring rate limit for per client for Mac OS client with WPA 2 Personal security with QOS as Silver	To configure rate limit for Mac OS client with open security and QOS as silver and check if the client gets the rate that is been configured or not.	Passed	
MEJ87S_BRL_04	Configuring rate limit for per client for IOS client with WPA 2 Personal security with QOS as Silver	To configure rate limit for IOS client with open security and QOS as silver and check if the client gets the rate that is been configured or not.	Passed	
MEJ87S_BRL_05	Configuring rate limit for per client with QOS as Gold for JOS client with WPA 2 Enterprise security	To configure rate limit per client with QOS as Gold and connecting a JOS client with WPA 2 Enterprise security and check if the rate limit is applied or not.	Failed	CSCvh48115

MEJ87S_BRL_06	Configuring rate limit for per client with QOS as Gold for Android client with WPA 2 Enterprise security	To configure rate limit per client with QOS as Gold and connecting a Android client with WPA 2 Enterprise security and check if the rate limit is applied or not.	Passed	
MEJ87S_BRL_07	Configuring rate limit for per client with QOS as Gold for IOS client with WPA 2 Enterprise security	To configure rate limit per client with QOS as Gold and connecting a IOS client with WPA 2 Enterprise security and check if the rate limit is applied or not.	Passed	
MEJ87S_BRL_08	Configuring rate limit for per client with QOS as Gold for Mac OS client with WPA 2 Enterprise security	To configure rate limit per client with QOS as Gold and connecting a Mac OS client with WPA 2 Enterprise security and check if the rate limit is applied or not.	Passed	
MEJ87S_BRL_09	Connecting a client to a WLAN configured with rate limit using two different AP	To configure rate limit for client and connecting a client to one AP and check the rate limit and making that AP down and connecting the client to other AP and check if the behavior of the client is same or not	Passed	
MEJ87S_BRL_10	Connecting a client to a WLAN configured with rate limit using one ME capable AP and Non Me capable AP in AP group	To Connecting a client to a WLAN configured with rate limit using one ME capable AP and Non Me capable AP in AP group	Passed	
MEJ87S_BRL_11	Creating a AVC rule for the WLAN for which rate limit is configured .	To configure lesser rate limit in WLAN and configuring higher rate limit in AVC and check if the rate limit for the client	Passed	

ME GUI with RLAN support for APs with multiple Ethernet ports

Logical ID	Title	Description	Status	Defect ID
------------	-------	-------------	--------	-----------

MEJ87S_RLAN_01	Creating a RLAN with Open security and connecting JOS windows 7 client to the RLAN .	To create a RLAN with Open security and connecting a JOS window 7 client to the RLAN and check if the client gets connected to the RLAN port in th AP and there is flow in traffic	Passed	
MEJ87S_RLAN_02	Creating a RLAN with Open security and connecting windows 10 client to the RLAN .	To create a RLAN with Open security and connecting a window 10 client to the RLAN and check if the client gets connected to the RLAN port in th AP and there is flow in traffic.	Passed	
MEJ87S_RLAN_03	Creating a RLAN with Open security and connecting Mac OS client to the RLAN .	To create a RLAN with Open security and connecting a Mac OS client to the RLAN and check if the client gets connected to the RLAN port in th AP and there is flow in traffic.	Passed	
MEJ87S_RLAN_04	Configuring a RLAN with Open security and Mac filtering with whitelist enabled and connecting JOS windows 7 client to the RLAN .	To configure a RLAN with Open security enabling MAC filtering with whitelist and connecting a JOS window 7 client to the RLAN and check if the client gets connected to the RLAN port in th AP and there is flow in traffic.	Passed	
MEJ87S_RLAN_05	Configuring a RLAN with Open security and Mac filtering with Blacklist enabled and connecting JOS windows 7 client to the RLAN .	To configure a RLAN with Open security enabling MAC filtering with whitelist and connecting a JOS window 7 client to the RLAN and check if the client gets connected to the RLAN port in th AP and there is flow in traffic.	Passed	

MEJ87S_RLAN_06	Creating a RLAN with Type 802.1X security and connecting JOS windows 7 client to the RLAN .	To create a RLAN with 802.1X security and connecting a JOS window 7 client to the RLAN and check if the client gets connected to the RLAN port in th AP and there is flow in traffic.	Failed	CSCvh65773
MEJ87S_RLAN_07	Creating a RLAN with 802.1X security and connecting windows 10 client to the RLAN .	To create a RLAN with 802.1X security and connecting a window 10 client to the RLAN and check if the client gets connected to the RLAN port in th AP and there is flow in traffic.	Failed	CSCvh65773
MEJ87S_RLAN_08	Creating a RLAN with Type 802.1X security and connecting Mac OS client to the RLAN .	To create a RLAN with 802.1X security and connecting a Mac OS client to the RLAN and check if the client gets connected to the RLAN port in th AP and there is flow in traffic.	Failed	CSCvh65773
MEJ87S_RLAN_09	Creating a RLAN with Type 802.1X security with host mode as single and connecting client to the RLAN .	To Create a RLAN with Type 802.1X security with host mode as single and authenticating server as External radius connecting client to the RLAN .	Failed	CSCvh65773
MEJ87S_RLAN_10	Creating a RLAN with Type 802.1X security with host mode as Multi keeping authentication server as External Radius and connecting client to the RLAN .	To Create a RLAN with Type 802.1X security with host mode as Multi keeping authentication server as External Radius and connecting client to the RLAN .	Failed	CSCvh65773
MEJ87S_RLAN_11	Configuring a RLAN with 802.1x security and Mac filtering with whitelist enabled and connecting JOS windows 7 client to the RLAN .	To configure a RLAN with 802.1x security enabling MAC filtering with whitelist and connecting a JOS window 7 client to the RLAN and check if the client gets connected to the RLAN port in th AP and there is flow in traffic.	Failed	CSCvh65773

MEJ87S_RLAN_12	Configuring a RLAN with 802.1x security and Mac filtering with Blacklist enabled and connecting JOS windows 7 client to the RLAN .	To configure a RLAN with 802.1x security enabling MAC filtering with whitelist and connecting a JOS window 7 client to the RLAN and check if the client gets connected to the RLAN port in th AP and there is flow in traffic.	Failed	CSCvh65773
MEJ87S_RLAN_13	Creating a RLAN with Guest network with different access type enabling MAB mode .	To create a RLAN with Guest network using different access type and enabling MAB mode and connecting a client to it.	Passed	
MEJ87S_RLAN_14	Configuring AVC profile for RLAN with 802.1x security and check if AVC profile is applied	To configure AVC profile for RLAN with 802.1x security and check fi the AVC profile gets applied to the client connecting to it or not.	Passed	
MEJ87S_RLAN_15	Enable AAA override and connecting a client to the AAA override enabled RLAN with 802.1x security .	To enable AAA override and connecting a IOS client to the AAA override enabled with 802.1x security RLAN and check if the VLAN from AAA server is overridden to the client	Passed	

ME GUI for Limit clients per radio

Logical ID	Title	Description	Status	Defect ID
MEJ87S_CPR_01	Configuring maximum Allowed Clients Per AP Radio as 4 and connecting client with WPA 2 Personal security.	To configure maximum allowed client Per AP radio as 4 and connecting 5 different client with radio policy as ALL and check if the number of client that is configured alone gets connected to the WLAN	Passed	

MEJ87S_CPR_02	Configuring maximum Allowed Clients Per AP Radio as 3 and connecting client with WPA 2 Enterprise security .	To configure maximum allowed client Per AP radio as 3 and connecting 4 different client with radio policy as ALL and now after 3 client disconnect one client and check if other client get authenticated to the WLAN	Passed	
MEJ87S_CPR_03	Configuring maximum allowed client per AP radio as 6 setting radio policy as 5 GHz and trying to connect 3 5GHZ client and 3 2.4GHz	To set radio policy as 5 GHz and trying to connect 3 5GHZ client and 3 2.4GHz while applying maximum allowed client per AP radio as 6 and check if only the 3 5 GHZ client get connected to it	Passed	
MEJ87S_CPR_04	Configuring maximum Allowed Clients Per AP Radio in RF profile as 4 and in WLAN as 3 and connecting the client	To configure maximum allowed client Per AP radio in RF profile and also setting the same in WLAN and check which of the configured number of clients gets connected .	Passed	
MEJ87S_CPR_05	Creating open security WLAN with radio policy as 5 GHz and configuring Maximum Allowed Clients Per AP Radio	To configure maximum allowed client per AP radio setting the WLAN security with Open and radio policy as 5 GHz and check if only the defined number of client alone connect to the WLAN.	Passed	
MEJ87S_CPR_06	Creating WPA 2 Personal security WLAN with radio policy as 5 GHz and configuring Maximum Allowed Clients Per AP Radio	To configure maximum allowed client per AP radio setting the WLAN security with WPA 2 Personal and radio policy as 5 GHz and check if only the defined number of client alone connect to the WLAN.	Passed	
MEJ87S_CPR_07	Creating WPA 2 Enterprise security WLAN with radio policy as 5 GHz and configuring Maximum Allowed Clients Per AP Radio	To configure maximum allowed client per AP radio setting the WLAN security with WPA 2 Enterprise and radio policy as 5 GHz and check if only the defined number of client alone connect to the WLAN.	Passed	

MEJ87S_CPR_08	Creating open security WLAN with radio policy as 2.4 GHz and configuring Maximum Allowed Clients Per AP Radio	To create open security WLAN configuring Maximum allowed client per AP radio with radio policy as 2.4 GHz and check if only the defined number of client alone connect to the WLAN.	Passed	
MEJ87S_CPR_09	Creating WPA 2 Personal security WLAN with radio policy as 2.4 GHz and configuring Maximum Allowed Clients Per AP Radio	To create WPA 2 Personal security WLAN configuring Maximum allowed client per AP radio with radio policy as 2.4 GHz and check if only the defined number of client alone connect to the WLAN.	Passed	
MEJ87S_CPR_10	Creating WPA 2 Enterprise security WLAN with radio policy as 2.4 GHz and configuring Maximum Allowed Clients Per AP Radio	To create WPA 2 Enterprise security WLAN configuring Maximum allowed client per AP radio with radio policy as 2.4 GHz and check if only the defined number of client alone connect to the WLAN.	Passed	

ME GUI for AAA Override of VLAN Name / VLAN Name-id template

Logical ID	Title	Description	Status	Defect ID
ME87S_AAA_VLAN_01	Enable AAA override and connecting a JOS window 7 client to the AAA override enabled WLAN with WPA 2 Personal security .	To enable AAA override and connecting a JOS window 7 client to the AAA override enabled with WPA 2 Personal security WLAN and check if the VLAN from AAA server is overridden to the client	Passed	
ME87S_AAA_VLAN_02	Enable AAA override and connecting a Android client to the AAA override enabled WLAN with WPA 2 Personal security .	To enable AAA override and connecting a Android client to the AAA override enabled with WPA 2 Personal security WLAN and check if the VLAN from AAA server is overridden to the client	Passed	

ME87S_AAA_VLAN_03	Enable AAA override and connecting a IOS client to the AAA override enabled WLAN with WPA 2 Personal security .	To enable AAA override and connecting a IOS client to the AAA override enabled with WPA 2 Personal security WLAN and check if the VLAN from AAA server is overridden to the client	Passed	
ME87S_AAA_VLAN_04	Enable AAA override and connecting a Mac OS client to the AAA override enabled WLAN with WPA 2 Personal security .	To enable AAA override and connecting a Mac OS client to the AAA override enabled with WPA 2 Personal security WLAN and check if the VLAN from AAA server is overridden to the client	Passed	
ME87S_AAA_VLAN_05	Connecting a JOS window 7 client to the AAA override enabled WLAN with WPA 2 Enterprise security enabled with AAA override .	To connect a JOS Window 7 client to AAA override enabled WLAN with WPA 2 Enterprise security and check if the Native VLAN is overridden or not.	Passed	
ME87S_AAA_VLAN_06	Connecting a Android client to the AAA override enabled WLAN with WPA 2 Enterprise security enabled with AAA override .	To connect a Android client to AAA override enabled WLAN with WPA 2 Enterprise security and check if the Native VLAN is overridden or not.	Passed	
ME87S_AAA_VLAN_07	Connecting a Android client to the AAA override enabled WLAN with WPA 2 Enterprise security enabled with AAA override .	To connect a IOS client to AAA override enabled WLAN with WPA 2 Enterprise security and check if the Native VLAN is overridden or not.	Passed	
ME87S_AAA_VLAN_08	Connecting a Android client to the AAA override enabled WLAN with WPA 2 Enterprise security enabled with AAA override .	To connect a Mac OS client to AAA override enabled WLAN with WPA 2 Enterprise security and check if the Native VLAN is overridden or not.	Passed	
ME87S_AAA_VLAN_09	Connecting a client to the WLAN enabled with AAA override but the configuration of VLAN on AAA is not done.	To connect a client to the WLAN enabled with AAA override and the configuration of VLAN is not done in the AAA server.	Passed	

ME GUI for Passive client support

Logical ID	Title	Description	Status	Defect ID
MEJ87S_PC_01	Configuring static IP for a wireless printer and enabling passive clients with security as Open	To configure static IP for Wireless printer and enabling passive client option in the controller with Open security and check if the clients details are shown in the client detail page or not.	Passed	
MEJ87S_PC_02	Configuring static IP for JOS Windows 7 client and enabling passive clients with security as Open	To configure static IP for JOS client and enabling passive client option in the controller with Open security and check if the clients details are shown in the client detail page or not.	Passed	
MEJ87S_PC_03	Configuring static IP for Windows 10 client and enabling passive clients with security as Open	To configure static IP for Windows client and enabling passive client option in the controller with Open security and check if the clients details are shown in the client detail page or not.	Passed	
MEJ87S_PC_04	Configuring static IP for Android client and enabling passive clients with security as Open	To configure static IP for Android client and enabling passive client option in the controller with Open security and check if the clients details are shown in the client detail page or not.	Passed	
MEJ87S_PC_05	Configuring static IP for IOS client and enabling passive clients with security as Open	To configure static IP for IOS client and enabling passive client option in the controller with Open security and check if the clients details are shown in the client detail page or not.	Passed	
MEJ87S_PC_06	Configuring static IP for Mac OS client and enabling passive clients with security as Open	To configure static IP for Mac OS client and enabling passive client option in the controller with Open security and check if the clients details are shown in the client detail page or not.	Passed	

MEJ87S_PC_07	Enabling passive clients with security as WPA 2 personal and configuring Static IP for JOS Windows 7 client	To enabling passive client option in the CME with WPA 2 personal while Configuring static IP for JOS client and check if the clients details are shown in the client detail page or not.	Passed	
MEJ87S_PC_08	Enabling passive clients with security as WPA 2 personal and configuring Static IP for Windows 10 client	To enabling passive client option in the CME with WPA 2 personal while Configuring static IP for Windows client and check if the clients details are shown in the client detail page or not.	Passed	
MEJ87S_PC_09	Enabling passive clients with security as WPA 2 personal and configuring Static IP for Android client	To enabling passive client option in the CME with WPA 2 personal while Configuring static IP for Android client and check if the clients details are shown in the client detail page or not.	Passed	
MEJ87S_PC_10	Enabling passive clients with security as WPA 2 personal and configuring Static IP for IOS client	To enabling passive client option in the CME with WPA 2 personal while Configuring static IP for IOS client and check if the clients details are shown in the client detail page or not.	Passed	
MEJ87S_PC_11	Enabling passive clients with security as WPA 2 personal and configuring Static IP for Mac OS client	To enabling passive client option in the CME with WPA 2 personal while Configuring static IP for Mac OS client and check if the clients details are shown in the client detail page or not.	Passed	
MEJ87S_PC_12	Connecting a JOS Windows 7 client to a WLAN configured with WPA 2 Enterprise security enabled with Passive client .	To connect a JOS client to a WPA 2 Enterprise security WLAN with Passive client option enabled by configuring the client with a static IP.	Passed	
MEJ87S_PC_13	Connecting a Windows 10 client to a WLAN configured with WPA 2 Enterprise security enabled with Passive client .	To connect a Windows client to a WPA 2 Enterprise security WLAN with Passive client option enabled by configuring the client with a static IP.	Passed	

MEJ87S_PC_14	Connecting a Android client to a WLAN configured with WPA 2 Enterprise security enabled with Passive client .	To connect a Android client to a WPA 2 Enterprise security WLAN with Passive client option enabled by configuring the client with a static IP.	Passed	
MEJ87S_PC_15	Connecting a IOS client to a WLAN configured with WPA 2 Enterprise security enabled with Passive client .	To connect a IOS client to a WPA 2 Enterprise security WLAN with Passive client option enabled by configuring the client with a static IP.	Passed	
MEJ87S_PC_16	Connecting a Mac OS client to a WLAN configured with WPA 2 Enterprise security enabled with Passive client .	To connect a Mac OS client to a WPA 2 Enterprise security WLAN with Passive client option enabled by configuring the client with a static IP.	Passed	
MEJ87S_PC_17	Configuring JOS client to Guest network with Internal splash page and access type as Local user account by enabling passive client .	To configuring JOS client to Guest network with Internal splash page and access type as Local user account by enabling passive client .	Passed	
MEJ87S_PC_18	Configuring a AVC rule to a passive client	To configure a AVC rule to a passive client and check if the AVC rule gets applied to the client successfully or not	Passed	
MEJ87S_PC_19	Connecting two passive client and enabling Peer to peer block.	To connect two passive client and enabling Peer to peer blocking for a wlan and check if both there is no traffic flow between the two connected passive clients.	Passed	
MEJ87S_PC_20	Configuring DHCP pool for the client by enabling passive client option.	To configure DHCP pool for the client and enabling passive client option for the WLAN.	Passed	

ME GUI for P2P Blocking

Logical ID	Title	Description	Status	Defect ID
------------	-------	-------------	--------	-----------

MEJ87S_P2P_01	Connecting two JOS client to a open security WLAN enabling Peer to Peer Block	To connect two JOS client to a open security WLAN enabling Peer to Peer Block and check if there is a traffic flow between two clients or not	Passed	
MEJ87S_P2P_02	Connecting two Windows client to a open security WLAN enabling Peer to Peer Block	To connect two Windows client to a open security WLAN enabling Peer to Peer Block and check if there is a traffic flow between two clients or not	Passed	
MEJ87S_P2P_03	Connecting two Android client to a open security WLAN enabling Peer to Peer Block	To connect two Android client to a open security WLAN enabling Peer to Peer Block and check if there is a traffic flow between two clients or not	Passed	
MEJ87S_P2P_04	Connecting two IOS client to a open security WLAN enabling Peer to Peer Block	To connect two IOS client to a open security WLAN enabling Peer to Peer Block and check if there is a traffic flow between two clients or not	Passed	
MEJ87S_P2P_05	Connecting two Mac OS client to a open security WLAN enabling Peer to Peer Block	To connect two Mac OS client to a open security WLAN enabling Peer to Peer Block and check if there is a traffic flow between two clients or not	Passed	
MEJ87S_P2P_06	Connecting two JOS client to a WPA 2 Personal security WLAN enabling Peer to Peer Block	To connect two JOS client to a WPA 2 Personal security WLAN enabling Peer to Peer Block and check if there is a traffic flow between two clients or not	Passed	
MEJ87S_P2P_07	Connecting two Windows client to a WPA 2 Personal security WLAN enabling Peer to Peer Block	To connect two Windows client to a WPA 2 Personal security WLAN enabling Peer to Peer Block and check if there is a traffic flow between two clients or not	Passed	

MEJ87S_P2P_08	Connecting two Android client to a WPA 2 Personal security WLAN enabling Peer to Peer Block	To connect two Android client to a WPA 2 Personal security WLAN enabling Peer to Peer Block and check if there is a traffic flow between two clients or not	Passed	
MEJ87S_P2P_09	Connecting two IOS client to a WPA 2 Personal security WLAN enabling Peer to Peer Block	To connect two IOS client to a WPA 2 Personal security WLAN enabling Peer to Peer Block and check if there is a traffic flow between two clients or not	Passed	
MEJ87S_P2P_10	Connecting two Mac OS client to a WPA 2 Personal security WLAN enabling Peer to Peer Block	To connect two Mac OS client to a WPA 2 Personal security WLAN enabling Peer to Peer Block and check if there is a traffic flow between two clients or not	Passed	
MEJ87S_P2P_11	Connecting two JOS client to a WPA 2 Enterprise security WLAN enabling Peer to Peer Block	To connect two JOS client to a WPA 2 Enterprise security WLAN enabling Peer to Peer Block and check if there is a traffic flow between two clients or not	Passed	
MEJ87S_P2P_12	Connecting two Windows client to a WPA 2 Enterprise security WLAN enabling Peer to Peer Block	To connect two Windows client to a WPA 2 Enterprise security WLAN enabling Peer to Peer Block and check if there is a traffic flow between two clients or not	Passed	
MEJ87S_P2P_13	Connecting two Android client to a WPA 2 Enterprise security WLAN enabling Peer to Peer Block	To connect two Android client to a WPA 2 Enterprise security WLAN enabling Peer to Peer Block and check if there is a traffic flow between two clients or not	Passed	
MEJ87S_P2P_14	Connecting two IOS client to a WPA 2 Enterprise security WLAN enabling Peer to Peer Block	To connect two IOS client to a WPA 2 Enterprise security WLAN enabling Peer to Peer Block and check if there is a traffic flow between two clients or not	Passed	

Flexconnect IOS Parity: Passive Client / Wireless Proxy ARP

MEJ87S_P2P_15	Connecting two Mac OS client to a WPA 2 Enterprise security WLAN enabling Peer to Peer Block	To connect two Mac OS client to a WPA 2 Personal Enterprise WLAN enabling Peer to Peer Block and check if there is a traffic flow between two clients or not	Passed	
MEJ87S_P2P_16	Connecting four different client to a open security WLAN enabling Peer to Peer Block	To connect four different client to a open security WLAN enabling Peer to Peer Block and check if there is a traffic flow between two clients or not	Passed	
MEJ87S_P2P_17	Connecting four different client to a WPA 2 Personal security WLAN enabling Peer to Peer Block	To connect four different client to a WPA 2 Personal security WLAN enabling Peer to Peer Block and check if there is a traffic flow between two clients or not	Passed	
MEJ87S_P2P_18	Connecting four different client to a WPA 2 Enterprise security WLAN enabling Peer to Peer Block	To connect four different client to a WPA 2 Enterprise security WLAN enabling Peer to Peer Block and check if there is a traffic flow between two clients or not	Passed	
MEJ87S_P2P_19	Connecting two Windows client to WLAN enabling Peer to Peer Block and trying Webex meeting between client	To connect two Windows client to WLAN enabling Peer to Peer Block and trying Webex meeting between client	Passed	

Flexconnect IOS Parity: Passive Client / Wireless Proxy ARP

Logical ID	Title	Description	Status	Defect ID
MEJ87S_ARP_01	Enable/Disable Passive client with multicast IP address	To verify whether Passive client with multicast enable/disable or not	Passed	
MEJ87S_ARP_02	Rebooting Ap after Passive client with multicast IP address	To verify whether Passive client with multicast details are showing properly or not after reboot	Passed	
MEJ87S_ARP_03	Enable/disable the Proxy ARP cache	To verify whether Proxy ARP cache details are enabling or not	Passed	

MEJ87S_ARP_04	Rebooting AP after Proxy ARP cache enable	To verify whether Proxy ARP details are showing properly or not after reboot th AP	Passed	
MEJ87S_ARP_05	Checking ARP with passive client details in standalone mode	To verify whether ARP with passive client details are showing properly or not in standalone	Passed	
MEJ87S_ARP_06	Roaming clients between AP with ARP and passive clients	To verify whether clients are roaming or not with ARP and passive client	Passed	
MEJ87S_ARP_07	Enable proxy and disable the passive client	To verify whether ARP details are transferring to the router or not when proxy is in enable and passive client disable state	Passed	
MEJ87S_ARP_08	Disable proxy and enable passive client	To verify whether ARP details are transferring to the router or not when proxy is in disable and passive client enable state	Passed	
MEJ87S_ARP_09	Enable proxy and enable the passive client	To verify whether ARP details are transferring to the router or not when proxy is in enable and passive client enable state	Passed	
MEJ87S_ARP_10	Disable proxy and disable passive client	To verify whether ARP details are transferring to the router or not when proxy is in disable and passive client disable state	Passed	
MEJ87S_ARP_11	Verifying the debug logs	To verify whether debug logs are showing properly or not	Passed	

External Guest Webauth in UI

Logical ID	Title	Description	Status	Defect ID
MEJ87S_Reg_141	Creating a WLAN with enabling Guest network and security Web-auth in ME UI	To check whether WLAN is created or not with security L3 Web-auth in ME UI	Passed	

MEJ87S_Reg_142	Checking the WLAN configurations after import/export the config file in ME	To check whether WLAN configurations gets retained or not after import/export the config file in CME	Passed	
MEJ87S_Reg_143	Associating Windows client to a WLAN in which security web-auth is enabled in ME	To check whether windows client able to connect successfully or not to a WLAN in which guest network+captive portal mapped to Radius is enabled.	Passed	
MEJ87S_Reg_144	Associating Apple IOS client to a WLAN in which security web-auth is enabled in ME	To check whether Apple IOS client able to connect successfully or not to a WLAN in which guest network+captive portal mapped to Radius is enabled.	Passed	
MEJ87S_Reg_145	Associating MAC OS client to a WLAN in which security web-auth is enabled in ME	To check whether MAC OS client able to connect successfully or not to a WLAN in which guest network+captive portal mapped to Radius is enabled.	Passed	
MEJ87S_Reg_146	Associating Android client to a WLAN in which security web-auth is enabled in ME	To check whether Android client able to connect successfully or not to a WLAN in which guest network+captive portal mapped to Radius is enabled.	Passed	
MEJ87S_Reg_147	Associating four clients to a WLAN in which security web-auth is enabled in ME	To check whether different OS clients are able to connect successfully or not to a WLAN in which guest network+captive portal mapped to Radius is enabled.	Passed	
MEJ87S_Reg_148	Checking the clients stats in Monitor dashboard in ME UI	To check whether different OS clients connected in ME are shown properly or not in Monitor Dashboard.	Passed	

Mobexp

Logical ID	Title	Description	Status	Defect ID
MEJ87IIS_mobexp_01	Checking the CWA ACL rule name in VLAN & Firewall tab	To check whether CWA ACL rule name is displaying properly or not in VLAN & Firewall tab	Failed	CSCvi35837
MEJ87IIS_mobexp_02	Creating a new user in Admin account in ME UI	To check whether new user gets created or not in Admin account without any message	Failed	CSCvi55283
MEJ87IIS_mobexp_03	Checking the Pre-Auth ACLs config via Read-Only user in ME	To check whether Pre-Auth ACLs config gets displayed or not for Read-only user	Failed	CSCvi65356
MEJ87IIS_mobexp_04	Trying to add the Pre-Auth ACL IP rules via Read-Only user in ME	To check whether Pre-Auth ACLs IP rules can be added or not for Read-only user	Failed	CSCvi74109
MEJ87IIS_mobexp_05	Adding/deleting the Radius server in a WLAN with CWA security policy	To check whether CWA security changes or not in a WLAN during deleting/adding the Radius Server in ME	Failed	CSCvi81672
MEJ87IIS_mobexp_06	Deleting the Guest WLAN profile in ME	To check whether proper error message thrown or not during deleting the Guest WLAN profile	Failed	CSCvi90865
MEJ87IIS_mobexp_07	Changing the security in a WLAN with hotspot configured in ME	To check whether security profile can be changed or not in a WLAN when hotspot is enabled	Failed	CSCvi90922
MEJ87IIS_mobexp_08	Adding the channel 165 in ME UI under RF optimization	To check whether Channel 165 able to add or not in ME UI under RF optimization	Failed	CSCvi96981
MEJ87IIS_mobexp_09	Enabling the Sensor provisioning in ME	To check whether sensor provisioning can be enabled or not in ME after creating 16 WLANs	Failed	CSCvj04336
MEJ87IIS_mobexp_10	Checking the functionality of show password button in SSH tab in ME	To check whether show password functionality works properly or not in SSH/802.1x tab in ME	Passed	
MEJ87IIS_mobexp_11	Adding new syslog server in ME UI	To check whether syslog server can be added or not with same series of IP in ME UI	Passed	
MEJ87S_mobexp_01	Checking the Peer-to-Peer blocking functionality for clients with enabling Central NAT	To check whether peer-to-peer config works or not for clients after enabling Central NAT	Failed	CSCvh05341
MEJ87S_mobexp_02	Checking the WLAN profile name length between CLI and UI in ME	To check whether WLAN profile name length is same or not between CLI and UI in ME	Failed	CSCvh17235

MEJ87S_mobexp_03	Checking the radius response in ME via Troubleshooting tools	To check whether radius response for WLAN can be tested or not in CME with security type CWA	Passed	
MEJ87S_mobexp_04	Deploying the WLAN template from PI to CME	To check whether WLAN template is deployed or not from PI to CME without changing the WLAN security	Failed	CSCvh30911
MEJ87S_mobexp_05	Creating the Domain and Realm name with Special characters in 802.11u	To check whether Domain and Realm name is created or not with special characters in 802.11u	Passed	
MEJ87S_mobexp_06	Checking the show password functionality in 802.1x tab	To check whether show password option gets enabled or not in SSH tab while enabling in 802.1x tab	Passed	
MEJ87S_mobexp_07	Checking the 1562 series name in ME UI	To check whether 1562 series name shown correctly or not in ME UI when this comes as ME	Failed	CSCvh61417
MEJ87S_mobexp_08	Checking the abort function in Software update page in CME	To check whether software image update can be aborted or not in CME	Failed	CSCvh61484
MEJ87S_mobexp_09	Adding Radius server in WLAN/RLAN in CME UI	To check whether Radius server can be added or not in WLAN/RLAN in CME	Failed	CSCvh65773



CHAPTER 5

CFD Derived Test cases

- [CFD derived Test Cases, on page 263](#)

CFD derived Test Cases

Table 1:

Logical ID	Title	Description	Status	Defect ID
WLJ87PhIIS_SR_01	Performing Inter-roaming of Windows clients for multiple times	To check whether windows clients roamed successfully or not for multiple times between 2 WLC's.	Passed	
WLJ87PhIIS_SR_02	Performing Inter-roaming of Mac-OS clients for multiple times	To check whether Mac OS clients roamed successfully or not for multiple times between 2 WLC's.	Passed	
WLJ87PhIIS_SR_03	Performing Inter-roaming of Android and IOS clients for multiple times	To check whether Android and IOS clients roamed successfully or not for multiple times between 2 WLC's.	Passed	
WLJ87PhIIS_SR_04	Performing Inter-roaming of IPphones	To check whether IPphones roamed successfully or not for between 2 WLC's.	Passed	

Logical ID	Title	Description	Status	Defect ID
WLJ87PhIIS_SR_05	Checking the Idle timeout functionality of Windows clients	To check whether windows clients gets timeout or not as configured when clients user idle timeout gets expired.	Passed	
WLJ87PhIIS_SR_06	Checking the Idle timeout functionality of Android and IOS clients	To check whether Android and IOS clients gets timeout or not as configured when clients user idle timeout gets expired.	Passed	
WLJ87PhIIS_SR_07	Checking the clients in heat map after upgrading the CMX	To check whether clients details are shown properly or not in heat map once after upgrading the CMX to latest image	Passed	
WLJ87PhIIS_SR_08	Checking autoconvert for Monitor mode after upgrading WLC	Verifying auto convert option for monitor after upgrading the WLC	Passed	
WLJ87PhIIS_SR_09	Checking autoconvert for Monitor mode after downgrading WLC	Verifying auto convert option for monitor after downgrading the WLC	Passed	
WLJ87PhIIS_SR_10	Checking AP is automatically joining in autoconvert mode enabled	Verifying Ap is joining to WLC in the mode which auto convert is enabled	Passed	
WLJ87PhIIS_SR_11	Checking MacFilter templet is getting imported or not	Verifying whether MacFilter templet is imported successfully or not	Passed	
WLJ87PhIIS_SR_12	Checking whether PI templet exported in one device is importing in another device	Verifying whether templet exported in one device is importing in another device	Passed	

Logical ID	Title	Description	Status	Defect ID
WLJ87PhIIS_SR_13	Checking whether PI templet is importing after changing the xml file	Verifying templet is importing successfully after changing the xml file	Passed	
WLJ87PhIIS_SR_14	Generating a custom for Client count	To check whether a custom report for client count is generated or not	Passed	
WLJ87PhIIS_SR_15	Generating a custom for top ap for client count	To check whether a custom report for top AP for client count is generated or not	Passed	
WLJ87PhIIS_SR_16	Scheduling a report for client summary in PI Japanese UI	To check whether a report for client summary is generated or not for scheduled time	Passed	
WLJ87PhIIS_SR_17	Scheduling a report for Ap utilization in PI Japanese UI	To check whether a report for ap utilization is generated or not for scheduled time	Passed	
WLJ87PhIIS_SR_18	Scheduling a report for Ap Summary in PI HA Mode	To check whether report for AP Summary is generating in PI HA mode	Passed	
WLJ87PhIIS_SR_19	Generating composite report in PI Japanese UI	To check composite report is generated or not	Passed	
WLJ87PhIIS_SR_20	Checking any exception in ncs server while checking android client details	To Verify any exception or errors are generating in ncs server while checking android client details in pi	Passed	
WLJ87PhIIS_SR_21	Checking any exception in ncs server while checking windows client details	To verify any exception or errors are generating in ncs server while checking windows client details in pi	Passed	

Logical ID	Title	Description	Status	Defect ID
WLJ87PhIIS_SR_22	Checking export is working fine for client and users table	To verify export option is working fine or not for client and user table	Passed	
WLJ87PhIIS_SR_23	Checking client reauthenticating with WPA+WPA2 dot1x in AP local	To verify client is reauthenticating after session time out	Passed	
WLJ87PhIIS_SR_24	Checking Audit session ID after reauthenticating of client with dot1x in AP flex	To verify whether Audit ID is showing after reauthentication of client	Passed	
WLJ87PhIIS_SR_25	Checking local policy is applying to client with l2 security in Ap local mode	To verify local policy is applying to client with l2 security type in AP local mode	Passed	
WLJ87PhIIS_SR_26	Checking country code after downloading the config file	To verify the country code after downloading the config file	Passed	
WLJ87PhIIS_SR_27	Checking Ap is joining automatically after downloading the config file	To verify Ap joining after downloading the config file	Passed	
WLJ87PhIIS_SR_28	Checking WLC country code after upgrading the WLC and downloading the config file	To verify WLC country code after upgrading the WLC and downloading the config file	Passed	
WLJ87PhIIS_SR_29	Checking CME is able to config with country code j2	To Verify whether ME is able to config with country code j2	Passed	
WLJ87PhIIS_SR_30	Verifying the AP logs when changing AP mode connected to standalone after client connection	To check whether is there any Radius log or not for the EAPOL-Key msg when AP mode is changed to connected to standalone after client connectivity	Passed	

Logical ID	Title	Description	Status	Defect ID
WLJ87PhIIS_SR_31	Verifying the AP logs when changing AP mode connected to standalone before client connection	To check whether is there any Radius log or not for the EAPOL-Key msg when AP mode is changed to connected to standalone before client connectivity	Passed	
WLJ87PhIIS_SR_32	Verifying the AP logs when changing AP mode standalone to connected after client connection	To check whether is there any Radius log or not for the EAPOL-Key msg when AP mode is changed to standalone mode to connected mode after client connectivity	Passed	
WLJ87PhIIS_SR_33	Verifying the AP logs when changing AP mode standalone to connected before client connection	To check whether is there any Radius log or not for the EAPOL-Key msg when AP mode is changed to standalone mode to connected mode before client connectivity	Passed	
WLJ87PhIIS_SR_34	Verifying the AP logs for every client connectivity and disconnectivity during the changing mode of AP	To check whether is there any Radius log or not for the EAPOL-Key msg when AP mode is changed to standalone mode to connected mode when client connects/disconnects and vice-versa.	Passed	

Logical ID	Title	Description	Status	Defect ID
WLJ87PhIIS_SR_35	Verifying the AP log for local authentication of client when AP is in connected mode	To check whether is there any Radius log or not for the EAPOL-Key msg when AP is in connected mode when client connects/disconnects .	Passed	
WLJ87PhIIS_SR_36	Verifying the AP log for local authentication of client when AP is in standalone mode	To check whether is there any Radius log or not for the EAPOL-Key msg when AP is in standalone mode when client connects/disconnects .	Passed	
WLJ87PhIIS_SR_37	Verifying the AP log Central authentication of client when AP is in connected mode or standalone	To check whether the client authentication has done with WLC and data packet switching with AP has been done with locally or not with Cisco Wave2 AP (AP 1832)	Passed	
WLJ87PhIIS_SR_38	Verifying the AP log of the client in the case of central switching and central Authentication with Cisco Wave2 AP	To check whether the client authentication and data packet switching has done with WLC or not with Cisco Wave2 AP (AP 1832)	Passed	
WLJ87PhIIS_SR_39	Verifying the error message "AP error: %APERRUPGRD" during upgrading AP	To check whether error message is displayed or not during the upgrading of AP	Passed	
WLJ87PhIIS_SR_40	Verifying DCA to AP for 802.11a/an/ac for WLC when two WLC are part of same RF group	To Check whether RF Group members WLC send exact channel to DCA or not for 5 GHZ	Passed	

Logical ID	Title	Description	Status	Defect ID
WLJ87PhIIS_SR_41	Verifying dynamic channel assignment to AP for 802.11b/g/n for WLC when two WLC are part of same RF group	To Check whether RF Group members WLC send exact channel to DCA or not for 2.4 GHZ	Passed	
WLJ87PhIIS_SR_42	Verifying dynamic channel assignment to AP for 802.11a/an/ac	To check whether channel has allocated or not dynamically	Passed	
WLJ87PhIIS_SR_43	Verifying dynamic channel assignment to AP for 802.11b/g/n	To check whether channel has allocated or not dynamically	Passed	
WLJ87PhIIS_SR_44	Verifying IDS signature attack trap log in WLC 8540 when signature is disabled	To Check whether the trap is generated or not when IDS signature is enabled	Passed	
WLJ87PhIIS_SR_45	Verifying IDS signature attack trap log in WLC 8540 when signature is enabled	To Check whether the trap is generated or not when IDS signature is enabled	Passed	
WLJ87PhIIS_SR_46	Verifying IDS signature attack trap log in WLC 5520 when signature is enabled	To Check whether the trap is generated or not when IDS signature is disabled	Passed	
WLJ87PhIIS_SR_47	Verifying the Reason code for challenge failure in trap log	To check whether that the displayed reason code is correct or not in trap log for the challenge failure	Passed	
WLJ87PhIIS_SR_48	Verifying the Reason code for DE authentication in trap log	To check whether that the displayed reason code is correct or not in trap log for DE authentication	Passed	

Logical ID	Title	Description	Status	Defect ID
WLJ87PhIIS_SR_49	Verifying the Reason code for disassociation in trap log	To check whether that the displayed reason code is correct or not in trap log for the disassociation	Passed	
WLJ87PhIIS_SR_50	Verifying the Reason code for association in trap log	To check whether that the displayed reason code is correct or not in trap log for the association failure	Passed	
WLJ87PhIIS_SR_51	Authenticating the iOS client with 2.4 Ghz radio's Rx Sop Threshold default of 1542 AP	To verify that iOS client got authenticated successfully or not with 1542 AP's in 2.4 GHz radio	Passed	
WLJ87PhIIS_SR_52	Authenticating the Window client with 5 Ghz radio's Rx Sop Threshold High of 3702 AP Flex mode	To verify that window client got authenticated with 5 GHz radio 1542 AP or not	Passed	
WLJ87PhIIS_SR_53	Authenticating the Window client with 5 Ghz radio's Rx Sop Threshold Medium of 1570 AP Flex mode	To verify that window client got authenticated with 5 GHz radio 1542 AP or not	Passed	
WLJ87PhIIS_SR_54	Checking the ARP Entry for Android client with 1562 AP in local mode	To verify that ARP entry present in table for Android client after associated with 1562 AP	Passed	
WLJ87PhIIS_SR_55	Checking the ARP Entry after disassociation of Window client with 1562 AP in Flexconnect mode	To verify that window client ARP entry not present in WLC ARP table after dissociation of client from 1562 AP	Passed	

Logical ID	Title	Description	Status	Defect ID
WLJ87PhIIS_SR_56	Checking the ARP Entry after association/disassociation of Window client with CME 1832	To verify that window client ARP entry not present in WLC ARP table after association/dissociation of client from CME 1832	Passed	
WLJ87PhIIS_SR_57	Configuring WLAN PSK layer 2 security, with Radius NAC and connect iOS client	To verify the iOS client connect or not with PSK-Radius NAC	Passed	
WLJ87PhIIS_SR_58	Configuring WLAN PSK layer 2 security, with Radius NAC and connect Android client with invalid password	To verify that Android client authenticated successfully or not with PSK-Radius NAC	Passed	
WLJ87PhIIS_SR_59	Configuring WLAN PSK layer 2 security, with Radius NAC and connect Android client with invalid password	To verify that Android client authenticated successfully or not with PSK-Radius NAC	Passed	
WLJ87PhIIS_SR_60	Create WLAN with l2 security none and l3 security none with CWA config , Enable mac filtering and connect window client	To verify that iOS client authenticated successfully with CWA config wlan and guest URL redirected	Passed	
WLJ87PhIIS_SR_61	Changing DCA Channel in RF group where 5520 as a leader and 8540 WLC as a auto are in same RF group	To verify that DCA Channel changed successfully for Ap in RF group and channel not changed for other AP in same RF group	Passed	

Logical ID	Title	Description	Status	Defect ID
WLJ87PhIIS_SR_62	Changing DCA Channel in one RF group where 5520 as a leader and verifying second RF group that have 8540 WLC 's group mode as auto	To verify that DCA Channel changed successfully for first RF group and not applied for second RF group	Passed	
WLJ87PhIIS_SR_63	Scheduling Restart in MSE and verify that MSE come up properly	To verify that MSE restarted after scheduled and come up properly	Passed	
WLJ87PhIIS_SR_64	Creating a heat map adding 3700 AP and connecting a client.	To create a heat map in prime infra and connecting a client to 3700 AP's in the floor to check different parameters.	Passed	
WLJ87PhIIS_SR_65	Creating a heat map adding 1810 AP and connecting a client.	To create a heat map in prime infra and connecting a client to 1810 AP's in the floor to check different parameters.	Passed	
WLJ87PhIIS_SR_66	Adding a autonomous AP and 2700 AP to the map and checking different parameters in the maps	To add the autonomous AP and 2700 AP to the map and check if the details of the autonomous ap and 2700 AP are shown and check different parameters .	Passed	
WLJ87PhIIS_SR_67	Exporting a map with different AP's and again importing the same thing to PI and check if	To Export a map from PI adding different AP's and again import the same file to PI and check if the AP details are shown properly	Passed	

Logical ID	Title	Description	Status	Defect ID
WLJ87PhIIS_SR_68	Exporting a map with different AP's and importing the same thing to CMX and check the details in CMX	To Export a map from PI adding different AP's and again import the same file to CMX and check if the AP details are shown in CMX properly or not	Passed	
WLJ87PhIIS_SR_69	Checking the Controller Count and AP limit	To check the controller count and AP limit in the Licence Summary Page	Passed	
WLJ87PhIIS_SR_70	Checking the Details in the Licence Summary page	To check if the Details shown in Licence summary is shown correctly and check if all details are shown or not	Passed	
WLJ87PhIIS_SR_71	Checking the EULA details and expiry date details of the controller .	To check the EULA details and expiry date details of the controller in Pi and check if the details are same as of WLC.	Passed	
WLJ87PhIIS_SR_72	Provide the daslets with Japanese character in Overview page in Dashboard.	To Provide the dashlets name with Japanese character to overview page in Dashboard and check if japanese characters are displayed properly or not.	Passed	
WLJ87PhIIS_SR_73	Provide the daslets with Japanese character in Wireless page in Dashboard.	To Provide the dashlets name with Japanese character to Wireless page in Dashboard and check if japanese characters are displayed properly or not.	Passed	

Logical ID	Title	Description	Status	Defect ID
WLJ87PhIIS_SR_74	Connecting a Android client to 2700 AP in local mode with Local EAP Authentication	To connect a Android client to 2700 AP in local mode with Local EAP Authentication and check if the client gets connected to AP without any errors or not and capture the MTU logs.	Passed	
WLJ87PhIIS_SR_75	Connecting a IOS client to 2700 AP in local mode with Local EAP Authentication.	To connect a IOS client to 2700 AP in local mode with Local EAP Authentication and check if the client gets connected to AP without any errors or not and capture the MTU logs..	Passed	
WLJ87PhIIS_SR_76	Connecting a Windows JOS client to 2700 AP in flexconnect local authentication with Local EAP	To connect a Window client to 2700 AP in in flexconnect local authentication with Local EAP and check if the client gets connected to AP without any errors or not and capture the MTU logs..	Passed	
WLJ87PhIIS_SR_77	Connecting a Mac OS client to 2700 AP in flexconnect local authentication with Local EAP	To connect a Mac OS client to 2700 AP in flexconnect local authentication with Local EAP and check if the client gets connected to AP without any errors or not and capture the MTU logs..	Passed	

Logical ID	Title	Description	Status	Defect ID
WLJ87PhIIS_SR_78	Checking whether becon packets are broadcasting when AP is in local mode	To verify the whether AP is broadcasting becon frame when it is in local mode	Passed	
WLJ87PhIIS_SR_79	Checking whether becon packets are broadcasting when AP is in flexconnect mode	To verify the whether AP is broadcasting becon frame when it is in Flexconnect mode	Passed	
WLJ87PhIIS_SR_80	Checking JOS client connectivity by changing the DCA channel	To verify client connectivity by changing the DCA channel of particular radio	Passed	
WLJ87PhIIS_SR_81	Checking Mac OS client connectivity by changing the DCA channel	To verify client connectivity by changing the DCA channel of particular radio	Passed	
WLJ87PhIIS_SR_82	Connecting a client using Indian extended channels enabled in DCA channels.	To connect a client enabling the indian extended channnels and check if the clients is connected in the channel allocated for the extended one or not.	Passed	
WLJ87PhIIS_SR_83	Connecting two IP phones and making a call .	To connect two IP phones and making a call from one IP phone to the other and check the connectivity.	Passed	
WLJ87PhIIS_SR_84	Connecting two IP phones to make a call and using call blocking option in one phone.	To connect two IP phone and make a call from one IP phone to other enabling call blocking option on one IP phone and check if call blocking option works fine or not.	Passed	

Logical ID	Title	Description	Status	Defect ID
WLJ87PhIIS_SR_85	Connecting clients to the 5520 controller and checking radius fallback through UI	To check whether 5520 controller is sending probe request to primary server or not	Passed	
WLJ87PhIIS_SR_86	Connecting clients to the 3504 controller and checking radius fallback through UI	To check whether 3504 controller is sending probe request to primary server or not	Passed	
WLJ87PhIIS_SR_87	Connecting clients to the 5520 controller and checking tacacs fallback	To check whether 5520 controller is sending probe request to primary server or not	Passed	
WLJ87PhIIS_SR_88	Connecting clients to the 3504 controller and checking radius fallback through CLI	To check whether the controller is sending probe request to primary server or not	Passed	
WLJ87PhIIS_SR_89	Verifyng ARP requests were forwarded from AP to client using 3700 AP	To check whether clients gets associated or not using 2700 AP	Passed	
WLJ87PhIIS_SR_90	Verifyng ARP requests were forwarded from AP to client using 2700 AP	To check whether clients gets associated or not using 3700 AP	Passed	
WLJ87PhIIS_SR_91	Checking 5GHZ clients associated for enough period of time without any radio reset	To verify whether clients with 5GHZ is getting connected or not for certain period of time without any radio reset	Passed	
WLJ87PhIIS_SR_92	Checking 2.4GHZ clients associated for enough period of time without any radio reset	To verify whether clients with 2.4GHZ is getting connected or not for certain period of time without any radio reset	Passed	

Logical ID	Title	Description	Status	Defect ID
WLJ87PhIIS_SR_93	Checking 5GHZ clients associated for enough period of time without any radio reset keeping AP in "local mode"	To verify whether clients with 5GHZ is getting connected or not for certain period of time without any radio reset with AP in "local mode"	Passed	
WLJ87PhIIS_SR_94	Checking 5GHZ clients associated for enough period of time without any radio reset keeping AP in "flexconnect mode"	To verify whether clients with 5GHZ is getting connected or not for certain period of time without any radio reset with AP in "flexconnect mode"	Passed	
WLJ87PhIIS_SR_95	Checking MC2UC video streaming clients associated for enough period of time without any radio reset keeping AP in "flexconnect mode"	To check whether MC2UC video streaming clients is getting connected or not for certain period of time without any radio reset	Passed	
WLJ87PhIIS_SR_96	Ensuring whether 802.11a global parameters are displaying properly in controllers and in AP'S	To verify whether 802.11a Global Parameters Operational status is displaying properly in both controllers and in AP's when Disable it.	Passed	
WLJ87PhIIS_SR_97	Ensuring whether 802.11b global parameters are displaying properly in controllers and in AP'S	To verify whether 802.11b Global Parameters Operational status is displaying properly in both controllers and in AP's when Disable it.	Passed	
WLJ87PhIIS_SR_98	Enabling flexconnect local Switching and also map vlan to a WLAN	To check client connectivity when wlan is enabled of local Switching and vlan mapped to SSID	Passed	

Logical ID	Title	Description	Status	Defect ID
WLJ87PhIIS_SR_99	Verifying the configuration of mapped ACL in flex mode and also verify the client connectivity	To check the mapped ACL is applied or not in flex group for specific WLAN	Passed	
WLJ87PhIIS_SR_100	Verifying the client connectivity for 1852 AP when AP is standalone mode and mac filter is enabled	To check whether client can be connected or not to AP 1852	Passed	
WLJ87PhIIS_SR_101	Roaming the Android clients between 5520\8540 WLC's after enabling New mobility converged access	To check whether Android clients gets roamed successfully or not between 5520 & 8540 WLC's after enabling New mobility converged access	Passed	
WLJ87PhIIS_SR_102	Roaming the Windows JOS clients between 3504/8540 WLC's after enabling New mobility converged access	To check whether Windows JOS clients gets roamed successfully or not between 3504 & 8540 WLC's after enabling New mobility converged access	Passed	
WLJ87PhIIS_SR_103	Roaming the Apple iOS clients between 3504\8540 WLC's after enabling New mobility converged access	To check whether Apple iOS clients gets roamed successfully or not between 3504 & 8540 WLC's after enabling New mobility converged access	Passed	
WLJ87PhIIS_SR_104	Roaming the MAC OS clients between 3504\8540 WLC's after enabling New mobility converged access	To check whether MAC OS clients gets roamed successfully or not between 3504 & 8540 WLC's after enabling New mobility converged access	Passed	

Logical ID	Title	Description	Status	Defect ID
WLJ87PhIIS_SR_105	Verifying that ap 2702 2.4-GHz radio is transmitting / receiving frames or not in flexconnect mode	To verify that AP 2702 2.4 ghz band is transmitting /receiving the frames or not in flexconnect mode	Passed	
WLJ87PhIIS_SR_106	Verifying alarm to Aps in PI	To check whether alarm related to AP get cleared or not	Passed	
WLJ87PhIIS_SR_107	Verifying alarm to WLC in PI	To check whether Alarm is triggered when WLC goes down	Passed	
WLJ87PhIIS_SR_108	Checking the Rogue Detection config after AP1562 rebooting.	To verify after AP1562 rebooting rogue config is changed back to "Enable" or not	Passed	
WLJ87PhIIS_SR_109	Verifying the interfering devices with 5GHZ band	To verify that AP 1562 able to detect interfering device with 5GHZ band or not	Passed	
WLJ87PhIIS_SR_110	Verifying the AP connectivity from WLC to vWLC in HA mode	To verify whether the AP joins the high priority vWLC from WLC or not	Passed	
WLJ87PhIIS_SR_111	Verifying the AP connectivity from vWLC to WLC in HA mode	To verify whether the AP joins the high priority WLC from vWLC or not	Passed	
WLJ87PhIIS_SR_112	Verifying the AP connectivity from WLC to vWLC with AP fall back	Configuring vWLC with lowest priority and checking the connectivity of AP joining after resetting the AP	Passed	
WLJ87PhIIS_SR_113	Verifying the AP connectivity from vWLC to WLC with AP fall back	Configuring WLC with lowest priority and checking the connectivity of AP joining after resetting the AP	Passed	

Logical ID	Title	Description	Status	Defect ID
WLJ87PhIIS_SR_114	Verify the AP re-joining the controller after power shutdown	To verify whether AP re-joins or not after power shutdown	Passed	
WLJ87PhIIS_SR_115	AP associated with vWLC which is integrated with PI	Verifying whether AP is able to join the vWLC which is integrated with PI	Passed	
WLJ87PhIIS_SR_116	Verify AP joining the virtual controller after reloading the virtual controller	Verifying whether AP joins the virtual controller or not after reloading the virtual controller	Passed	
WLJ87PhIIS_SR_117	Creating 2 WLANs with same SSID & L2/L3 security	To check whether the user is able to create 2 WLANs with same name and same L2/L3 security or not	Passed	
WLJ87PhIIS_SR_118	Verifying 2 client joining the WLANs with same SSID name with different L2/L3 security	Checking whether the user can create 2 WLANs with same SSID & with different L2/L3 security or not and trying to connect two clients Android & IOS at the same time	Passed	
WLJ87PhIIS_SR_119	Creating 2 WLANs with same SSID & with different security type disable one and try connecting with the enabled one	Verify whether the client is able to join or not the WLAN which is enabled when other SSID with same SSID & security type is disabled	Passed	
WLJ87PhIIS_SR_120	Creating 2 WLANs with different name with same L2/L3 security from CLI	Whether we are able to create WLAN or not through cli commands with different name with same L2/L3 security	Passed	

Logical ID	Title	Description	Status	Defect ID
WLJ87PhIIS_SR_121	Creating WLAN in UI and security type through CLI	User creating a WLAN in UI & security type through CLI is created successfully or not	Passed	
WLJ87PhIIS_SR_122	Creating a WLAN in PI and changing its security type in the controller	Verifying whether the user is able to create a WLN from PI and able to change or not the security type from the controller	Passed	
WLJ87PhIIS_SR_123	Checking DCA Channel Sensitivity & Channel Width configurations after backup/restore via TFTP	To check whether the DCA Channel Sensitivity & Channel Width configuration are saved or not after Backup/restoring the WLC's config	Passed	
WLJ87PhIIS_SR_124	Checking the Clean Air configurations after backup/restore via TFTP	To check whether the Clean Air configuration are saved or not after Backup/restoring the WLC's config	Passed	
WLJ87PhIIS_SR_125	Checking the Client Roaming - RF Parameters configurations after backup/restore via TFTP	To check whether the Client Roaming - RF Parameters configuration are saved or not after Backup/restoring the WLC's config	Passed	
WLJ87PhIIS_SR_126	Checking the Coverage Threshold configurations after backup/restore via TFTP	To check whether the RRM > Coverage - Coverage Threshold configuration are saved or not after Backup/restoring the WLC's config	Passed	

Logical ID	Title	Description	Status	Defect ID
WLJ87PhIIS_SR_127	Checking the 802.11a(5 GHz) > Media configurations after backup/restore via TFTP	To check whether the 802.11a(5 GHz) > Media configuration are saved or not after Backup/restoring the WLC's config	Passed	
WLJ87PhIIS_SR_128	Checking the 802.11a Global Parameters after backup/restore via TFTP	To check whether the 802.11a Global Parameters configuration are saved or not after Backup/restoring the WLC's config	Passed	
WLJ87PhIIS_SR_129	Verifying the WLAN configuration after uploading/downloading WLC	To check whether all WLAN configuration are configure or not after uploading/downloading WLC	Passed	
WLJ87PhIIS_SR_130	Checking the WLAN is configured to the default AP-Groups after after backup/restore via TFTP	Add the WLAN to the AP group and check whether it is added or not after uploading/downloading WLC	Passed	
WLJ87PhIIS_SR_131	Verifying reconnection of clients with SSID with L2 security PSK	To verify if the client is reconnecting again, by disconnecting it.	Passed	
WLJ87PhIIS_SR_132	Verifying the Time-out period of WLAN	veryfing if the client is disconnected after the session timeout period	Passed	
WLJ87PhIIS_SR_133	Verifying the Idle time-out period of WLAN	Check if the client details are removed from the WLC, if it reaches the Idle timeout period.	Passed	

Logical ID	Title	Description	Status	Defect ID
WLJ87PhIIS_SR_134	Checking if client can connect automatically with secondary radius server, after disabling primary	Verifying client can connect with secondary Radius server.	Passed	
WLJ87PhIIS_SR_135	Checking if the Radius server time out after the mentioned fallback timeout period in WLC.	Verifying the timeout period of Radius server.	Passed	
WLJ87PhIIS_SR_136	Verify if the client is able to pick IP address from DHCP pool .	To verify if the client is able to pick IP address from DHCP pool .	Passed	
WLJ87PhIIS_SR_137	Validating if the client is able to pick IP address from network Default	To verify if the client picks up IP address from network.	Passed	
WLJ87PhIIS_SR_138	Upgrading the 5520 WLC on HA mode in WLC UI	Verifying wlc is able to upgrading on HA and able access SSH/service port	Passed	
WLJ87PhIIS_SR_139	Upgrading the 5520 WLC on HA mode in WLC CLI	To check whether wlc is able to upgrading on HA and able access SSH/service port	Passed	
WLJ87PhIIS_SR_140	WLC 8540 upgrading on HA mode in WLC UI	Validate the WLC is upgrading on HA mode and able to access SSH/service port	Passed	
WLJ87PhIIS_SR_141	WLC 8540 upgrading on HA mode in WLC CLI	To check whether WLC is upgrading on HA mode and able to access SSH/service port	Passed	
WLJ87PhIIS_SR_142	Checking the Client service on Wave1 1700AP	Validating client is connecting or not with Wave1 802.11ac on 1700 AP	Passed	

Logical ID	Title	Description	Status	Defect ID
WLJ87PhIIS_SR_143	Resetting the radio after client connecting with Wave 1 802.11ac on AP 3700	Verify whether client is disconnecting or not while resetting the radios	Passed	
WLJ87PhIIS_SR_144	To checking the client saving configuration on Cisco Wave1 1572APs	Validating the client configuration after modifying client parameters	Passed	
WLJ87PhIIS_SR_145	Configure the service statistics for 5520 active WLC on HA mode	Verifying the service statistic value on 5520 STANDBY WLC	Passed	
WLJ87PhIIS_SR_146	Configure the service statistics for 8540 active WLC on HA mode	To check whether service statistics gets reflected or not on STAND BY WLC	Passed	
WLJ87PhIIS_SR_147	Checking AP 2800/3800 alarms for associated AP to WLC	Verifying the AP alarms after joining to WLC in PI	Passed	
WLJ87PhIIS_SR_148	Checking the Alarm policy for AP 2800/3800 disassociated from the controller	To check whether AP alarms showing critical severity or not in PI	Passed	
WLJ87PhIIS_SR_149	checking AP 2800/3800 alarms once reassociated to WLC	Verifying the AP alarms after comeback to online	Passed	
WLJ87PhIIS_SR_150	Checking the Local AP parameter in default flex group	Verifying Local AP Parameter in default flex group	Passed	
WLJ87PhIIS_SR_151	Checking the Sensor AP parameter in default flex group	Verifying Sensor AP Parameter in default flex group	Passed	
WLJ87PhIIS_SR_152	Checking AP is joining successfully without any DTLS failure.	Verifying AP is joining successfully without any DTLS failure.	Passed	

Logical ID	Title	Description	Status	Defect ID
WLJ87PhIIS_SR_153	Checking Buffered log level after downloading Config File	Verifying Buffered log level after downloading config file	Passed	
WLJ87PhIIS_SR_154	Checking Console log level after downloading Config File	Verifying console log level after downloading config file	Passed	
WLJ87PhIIS_SR_155	Checking Syslog level after downloading Config File	Verifying Syslog level after downloading config file	Passed	
WLJ87PhIIS_SR_156	Changing the speed as 10 in particular interface and Checking in AP CLI	Verifying show interface command in AP CLI using AP 2700	Passed	
WLJ87PhIIS_SR_157	Changing the speed as 100 in particular interface and Checking in AP CLI	Verifying show interface command in AP CLI using AP 1810	Passed	
WLJ87S_SR_01	Checking the Wireless/Wired packets while associating JOS clients to a WLAN via Wireshark	To check whether all management packets gets captured or not while associating wireless/wired Windows JOS clients to a WLAN in WLC	Passed	
WLJ87S_SR_02	Checking the Wireless/Wired packets while associating Mac OS clients to a WLAN via Wireshark	To check whether all management packets gets captured or not while associating wireless/wired Mac OS clients to a WLAN in WLC	Passed	
WLJ87S_SR_03	Checking the MC2UC traffic for local-switching clients	To verify that the local-switching clients receives MC2UC traffic or not after associating to a WLAN in WLC	Passed	

Logical ID	Title	Description	Status	Defect ID
WLJ87S_SR_04	Radius server events data to Network Assurance	To verify whether the Radius server up/down event data is sending to Network Assurance server or not from WLC	Passed	
WLJ87S_SR_05	Checking the nearest AP neighbor data's to NA server from WLC	To check whether the WLC sends nearestAP neighbors data to NA server correctly or not.	Passed	
WLJ87S_SR_06	Checking the WLAN event notifications sent to NA server from WLC	To check whether the WLAN changes are reflecting in NA server or not once it is configured in WLC	Passed	
WLJ87S_SR_07	Moving AP's from Primary vWLC to Secondary vWLC and checking the failover functionality also	To check whether AP fallback functionality works properly or not from Primary to Secondary vWLC's.	Passed	
WLJ87S_SR_08	Join one 1562 AP in to 5520 controller which having different image	To verify that 1562 AP join successfully and download image from controller	Passed	
WLJ87S_SR_09	Clear config of 1810 AP joined with 5520 Controller	To verify that configuration is cleared for 1810 Ap and after reload it should join back to Controller	Passed	
WLJ87S_SR_10	Create SNMP Community in WLC 5520 and Sync WLC in PI with new SNMP Community	To verify that new SNMP Community created successfully and added WLC in to PI	Passed	
WLJ87S_SR_11	Create SNMP Community using CLI with read only mode	To verify that new SNMP Community created using WLC CLI	Passed	

Logical ID	Title	Description	Status	Defect ID
WLJ87S_SR_12	Enable consule service in CME and verify using command	To verify that consule service enabled or not	Passed	
WLJ87S_SR_13	Check the active WLC using cmxctl controllers show command	To verify that connected WLC showing using this command	Passed	
WLJ87S_SR_14	Checking whether window client is able to connect to AP 1815I through 5GHZ band in AP local mode	To verify whether client is able to connect or not to AP 702 through 5GHZ band in AP local mode	Passed	
WLJ87S_SR_15	Checking whether android client is able to connect to AP 1815I through 5GHZ band in AP Flexconnect mode	To verify whether client is able to connect or not to AP 702 through 5GHZ band in AP Flexconnect mode	Passed	
WLJ87S_SR_16	Checking whether becon packets are broadcastin when AP is in local mode	To verify the whether AP is broadcasting becon frame when it is in local mode	Passed	
WLJ87S_SR_17	Checking whether becon packets are broadcastin when AP is in flexconnect mode	To verify the whether AP is broadcasting becon frame when it is in Flexconnect mode	Passed	
WLJ87S_SR_18	Checking client connection by changing the DCA channel	To Verify client connectivity by changing the DCA channel of particular radio	Passed	
WLJ87S_SR_19	Verifying management frames between 3702 AP and client	To verify management frames between 3702 AP and client	Passed	
WLJ87S_SR_20	Checking the 5ghz client association for a period of time without any breakage	To verify whether client with 5GHZ is getting connected or not for certain period of time without breakage	Passed	

Logical ID	Title	Description	Status	Defect ID
WLJ87S_SR_21	Checking the 2.4ghz client association for a period of time without any breakage	To verify whether client with 2.4GHZ is getting connected or not for certain period of time without any breakage	Passed	
WLJ87S_SR_22	Configuring the Hostname for Click Ap through CLI and UI	To verify whether hostname is configured for Click AP through CLI and UI	Passed	
WLJ87S_SR_23	Configuring the Hostname for IOS AP through CLI and UI	To verify whether hostname is configured for IOS AP through CLI and UI	Passed	
WLJ87S_SR_24	AP sniffer mode not able to capture data frames from MESH backhaul link	To verify whether AP sniffer mode capturing the data frames for MESH backhaul or not	Passed	
WLJ87S_SR_25	RADIUS fail-over does not work when retransmit timeout is not set to default value in WLC	To verify whether Radius failover is happening or not after timeout value not configured to the default value in WLC	Passed	
WLJ87S_SR_26	RADIUS fail-over does not work when retransmit timeout is not set to default value in ME 1852/2800/3800	To verify whether Radius failover is happening or not after timeout value not configured to the default value in ME	Passed	
WLJ87S_SR_27	Trapflags do not sync for HA SSO	To verify whether Trap logs are showing properly or not	Passed	
WLJ87S_SR_28	Checking the Active controller details in standby controller for HA SSO	To verify standby controller showing same details or not	Passed	

Logical ID	Title	Description	Status	Defect ID
WLJ87S_SR_29	Flooding "Invalid checkpoint client ID (0)" message on Standby WLC	To verify whether Flooding happening or not after connect the client in standby controller	Passed	
WLJ87S_SR_30	Error saving configuration file happens Aps	To verify whether Configuration file is saving successfully or not without any error	Passed	
WLJ87S_SR_31	Saving the configurations and checking the configurations in AP	To verify whether configurations are saving or not per particular AP at the time of save	Passed	
WLJ87S_SR_32	Radius server failover for authentication and authorization server	To verify whether authentication and authorization both are happening for failover or not	Passed	
WLJ87S_SR_33	Client packet struck during Payload encryption for 1800/2800/3800	To verify whether Payload encryption happening or not	Passed	
WLJ87S_SR_34	Creating the Heatmaps for Aps 3800/802.11b/g/n	Verify whether 2.4ghz/802.11b/g/n Aps showing or not in heat map	Passed	
WLJ87S_SR_35	AP 3800/802.11a/n/ac 5ghz radio with prime heat MAP	To check whether 802.11n/ac (5 GHz) radio AP is showing or not in heat map	Passed	
WLJ87S_SR_36	Rebooting the MSE in pre-scheduled time	Verifying the MSE is come back or not after pre-scheduled reboot	Passed	
WLJ87S_SR_37	Roam the wireless client from MAP AP-A to another AP-B	To confirm after roaming the wireless client MAP AP-A to another AP-B client is disappeared or not on MAP	Passed	

Logical ID	Title	Description	Status	Defect ID
WLJ87S_SR_38	Inconsistent AP 1810 Radio usage in WLC Dashboard	To check the AP 1810 Radio usage without wireless client	Passed	
WLJ87S_SR_39	AP Radio usage with wireless client	Verify the AP 1572 radio usage after wireless client connects	Passed	
WLJ87S_SR_40	Checking the MSE service with latest version when Archive logs gets filled up	To Verifying the MSE service after Archive logs gets filled up	Passed	
WLJ87S_SR_41	MSE Archive logs not cleaned up automatically	Verifying the MSE Archive logs cleaned up or not automatically	Passed	
WLJ87S_SR_42	Configure the pmipv6 for wireless client	Verifying the WLC logs related to subnet mask when doing PMIPv6	Passed	
WLJ87S_SR_43	Configure the Heat Map for AP 2702 and 1810	Verifying Heat Map is working or not for AP 2702 and 1810	Passed	
WLJ87S_SR_44	Reloading the CAPWAP AP 2802,2702,3702	To check whether AP Preferred Mode is configured or not after reloading the AP	Passed	
WLJ87S_SR_45	Checking AP-1810 capwap Preferred Mode	Verified the AP Preferred Mode after rebooting the Aps	Passed	
WLJ87S_SR_46	Checking AP configuration after reloading the AP1700	Verifying the AP configuration is recovered or not after reloading	Passed	
WLJ87S_SR_47	Connecting different clients to 3702 AP with 5GHz radio type	To check if 3702 AP with 5GHz connect to clients and check if there is any stuck back while connecting a client	Passed	

Logical ID	Title	Description	Status	Defect ID
WLJ87S_SR_48	Capturing the POE status of AP-1562 and check the client connectivity.	To capture the POE status of AP-1562 and check the client connectivity	Passed	
WLJ87S_SR_49	Configuring Maximum Number of Clients per AP Radio in GUI page and check if clients get connected or not	To configure the Maximum Number of Clients per AP Radio in GUI page and check if clients get connected to th AP radio.	Passed	
WLJ87S_SR_50	Connecting the client after disabled/enabled AP radio	To verify that client connected after enabled/disabled the AP radio	Passed	
WLJ87S_SR_51	Checking the radio status of 1815 AP and disabled/enabled the radio using UI and check the client connectivity	To verify the radio of 1815 AP and verify the radio is disabled /enabled using UI and check the client connectivity	Passed	
WLJ87S_SR_52	Verifyng the clients are showing in exclusion list	To check whether the clients are showing in exclusion list or not.	Passed	
WLJ87S_SR_53	Connecting the clients to 3702 AP with 5GHz	To check that 3702 AP with 5GHz connect to different clients and check if there is any stuck back while connecting a client	Passed	
WLJ87S_SR_54	AP reboots Properly with new image in WLC.	To check whether AP is rebooting properly and joining to WLC after downloading new image or not.	Passed	
WLJ87S_SR_55	Checking Client MAC address in Association request	To verify whether the client MAC addr is correct or not in the Debug client <MAC Add> logs	Passed	

Logical ID	Title	Description	Status	Defect ID
WLJ87S_SR_56	Checking the ap 2.4-GHz radio is transmitting frames in flexconnect mode	To check the ap 2.4 ghz band is transmitting the frames or not in flexconnect mode	Passed	
WLJ87S_SR_57	Try Ping from different client to other IP on the network while AP in local mode.	To try ping other IP on the network form different client when the AP is in the local mode .	Passed	
WLJ87S_SR_58	Try Ping from different client to other IP on the network while AP in Flexconnect mode.	To try ping other IP on the network form different client when the AP is in the Flexconnect mode .	Passed	
WLJ87S_SR_59	Connecting a client to a 2700 AP in flexconnect mode with local switching enabled 802.1x security.	To connect a client to 2700 AP in flexconnect mode with local switching keeping the security in802.1x and check if the client is able to pass traffic succesfully.	Passed	
WLJ87S_SR_60	Connecting a client to a 3500 AP in flexconnect mode with local switching enabled 802.1x security.	To connect a client to 3500 AP in flexconnect mode with local switching keeping the security in802.1x and check if the client is able to pass traffic succesfully.	Passed	
WLJ87S_SR_61	Uploading a configuration file from the controller and again downloading the same file to the controller.	To Uploading a configuration file from the controller and again downloading the same file to the controller.	Passed	
WLJ87S_SR_62	Check the client statistics on the active and standby controller.	To check the client statics on the controller and check if all the details are correct in both GUI and CLI	Passed	

Logical ID	Title	Description	Status	Defect ID
WLJ87S_SR_63	check if the client connected to the active controller details is shown correctly	To check if the client connected details are shown correctly or not	Passed	
WLJ87S_SR_64	Enabling AP Retransmit Count and interval for a particular AP .	To enable AP Retransmit Count and interval for particular AP and check if there is error while applying .	Passed	
WLJ87S_SR_65	Connecting a JOS window 7 client to the AP 1562 and check if the client gets connected before AP reload .	To Connect a window 7 JOS client to a 1562 AP and check if the client gets connected to the AP before AP reload.	Passed	
WLJ87S_SR_66	Connecting a Windows 10 client to the AP 1562 and check if the client gets connected before AP reload .	To Connect a window 10 client to a 1562 AP and check if the client gets connected to the AP before AP reload.	Passed	
WLJ87S_SR_67	Creating a VLAN in a switch and connecting a client to VLAN created	To create a VLAN in switch and connecting a client to the VLAN created and check if the client gets the IP address from the VLAN created .	Passed	
WLJ87S_SR_68	Checking AP1700 is sending ACK packet even though client gets connected through 5GHZ band	To verify whether AP is sending packets to client even the client got connected to that AP	Passed	
WLJ87S_SR_69	Checking AP2700 is sending ACK packet even though client gets connected through 5GHZ band	To verify whether AP is sending packets to client even the client got connected to that AP	Passed	

Logical ID	Title	Description	Status	Defect ID
WLJ87S_SR_70	Checking AP3700 is sending ACK packet even though client gets connected through 5GHZ band	To verify whether AP is sending packets to client even the client got connected to that AP	Passed	
WLJ87S_SR_71	Checking AP1700/AP2700/AP3700 is able to join from 5520 WLC to 3504 WLC with latest image	To verify AP 1700/AP 2700/ AP 3700 is able to join to another WLC with latest image	Passed	
WLJ87S_SR_72	Checking AP1700/AP2700/AP3700 is able to join from 3504 WLC to 5520 WLC with latest image	To verify AP 1700/AP 2700/ AP 3700 is able to join to another WLC with latest image	Passed	
WLJ87S_SR_73	Checking downloading and uploading a configuration file into the WLC and regarding Multicast	To verify whether configuration to be uploaded from the WLC and then when downloading it it will give error message or not	Passed	
WLJ87S_SR_74	Checking whether AP2802 sends probe response while client gets connected and send sprobe request to AP	To verify whether 2802AP sends probe response while client gets connected and sends probe request to AP	Passed	
WLJ87S_SR_75	Checking whether controller reboots when the management port is changed nad LAG is in transision state	Change the Management Interface Port while LAG is enabled and it is in transision state. Check whether controller is rebooting or not	Passed	
WLJ87S_SR_76	Checking whether the AP configuration gets saved when it joins the secondary controler while primary controller is down	To verify the AP configurations are saved or not when the primary controller goes down and AP joins the secondary controller	Passed	

Logical ID	Title	Description	Status	Defect ID
WLJ87S_SR_77	Verifying AP re-joins the primary controller once its up from the secondary controller	To check when the primary controller comes up AP re-joins the primary controller from the secondary controller or not	Passed	
WLJ87S_SR_78	Checking whther Stand-By controller receives the ping from the Active controller	To verify whether Active controller ping request is received or not by the Stand-By controller	Passed	
WLJ87S_SR_79	Chnaging the global config credentials in AP and checking	To verify whether the user is able to login in or not in SSH/Telnet	Passed	
WLJ87S_SR_80	Create a WLAN with the AP and check the client summary through SSH/Telnet	To verify whether the client summary results are displayed successfully or not in SSH/Telnet	Passed	
WLJ87S_SR_81	Checking whether 5GHZ radio stuck while capturing Beacon packets	To verify 5GH radio got stuck or not while capturing Beacons packets	Passed	
WLJ87S_SR_82	Checking whether AP responds for the association request	To verify whether AP Reponses for the association request or not	Passed	
WLJ87S_SR_83	To check whether AP receives the ARP request after the connection lost.	To verify whether high quality video is streaming or not	Passed	
WLJ87S_SR_84	Checking the status of Channel Announcement after upgrading the controller	To verify whether Channel Announcement is disabled or enabled after upgrading the controller	Passed	

Logical ID	Title	Description	Status	Defect ID
WLJ87S_SR_85	Checking whether the 802.11h parameters are enabled /disabled through CLI commands are reflecting in UI	To verify whether Announcement, Channel Quiet Mode & Smart DFS are disbled/enabled through CLI commands are reflrcting in UI or not.	Passed	
WLJ87S_SR_86	Check whether the AP 3702 and switches both are configured to full duplex or half duples	To verify whether the connection exist or not for AP 3702 and switches when configured with half duplex or full duplex	Passed	
WLJ87S_SR_87	Check whether warning message appears when the AP 3702 is configured with full duplex and switch configured to half duplex	To verify mismatch warning messages displays or not when the AP 3702 is configured with full duplex and switch configured to half duplex	Passed	



CHAPTER 6

Related Documents

- [Related Documentation](#), on page 297

Related Documentation

CME 8.7 release Notes

https://www.cisco.com/c/en/us/td/docs/wireless/access_point/mob_exp/87/release_notes/b_ME_RN_87.html

WLC 8.7 Configuration Guide

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-7/config-guide/b_cg87/monitoring_cisco_wlc.html

CMX 10.4 Configuration Guide

https://www.cisco.com/c/en/us/td/docs/wireless/mse/10-4/cmx_config/b_cg_cmx104.html

PI 3.4 User Guide

https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-4/user/guide/bk_CiscoPrimeInfrastructure_3_4_0_UserGuide/bk_CiscoPrimeInfrastructure_3_4_0_UserGuide_chapter_01100.html

ACS 5.8 User Guide

https://www.cisco.com/c/en/us/td/docs/net_mgmt/cisco_secure_access_control_system/5-8-1/user/guide/acsuserguide.pdf

ISE 2.3 Release Notes

https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/release_notes/b_ise_24_rn.html

