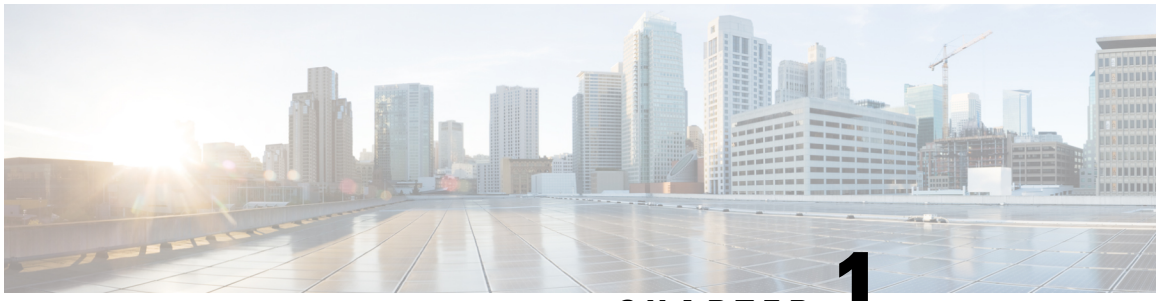
Test Results Summary for Cisco Wireless LAN Controller AireOS 8.8 & CME 8.8 for Japan (Release Version 8.8.100.0)

First Published: 2018-09-03

Last Modified: 2018-11-19

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

CONTENTS



CHAPTER 1

Overview

Cisco Wireless LAN Solution Test

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

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

- New features in WLC 8.8 and CME 8.8
- High priority scenarios and basic regression features
- Inputs from Cisco SEs/ TAC

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

The following products are covered in the test execution:

- Cisco Wireless LAN Controller 8540
- Cisco Wireless LAN Controller 5520
- Cisco Wireless LAN Controller 3504
- Virtual Controller
- Cisco Mobility Express 4800
- Cisco Mobility Express 3800
- Cisco Mobility Express 2800
- Cisco Mobility Express 1562
- Cisco Mobility Express 1542
- Cisco Mobility Express 1852

- Cisco Mobility Express 1832
- Cisco Mobility Express 1815I
- APIC-EM Controller appliance
- CMX
- Cisco DNA Center
- Access Point 4800
- Access Point 3800
- Access Point 2800
- Access Point 3700
- Access Point 2700
- Access Point 1700
- Access Point 1850
- Access Point 1830
- Access Point 1815I
- Access Point 1815W
- Access Point 1810
- Access Point 1572
- Access Point 1562
- Access Point 1542
- Access Point 1530
- Access Point 702I
- Cisco Prime Infrastructure (Physical-UCS,VM)
- ISE (VM)

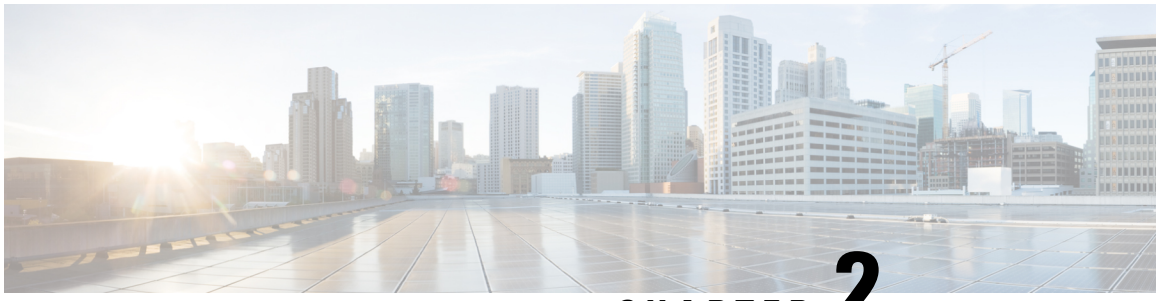
Acronyms

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

Acronym	Description
APIC-EM	Application Policy Infrastructure Controller - Enterprise Module
ATF	Air-Time Fairness
AVC	Application Visibility and Control.
BGN	Bridge Group Network
BLE	Bluetooth Low Energy
BYOD	Bring Your Own Device
CA	Central Authentication
CAC	Call Admissions Control
CAPWAP	Control and Provisioning of Wireless Access Point
CCKM	Cisco Centralized Key Management
CCN	Channel Change Notification
CCX	Cisco Compatible Extensions
CDP	Cisco Discovery Protocol
CKIP	Cisco Key Integrity Protocol
CMX	Connected Mobile Experience
CVBF	Cisco Vector Beam Forming
CWA	Central Web Authentication
DCA	Dynamic Channel Assignment
DMZ	Demilitarized Zone
Cisco DNA Center	Cisco Digital Network Architecture Center
DNS	Domain Name System
DTIM	Delivery Traffic Indication Map
DSCP	Differentiated Services Code Point
DTLS	Datagram Transport Layer Security
EAP	Extensible Authentication Protocol
EULA	End User Licence Agreement
FLA	Flex Local Authentication
FLS	Flex Local Switching
FT	Fast Transition
FTP	File Transfer Protocol
FW	Firm Ware
HA	High Availability

Acronym	Description
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
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

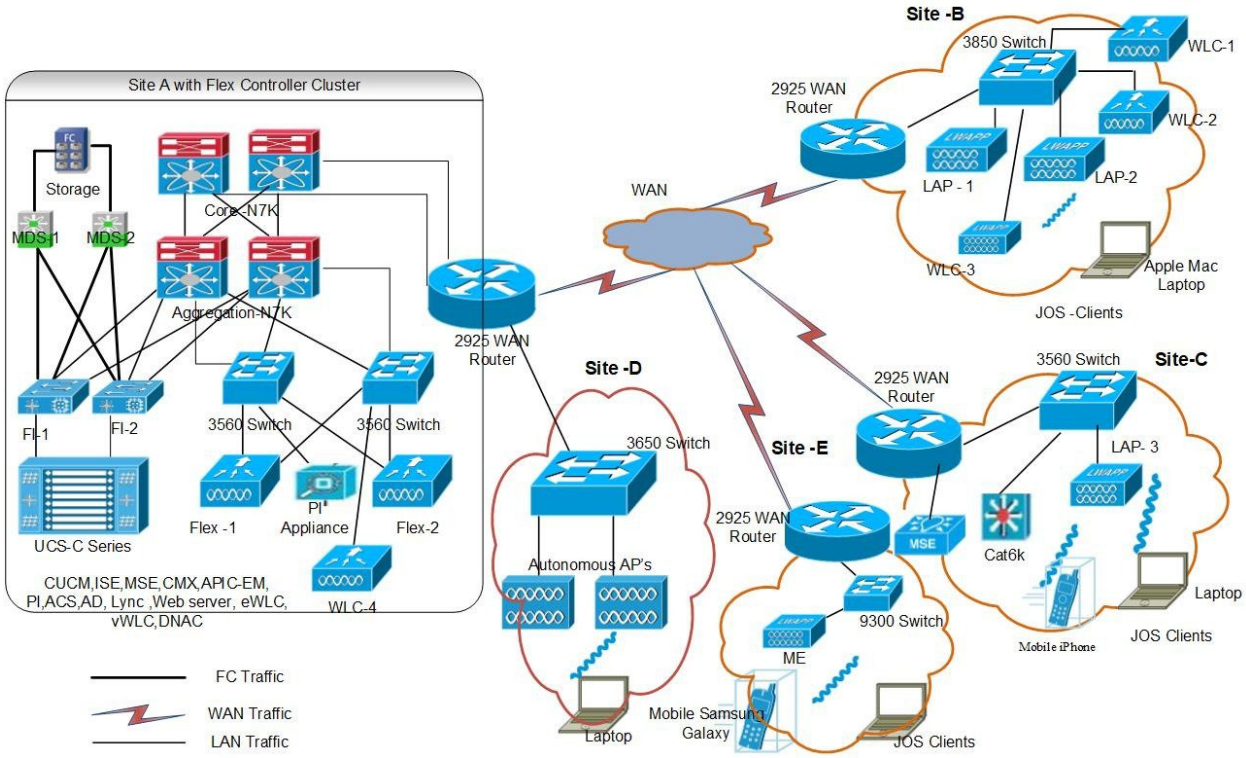
Acronym	Description
RRM	Radio Resource Management
SDN	Software Defined Networking
SOAP	Simple Object Access Protocol
SFTP	Secure File Transfer Protocol
SNMP	Simple Network Management Protocol
SS	Spatial Stream
SSID	Service Set Identifier
SSO	Single Sign On
SSO	Stateful Switch Over
TACACS	Terminal Access Controller Access Control System
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
vWLC	Virtual Wireless LAN Controller
VPC	Virtual port channel
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WGB	Workgroup Bridge
wIPS	Wireless Intrusion Prevention System
WLAN	Wireless LAN
WLC	Wireless LAN Controller
WPA	Wi-Fi Protected Access
WSM	Wireless Security Module



CHAPTER 2

Test Topology and Environment Matrix

Test Topology



Component Matrix

Category	Component	Version
Controller	Wireless LAN Controller 8540	8.8.100.0
	Wireless LAN controller 5520	8.8.100.0
	Wireless LAN controller 3504	8.8.100.0
	Virtual Controller	8.8.100.0
	CME 1562	8.8.100.0
	CME 4800/3800/2800	8.8.100.0
Applications	Prime Infrastructure (Virtual Appliance, UCS based)	3.5.0.0.235
	ISE(VM)	2.5
	CMX(Physical (3365), VM)	10.5
	Cisco DNA Center	1.2
	MSE(Physical (3365), VM)	8.0.150.0
	APIC-EM Controller appliance	1.6
	Cisco Jabber for Windows, iPhone	11.9.1
	Cisco Air Provisioning App	1.4
	Cisco Wireless App	1.0.228

Category	Component	Version
Access Point	Cisco AP 4800	15.3
	Cisco AP 3800	15.3
	Cisco AP 2800	15.3
	Cisco AP 3700	15.3
	Cisco AP 2700	15.3
	Cisco AP 1700	15.3
	Cisco AP 1850	15.3
	Cisco AP 1830	15.3
	Cisco AP 1815	15.3
	Cisco AP 1810	15.3
	Cisco AP 1570	15.3
	Cisco AP 1562	15.3
	Cisco AP 1542	15.3
	Cisco AP 1532	15.3
	Cisco AP 702I	15.3
Switch	Cisco 3750V2 switch	15.0(2)SE2
	Cisco Cat 6509-E	15.1(1)SY1
	Cisco Cat 9300	16.09.01
Chipset	5300, 6300 AGN	15.13.0.2
	7265 AC	19.51.10.1
	Airport Extreme	7.7

Category	Component	Version
Client	Operating System(JOS)	Windows 7 Enterprise
		Windows 8 & 8.1 Enterprise
		Windows XP Professional
		Windows 10
	Apple Mac Book Pro, Apple Mac Book Air (JP Locale)	Mac OS 10.14.1
	iPad Pro	iOS 11.4.1(15G77)
	iPhone 6, 6S & 7 (JP Locale)	iOS 11.4.1(15G77)
	Samsung Galaxy S4 & S7, Nexus 6P, Sony Xperia XZ	Android 8.0 Oreo
	Wireless IP Phone 8821	11.0.4-14
	End points	Windows 7 Enterprise
		Apple Mac 10.11.6
		Windows 8 & 8.1
		iPhone 6,6S & 7
		Windows 10
		Samsung Galaxy S4, S7, Nexus 6P, Sony Xperia
	Cisco AnyConnect VPN Client	4.6
Module	Hyper location Module	NA
Active Directory	AD	Windows 2008R2 Enterprise
Call Control	Cisco Unified Communications Manager	12.5.0.99832-3/12.5.0.99832-3-1(JP)
Browsers	IE	11.0.11
	Mozilla Firefox	62.0
	Safari	11.0.2
	Chrome	68.0

What's New ?

WLC AireOS

- DNS Pre-auth ACLs Wave 2 Aps
- Intelligent Capture
- Default DSCP for AVC Profile

- Split Tunneling
- Cisco Wave 2 APs as Workgroup Bridges
- Flex+Mesh Support
- Identity PSK with Peer-to-Peer Blocking
- AP acting as supplicant with EAP-FASTv1 and 802.1X authentication
- CMX 10.5 Support

CME

- AP 4800 support
- SFTP Domain Name support
- ME GUI - MC2UC (Videostreaming)
- mDNS Support
- EoGRE Support on ME
- Schedule WLAN Support
- Optimized Roaming
- Capwap Image Conversion
- No reboot of AP when AP joins AP group
- ME AP convert to CAPWAP via DHCP Option
- Cisco DNA Center Support for ME
- CMX 10.5 Support
- Aging Test Cases

Open Caveats

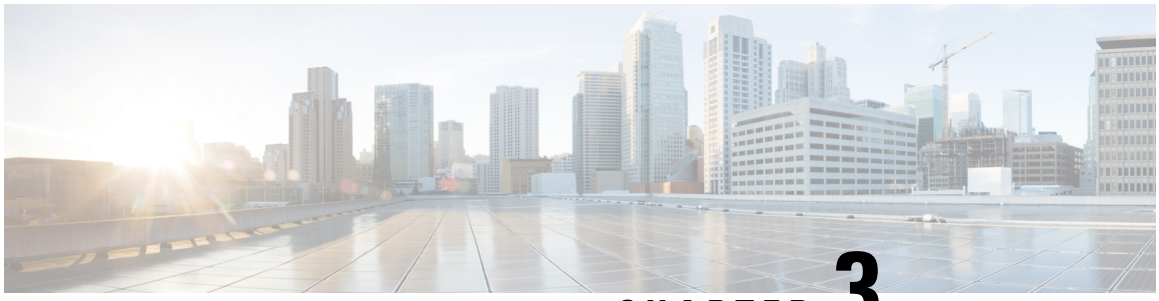
Defect ID	Title	Status
CSCvj74163	Monitor mode should not be allowed for AP1542	Fixed in 8.9
CSCvj93292	IOS AP is changing to sensor mode without WSA enabled from AP console	Fixed in 8.9
CSCvk03093	Access to Intelligent Capture parameter is different in Read only user	Fixed in 8.9
CSCvk26409	OEAP ACL rule is creating when given with invalid subnet mask.	Fixed in 8.9
CSCvk52187	Unable to configure TGW list with TACACS controller user in WLC UI	Fixed in 8.9
CSCvk23585	Output of show flex client url-acl not displayed properly in AP CLI	Fixed in 8.9
CSCvk03882	Sensor mode AP coming as FlexConnect after ME forced failover	Fixed in 8.9
CSCvk12422	ME Controller rebooting twice after LSC AP Auth State to 802.1x port authentication /both	Fixed in 8.9
CSCvk13835	Sensor mode APs is not downloading the image after master failover	Fixed in 8.9

CSCvk32119	User admin state changes as per the schedule when WLAN is created after scheduled hours	Fixed in 8.9
CSCvk23248	ME controller rebooting twice after changing the LSC AP Auth configuration in UI	Fixed in 8.9
CSCvk05680	WLAN admin status not changing from current to expected when changes made during Schedule interval	Fixed in 8.9
CSCvk20402	Last reset details not showing after reset/upgrade/downgrade	Fixed in 8.9
CSCvk41500	Hotspot is enabling with Open/Guest security after change from WPA Enterprise	Fixed in 8.9
CSCvk47740	Pre-auth ACLs are not configuring for RLAN in ME UI	Fixed in 8.9
CSCvk25119	Radius server status mismatch in admin accounts and WLAN page	Fixed in 8.9
CSCvk26607	Global Multicast is disabling after ME reset	Fixed in 8.9
CSCvk68911	Day0 CLI manually configured Time not reflecting same in day1 ME 1800/4800	Fixed in 8.9
CSCvm17349	AP is rebooting with "ap-type capwap" command even AP is in capwap type	Fixed in 8.9
CSCvm17545	2.4 GHz band and Optimized roaming not disabling together in UI	Fixed in 8.9
CSCvm24712	Scheduling hours are applied for first WLAN and not reflected for second WLAN	Fixed in 8.9
CSCvm50951	WLAN created in CLI and Multicast disabled from UI, QOS value is always set to Platinum	Fixed in 8.9
CSCvm65289	Able to add/delete IP rules and URL rules in security settings tab for Read-only user in ME UI	Fixed in 8.9

Resolved Caveats

Defect ID	Title
CSCvj78824	Controller getting crash due to invalid URL in Network Assurance server
CSCvj68796	Unable to filter out Multicast Group Client Details under Monitor page
CSCvk07124	All AP's are changing the floor when user select particular AP in Export Bulk AP
CSCvj69146	CME reloads unexpectedly in a loop due to PMALLOC_DOUBLE_FREE (capwap_ac_sm.c)
CSCvj96736	Not possible to change the sensor mode AP details after edit in ME
CSCvj92674	Failed to execute the ME CLI commands very first time under mob-exp
CSCvj65028	Mismatch in configuring RRC parameters under media-stream between UI and CLI
CSCvj53266	Services and RF-profile page details are showing in standard view page

CSCvj70836	"show system slabtop" command not showing the system details



CHAPTER 3

New Features - Test Summary

WLC AireOS

DNS Pre-auth ACLs Wave 2 APs

Logical ID	Title	Description	Status	Defect ID
WLJ88S_DPA_01	Configure URL ACL with permit action on the controller and connect the windows client	To verify whether clients get connected and redirect to permit URL	Passed	
WLJ88S_DPA_02	Configure URL ACL with deny action on the controller and connect the windows client	To verify whether clients get connected and redirect to deny URL	Passed	
WLJ88S_DPA_03	Configure Flexconnect URL ACL with webpolicy as authentication and connect the clients	To verify that Windows client connected succesfully with authentication policy	Passed	
WLJ88S_DPA_04	Configure Flexconnect URL ACL with webpolicy as passthrough and connect the clients	To verify that Windows client connected succesfully with passthrough policy	Failed	CSCvk23585

WLJ88S_DPA_05	Configure Flexconnect URL ACL with webpolicy as Conditional Web Redirect and connect the clients	To verify that Windows client connected succesfully with Conditional Web Redirect policy	Passed	
WLJ88S_DPA_06	Configure Flexconnect URL ACL with webpolicy as Splash Page Web Redirect and connect the clients	To verify that Windows client connected succesfully with Splash Page Web Redirect policy	Passed	
WLJ88S_DPA_07	Configure WebAuth ACL through WLAN -ACL mapping with permit action and connect the clients	To verify whether Windows client getting connected and redirected through WebAuth ACL at WLAN-ACL mapping	Passed	
WLJ88S_DPA_08	Configure WebAuth ACL through WLAN -ACL mapping with deny action and connect the clients	To verify whether Windows client getting connected through WebAuth ACL at WLAN-ACL mapping	Passed	
WLJ88S_DPA_09	Configure WebAuth ACL through 1800/2800/3800/1542 AP level with permit action and connect the clients	To verify whether Windows client getting connected through WebAuth ACL at AP level	Passed	
WLJ88S_DPA_10	Configure WebAuth ACL through 1800/2800/3800 AP level mapping with deny action and connect the clients	To verify whether Windows client getting connected and denied through WebAuth ACL at AP level	Passed	

WLJ88S_DPA_11	Configure WebAuth ACL through Policies on flexconnect group with permit action and connect the clients	To verify whether Windows client getting connected through WebAuth ACL at Policies	Passed	
WLJ88S_DPA_12	Configure WebAuth ACL through Policies on flexconnect group with deny actions and connect the clients	To verify whether Windows client getting connected and denied through WebAuth ACL at Policies	Passed	
WLJ88S_DPA_13	Configure WebAuth ACL through Policies on AP level with permit action and connect the clients	To verify whether Windows client getting connected and permitted through WebAuth ACL using Policies	Passed	
WLJ88S_DPA_14	Configure WebAuth ACL through Policies on and AP level with deny action and connect the clients	To verify whether Windows client getting connected and denied through WebAuth ACL using Policies	Passed	
WLJ88S_DPA_15	Configure URL ACL on the controller map with local policy permiting action and connect the clients	To verify whether policy URL override during permit WLAN URL ACL	Passed	
WLJ88S_DPA_16	Configure URL ACL on the controller map with local policy denying action and connect the clients	To verify whether policy URL override WLAN URL ACL	Passed	
WLJ88S_DPA_17	Configuring RLAN with permit URL ACL rule on the controller and connect the clients	To verify whether clients get permitted and redirected to URL	Passed	

WLJ88S_DPA_18	Configuring RLAN with deny URL ACL rule on the controller and connect the clients	To verify whether clients get denied and redirected to URL	Passed	
WLJ88S_DPA_19	Configure WebAuth ACL through AAA Vlan-ACL mapping and connect the clients	To verify whether Windows client getting connected and redirected through WebAuth ACL at AAA-ACL mapping	Passed	

Intelligent Capture

Logical ID	Title	Description	Status	Defect ID
WLJ88S_ICAP_01	Configuring Intelligent Capture parameter details on 2800/3800 AP	To configure Intelligent capture parameters in different Aps 2800/3800	Failed	CSCvj92772
WLJ88S_ICAP_02	Check Configuration after the AP reboot	To Configure Intelligent capture parameters in different Aps 2800/3800 and check if the configuration remains same after the AP reboot.	Passed	
WLJ88S_ICAP_03	Configure Intelligent Capture parameters on WLC CLI	To configure Intelligent Capture parameters on WLC CLI and check if all the parameters can be configured using CLI or not	Passed	
WLJ88S_ICAP_04	Packet capture of client when the client is connected to 2800/3800 AP with 2.4 GHz	To capture the Packet of the client when the client is connected to AP with radio as 2.4GHz	Failed	CSCvk03093

WLJ88S_ICAP_05	Packet capture of client when the client is connected to 2800/3800 AP with 5 GHz	To capture the Packet of the client when the client is connected to AP with radio as 5 GHz	Passed	
WLJ88S_ICAP_06	Capturing of Packet of the client when the client is connected with open security.	To capture packet when the client is connected to the 2800/3800 AP with security as OPEN	Passed	
WLJ88S_ICAP_07	Capturing of Packet of the client when the client is connected with WPA 2 PSK security.	To capture packet when the client is connected to the 2800/3800 AP with security as WPA 2 PSK	Passed	
WLJ88S_ICAP_08	Capturing of Packet of the client when the client is connected with WPA 2 802.1x security.	To capture packet when the client is connected to the 2800/3800 AP with security as WPA 2 802.1x	Passed	
WLJ88S_ICAP_09	Capturing of Packet of the client when the client is connected with Static WEP security.	To capture packet when the client is connected to the 2800/3800 AP with security as Static WEP	Passed	
WLJ88S_ICAP_10	Verifying the packet caputure happen when the AP configured with different channel.	To verify if the packet capture happens when the AP is configured with different channel width and packet capture shows correct information.	Passed	
WLJ88S_ICAP_11	Verify the packet capture when the AP is in Flexconnect Local switching .	To verify if the packet capture happens when the AP is in Flexconnect Local switching mode with a client connected to it	Passed	

WLJ88S_ICAP_12	Verify the packet capture when the AP is in Flexconnect Local switching with local authentication .	To verify if the packet capture happens when the AP is in Flexconnect Local switching mode and local authentication with a client connected to it	Passed	
WLJ88S_ICAP_13	Performing Intra controller roaming of client and capturing of packet using Intelligent capture	To check whether intra controller roaming of clients works properly or not and check if packet capture works properly or not.	Passed	
WLJ88S_ICAP_14	Performing Inter controller roaming of client and capturing the packet .	To check whether inter controller roaming of Android clients works properly or not	Passed	
WLJ88S_ICAP_15	Configuring WLAN session timeout and capturing the packet.	To configure WLAN session timeout and check if the packet capture shows deauth and re association packets or not.	Passed	
WLJ88S_ICAP_16	Packet Capture for the WGB based client using Intelligent Capture.	To Capture Packet for the WGB based client and check if packet capture for WGB based client is shown.	Passed	
WLJ88S_ICAP_17	Packet capture using the AP group with 2800 AP	To capture the packet using the Intelligent packet capture option in AP Group with 2800 AP	Passed	
WLJ88S_ICAP_18	Packet capture using the AP group with 3800 AP	To capture the packet using the Intelligent packet capture option in AP Group with 3800 AP	Passed	

WLJ88S_ICAP_20	Packet Capture using AP group without a AP in it	To Check if packet capture occurs or not if no AP is in the AP group.	Passed	
WLJ88S_ICAP_21	Packet capture using the AP group with different security	To capture packet when the client is connected to the 2800/3800 AP with different security	Passed	
WLJ88S_ICAP_22	Packet capture using roaming scenario in AP group using different Aps	To capture the Packet by using different AP in AP group and check if the client roams between different Aps	Passed	
WLJ88S_ICAP_23	Packet Capture for Android client using intellingent capture option in AP group.	To verify the packet capture for Android client using Intelligent capture in AP Group.	Passed	
WLJ88S_ICAP_24	Packet Capture for Windows client using intellingent capture option in AP group.	To verify the packet capture for Windows client using Intelligent capture in AP Group.	Passed	
WLJ88S_ICAP_25	Packet Capture for IOS client using intellingent capture option in AP group.	To verify the packet capture for IOS client using Intelligent capture in AP Group.	Passed	
WLJ88S_ICAP_26	Packet Capture for Mac OS client using intellingent capture option in AP group.	To verify the packet capture for Mac OS client using Intelligent capture in AP Group.	Passed	

Default DSCP for AVC Profile

Logical ID	Title	Description	Status	Defect ID

WLJ88S_DSCP_01	Configure default dscp as Platinum for AVC profile and connect the clients	To verify whether clients get connected and applied dscp as platinum	Passed	
WLJ88S_DSCP_02	Configure default dscp as gold for AVC profile and connect the clients	To verify whether clients get connected and applied dscp as gold	Passed	
WLJ88S_DSCP_03	Configure default dscp as silver for AVC profile and connect the clients	To verify whether clients get connected and applied dscp as silver	Passed	
WLJ88S_DSCP_04	Configure default dscp as bronze for AVC profile and connect the clients	To verify whether clients get connected and applied dscp as bronze	Passed	
WLJ88S_DSCP_05	Configure default dscp as custom for AVC profile and connect the clients	To verify whether clients get connected and applied dscp as custom	Passed	
WLJ88S_DSCP_06	Configure default dscp as platinum in flexconnect AVC profile and connect the clients	To verify whether clients get connected and applied in Flexconnect AVC profile	Passed	
WLJ88S_DSCP_07	Configure default dscp as gold in flexconnect AVC profile and connect the clients	To verify whether clients get connected and applied in Flexconnect AVC profile	Passed	

WLJ88S_DSCP_08	Configure default dscp as silver in flexconnect AVC profile and connect the clients	To verify whether clients get connected and applied in Flexconnect AVC profile	Passed	
WLJ88S_DSCP_09	Configure default dscpas bronze in flexconnect AVC profile and connect the clients	To verify whether clients get connected and applied in Flexconnect AVC profile	Passed	
WLJ88S_DSCP_10	Configure default dscp as custom in flexconnect AVC profile and connect the clients	To verify whether clients get connected and applied in Flexconnect AVC profile	Passed	
WLJ88S_DSCP_11	Configure default dscp in flexconnect AVC profile and map with flexconnect group connect the clients	To verify whether clients get connected and able to browse AVC application	Passed	
WLJ88S_DSCP_12	Configure dscp in flexconnect group with wlan Avc Mapping in AP and connect the clients	To verify whether Wlan Mapping is applied in AP and clients getting connected	Passed	
WLJ88S_DSCP_13	Configure a acl rule with dscp value and connect the clients	To verify whether client gets connected	Passed	
WLJ88S_DSCP_14	Configure a flexconnect acl rule with dscp value and connect the clients	To verify whether client gets connected with flexconnect acl rule	Passed	

WLJ88S_DSCP_15	Configure a AVC profile map it with local policy and connect the clients	To verify whether policy AVC override WLAN AVC	Passed	
WLJ88S_DSCP_16	Configure ACL with permit and AVC with drop and connect the clients	To verify clients gets connected with AVC or ACL rule	Passed	

Split Tunneling

Logical ID	Title	Description	Status	Defect ID
WLJ88S_sts_01	Verifying permit rule of split tunnel ACL with Windows client At flex group level	To check whether traffic is routing or not when Windows client is connected to ACL enabled WLAN	Passed	
WLJ88S_sts_02	Verifying deny rule of split tunnel ACL with Windows client at flex group level	To check whether traffic is blocked or not when Windows client is connected to ACL enabled WLAN	Passed	
WLJ88S_sts_03	Verifying permit rule of split tunnel ACL with MAC/iOS client at flex group level	To check whether traffic is routing or not when MAC/iOS client is connected to ACL enabled WLAN	Passed	
WLJ88S_sts_04	Verifying deny rule of split tunnel ACL with MAC/iOS client at flex group level	To check whether traffic is blocked or not when Windows client is connected to ACL enabled WLAN	Passed	
WLJ88S_sts_05	Verifying permit rule of split tunnel ACL with Android client at flex group level	To check whether traffic is routing or not when Android client is connected to ACL enabled WLAN	Passed	
WLJ88S_sts_06	Verifying deny rule of split tunnel ACL with Android client at flex group level	To check whether traffic is blocked or not when Android client is connected to ACL enabled WLAN	Passed	

WLJ88S_sts_07	Verifying permit rule of split tunnel ACL with Windows / Android / MAC / iOS clients at AP level	To check whether traffic is routing or not when Windows / Android / MAC / iOS clients are connected to ACL enabled WLAN	Passed	
WLJ88S_sts_08	Verifying deny rule of split tunnel ACL with Windows / Android /MAC / iOS clients at AP level	To check whether traffic is blocked or not when Windows / Android / MAC / iOS clients are connected to ACL enabled WLAN	Passed	
WLJ88S_sts_09	Verifying connectivity of corporate network from Private network of OEAP enabled AP	To check whether clients connected to Private network are able to ping the corporate network or not	Passed	
WLJ88S_sts_10	Verifying connectivity of Private network from corporate network in OEAP enabled Network	To check whether clients connected to corporate network are able to ping the private network of OEAP or not	Passed	
WLJ88S_sts_11	Verifying of inter connectivity of connectivity of Clients when connected to corporate clients through the OEAP	To check whether clients connected to private network OEAP are able to ping each other or not	Passed	
WLJ88S_sts_12	Verifying split tunnel ACL configuration at flexgroup level through WLC UI	To verify whether split tunnel ACL can be configured at flex group level or not through WLC UI	Passed	
WLJ88S_sts_13	Verifying split tunnel ACL configuration at flexgroup level through WLC CLI	To verify whether split tunnel ACL can be configured at flex group level or not through WLC CLI	Passed	
WLJ88S_sts_14	Verifying split tunnel ACL configuration at AP level through WLC UI	To verify whether local split tunnel ACL can be applied to AP level or not from WLC UI	Passed	

WLJ88S_sts_15	Verifying split tunnel ACL configuration at AP level through WLC CLI	To verify whether local split tunnel ACL can be applied to AP level or not from WLC UI	Passed	
WLJ88S_sts_16	Verifying Split tunnel Statistics on AP console	To verify whether the Split tunnel statistics is displayed to AP console or not	Passed	
WLJ88S_sts_17	Verifying Split tunnel mapping of ACL to WLAN on AP console	To verify whether mapped wlan list is displayed or not in AP console	Passed	

Cisco Wave 2 APs as Workgroup Bridges

Logical ID	Title	Description	Status	Defect ID
WLJ88S_WGB_01	Configuring the LWAPP AP to autonomous AP	To change the LWAPP APto autonomous AP and check if the AP is converted	Passed	
WLJ88S_WGB_02	Configuring the Autonomous AP as the WGB	To configure the autonomous AP as WGB and check if the AP changes as WGB.	Passed	
WLJ88S_WGB_03	Associating the WGB on open authentication with AP on local mode	To associate the WGB on open authentication when AP in local mode and check if the WGB associates with the open WLAN or not.	Passed	
WLJ88S_WGB_04	Associating the WGB on WPA 2 with PSK with AP on local mode	To associate the WGB on WPA 2 PSK security when AP in local mode and check if the WGB associates with the WLAN or not.	Passed	

WLJ88S_WGB_05	Associating the WGB on WPA 2 with 802.1x with AP on local mode	To associate the WGB on WPA 2 802.1x security when AP in local mode and check if the WGB associates with the WLAN or not.	Passed	
WLJ88S_WGB_06	Associating the WGB on WPA 2 CCKM with AP on local mode	To associate the WGB on WPA 2 CCKM security when AP in local mode and check if the WGB associates with the WLAN or not.	Passed	
WLJ88S_WGB_07	Associating the WGB on open authentication with AP on Flex mode	To associate the WGB on open authentication when AP in Flex mode and check if the WGB associates with the open WLAN or not.	Passed	
WLJ88S_WGB_08	Associating the WGB on WPA 2 with PSK with AP on Flex mode	To associate the WGB on WPA 2 PSK security when AP in local mode and check if the WGB associates with the WLAN or not.	Passed	
WLJ88S_WGB_09	Associating the WGB on WPA 2 with 802.1x with AP on Flex mode	To associate the WGB on WPA 2 802.1x security when AP in local mode and check if the WGB associates with the WLAN or not.	Passed	
WLJ88S_WGB_10	Associating the WGB on WPA 2 CCKM with AP on Flex mode	To associate the WGB on WPA 2 CCKM security when AP in local mode and check if the WGB associates with the WLAN or not.	Passed	

WLJ88S_WGB_11	Checking of WGB roaming from one AP to another AP in local mode	To check the roaming of WGB from one AP to another AP when the AP is in local mode .	Passed	
WLJ88S_WGB_12	Checking of WGB roaming from one AP to another AP in flex mode	To check the roaming of WGB from one AP to another AP when APs arein flex mode	Passed	

Flex+Mesh Support

Logical ID	Title	Description	Status	Defect ID
WLJ88S_FMS_01	1702I/2702I/1562 AP: Connected to Standalone mode transition	To verify the 1702I/2702I/1562 AP in flex+bridge moves to standalone mode when no WLC is detected.	Passed	
WLJ88S_FMS_02	1702I/2702I/1562: Reboot AP in standalone mode.	To verify whether the config is persistent upon rebooting the AP.	Passed	
WLJ88S_FMS_03	1702I/2702I/1562 AP: Standalone to Connected mode transition	To verify the 1702I/2702I/1562 AP(same VLAN) configured as flex+bridge moves to connected mode from Standalone mode after WLC is UP.	Passed	
WLJ88S_FMS_04	Client connectivity to the flex+bridge AP - central switching	To verify the client connectivity with Central Switching in Connected mode.	Passed	
WLJ88S_FMS_05	Client connectivity to the flex AP - local switching	To verify the client connectivity with local Switching in Connected mode.	Passed	

WLJ88S_FMS_06	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	
WLJ88S_FMS_07	Central auth Client status when AP moves back to connected mode.	To veify the central auth client connectivity when AP moves back to connected mode.	Passed	
WLJ88S_FMS_08	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	
WLJ88S_FMS_09	Local auth Client status when AP moves back to connected mode.	To veify the local auth client connectivity when AP moves back to connected mode.	Passed	
WLJ88S_FMS_10	Client connectivity test with all wireless clients	To verify the client connectivity	Passed	
WLJ88S_FMS_11	Client statistics in AP and WLC.	To verify the client status in WLC and AP.	Passed	
WLJ88S_FMS_12	WLAN deletion in standalone mode.	To verify WLAN deletion in Standalone mode is not showing up when moves to connected mode.	Passed	
WLJ88S_FMS_13	Client connectivity to 802.11a radio	To verify the client connectivity to 802.11a radio	Passed	
WLJ88S_FMS_14	Client connectivity to 802.11b radio	To verify the client connectivity to 802.11b radio.	Passed	

Identity PSK with Peer-to-Peer blocking

Logical ID	Title	Description	Status	Defect ID

WLJ88S_iPSK_01	Verifying the iPSK tag generation for the Connected Window JOS Client in WLC UI/CLI	To verify whether iPSK tag generated or not When Window JOS connected to iPSK enabled WLAN Profile	Passed	
WLJ88S_iPSK_02	Verifying the iPSK tag generation for the Connected MAC OS Client in WLC UI/CLI	To verify whether iPSK tag generated or not When MAC OS connected to iPSK enabled WLAN Profile	Passed	
WLJ88S_iPSK_03	Verifying the iPSK tag generation for the Connected iOS Client in WLC UI/CLI	To verify whether iPSK tag generated or not When iOS connected to iPSK enabled WLAN Profile	Passed	
WLJ88S_iPSK_04	Verifying the iPSK tag generation for the Connected Android Client in WLC UI/CLI	To verify whether iPSK tag generated or not When Window JOS connected to iPSK enabled WLAN Profile	Passed	
WLJ88S_iPSK_05	Verifying peer to peer communication of Windows JOS clients while sharing same iPSK tag	To verify whether windows JOS clients are able to ping each other or not when they share the same iPSK tag	Passed	
WLJ88S_iPSK_06	Verifying peer to peer communication of MAC clients while sharing same iPSK tag	To verify whether MAC OS clients are able to ping each other or not when they share the same iPSK tag	Passed	
WLJ88S_iPSK_07	Verifying peer to peer communication of iOS clients while sharing same iPSK tag	To verify whether iOS clients are able to ping each other or not when they share the same iPSK tag	Passed	

WLJ88S_iPSK_08	Verifying peer to peer communication of Android clients while sharing same iPSK tag	To verify whether windows Android OS clients are able to ping each other or not when they share the same iPSK tag	Passed	
WLJ88S_iPSK_09	Verifying peer to peer communication of Windows JOS clients while sharing different iPSK tag	To verify whether windows JOS clients are able to ping each other or not when they share the different iPSK tag	Passed	
WLJ88S_iPSK_10	Verifying peer to peer communication of MAC clients while sharing different iPSK tag	To verify whether MAC OS clients are able to ping each other or not when they share the different iPSK tag	Passed	
WLJ88S_iPSK_11	Verifying peer to peer communication of iOS clients while sharing different iPSK tag	To verify whether iOS clients are able to ping each other or not when they share the different iPSK tag	Passed	
WLJ88S_iPSK_12	Verifying peer to peer communication of Android clients while sharing different iPSK tag	To verify whether windows Android OS clients are able to ping each other or not when they share the different iPSK tag	Passed	
WLJ88S_iPSK_13	Verifying peer to peer communication of different OS clients when clients share same iPSK Tag	To verify whether the different platform OS clients can ping each other or not when they share the same iPSK tag	Passed	
WLJ88S_iPSK_14	Verifying peer to peer communication of different OS clients when clients share different iPSK Tag	To verify whether the different platform OS clients can ping each other or not when they share the same iPSK tag	Passed	

WLJ88S_iPSK_15	Verifying peer to peer action of connected clients with same iPSK tag in case of central switching mode	To verify whether the different platform OS clients can ping each other or not when they share the same iPSK tag with central Switching	Passed	
WLJ88S_iPSK_16	Verifying peer to peer action of connected clients with same iPSK tag in case of local switching	To verify whether the different platform OS clients can ping each other or not when they share the same iPSK tag with local switching	Passed	
WLJ88S_iPSK_17	Verifying peer to peer action of connected clients with different iPSK tag in case of central switching mode	To verify whether the different platform OS clients can ping each other or not when they share the different iPSK tag with central Switching	Passed	
WLJ88S_iPSK_18	Verifying peer to peer action of connected clients with different iPSK tag in case of local switching	To verify whether the different platform OS clients can ping each other or not when they share the different iPSK tag with local switching	Passed	
WLJ88S_iPSK_19	Verifying connected clients with the particular iPSK tag in CLI	To verify whether all the clients sharing iPSK tag are shown or not in WLC CLI	Passed	
WLJ88S_iPSK_20	Verifying the wlan configuration with iPSK tag Configuration through WLC Web	To verify whether wlan profile can be created or not with the iPSK configuration through the WLC Web	Passed	

WLJ88S_iPSK_21	Verifying the wlan generation with iPSK tag Configuration through WLC CLI	To verify whether wlan profile can be created or not with the iPSK configuration through the WLC CLI	Passed	
WLJ88S_iPSK_22	Verifying iPSK tag for the for different OS clients with Flex+Bridge Mode	To verify whether iPSK tag is generated or not for the connected clients	Passed	
WLJ88S_iPSK_23	Verifying clients connectivity with iPSK tag while radius fallback is enabled	To verify whether clients iPSK is being generated from secondary AAA server or not	Passed	
WLJ88S_iPSK_24	Verifying generation of iPSK tag with FT-PSK for different OS clients	To verify whether iPSK generated or not when WLAN is enabled with FT-PSK	Passed	
WLJ88S_iPSK_25	Verifying clients roaming with iPSK tag	To verify whether iPSK generated or not when WLAN is enabled with FT-PSK	Passed	
WLJ88S_iPSK_26	verifying connectivity among the clients when clients are connected to different WLAN	To verify whether the different platform OS clients can ping each other or not based on the iPSK tag	Passed	
WLJ88S_iPSK_27	Verifying iPSK WLAN configuration after importing and exporting thhe same configuration file	To verify whether the wlan configuration retains same or not after exporting the same configuration file	Passed	

AP acting as supplicant with EAP-FASTv1 and 802.1X authentication

Logical ID	Title	Description	Status	Defect ID

WLJ88S_dot1x_01	Enabling dot1x auth for AP and ioining AP to WLC	To check whether AP joins WLC or not after dot1x authentication from Switch/ISE	Passed	
WLJ88S_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	
WLJ88S_dot1x_03	Joining COS AP to WLC through Dot1x+PEAP authentication	To check whether COS AP joins WLC or not after dot1x authentication from Switch/ISE via EAP method PEAP	Passed	
WLJ88S_dot1x_04	Joining iOS AP to WLC through Dot1x+EAP TLS authentication	To check whether iOS AP joins WLC or not after dot1x authentication from Switch/ISE via EAP method TLS	Passed	
WLJ88S_dot1x_05	Trying to join AP's through Dot1x authentication with LSC provisioning	To check whether AP's joins WLC or not through LSC provisioning & dot1x authentication	Passed	
WLJ88S_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	
WLJ88S_dot1x_07	Disabling dot1x support in Switch and trying to associate AP via Dot1x authentication to WLC	To check whether AP joins WLC or not even dot1x is disabled in switch	Passed	

WLJ88S_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	
WLJ88S_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 WLC UI via TFTP	Passed	
WLJ88S_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	
WLJ88S_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	
WLJ88S_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	
WLJ88S_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 WLC UI	Passed	

CMX 10.5 Support

Logical ID	Title	Description	Status	Defect ID
WLJ88S_CMX10.5_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	
WLJ88S_CMX10.5_02	Adding a 3800 AP to the to Prime Infrastructure maps	To Add 3800 AP to Prime Infrastructure maps and check if the AP is added to the floor of the AP .	Passed	
WLJ88S_CMX10.5_03	Importing the Maps added with 3800 AP to CMX	To import the Site map added with 3800 AP and from Prime Infrastructure to CMX and check if the deatails of the AP are shown correctly and clint are able to join or not.	Passed	
WLJ88S_CMX10.5_04	Importing the maps with 2 to 3 Access points from Prime Infrastructure to CMX	To import the maps from Prime Infrastructure to CMX with 2 to 3 access point and check if the access point details are shown correctly including clients connected .	Passed	
WLJ88S_CMX10.5_05	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	

WLJ88S_CMX10.5_06	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	
WLJ88S_CMX10.5_07	Searching the client by MAC address	To check whether client device can be searched by specifying its MAC address or not	Passed	
WLJ88S_CMX10.5_08	Searching the client using its IP address	To check whether client device can be searched by specifying its IP address or not	Passed	
WLJ88S_CMX10.5_09	Searching client using its SSID	To verify whether client device can be searched by specifying the SSID or not	Passed	
WLJ88S_CMX10.5_10	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	
WLJ88S_CMX10.5_11	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	
WLJ88S_CMX10.5_12	Checking the activity on the floor using the heat map option.	To check the activity on the floor using the heat map and check the playback of the heatmap .	Passed	

CME

AP 4800 Support

Logical ID	Title	Description	Status	Defect ID
MEJ88PH2S_4800AP_01	Making the 4800 AP as ME controller	To verify whether 4800 AP is coming as ME controller or not	Failed	CSCvk68911
MEJ88PH2S_4800AP_02	Checking MC2UC traffic when clients connected with different securities in 4800 ME	Verifying MC2UC traffic for clients connected with different securities in 4800 ME	Passed	
MEJ88PH2S_4800AP_03	Checking mDNS services are Applied to MacOS and IOS with WLAN WPA2 personal security in 4800 ME	Verifying mDNS services are Applied to MacOS and IOS with WPA2 personal security	Passed	
MEJ88PH2S_4800AP_04	Checking the Roaming between APs	To verify whether Roaming successfully happening or not in 4800 ME	Passed	
MEJ88PH2S_4800AP_05	Creating WLAN with Guest security and connecting clients	To verify whether client is connecting with Guest security or not	Passed	
MEJ88PH2S_4800AP_06	Creating the WLAN with WPA2 Enterprise	To verify whether client is able to connect WLAN with enterprise or not	Passed	
MEJ88PH2S_4800AP_07	Downgrading the 4800 ME controller with old image using http/TFTP/ftp	To verify whether 4800 ME Controller downgrading with old version or not	Passed	
MEJ88PH2S_4800AP_08	Updating the 4800 ME Controller with latest image using http/TFTP/ftp	To verify whether 4800 ME Controller upgrading with latest version or not	Passed	

MEJ88PH2S_4800AP_09	Rebooting the 4800 ME controller and checking the configurations	To check whether 4800 ME controller configuration are showing proper or not after reboot	Passed	
MEJ88PH2S_4800AP_10	Disabling the 802.11 radios and checking the SSID broadcasting or not	To verify whether SSID are broadcasting or not after 802.11 radios are in disable state	Failed	CSCvm39467
MEJ88PH2S_4800AP_11	Configuring the 4800 AP dot1x credentials	To verify whether 4800 AP dot.1x credentials are Applying successfully or not	Passed	
MEJ88PH2S_4800AP_12	Performing the Master AP failover with 4800 AP	To verify whether 4800 AP coming as ME controller or not after master failover	Passed	
MEJ88PH2S_4800AP_13	Joining the 4800 CAPWAP AP to ME as external AP	To verify whether 4800 AP joining to ME controller as external AP or not	Passed	
MEJ88PH2S_4800AP_14	Changing the 4800 External AP between different AP groups	To verify whether 4800 External AP changing groups without reboot or not	Passed	
MEJ88PH2S_4800AP_15	Changing the 4800 Internal AP between different AP groups	To verify whether 4800 Internal AP changing groups without reboot or not	Passed	
MEJ88PH2S_4800AP_16	Performing the master failover in read-only access	To verify whether Master AP failover happening in read-only access or not	Passed	
MEJ88PH2S_4800AP_17	Interchanging the 4800 ME AP image and check the details	To verify whether Image inter change happening or not	Passed	
MEJ88PH2S_4800AP_18	Performing the 4800 ME AP LED blink	To verify whether 4800 ME AP LED is blinking or not	Passed	

MEJ88PH2S_4800AP_19	Performing PING and Radius test	To verify whether PING and Radius test passed successfully or not	Passed	
MEJ88PH2S_4800AP_20	Login to the 4800 ME with different users	To verify whether User is able to login successfully with different users or nor	Passed	
MEJ88PH2S_4800AP_21	Restrict/grant the access to ME controller using http/https/SSH/telnet	To verify whether user is able to restrict the access or not	Passed	
MEJ88PH2S_4800AP_22	Checking the Application details after connect the clients to AVC	To verify whether accessed Applications details showing properly or not in monitor page	Passed	
MEJ88PH2S_4800AP_23	Enabling more than 2 next preferred controllers	To verify whether more than 2 AP are possible to make as next preferred APs	Passed	
MEJ88PH2S_4800AP_24	Configuring the Mac address of client in white list	To verify whether White list configured MAC address are accessing successfully or not	Passed	
MEJ88PH2S_4800AP_25	Configuring the Mac address of client in black list	To verify whether Black list configured MAC address are not accessing successfully or not	Passed	
MEJ88PH2S_4800AP_26	Assigning the IP address to Internal/External AP using Static/DHCP	To verify whether possible to assign the IP address to Internal/External AP using static/DHCP	Passed	
MEJ88PH2S_4800AP_27	Assigning the IP address to ME controller using Static/DHCP	To verify whether possible to assign the IP address to ME controller using static/DHCP	Passed	

MEJ88PH2S_4800AP_28	Configuring the AP default location details with Japanese/English language	To verify whether AP location details are possible to add with Japanese/English	Passed	
MEJ88PH2S_4800AP_29	Assigning the internal DHCP to WLAN	To verify whether client is getting the valid IP address from Internal DHCP or not	Failed	CSCvm34007
MEJ88PH2S_4800AP_30	Enabling the Schedule details in WLAN with Cisco any connect	To verify whether schedule details are enabling successfully or not with cisco any connect	Passed	
MEJ88PH2S_4800AP_31	Enabling the SSH to AP	To verify whether AP SSH details are changing successfully or not	Passed	
MEJ88PH2S_4800AP_32	Verifying ME backup image version after upgrade/downgrade	To check whether the backup image version showing properly or not after upgrade/downgrade	Failed	CSCvm10205
MEJ88PH2S_4800AP_33	Monitoring the client details in 4800 ME controller	To check whether clients are able to show on the monitoring page or not.	Passed	
MEJ88PH2S_4800AP_34	Creating the WLAN with English/Japanese language	To check whether the WLAN with Japanese/English character is creating or not	Passed	
MEJ88PH2S_4800AP_35	Associating the different client to SSID with Invalid credentials	To check whether different clients connecting to SSID with invalid credentials or not	Passed	
MEJ88PH2S_4800AP_36	Checking disabled SSID is broadcasting or not	To verify whether disabled WLAN is broadcasting or not	Passed	

MEJ88PH2S_4800AP_37	Configuring CME name with Japanese character	To check whether the CME name is possible configure with Japanese or not	Passed	
MEJ88PH2S_4800AP_38	Connecting the client with invalid credentials as WLAN created with mac filtering +WPA personal	To verify whether client is connecting with invalid credentials as WLAN created with mac filtering +WPA personal	Passed	
MEJ88PH2S_4800AP_39	Creating the NTP server with invalid IP and syncing the time	To check whether NTP server with invalid IP adding successfully or not on CME	Passed	
MEJ88PH2S_4800AP_40	Searching the AP and client	To check whether AP and client search details are showing proper or not	Passed	
MEJ88PH2S_4800AP_41	Clearing controller configuration	To check whether configuration can be cleared or not from CME GUI	Passed	
MEJ88PH2S_4800AP_42	Integrating the CMX setup with 4800 ME controller	To check whether CMX can be integrated or not in CME GUI	Passed	
MEJ88PH2S_4800AP_43	Creating invalid SNMP communities and traps	To check whether able to create invalid SNMP communities and traps or not through CLI	Passed	
MEJ88PH2S_4800AP_44	Exporting configuration file to controller through CLI/UI	To check whether configuration file can be exported or not to the controller in CME CLI/UI	Passed	
MEJ88PH2S_4800AP_45	Importing configuration file from controller through CLI/UI	To check whether configuration file can be imported or not from the controller UI/CLI	Passed	

MEJ88PH2S_4800AP_46	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	
MEJ88PH2S_4800AP_47	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	
MEJ88PH2S_4800AP_48	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	
MEJ88PH2S_4800AP_49	Monitoring multiple client mac address in CME and checking the clients status in Monitoring page	To check whether able to connect the multiple clients mac address in mac filtering and checking the clients status are shown properly or not in Monitoring page.	Passed	
MEJ88PH2S_4800AP_50	Converting a 4800 ME AP into a CAPWAP AP	To check whether able to convert the ME AP into a CAPWAP AP	Passed	
MEJ88PH2S_4800AP_51	Joining the external AP if Internal AP name is configured with Japanese characters	To check whether External AP able to join ME Controller name with Japanese or not	Passed	
MEJ88PH2S_4800AP_52	Configuring the System time manually/time zone based	To verify whether TIME configured successful with manual or time zone base	Failed	CSCvk68911

MEJ88PH2S_4800AP_53	Adding the 4800 ME controller in PI	To verify whether 4800 ME controller adding successfully to PI or not	Passed	
MEJ88PH2S_4800AP_54	Configuring the 4800 ME details from PI	To verify whether 4800 ME controller details possible to configure from PI or not	Passed	
MEJ88PH2S_4800AP_55	Monitoring the 4800 ME details in PI	To verify whether 4800 ME details are showing properly in PI or not	Passed	
MEJ88PH2S_4800AP_56	Joining the multiple external APs with same name to 4800 ME	To verify whether multiple external APs joining with same name to 4800 ME or not	Passed	

ME GUI - MC2UC (Videostreaming)

Logical ID	Title	Description	Status	Defect ID
MEJ88PH2S_MC2UC_01	Checking MC2UC traffic when clients connected with open security	Verifying MC2UC traffic for clients connected with open security	Passed	
MEJ88PH2S_MC2UC_02	Checking MC2UC traffic when clients connected with WPA2 Personal security	Verifying MC2UC traffic for clients connected with WPA2 Personal security	Passed	
MEJ88PH2S_MC2UC_03	Checking MC2UC traffic when clients connected with WPA2 Enterprise security with Radius as authentication server	Verifying MC2UC traffic for clients connected with WPA2 Enterprise security with radius as authentication server	Passed	
MEJ88PH2S_MC2UC_04	Checking MC2UC traffic when clients connected with WPA2 Enterprise security with AP as authentication server	Verifying MC2UC traffic for clients connected with WPA2 Enterprise security with AP as authentication server	Passed	

MEJ88PH2S_MC2UC_05	Checking MC2UC traffic when clients switches between AP radios	Verifying MC2UC traffic for clients when it roams between AP radios	Passed	
MEJ88PH2S_MC2UC_06	Performing Intra controller roaming for client and checking MC2UC traffic	Verifying MC2UC traffic for clients when it roams between AP's	Passed	
MEJ88PH2S_MC2UC_07	Verifying Multicast-direct is enabling from CLI globally	To verify whether multicast-direct is enabling from cli globally	Passed	
MEJ88PH2S_MC2UC_08	Checking MC2UC traffic when clients connected with QOS Platinum	Verifying MC2UC traffic for clients connected with QOS Platinum	Passed	
MEJ88PH2S_MC2UC_09	Checking MC2UC traffic while blocking rtp server	Verifying MC2UC traffic while blocking rtp server	Passed	
MEJ88PH2S_MC2UC_10	Checking MC2UC traffic when AP changed to different group	Verifying MC2UC traffic when AP changed to different group	Passed	
MEJ88PH2S_MC2UC_11	Checking MC2UC traffic after updating MAC address profile	Verifying MC2UC traffic after updating MAC address profile	Passed	
MEJ88PH2S_MC2UC_12	Checking MC2UC traffic for client using different DHCP pool	Verifying MC2UC traffic for client using different DHCP pool	Passed	
MEJ88PH2S_MC2UC_13	Checking MC2UC traffic for client with NAT enabled	Verifying MC2UC traffic for client with NAT enabled	Passed	
MEJ88PH2S_MC2UC_14	Checking MC2UC traffic for client when applying AVC with rtp application drop	Verifying MC2UC traffic for client when applying AVC with rtp application drop	Passed	
MEJ88PH2S_MC2UC_15	Checking MC2UC traffic for client when applying AVC with rtp-video application drop	Verifying MC2UC traffic for client when applying AVC with rtp-video application drop	Passed	

MEJ88PH2S_MC2UC_16	Checking MC2UC traffic for client when applying AVC with rtp-audio application drop	Verifying MC2UC traffic for client when applying AVC with rtp-audio application drop	Passed	
MEJ88PH2S_MC2UC_17	Creating media stream with Valid data	Verifying media stream is created with valid data	Passed	
MEJ88PH2S_MC2UC_18	Creating media stream with duplicated data	Verifying media stream is created with duplicated data or not	Passed	
MEJ88PH2S_MC2UC_19	Creating media stream parameters with valid data	Verifying media stream parameters are creating with valid data or not	Passed	
MEJ88PH2S_MC2UC_20	Creating media stream parameters with invalid data	Verifying media stream parameters are creating with invalid data or not	Passed	
MEJ88PH2S_MC2UC_21	Creating media stream with read-only user	Verifying media stream is able to create with read only user or not	Passed	
MEJ88S_MC2UC_01	Checking MC2UC traffic when clients connected with open security	Verifying MC2UC traffic for clients connected with open security	Passed	
MEJ88S_MC2UC_02	Checking MC2UC traffic when clients connected with WPA2 Personal security	Verifying MC2UC traffic for clients connected with WPA2 Personal security	Passed	
MEJ88S_MC2UC_03	Checking MC2UC traffic when clients connected with WPA2 Enterprise security with Radius as authentication server	Verifying MC2UC traffic for clients connected with WPA2 Enterprise security with radius as authentication server	Passed	

MEJ88S_MC2UC_04	Checking MC2UC traffic when clients connected with WPA2 Enterprise security with AP as authentication server	Verifying MC2UC traffic for clients connected with WPA2 Enterprise security with AP as authentication server	Passed	
MEJ88S_MC2UC_05	Checking MC2UC traffic when clients switches between AP radios	Verifying MC2UC traffic for clients when it roams between AP radios	Passed	
MEJ88S_MC2UC_06	Performing Intra controller roaming for client and checking MC2UC traffic	Verifying MC2UC traffic for clients when it roams between AP's	Passed	
MEJ88S_MC2UC_07	Verifying Multicast-direct is enabling from CLI globally	To verify whether multicast-direct is enabling from cli globally	Passed	
MEJ88S_MC2UC_08	Checking MC2UC traffic when clients connected with QOS Platinum	Verifying MC2UC traffic for clients connected with QOS Platinum	Passed	
MEJ88S_MC2UC_09	Checking MC2UC traffic while blocking rtp server	Verifying MC2UC traffic while blocking rtp server	Passed	
MEJ88S_MC2UC_10	Checking MC2UC traffic when AP changed to different group	Verifying MC2UC traffic when AP changed to different group	Passed	
MEJ88S_MC2UC_11	Checking MC2UC traffic after updating MAC address profile	Verifying MC2UC traffic after updating MAC address profile	Passed	
MEJ88S_MC2UC_12	Checking MC2UC traffic for client using different DHCP pool	Verifying MC2UC traffic for client using different DHCP pool	Passed	
MEJ88S_MC2UC_13	Checking MC2UC traffic for client with NAT enabled	Verifying MC2UC traffic for client with NAT enabled	Passed	

MEJ88S_MC2UC_14	Checking MC2UC traffic for client when applying AVC with rtp application drop	Verifying MC2UC traffic for client when applying AVC with rtp application drop	Passed	
MEJ88S_MC2UC_15	Checking MC2UC traffic for client when applying AVC with rtp-video application drop	Verifying MC2UC traffic for client when applying AVC with rtp-video application drop	Passed	
MEJ88S_MC2UC_16	Checking MC2UC traffic for client when applying AVC with rtp-audio application drop	Verifying MC2UC traffic for client when applying AVC with rtp-audio application drop	Passed	
MEJ88S_MC2UC_17	Creating media stream with Valid data	Verifying media stream is created with valid data	Passed	
MEJ88S_MC2UC_18	Creating media stream with duplicated data	Verifying media stream is created with duplicated data or not	Passed	
MEJ88S_MC2UC_19	Creating media stream parameters with valid data	Verifying media stream parameters are creating with valid data or not	Passed	
MEJ88S_MC2UC_20	Creating media stream parameters with invalid data	Verifying media stream parameters are creating with invalid data or not	Passed	
MEJ88S_MC2UC_21	Creating media stream with read-only user	Verifying media stream is able to create with read only user or not	Passed	

mDNS Support

Logical ID	Title	Description	Status	Defect ID
MEJ88PH2S_mDNS_01	Checking mDNS services are applied to MAC OS with WLAN open security	Verifying mDNS services are applied to Mac OS with open SSID	Passed	

MEJ88PH2S_mDNS_02	Checking mDNS services are applied to MacOS and IOS with WLAN WPA2 personal security	Verifying mDNS services are applied to MacOS and IOS with WPA2 personal security	Passed	
MEJ88PH2S_mDNS_03	Checking mDNS services are applied to Apple TV and IOS with WLAN WPA2 Enterprise security and authentication server as radius	Verifying mDNS services are applied to AppleTV and IOS with WPA2 Enterprise security and radius as authentication server	Passed	
MEJ88PH2S_mDNS_04	Checking mDNS services are applied to Apple Devices with WLAN WPA2 Enterprise security and authentication server as AP	Verifying mDNS services are applied to AppleTV and IOS with WPA2 Enterprise security and AP as authentication server	Passed	
MEJ88PH2S_mDNS_05	Checking mDNS services are applied to Apple Devices with security Internal Splash and Radius as access type	Verifying mDNS services are applied to Apple Devices with security Internal Splash and Radius as access type	Passed	
MEJ88PH2S_mDNS_06	Checking mDNS services are applied to Apple Devices with security Internal Splash and WPA2 Personal as access type	Verifying mDNS services are applied to Apple Devices with security Internal Splash and WPA2 Personal as access type	Passed	
MEJ88PH2S_mDNS_07	Checking mDNS services are applied to MacOS and IOS with WLAN CWA security	Verifying mDNS services are applied to MacOS and IOS with CWA security	Passed	
MEJ88PH2S_mDNS_08	Checking mDNS services are applied to Apple Devices with Fastlane enabled	Verifying mDNS services are applied to Apple Devices with fastlane enabled	Passed	

MEJ88PH2S_mDNS_09	Performing client communication between two clients connected two different VLAN	Checking client communication between two clients connected to different VLAN	Passed	
MEJ88PH2S_mDNS_10	Performing client communication between two clients connected two different VLAN with NAT enabled	Checking client communication between two clients connected to different VLAN with NAT enabled	Passed	
MEJ88PH2S_mDNS_11	Performing roaming operation when mDNS is applied	Checking roaming when mDNS is applied	Passed	
MEJ88PH2S_mDNS_12	Exporting config file after upgrading ME	Checking mDNS config after exporting config file	Passed	
MEJ88PH2S_mDNS_13	Creating mDNS profile by adding required services	Verifying mDNS profile is creating with required services	Passed	
MEJ88PH2S_mDNS_14	Enabling mDNS Snooping and mDNS Policy from UI	Verifying mDNS snooping and mDNS Policy is enabling	Passed	
MEJ88PH2S_mDNS_15	Disabling mDNS Snooping and mDNS Policy from CLI	Verifying mDNS snooping and mDNS Policy is disabling from CLI	Passed	
MEJ88PH2S_mDNS_16	Checking mDNS services are applied to android and Chromecast with WLAN open security	Verifying DNS services are applied to android and Chromecast with open SSID	Passed	
MEJ88PH2S_mDNS_17	Checking mDNS services are applied to android and Chromecast with WLAN WPA2 personal security	Verifying mDNS services are applied to android and Chromecast with WPA2 personal security	Passed	

MEJ88PH2S_mDNS_18	Checking mDNS services are applied to android and Chromecast with WLAN WPA2 Enterprise security and authentication server as radius	Verifying mDNS services are applied to android and Chromecast with WPA2 Enterprise security and radius as authentication server	Passed	
MEJ88PH2S_mDNS_19	Checking mDNS services are applied to android and Chromecast with WLAN WPA2 Enterprise security and authentication server as AP	Verifying mDNS services are applied to android and Chromecast with WPA2 Enterprise security and AP as authentication server	Passed	
MEJ88PH2S_mDNS_20	Checking mDNS services are applied to android and Chromecast with security Internal Splash and Radius as access type	Verifying mDNS services are applied to Apple Devices with security Internal Splash and Radius as access type	Passed	
MEJ88PH2S_mDNS_21	Checking mDNS services are applied to android and Chromecast with security Internal Splash and WPA2 Personal as access type	Verifying mDNS services are applied to android and Chromecast with security Internal Splash and WPA2 Personal as access type	Passed	
MEJ88S_mDNS_1	Checking mDNS services are applied to MAC OS with WLAN open security	Verifying mDNS services are applied to Mac OS with open SSID	Passed	
MEJ88S_mDNS_2	Checking mDNS services are applied to MacOS and IOS with WLAN WPA2 personal security	Verifying mDNS services are applied to MacOS and IOS with WPA2 personal security	Passed	

MEJ88S_mDNS_3	Checking mDNS services are applied to Apple TV and IOS with WLAN WPA2 Enterprise security and authentication server as radius	Verifying mDNS services are applied to AppleTV and IOS with WPA2 Enterprise security and radius as authentication server	Passed	
MEJ88S_mDNS_4	Checking mDNS services are applied to Apple Devices with WLAN WPA2 Enterprise security and authentication server as AP	Verifying mDNS services are applied to AppleTV and IOS with WPA2 Enterprise security and AP as authentication server	Passed	
MEJ88S_mDNS_5	Checking mDNS services are applied to Apple Devices with security Internal Splash and Local User as access type	Verifying mDNS services are applied to Apple Devices with security Internal Splash and local user as access type	Passed	
MEJ88S_mDNS_6	Checking mDNS services are applied to Apple Devices with security Internal Splash and Web Consent as access type	Verifying mDNS services are applied to Apple Devices with security Internal Splash and Web Consent as access type	Passed	
MEJ88S_mDNS_7	Checking mDNS services are applied to Apple Devices with security Internal Splash and Email as access type	Verifying mDNS services are applied to Apple Devices with security Internal Splash and Email as access type	Passed	
MEJ88S_mDNS_8	Checking mDNS services are applied to Apple Devices with security Internal Splash and Radius as access type	Verifying mDNS services are applied to Apple Devices with security Internal Splash and Radius as access type	Passed	

MEJ88S_mDNS_9	Checking mDNS services are applied to Apple Devices with security Internal Splash and WPA2 Personal as access type	Verifying mDNS services are applied to Apple Devices with security Internal Splash and WPA2 Personal as access type	Passed	
MEJ88S_mDNS_10	Checking mDNS services are applied to MacOS and IOS with WLAN CWA security	Verifying mDNS services are applied to MacOS and IOS with CWA security	Passed	
MEJ88S_mDNS_11	Checking mDNS services are applied to Apple Devices with Fastlane enabled	Verifying mDNS services are applied to Apple Devices with fastlane enabled	Passed	
MEJ88S_mDNS_12	Performing client communication between two clients connected two different VLAN	Checking client communication between two clients connected to different VLAN	Passed	
MEJ88S_mDNS_13	Performing client communication between two clients connected two different VLAN with NAT enabled	Checking client communication between two clients connected to different VLAN with NAT enabled	Passed	
MEJ88S_mDNS_14	Performing roaming operation when mDNS is applied	Checking roaming when mDNS is applied	Passed	
MEJ88S_mDNS_15	Exporting config file after upgrading ME	Checking mDNS config after exporting config file	Passed	
MEJ88S_mDNS_16	Creating mDNS profile by adding required services	Verifying mDNS profile is creating with required services	Passed	
MEJ88S_mDNS_17	Enabling mDNS Snooping and mDNS Policy from UI	Verifying mDNS snooping and mDNS Policy is enabling	Passed	
MEJ88S_mDNS_18	Disabling mDNS Snooping and mDNS Policy from CLI	Verifying mDNS snooping and mDNS Policy is disabling from CLI	Passed	

EoGRE Support on ME

Logical ID	Title	Description	Status	Defect ID
MEJ88PH2S_EoGRE_01	Establishing the EoGRE tunnel and connecting the Windows client	To verify whether Windows client communicating with device through tunnel or not	Passed	
MEJ88PH2S_EoGRE_02	Establishing the EoGRE tunnel and connecting the IOS client	To verify whether IOS client communicating with device through tunnel or not	Passed	
MEJ88PH2S_EoGRE_03	Establishing the EoGRE tunnel and connecting the MAC client	To verify whether MAC client communicating with device through tunnel or not	Passed	
MEJ88PH2S_EoGRE_04	Establishing the EoGRE tunnel and connecting the Japanese client	To verify whether Japanese client communicating with device through tunnel or not	Passed	
MEJ88PH2S_EoGRE_05	Establishing the EoGRE tunnel and connecting the Android client	To verify whether Android client communicating with device through tunnel or not	Passed	
MEJ88PH2S_EoGRE_06	Rebooting the AP and checking the EoGRE configurations	To verify whether after reboot EoGRE configurations are available or not	Passed	
MEJ88PH2S_EoGRE_07	Upgrading the ME and checking the ME configuration	To verify whether after Image upgrade EoGRE details are showing properly or not	Passed	
MEJ88PH2S_EoGRE_08	Copying the EoGRE rule details to other profile	To verify whether EoGRE rules are copying to the other profile or not	Passed	
MEJ88PH2S_EoGRE_09	Modifying the EoGRE profile details	To verify whether EoGRE profile details are modifying or not	Passed	

MEJ88S_EoGRE_01	Establishing the EoGRE tunnel and connecting the Windows client	To verify whether Windows client communicating with device through tunnel or not	Passed	
MEJ88S_EoGRE_02	Establishing the EoGRE tunnel and connecting the IOS client	To verify whether IOS client communicating with device through tunnel or not	Passed	
MEJ88S_EoGRE_03	Establishing the EoGRE tunnel and connecting the MAC client	To verify whether MAC client communicating with device through tunnel or not	Passed	
MEJ88S_EoGRE_04	Establishing the EoGRE tunnel and connecting the Japanese client	To verify whether Japanese client communicating with device through tunnel or not	Passed	
MEJ88S_EoGRE_05	Establishing the EoGRE tunnel and connecting the Android client	To verify whether Android client communicating with device through tunnel or not	Passed	
MEJ88S_EoGRE_06	Rebooting the AP and checking the EoGRE configurations	To verify whether after reboot EoGRE configurations are available or not	Passed	
MEJ88S_EoGRE_07	Upgrading the ME and checking the ME configuration	To verify whether after Image upgrade EoGRE details are showing properly or not	Passed	
MEJ88S_EoGRE_08	Copying the EoGRE rule details to other profile	To verify whether EoGRE rules are copying to the other profile or not	Passed	
MEJ88S_EoGRE_09	Modifying the EoGRE profile details	To verify whether EoGRE profile details are modifying or not	Passed	

Schedule WLAN Support

Logical ID	Title	Description	Status	Defect ID
MEJ88PH2S_SWLAN_01	Schedule the WLAN with open security for enabled hours/days	To check whether SSID is broadcasting or not on enabled time	Failed	CSCvm24712
MEJ88PH2S_SWLAN_02	Schedule the WLAN with open security for disabled hours/days	To check whether SSID is stopped broadcasting or not on disabled time	Passed	
MEJ88PH2S_SWLAN_03	Configure the schedule WLAN with WPA2 Personal security for enabled hours/days	Verify whether Scheduled WLAN is broadcasting or not on enabled time	Passed	
MEJ88PH2S_SWLAN_04	Configure the schedule WLAN with WPA2 Personal security for disabled hours/days	Verify whether SSID is stopped broadcasting or not on disabled time	Passed	
MEJ88PH2S_SWLAN_05	Configure the None option for scheduled WLAN	Verify whether Scheduled WLAN configuration get cleared or not after enabling the None option	Passed	
MEJ88PH2S_SWLAN_06	Schedule the WLAN with WPA2 Enterprise for enabled hours/days	To check whether WLAN is broadcasting or not on Scheduled time	Passed	
MEJ88PH2S_SWLAN_07	Schedule the WLAN with WPA2 Enterprise for disabled hours/days	To check whether WLAN is stopped broadcasting or not on Scheduled time	Passed	
MEJ88PH2S_SWLAN_08	Configure the schedule WLAN with Internal Splash Page with WPA2 PSK for enabled hours/days/week	Verify the schedule WLAN is broadcasting or not on scheduled WLAN enabled hours	Passed	
MEJ88PH2S_SWLAN_09	Configure the schedule WLAN with Internal Splash Page for disabled hours/days/week	Verifying whether SSID is stopped broadcasting or not on disabled time/hours	Passed	

MEJ88PH2S_SWLAN_10	Configure the Schedule WLAN with CWA for enabled hours/days/week	To check whether SSID is broadcasting or not on enabled hours/days/time	Passed	
MEJ88PH2S_SWLAN_11	Configure the Schedule WLAN with CWA for disabled hours/days/time	To check whether SSID is stopped broadcasting or not on disabled hours/days/time	Passed	
MEJ88PH2S_SWLAN_12	Verify the Schedule WLAN with Authentication Server(AP) for enabled hours/days/time	Validate the SSID is broadcasting or not for enabled Scheduled WLAN	Passed	
MEJ88PH2S_SWLAN_13	Verify the Schedule WLAN with Authentication Server(AP) for disabled hours/days/time	Validate the SSID is stopped broadcasting or not for disabled hours/time/days	Passed	
MEJ88PH2S_SWLAN_14	Verifying the CMX connect with Schedule WLAN broadcasting for enabled hours/days/time	To check whether scheduled WLAN broadcasting and client is connecting successfully on enabled scheduled time/day	Passed	
MEJ88PH2S_SWLAN_15	Verifying the CMX connect with Schedule WLAN broadcasting for disabled hours/days/time	To check whether scheduled WLAN is stopped broadcasting and client is disconnecting successfully for disabled time	Passed	
MEJ88PH2S_SWLAN_16	Configuring the Schedule WLAN with Web Consent for enabled hours/days	Validate the scheduled WLAN is broadcasting or not on particular day/time	Passed	
MEJ88PH2S_SWLAN_17	Configuring the Schedule WLAN with Web Consent for disabled hours/days/time	To check whether scheduled WLAN is stopped broadcasting on particular day/time	Passed	

MEJ88PH2S_SWLAN_18	Configure the Local User Account with Scheduled WLAN for enabled hours	To check whether SSID is broadcasting and client is able to connect successfully via Local User Account	Passed	
MEJ88PH2S_SWLAN_19	Configure the Local User Account with Scheduled WLAN for disabled hours	To check whether SSID is stopped broadcasting on particular time and client disconnect.	Passed	
MEJ88PH2S_SWLAN_20	Configure the Scheduled WLAN with Internal Splash Page Email Address for enabled hours	Validate the Scheduled WLAN SSID is broadcasting successfully on particular time.	Passed	
MEJ88PH2S_SWLAN_21	Configure the Internal Splash Page Email Address for Scheduled WLAN disabled hours	Validate the Scheduled WLAN SSID is stopped broadcasting successfully or not on particular time.	Passed	
MEJ88PH2S_SWLAN_22	Configure the Schedule WLAN with external Splash page Local User Account for enabled hours	Validate scheduled WLAN is broadcasting on time and client is connecting successfully	Passed	
MEJ88PH2S_SWLAN_23	Configure the Schedule WLAN with external Splash page Local User Account for disabled hours	Validate scheduled WLAN is stopped broadcasting on time and client is disconnecting successfully	Passed	
MEJ88PH2S_SWLAN_24	Verifying the Schedule WLAN with External Splash Page Web Consent for enabled hours	To check whether the schedule WLAN is broadcasting or not on particular time	Passed	

MEJ88PH2S_SWLAN_25	Verifying the Schedule WLAN with External Splash Page Web Consent for disabled hours	To check whether the schedule WLAN is stopped broadcasting on time	Passed	
MEJ88PH2S_SWLAN_26	Configure the Schedule WLAN via cli with WPA security for enabled hours	To check whether SSID is broadcasting or not on time	Passed	
MEJ88PH2S_SWLAN_27	Configure the Schedule WLAN via cli with WPA security for disabled hours	To check whether WLAN is stopped broadcasting or not on disabled time	Passed	
MEJ88PH2S_SWLAN_28	Configure the Schedule WLAN as per system time for enabled hours	Verifying whether Schedule WLAN SSID is broadcasting or not as per system time	Passed	
MEJ88PH2S_SWLAN_29	Change the SSID name of Scheduled WLAN for enabled hours	To check whether SSID is stopped broadcasting or not after changing the SSID Name for enabled hours	Passed	
MEJ88PH2S_SWLAN_30	Verify the client connectivity if disabled hrs. have been changed to current system time	Verifying the client connectivity after changing the disabled hours of Scheduled WLAN	Passed	
MEJ88PH2S_SWLAN_31	Verify the roaming client states of Scheduled WLAN for enabled hours	To check whether client is roaming or not from AP1 to AP2	Passed	
MEJ88PH2S_SWLAN_32	Verifying the Scheduled WLAN configuration after importing and exporting the same config file for enabled hours	To check whether the Scheduled WLAN configuration importing/exporting same file or not for enabled hours	Passed	

MEJ88PH2S_SWLAN_33	Verifying the client connectivity of scheduled WLAN if controller is made up during the enable time duration	To check whether SSID is broadcasting or not after WLC made-up	Passed	
MEJ88PH2S_SWLAN_34	Verifying the scheduled WLAN status if controller is rebooted at the scheduled end time	To check whether SSID is stopped broadcasting or not after WLC reboot at end of scheduled time	Passed	
MEJ88S_SWLAN_01	Schedule the WLAN with open security for enabled hours/days	To check whether SSID is broadcasting or not on enabled time	Passed	
MEJ88S_SWLAN_02	Schedule the WLAN with open security for disabled hours/days	To check whether SSID is stopped broadcasting or not on disabled time	Passed	
MEJ88S_SWLAN_03	Configure the schedule WLAN with WPA2 Personal security for enabled hours/days	Verify whether Scheduled WLAN is broadcasting or not on enabled time	Passed	
MEJ88S_SWLAN_04	Configure the schedule WLAN with WPA2 Personal security for disabled hours/days	Verify whether SSID is stopped broadcasting or not on disabled time	Passed	
MEJ88S_SWLAN_05	Configure the None option for scheduled WLAN	Verify whether Scheduled WLAN configuration get cleared or not after enabling the None option	Passed	
MEJ88S_SWLAN_06	Schedule the WLAN with WPA2 Enterprise for enabled hours/days	To check whether WLAN is broadcasting or not on Scheduled time	Passed	
MEJ88S_SWLAN_07	Schedule the WLAN with WPA2 Enterprise for disabled hours/days	To check whether WLAN is stopped broadcasting or not on Scheduled time	Passed	

MEJ88S_SWLAN_08	Configure the schedule WLAN with Internal Splash Page with WPA2 PSK for enabled hours/days/week	Verify the schedule WLAN is broadcasting or not on scheduled WLAN enabled hours	Passed	
MEJ88S_SWLAN_09	Configure the schedule WLAN with Internal Splash Page for disabled hours/days/week	Verifying whether SSID is stopped broadcasting or not on disabled time/hours	Passed	
MEJ88S_SWLAN_10	Configure the Schedule WLAN with CWA for enabled hours/days/week	To check whether SSID is broadcasting or not on enabled hours/days/time	Passed	
MEJ88S_SWLAN_11	Configure the Schedule WLAN with CWA for disabled hours/days/time	To check whether SSID is stopped broadcasting or not on disabled hours/days/time	Passed	
MEJ88S_SWLAN_12	Verify the Schedule WLAN with Authentication Server(AP) for enabled hours/days/time	Validate the SSID is broadcasting or not for enabled Scheduled WLAN	Passed	
MEJ88S_SWLAN_13	Verify the Schedule WLAN with Authentication Server(AP) for disabled hours/days/time	Validate the SSID is stopped broadcasting or not for disabled hours/time/days	Passed	
MEJ88S_SWLAN_14	Verifying the CMX connect with Schedule WLAN broadcasting for enabled hours/days/time	To check whether scheduled WLAN broadcasting and client is connecting successfully on enabled scheduled time/day	Passed	

MEJ88S_SWLAN_15	Verifying the CMX connect with Schedule WLAN broadcasting for disabled hours/days/time	To check whether scheduled WLAN is stopped broadcasting and client is disconnecting successfully for disabled time	Passed	
MEJ88S_SWLAN_16	Configuring the Schedule WLAN with Web Consent for enabled hours/days	Validate the scheduled WLAN is broadcasting or not on particular day/time	Passed	
MEJ88S_SWLAN_17	Configuring the Schedule WLAN with Web Consent for disabled hours/days/time	To check whether scheduled WLAN is stopped broadcasting on particular day/time	Passed	
MEJ88S_SWLAN_18	Configure the Local User Account with Scheduled WLAN for enabled hours	To check whether SSID is broadcasting and client is able to connect successfully via Local User Account	Passed	
MEJ88S_SWLAN_19	Configure the Local User Account with Scheduled WLAN for disabled hours	To check whether SSID is stopped broadcasting on particular time and client disconnect.	Passed	
MEJ88S_SWLAN_20	Configure the Scheduled WLAN with Internal Splash Page Email Address for enabled hours	Validate the Scheduled WLAN SSID is broadcasting successfully on particular time.	Passed	
MEJ88S_SWLAN_21	Configure the Internal Splash Page Email Address for Scheduled WLAN disabled hours	Validate the Scheduled WLAN SSID is stopped broadcasting successfully or not on particular time.	Passed	

MEJ88S_SWLAN_22	Configure the Schedule WLAN with external Splash page Local User Account for enabled hours	Validate scheduled WLAN is broadcasting on time and client is connecting successfully	Passed	
MEJ88S_SWLAN_23	Configure the Schedule WLAN with external Splash page Local User Account for disabled hours	Validate scheduled WLAN is stopped broadcasting on time and client is disconnecting successfully	Passed	
MEJ88S_SWLAN_24	Verifying the Schedule WLAN with External Splash Page Web Consent for enabled hours	To check whether the schedule WLAN is broadcasting or not on particular time	Passed	
MEJ88S_SWLAN_25	Verifying the Schedule WLAN with External Splash Page Web Consent for disabled hours	To check whether the schedule WLAN is stopped broadcasting on time	Passed	
MEJ88S_SWLAN_26	Configure the Schedule WLAN via cli with WPA security for enabled hours	To check whether SSID is broadcasting or not on time	Passed	
MEJ88S_SWLAN_27	Configure the Schedule WLAN via cli with WPA security for disabled hours	To check whether WLAN is stopped broadcasting or not on disabled time	Passed	
MEJ88S_SWLAN_28	Configure the Schedule WLAN as per system time for enabled hours	Verifying whether Schedule WLAN SSID is broadcasting or not as per system time	Passed	
MEJ88S_SWLAN_29	Change the SSID name of Scheduled WLAN for enabled hours	To check whether SSID is stopped broadcasting or not after changing the SSID Name for enabled hours	Passed	

MEJ88S_SWLAN_30	Verify the client connectivity if disabled hrs. have been changed to current system time	Verifying the client connectivity after changing the disabled hours of Scheduled WLAN	Passed	
MEJ88S_SWLAN_31	Verify the roaming client states of Scheduled WLAN for enabled hours	To check whether client is roaming or not from AP1 to AP2	Passed	
MEJ88S_SWLAN_32	Verifying the Scheduled WLAN configuration after importing and exporting the same config file for enabled hours	To check whether the Scheduled WLAN configuration importing/exporting same file or not for enabled hours	Passed	
MEJ88S_SWLAN_33	Verifying the client connectivity of scheduled WLAN if controller is made up during the enable time duration	To check whether SSID is broadcasting or not after WLC made-up	Passed	
MEJ88S_SWLAN_34	Verifying the scheduled WLAN status if controller is rebooted at the scheduled end time	To check whether SSID is stopped broadcasting or not after WLC reboot at end of scheduled time	Passed	

Optimized Roaming

Logical ID	Title	Description	Status	Defect ID
MEJ88PH2S_OptRoam_01	Configuring optimized roaming with 2.4 GHz band & default interval and roam Android client	To verify that optimized roaming with 2.4 GHz band & default interval gets configured or not and check association of Android client	Passed	

MEJ88PH2S_OptRoam_02	Configuring optimized roaming with 2.4 GHz band & customized interval ,1 MBPS Thresholds and roam Android client	To verify that optimized roaming with 2.4 GHz band & customized interval ,1 MBPS Thresholds gets configured or not and check association of Android client	Passed	
MEJ88PH2S_OptRoam_03	Configuring optimized roaming with 5 GHz band & customized interval and roam Android client	To verify that optimized roaming with 5 GHz band &customized interval configured and check association of Android client	Passed	
MEJ88PH2S_OptRoam_04	Configuring optimized roaming with 5 GHz band & default interval , 6 MBPS Threshold and roam Android client	To verify that optimized roaming with 5 GHz band &default interval , 6 MBPS Threshold configured and check association of Android client	Passed	
MEJ88PH2S_OptRoam_05	Configuring optimized roaming with 2.4 GHz band & default interval ,5.5 MBPS Threshold and roam iOS client	To verify that optimized roaming with 2.4 GHz band &default interval ,5.5 MBPS Threshold configured successfully and check association of iOS client	Passed	
MEJ88PH2S_OptRoam_06	Configuring optimized roaming with 2.4 GHz band & customized interval(5 Sec) ,9 MBPS Threshold and roam iOS client	To verify that optimized roaming with 2.4 GHz band &customized interval(5 Sec) ,9 MBPS Threshold configured and check association of iOS client	Passed	

MEJ88PH2S_OptRoam_07	Configuring optimized roaming with 5 GHz band & customized interval(40 Sec) and roam iOS client	To verify that optimized roaming with 5 GHz band &customized interval(40 Sec) configured successfully and check association of iOS client	Passed	
MEJ88PH2S_OptRoam_08	Configuring optimized roaming with 5 GHz band & default interval , 12 MBPS Threshold and roam iOS client	To verify that optimized roaming with 5 GHz band & default interval , 12 MBPS Threshold configured successfully and check association of iOS client	Passed	
MEJ88PH2S_OptRoam_09	Moving the Android client from AP after enable optimized roaming	To verify that client got disassociated when signal is poor while moving from AP	Passed	
MEJ88PH2S_OptRoam_10	Moving the Android client from 4800 ME AP after enable optimized roaming	To verify that client got disassociated when signal is poor while moving from 4800 AP	Passed	
MEJ88PH2S_OptRoam_11	Moving the iOS client from AP after disabling the optimized roaming	To verify that client wouldn't disassociated when signal is poor while moving from AP	Failed	CSCvm17545
MEJ88PH2S_OptRoam_12	Moving the Android client from 2700 AP after enable optimized roaming in ME	To verify that client got disassociated when signal is poor while moving from 2700 AP	Passed	
MEJ88PH2S_OptRoam_13	Moving the Android client from AP after enable optimized roaming in ME with interference availability	To verify that client got disassociated when signal is poor while moving from 2700 AP with interference availability	Passed	

MEJ88PH2S_OptRoam_14	Configuring optimized roaming in ME 1815 with 2.4 GHz band & default interval ,5.5 MBPS Threshold and roam iOS client	To verify that optimized roaming in ME 1815 with 2.4 GHz band & default interval ,5.5 MBPS Threshold configured successfully and check association of iOS client	Passed	
MEJ88PH2S_OptRoam_15	Configuring optimized roaming in ME 2800 with 2.4 GHz band & default interval ,5.5 MBPS Threshold and roam iOS client	To verify that optimized roaming in ME 2800 with 2.4 GHz band & default interval ,5.5 MBPS Threshold configured successfully and check association of iOS client	Passed	
MEJ88PH2S_OptRoam_16	Connect iOS client from where SSID signal is week	To verify that iOS client connecting or not from where SSID signal is week	Passed	
MEJ88PH2S_OptRoam_17	Configuring the 802.11a optimized roaming in CLI and roam Android client	To verify that optimized roaming with 802.11a gets configured or not and check association of Android client	Passed	
MEJ88PH2S_OptRoam_18	Configuring the 802.11b optimized roaming in CLI and roam iOS client	To verify that optimized roaming with 802.11b gets configured or not and check association of iOS client	Passed	
MEJ88PH2S_OptRoam_19	Restarting the ME Controller after optimized roaming configuration	To verify that optimization roaming configuration remain same after reboot	Passed	

MEJ88PH2S_OptRoam_20	Importing/exporting configuration file after optimized roaming configuring	To verify that optimization roaming configuration remain same after import and export configuration file	Passed	

Conversion of AP type default configuration from CAPWAP to Cisco Mobility Express

Logical ID	Title	Description	Status	Defect Id
MEJ88S_CAPWAP_01	Joining the AP image with less than 8.8 to ME and checking the details	To verify whether AP join to the CME with AP version 8.8 and downloading the image or not	Failed	CSCvk21890
MEJ88S_CAPWAP_02	Joining the AP after Efficient join enable state	To verify whether AP is joining & downloading image from ME or not after efficient join enable state	Passed	
MEJ88S_CAPWAP_03	Joining the AP after Efficient join Disable state	To verify whether AP is joining & downloading image from ME or not after efficient join disable state	Passed	
MEJ88S_CAPWAP_04	COS AP with CAPWAP image joins to ME WLC with both COS AP & ME same versions	To verify whether COS AP is joining to the ME with both AP and ME same version and downloading the image directly or not	Passed	
MEJ88S_CAPWAP_05	COS AP with CAPWAP image joins to ME WLC with both COS AP & ME different versions	To verify whether COS AP is joinging to the ME with AP & ME different version and not downloading the image	Failed	CSCvk21890

MEJ88S_CAPWAP_06	IOS AP with CAPWAP image joins to ME WLC with both COS AP & ME same versions	To verify whether IOS AP is joining to the ME with both AP and ME same version and downloading the image directly or not	Passed	
MEJ88S_CAPWAP_07	IOS AP with CAPWAP image joins to ME WLC with both COS AP & ME different versions	To verify whether IOS AP is joining to the ME with AP & ME different version and not downloading the image	Passed	
MEJ88S_CAPWAP_08	Upgrading the ME image and making the CAPWAP APs to ME capable	To verify whether APs converting the ME capable or not after upgrade the ME image	Failed	CSCvk13835
MEJ88S_CAPWAP_09	Downgrading the ME image and making the CAPWAP APs to ME capable	To verify whether APs converting the ME capable or not after downgrade the ME image	Failed	CSCvk20402
MEJ88S_CAPWAP_10	Making the ME capable AP to Controller	To verify whether after Make me as controller CAPWAP are converting to ME or not	Failed	CSCvk03882
MEJ88S_CAPWAP_11	Removing the Master AP at the time of AP downloading the image	To verify whether it is possible to remove the Master AP at the time of AP downloading the image	Passed	
MEJ88S_CAPWAP_12	Chaging the ME time and trying to join the AP	To verify whether AP joining to the ME or not with AP and ME times are differe	Passed	
MEJ88S_CAPWAP_13	Performing the Master AP Failover	To verify whether after Master AP Failover, AP is again downloading the images or not	Failed	CSCvk03882

AP does not reboot when it joins an AP group

Logical ID	Title	Description	Status	Defect Id
MEJ88S_APG_01	Creating the AP group with Japanese language and assigning the COS AP	To verify whether AP associating to the AP group or not	Passed	
MEJ88S_APG_02	Moving the 1852 COS AP between different Groups in CME(1800/2800/3800/1500)	To verify whether 1852 COS AP Changing the groups or not without reboot in 1800/2800/3800/1500 CME models	Failed	CSCvj96753
MEJ88S_APG_03	Moving the 1542 COS AP between different AP Groups in CME(1800/2800/3800/1500)	To verify whether 1542 COS AP moving between different groups or not without reboot in CME(1800/2800/3800/1500)	Passed	
MEJ88S_APG_04	Moving the 1562 COS AP between different AP Groups in CME(1800/2800/3800/1500)	To verify whether 1562 COS AP moving between different groups or not without reboot in CME(1800/2800/3800/1500)	Passed	
MEJ88S_APG_05	Moving the 1832 COS AP between different AP Groups in CME(1800/2800/3800/1500)	To verify whether 1832 COS AP moving between different groups or not without reboot in CME(1800/2800/3800/1500)	Passed	
MEJ88S_APG_06	Moving the 2802I COS AP between different AP Groups in CME(1800/2800/3800/1500)	To verify whether 2802I2 COS AP moving between different groups or not without reboot in CME(1800/2800/3800/1500)	Passed	
MEJ88S_APG_07	Moving the 3802I COS AP between different AP Groups in CME(1800/2800/3800/1500)	To verify whether 3802I COS AP moving between different groups or not without reboot in CME(1800/2800/3800/1500)	Passed	

MEJ88S_APG_08	Moving the 3802E COS AP between different AP Groups in CME(1800/2800/3800/1500)	To verify whether 3802E COS AP moving between different groups or not without reboot in CME(1800/2800/3800/1500)	Passed	
MEJ88S_APG_09	Moving the 1815I COS AP between different AP Groups in CME(1800/2800/3800/1500)	To verify whether 1815I COS AP moving between different groups or not without reboot in CME(1800/2800/3800/1500)	Passed	
MEJ88S_APG_10	Moving the 1810 COS AP between different AP Groups in CME(1800/2800/3800/1500)	To verify whether 1810 COS AP moving between different groups or not without reboot in CME(1800/2800/3800/1500)	Passed	
MEJ88S_APG_11	Changing the AP between groups at the time of software upgrade/downgrade	To verify whether it is possible to change the AP group or not at the time upgrading the image	Passed	
MEJ88S_APG_12	Master/Next-preferred AP Changing between different groups at the time of software upgrade/downgrade	To verify whether after AP group change Master/Next-preferred AP downloading the image or not	Passed	
MEJ88S_APG_13	Changing the AP between different AP group in read-only mode	To verify whether AP is Changing the Groups or not in read-only mode	Passed	
MEJ88S_APG_14	Moving the 702 IOS AP between different AP Groups in CME(1800/2800/3800/1500)	To verify whether 702 COS AP moving between different groups or not without reboot in CME(1800/2800/3800/1500)	Passed	
MEJ88S_APG_15	Moving the 3700 IOS AP between different AP Groups in CME(1800/2800/3800/1500)	To verify whether 3700 COS AP moving between different groups or not without reboot in CME(1800/2800/3800/1500)	Passed	

MEJ88S_APG_16	Moving the 2700 IOS AP between different AP Groups in CME(1800/2800/3800/1500)	To verify whether 2700 COS AP moving between different groups or not without reboot in CME(1800/2800/3800/1500)	Passed	
MEJ88S_APG_17	Changing the AP group of AP from Prime infrastructure	TO verify whether AP is Changing the Group from prime infrastucture or not	Passed	
MEJ88S_APG_18	Assigning the defualt RF-Profile to AP group	To verify whether defualt RF-Profile is appying to the AP-group or not	Passed	
MEJ88S_APG_19	Assigning the user defined RF-Profile with 2.4GHZ to AP group	To verify whether user defined RF-profile with 2.4GHZ is applying to the AP-group or not	Passed	
MEJ88S_APG_20	Assigning the user defined RF-Profile with 5GHZ to AP group	To verify whether user defined RF-profile with 5GHZ is applying to the AP-group or not	Passed	
MEJ88S_APG_21	PI: Changing the COS Aps between different AP-groups	To verify whether COS APS are changing successfully between AP groups without reboot or not	Passed	
MEJ88S_APG_22	PI: Changing the IOS Aps between different AP-groups	To verify whether IOS APS are changing successfully between AP groups without reboot or not	Passed	
MEJ88S_APG_23	PI: Applying the defualt rf-profile to AP group	To verify whether defualt RF-profile is applying to the AP-group or not	Passed	
MEJ88S_APG_24	PI: Applying the user defined 2.4 GHZ rf-profile to AP group	To verify whether user defined 5 GHZ is applying to the AP group or not	Passed	
MEJ88S_APG_25	PI: Applying the user defined 5 GHZ rf-profile to AP group	To verify whether user defined 5 GHZ is applying to the AP group or not	Passed	

ME AP convert to CAPWAP via DHCP Option

Logical ID	Title	Description	Status	Defect ID
MEJ88S_DHCP43_01	Configuring the DHCP 43 in switch	To configure the DHCP 43 in switch	Passed	
MEJ88S_DHCP43_02	Change the 1852 ME AP type to CAPWAP using DHCP 43	To change the AP type to CAPWAP using DHCP 43	Passed	
MEJ88S_DHCP43_03	Change the 2800 ME AP type to CAPWAP using DHCP 43	To change the AP type to CAPWAP using DHCP 43	Passed	
MEJ88S_DHCP43_04	Change the 1542 ME AP type to CAPWAP using DHCP 43	To change the AP type to CAPWAP using DHCP 43	Passed	
MEJ88S_DHCP43_05	Change the 1815i ME AP type to CAPWAP using DHCP 43	To change the AP type to CAPWAP using DHCP 43	Passed	
MEJ88S_DHCP43_06	Change the AP mode after converting in to CAPWAP	To change the AP mode after converting in to CAPWAP	Passed	
MEJ88S_DHCP43_07	Connect iOS client to CAPWAP converted AP from ME with WPA2-PSK security	To connect the iOS client to CAPWAP converted AP from ME with WPA2-PSK security	Passed	
MEJ88S_DHCP43_08	Connect Android client to CAPWAP converted AP from ME with WPA2-PSK security	To connect the Android client to CAPWAP converted AP from ME with WPA2-PSK security	Passed	
MEJ88S_DHCP43_09	Config primary, secondary controller in AP and reload ME controller	To verify that ME changed to CAPWAP and send join request to controller that configured using DHCP option 43	Passed	

MEJ88S_DHCP43_10	Config two controller IP in DHCP option 43 and first should be wrong IP	To verify that AP joined to second controller if first IP is wrong in DHCP	Passed	
MEJ88S_DHCP43_11	Change the 1815i ME AP type to CAPWAP using DHCP 43 and join in to vWLC	To change the AP type to CAPWAP using DHCP 43and join in to vWLC	Passed	
MEJ88S_DHCP43_12	Make the Preferred Master one ME capable AP and reload ME Controller	To verify that ME Controller changed to CAPWAP after make Preferred master as another ME capable AP	Passed	

Cisco DNA Center Support for ME

Logical ID	Title	Description	Status	Defect Id
MEJ88S_Cisco DNA Center_01	Adding the ME in Cisco DNA Center via inventory method	Verify that user is able to add ME in Cisco DNA Center via inventory method or not	Passed	
MEJ88S_Cisco DNA Center_02	Provisoning ME via Cisco DNA Center	Verify that user is able to add ME in Cisco DNA Center via provisioning method or not	Passed	
MEJ88S_Cisco DNA Center_03	Importing maps from Cisco DNA Center	To import maps from Cisco DNA Center and check if the maps gets imported to the cmx .	Passed	
MEJ88S_Cisco DNA Center_04	Adding Access Pointss from CME to the imported maps from Cisco DNA Center to CMX	To check whther the imported Access Pointss are shown correctly in CMX or not	Passed	
MEJ88S_Cisco DNA Center_05	Checking the client details by connecting to the Access Pointss	Connecting the client to the Access Pointss and checking the connectivity	Passed	

MEJ88S_Cisco DNA Center_06	Discovering CME device IP in Cisco DNA Center	To check whther the added CME device IP is discovered in Cisco DNA Center or not	Passed	
MEJ88S_Cisco DNA Center_07	Updating the credentials, management IP and resync interval of CME from Cisco DNA Center	Verifying whether we can update the credentials, management IP and resync interval of CME from Cisco DNA Center or not	Passed	

CMX 10.5 Support

Logical ID	Title	Description	Status	Defect Id
MEJ88S_CMX10.5_01	Adding Cisco CME to CMX	To add a Cisco CME to CMX and check if the CME gets added to the CMX with the CME status showing	Passed	
MEJ88S_CMX10.5_02	Importing maps from prime infrastructure	To import maps from prime infrastructure and check if the maps gets imported to the cmx .	Passed	
MEJ88S_CMX10.5_03	Importing the maps with Access points from PI to CMX	To import the maps from prime infra to CMX with Access points and check if the access point details are shown correctly including clients connected .	Passed	
MEJ88S_CMX10.5_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	

MEJ88S_CMX10.5_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	
MEJ88S_CMX10.5_06	Using MAC address the client devices are searched	To check whether client device can be searched by specifying its MAC address or not	Passed	
MEJ88S_CMX10.5_07	Using IP address the client devices are searched	To check whether client device can be searched by specifying its IP address or not	Passed	
MEJ88S_CMX10.5_08	Using SSID the client devices are searched	To verify whether client device can be searched by specifying the SSID or not	Passed	
MEJ88S_CMX10.5_09	Number of clients visting the building and floor in hourly and daily basis	Verifying the number of clients visiting the building or floor on hourly and daily basis	Passed	
MEJ88S_CMX10.5_10	Number of client vists to the building and the floor	To check the number of new clients and repeated clients to the building or floor .	Passed	

Aging Test Cases

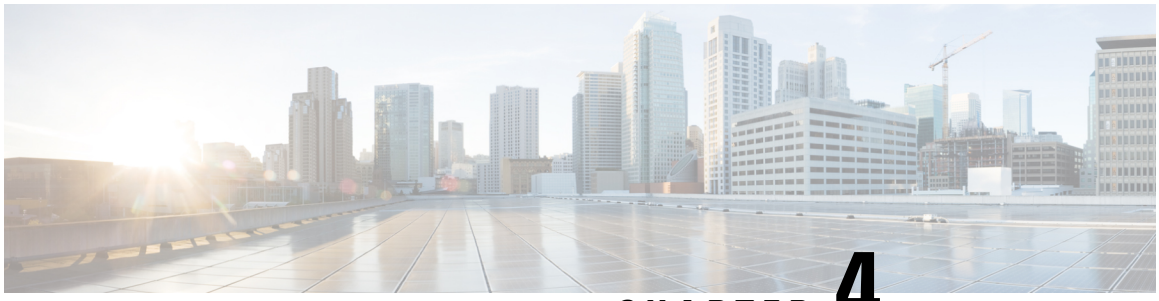
Logical ID	Title	Description	Status	Defect Id
MEJ88S_Aging_01	Trasfering the data via http between IOS client with fastlane enabled app	Transfering the traffic between two IOS client with fastlane coverage	Passed	
MEJ88S_Aging_02	Validate the Application library scenarios by adding applications in the Ixchariot	To validate the Application in the Ixchariot library and check the output of each library	Passed	

MEJ88S_Aging_03	Transfering the data via UDP and measure the throughput between IOS client with fastlane enabled wlan	Verify that user is able to transfer the data via UDP and measure the throughput between IOS client with fastlane enabled app	Passed	
MEJ88S_Aging_04	Transfering the data via UDP and measure the throughput between Windows and IOS client with fastlane enabled wlan	Verify that user is able to transfer the data via UDP and measure the throughput between IOS and non IOS client with fastlane enabled wlan	Passed	
MEJ88S_Aging_05	Measuring the throughput of TCP packets between client	To mesure throughput of TCP packet tranfer between client	Passed	
MEJ88S_Aging_06	Connecting the client with local mode ap and perform the UDP perfomance test	Testing the UDP performance between different client that associated with local mode ap	Passed	
MEJ88S_Aging_07	Connecting the IOS and android/windows/mac client with flexconnect mode ap and performe UDP perfomance test	Testing the UDP performance between different client that associated with flexconnect mode ap	Passed	
MEJ88S_Aging_08	Connecting the client with local mode ap and perform the TCP perfomance test	Testing the TCP performance between different client that associated with local mode ap	Passed	
MEJ88S_Aging_09	Connecting the client with flexconnect mode ap and perform the measeue the TCP perfomance	Testing the TCP performance between different client that associated with flexconnect mode ap	Passed	
MEJ88S_Aging_10	Connecting the IOS client with fast lane coverage wlan and test the facetime app througput	Measure the performance of factime app with fastlane coverage	Passed	

MEJ88S_Aging_11	Connecting a client and stream a video file and check the performance of the client using IXchariot	To stream a video from the client and check if the streaming occurs without any lag in performance using the IX chariot	Passed	
MEJ88S_Aging_12	Connecting a client continueously to the same WLAN by disconnecting and connecting	To connect the same client to the same WLAN by connecting and disconnecting contineously and check the behaviour .	Passed	
MEJ88S_Aging_13	Throughput test using the 5 GHz radio using Ixchariot for 2 to 3 hours	To test the throughput of the 5 GHz radio using Ixchariot for a period of 2 to 3 hours	Passed	
MEJ88S_Aging_14	Throughput test using the 2.4 GHz radio using Ixchariot for 2 to 3 hours	To test the throughput of the 2.4 GHz radio using Ixchariot for a period of 2 to 3 hours	Passed	
MEJ88S_Aging_15	Configuring session timeout for the client and monitoring the client activity	To configure the session timeout for the clients and monitoring the client activity .	Passed	
MEJ88S_Aging_16	AVC profile creation with Drop rule	To verify whether AVC profile created or not with Drop rule	Passed	
MEJ88S_Aging_17	AVC profile creation with Mark rule	To verify whether AVC profile creating or not with Mark rule	Passed	
MEJ88S_Aging_18	AVC profile creation with Rate-limit rule	To verify whether AVC profile creating or not with Rate-limit rule	Passed	

MEJ88S_Aging_19	Checking the AVC scenarios without enabling the AVC	To verify whether AVC rule are applying or not without enabling the AVC	Passed	
MEJ88S_Aging_20	Varying the Lease period after client connected to the DHCP Pool	To verify whether Client is connecting or not after DHCP Pool lease period change	Passed	
MEJ88S_Aging_21	Checking the Clients details after lease period expires	To verify whether Client is connecting or not after lease period expires also	Passed	
MEJ88S_Aging_22	Checking the RSSI values after client connect to the WLAN near to AP	To verify whether RSSI values are showing properly or not after client connected to the WLAN	Passed	
MEJ88S_Aging_23	Checking the RSSI values after client connect to the WLAN with certain range	To verify whether Client is showing the proper RSSI details or not	Passed	
MEJ88S_Aging_24	Perfoming the PING test after client connect	To verify whether PING test is performing or not after client connect	Passed	
MEJ88S_Aging_25	Capturing the TCP Packets after Client connected to WLAN	To verify whether TCP Packets are transfering or not after client connect	Passed	
MEJ88S_Aging_26	Capturing the UDP Packets after client connect to WLAN	To verify whether UDP packets are transfering or not	Passed	
MEJ88S_Aging_27	Performing the FTP operation after client connected to WLAN	To verify whether FTP operation is performing or not	Passed	
MEJ88S_Aging_28	Configuring the Radius server from UI	To verify whether Radius server is creating or not from UI	Passed	

MEJ88S_Aging_29	Configuring the Radius server from CLI	To verify whether Radisu server is creating with CLI or not	Passed	



CHAPTER 4

Regression Features - Test Summary

WLC AireOS

Private PSK

Logical ID	Title	Description	Status	Defect ID
WLJ88S_REG_01	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	
WLJ88S_REG_02	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	
WLJ88S_REG_03	Trying to connect client that identitiy 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	
WLJ88S_REG_04	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	

WLJ88S_REG_05	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	
WLJ88S_REG_06	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	
WLJ88S_REG_07	Verify that client is able to connect via private psk after forgeting the network once and try again	Checking that client is able to connect via private psk after forgeting the network once and try again	Passed	
WLJ88S_REG_08	Verify that radius fallback working with private psk or not	Checking that radius fallback is working with private psk or not	Passed	
WLJ88S_REG_09	debuging the client connection while connecting with private psk	To debug the client connection and verify the debug log while connecting with private psk	Passed	
WLJ88S_REG_10	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	

MAB Bypass Support

Logical ID	Title	Description	Status	Defect ID
WLJ88S_REG_11	JSSID client with vaild MAC address	check whether japanese client connecting or not with MAB	Passed	

WLJ88S_REG_12	Invalid MAC adress with Japanese client	verify the Japanese client is able connect or not with invalid MAB	Passed	
WLJ88S_REG_13	Connecting different OS japanese client with MAB	Check whether japanese client is able connect different OS or not with MAB	Passed	
WLJ88S_REG_14	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	
WLJ88S_REG_15	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	
WLJ88S_REG_16	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	
WLJ88S_REG_17	Configuring specifc 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	

WLJ88S_REG_18	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	
WLJ88S_REG_19	verifying japanese client maximum retries failed.	To check whether japanese client after maximum retries failed moved or not in excluded list	Passed	
WLJ88S_REG_20	Verifying that client reauthenticated after session timeout or not	Checking that after session timeout client is reauthenticated or not	Passed	
WLJ88S_REG_21	Japanese client reauthenticated after session expired	To check whether Japanese client reauthenticated or not after client session expired	Passed	
WLJ88S_REG_22	Japanese client status on monitor page	validate the japanese client details on monitor page	Passed	
WLJ88S_REG_23	JSSID client with vaild MAC address	check whether japanese client connecting or not with MAB	Passed	
WLJ88S_REG_24	Invalid MAC adress with Japanese client	verify the Japanese client is able connect or not with invalid MAB	Passed	
WLJ88S_REG_25	Connecting different OS japanese client with MAB	Check whether japanese client is able connect different OS or not with MAB	Passed	
WLJ88S_REG_26	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	

WLJ88S_REG_27	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	
WLJ88S_REG_28	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	
WLJ88S_REG_29	Configuring specifc 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	
WLJ88S_REG_30	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	
WLJ88S_REG_31	verifying japanese client maximum retries failed.	To check whether japanese client after maximum retries failed moved or not in excluded list	Passed	
WLJ88S_REG_32	Verifying that client reauthenticated after session timeout or not	Checking that after session timeout client is reauthenticated or not	Passed	
WLJ88S_REG_33	Japanese client reauthenticated after session expired	To check whether Japanese client reauthenticated or not after client session expired	Passed	

WLJ88S_REG_34	Japanese client status on monitor page	validate the japanese client details on monitor page	Passed	

Passive Client ARP Unicast

Logical ID	Title	Description	Status	Defect ID
WLJ88S_REG_52	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	
WLJ88S_REG_53	Enabling the Passive client data in 5520/8510/8540 controllers	To verify whether Passive client or sending the Unicast data from AP to client or not	Passed	
WLJ88S_REG_54	Cheking the ARP Packet with Multicast-multicast enable	To verify whether ARP packet is sending or not whether Multicast mode enabled	Passed	
WLJ88S_REG_55	Cheking the ARP packet when Multicast-unicast enable	To verify whether Packed is sending or not whether Multicast-unicast enable	Passed	
WLJ88S_REG_56	Connecting with two WLAN with different client ARP	To verify whether WLAN will support with two different ARP methods in same Interface	Passed	
WLJ88S_REG_57	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	
WLJ88S_REG_58	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	

WLJ88S_REG_59	Testing with non-Cisco WGB with wired clients	To verify whether non-cisco WGB with wired clients will connect or not	Passed	
WLJ88S_REG_60	Rebootinthe AP after Client ARP unicast enable	To verify whether WLAN showing the information correctly after reboot also	Passed	
WLJ88S_REG_61	Checking after Upgrade/Downgrade	To verify whether Client is connecting or not after Upgrade/Downgrade	Passed	
WLJ88S_REG_62	Debuging the ARPclient data	To verify whether ARP details are showing properly or not	Passed	
WLJ88S_REG_63	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
WLJ88S_REG_64	Reboot the Controller after Re-anchor enabling	To verify whether Configurations are showing same or different after controller reboot	Passed	
WLJ88S_REG_65	Downgrade/upgrade the controller with Re-anchor enable	To verify whether Downgrade/upgrade the controller with Re-anchor enable	Passed	
WLJ88S_REG_66	Checking the Windows JOS Client connectivity after enabling Selective reanchor in WLAN	To verify whether windows jos client is connecting properly or not	Passed	

WLJ88S_REG_67	Checking the android Client connectivity after enabling Selective reanchor in WLAN	To verify whether android client is connecting properly or not	Passed	
WLJ88S_REG_68	Checking the IOS Client connectivity after enabling Selective reanchor in WLAN	To verify whether IOS client is connecting properly or not	Passed	
WLJ88S_REG_69	Roaming the client between 2 controllers	To verify whether client roaming successfully between two controllers	Passed	
WLJ88S_REG_70	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
WLJ88S_REG_71	Adding the NA server	Verify that user is able to add NA server in WLC or not	Passed	
WLJ88S_REG_72	Creating the SSID and connecting the sensor mode AP	Verify that user is able to connect the sensor mode ap as a client	Passed	
WLJ88S_REG_73	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	
WLJ88S_REG_74	Verify that user is able to disabled NAC via CLI	Checking that user is able to disable NAC via CLI or not	Passed	
WLJ88S_REG_75	Verify that JSON data is sending out from WLC	Checking that JSON data is sending out from WLC to NA server or not	Passed	

WLJ88S_REG_76	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	
WLJ88S_REG_77	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	
WLJ88S_REG_78	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	
WLJ88S_REG_79	Verify that wsa server url config is syncing to standby wlc or not	Checking that wsa config syncing with standby in HA mode	Passed	
WLJ88S_REG_80	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	
WLJ88S_REG_81	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	
WLJ88S_REG_82	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	

Roaming

Logical ID	Title	Description	Status	Defect ID
WLJ88S_REG_83	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	

WLJ88S_REG_84	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	
WLJ88S_REG_85	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	
WLJ88S_REG_86	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	
WLJ88S_REG_274	L2 Security Roaming between WLANs with differenet security	To verify whether Mobility Management can be successfully configured between two controllers or not	Passed	
WLJ88S_REG_275	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	
WLJ88S_REG_276	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	

WLJ88S_REG_277	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	
WLJ88S_REG_278	Monitoring the Client details before/after Roaming	To verify whether Client details are showing properly or not in Monitoring page	Passed	
WLJ88S_REG_279	L3 Roaming between WLANs with Differenet security	To verify whether Client is Moving between Controllers with Different sercurity or not with L3 Roaming	Passed	
WLJ88S_REG_280	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	
WLJ88S_REG_281	L3 Roaming between Controllers with Differenet Radio type	To verify whether Client is Roaming between the Controllers with differenet Radio type or not	Passed	
WLJ88S_REG_282	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	
WLJ88S_REG_283	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	

WLJ88S_REG_284	debuging the Client details	To verify whether Client details are shoing or not at the time of Roaming	Passed	
WLJ88S_REG_285	Enabling the New Converged Access	To verify whether New Converged Access and Mobility parameters are enabling or not	Passed	
WLJ88S_REG_286	Roaming the Client with Different QOS details	To verify whether Client is roaming or not with different QOS details	Passed	
WLJ88S_REG_287	Roaming the Client with AVC rules	To verify whether after client Roaming the AVC rules will apply or not	Passed	
WLJ88S_REG_288	Roaming the Client with ACL rules	To verify whether after Client Roam the ACL rules are applying or not	Passed	
WLJ88S_REG_289	Roaming the Client with HA mode	To verify whether Client is connecting or not after Active controller is down	Passed	
WLJ88S_REG_290	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	
WLJ88S_REG_291	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	
WLJ88S_REG_292	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
WLJ88S_REG_87	Performing Dot1x authentication over flexconnectAP with RADIUS servers configured(Secondary)	To verify whether Dot1x authentication can be performed successfully to the clients associated via the secondary RADIUS server over the flexconnect connection with the Vlan mapped	Passed	
WLJ88S_REG_88	Performing Dot1x authentication over flexconnectAP with RADIUS servers configured(Primary failover)	To verify whether Dot1x authentication can be performed successfully to the clients associated via the secondary RADIUS server over the flexconnect connection with the Vlan mapped	Passed	
WLJ88S_REG_89	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	Passed	
WLJ88S_REG_90	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	Passed	

Dot1x and WEB-Auth Support

Logical ID	Title	Description	Status	Defect ID
WLJ88S_REG_91	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	
WLJ88S_REG_92	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	
WLJ88S_REG_93	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	
WLJ88S_REG_94	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	
WLJ88S_REG_95	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.	Passed	
WLJ88S_REG_96	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.	Passed	

WLJ88S_REG_97	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.	Passed	
WLJ88S_REG_98	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.	Passed	
WLJ88S_REG_99	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.	Passed	
WLJ88S_REG_100	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.	Passed	
WLJ88S_REG_101	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.	Passed	
WLJ88S_REG_102	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.	Passed	

WLJ88S_REG_103	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.	Passed	
WLJ88S_REG_104	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.	Passed	
WLJ88S_REG_105	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.	Passed	
WLJ88S_REG_106	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.	Passed	
WLJ88S_REG_107	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.	Passed	
WLJ88S_REG_108	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.	Passed	

WLJ88S_REG_109	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.	Passed	
WLJ88S_REG_110	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.	Passed	

Autonomous AP

Logical ID	Title	Description	Status	Defect ID
WLJ88S_REG_111	Client association with no security	To check whether clients gets associated or not Autonomous AP with Open security.	Passed	
WLJ88S_REG_112	Client association with WEP security	To check whether clients gets associated or not Autonomous AP with WEP security.	Passed	
WLJ88S_REG_113	Client association with WPA2+PSK	To check whether clients gets associated or not Autonomous AP with WPA2+PSK security.	Passed	
WLJ88S_REG_114	Client association with 802.11x	To check whether clients gets associated or not Autonomous AP with 802.11x security.	Passed	
WLJ88S_REG_115	Checking the traffic flow between two wireless clients	To Traffic flow between two wireless clients	Passed	

WLJ88S_REG_116	Checking the Trap logs for connected client	To verify the Trap Logs for connected client	Passed	

Flex Video streaming

Logical ID	Title	Description	Status	Defect ID
WLJ88S_REG_117	MC2UC traffic to local-switching client	To verify that the local-switching client subscribed to videostreaming receives MC2UC traffic	Passed	
WLJ88S_REG_118	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	
WLJ88S_REG_119	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	
WLJ88S_REG_120	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	
WLJ88S_REG_121	Client disassociates when receiving MC2UC traffic	To verify whether AP stops sending traffic when client disassociates	Passed	
WLJ88S_REG_122	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	

WLJ88S_REG_123	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	
WLJ88S_REG_124	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	
WLJ88S_REG_125	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	
WLJ88S_REG_126	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	
WLJ88S_REG_127	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	
WLJ88S_REG_128	LS client with MC2UC enabled receiving traffic after switchover in HA pair	To verify whether LS client with MC2UC enabled receives unicast traffic after switchover	Passed	

Hyperlocation Module supports for AP 3702

Logical ID	Title	Description	Status	Defect ID

WLJ88S_REG_129	Importing maps to CMX through Japanese PI	To check whether the maps can be imported in CMX from PI	Passed	
WLJ88S_REG_130	Sync the WLC in to CMX	To check whether the WLC and CMX gets synced up	Passed	
WLJ88S_REG_131	Tracking the Window,iPhone client devices in CMX	To check the tracking of Window ,iphone devices using CMX	Passed	
WLJ88S_REG_132	Android,iOS Client Locate in CMX	To verify the Location of the clients	Passed	
WLJ88S_REG_133	Location Accuracy Test in CMX of Window client	To verify the location accuracy of the clients	Passed	
WLJ88S_REG_134	History of client location(Client Playback)	To verify the client location history	Passed	

Domain Based URL ACL

Logical ID	Title	Description	Status	Defect ID
WLJ88S_REG_135	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	
WLJ88S_REG_136	Add new URL domain on created url acl	To verify that new URL domain (www.cisco.com,www.yahoo.com) added or not	Passed	
WLJ88S_REG_137	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	

WLJ88S_REG_138	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	
WLJ88S_REG_139	Delete URL ACL rule after applied	To verify that URL ACL rule delete succesfully or not	Passed	
WLJ88S_REG_140	Modified rule of URL ACL and connect Android client	To verify that rule action modified or not and Android client connectivity	Passed	
WLJ88S_REG_141	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	
WLJ88S_REG_142	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
WLJ88S_REG_143	Config Mesh setup and apply config on Mesh Aps	To verify that Mesh setup configured and ATF applied on Mesh Aps	Passed	
WLJ88S_REG_144	Apply ATF Enforcement mode on MESH AP	To verify that ATF Enforcement mode applied on MESH AP or not	Passed	
WLJ88S_REG_145	Apply ATF policy on wlan and connect Android client	To verify that policy applied on WLAN or not and client connected succesfully	Passed	
WLJ88S_REG_146	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	

WLJ88S_REG_147	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	
WLJ88S_REG_148	Mac OS client connectivity with l2 security WLAN which having different Policy weight	To verify the client connectivity with two SSID having different weight	Passed	
WLJ88S_REG_149	Apply ATF Enforcement mode on AP group	To verify that ATF Enforcement mode applied on AP group or not	Passed	
WLJ88S_REG_150	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	
WLJ88S_REG_151	Monitoring ATF statistics after atf allocation on universal client access radio	To verify the ATF statstics after allocation on universal client access radio is showing properly or not	Passed	
WLJ88S_REG_152	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	
WLJ88S_REG_153	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	
WLJ88S_REG_154	Monitoring the ATF statistics of client using CLI	To verify that ATF statistics of client is showing properly in CLI	Passed	
WLJ88S_REG_155	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
WLJ88S_REG_156	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	
WLJ88S_REG_157	Active controller ports status when it is in Link Aggregation (LAG) failover	To check active controller ports status in Link Aggregation failover	Passed	
WLJ88S_REG_158	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	
WLJ88S_REG_159	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	
WLJ88S_REG_160	Checking the enhanced warnings for LAT state config changes	To check whether the warning are raised when the user reverts the LAG state	Passed	
WLJ88S_REG_161	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	
WLJ88S_REG_162	configure the port channel on the neighbor switch to support LAG	validate the port channel on the neighbor switch to support LAG.	Passed	

WLJ88S_REG_163	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
WLJ88S_REG_164	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	
WLJ88S_REG_165	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	
WLJ88S_REG_166	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	
WLJ88S_REG_167	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	
WLJ88S_REG_168	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	

WLJ88S_REG_169	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	
WLJ88S_REG_170	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	
WLJ88S_REG_171	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	
WLJ88S_REG_172	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	
WLJ88S_REG_173	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	
WLJ88S_REG_174	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	
WLJ88S_REG_175	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	

WLJ88S_REG_176	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	
WLJ88S_REG_177	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	

TrustSec Enhancements

Logical ID	Title	Description	Status	Defect ID
WLJ88S_REG_178	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	
WLJ88S_REG_179	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	
WLJ88S_REG_180	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	

WLJ88S_REG_181	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	
WLJ88S_REG_182	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	
WLJ88S_REG_183	Performing Inter controller roaming of Windows client in TrustSec enabled WLC's with WPA2-dot1x security.	To check whether inter controller roaming of windows clients works properly or not between WLC's with WPA2-dot1xsecurity.	Passed	
WLJ88S_REG_184	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	
WLJ88S_REG_185	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	
WLJ88S_REG_186	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	

WLJ88S_REG_187	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	
WLJ88S_REG_188	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
WLJ88S_REG_189	Redirection to Facebook Page	To verify redirection to facebook page for logging in is successful or not	Passed	
WLJ88S_REG_190	Restricting free internet access for unauthenticated Windows client	To verify denial of internet access for unauthenticated Windows users is successful or not	Passed	
WLJ88S_REG_191	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	
WLJ88S_REG_192	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	
WLJ88S_REG_193	Show Logs tab	To Verify successful download of each individual log file listed in the show logs tab	Passed	

WLJ88S_REG_194	User data statistics	To verify whether the user's data statistics are displayed correctly or not	Passed	
WLJ88S_REG_195	KNOWN Users	To verify whether authenticated users are listed in the user data tab or not	Passed	
WLJ88S_REG_196	UNKNOWN Users	To verify whether users not authenticated are listed in the user data tab or not	Passed	
WLJ88S_REG_197	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
WLJ88S_REG_198	Access points in the Floor map	To verify whether client devices are displayed in the floor map or not	Passed	
WLJ88S_REG_199	Wireless Laptop Client Location in Floor map	To verify whether laptop client devices are displayed in the floor map or not	Passed	
WLJ88S_REG_200	Wireless mobile Client Location in Floor map	To verify whether mobile client devices are displayed in the floor map or not	Passed	
WLJ88S_REG_201	Search client by MAC address	To verify whether client device can be searched by specifying its MAC address or not	Passed	
WLJ88S_REG_202	Search client by IP	To verify whether client device can be searched by specifying its IP address or not	Passed	

WLJ88S_REG_203	Search client by SSID	To verify whether client device can be searched by specifying the SSID or not	Passed	
WLJ88S_REG_204	Interferers in Floor map	To verify whether interferers are displayed in the floor map or not	Passed	
WLJ88S_REG_205	Rogue Devices in Floor map	To verify whether rogues are displayed in the floor map or not	Passed	
WLJ88S_REG_206	Client movement history playback	To verify whether client's movement history is shown or not	Passed	
WLJ88S_REG_207	Creating New Report	To verify whether new report can be created or not	Passed	

Internal DHCP Server

Logical ID	Title	Description	Status	Defect ID
WLJ88S_REG_208	Assigning the Internal DHCP server to WLAN	To verify whether Internal DHCP server assigend successfully to WLAN or not	Passed	
WLJ88S_REG_209	configure the internal DHCP server to JSSID WLAN	To check Internal DHCP server assigned successfully or not to JSSID WLAN	Passed	
WLJ88S_REG_210	Disabling the DHCP Proxy server	To verify whether without DHCP proxy server enable client will get IP address or not	Passed	
WLJ88S_REG_211	Configuring the DHCP option 82 with binary format	To verify whether DHCP option 82 configured client is showing binary format or not	Passed	

WLJ88S_REG_212	Configuring the DHCP option 82 with ascii format	To verify whether DHCP option 82 configured client is showing ASCII format or not	Passed	
WLJ88S_REG_213	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	
WLJ88S_REG_214	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	
WLJ88S_REG_215	DHCP option 82 with AP-Group-Name & Flex-Group-Name format	To verify whether AP-Group-Nmae & Flex-Group-Name details are showing or not at the time of debug	Passed	
WLJ88S_REG_216	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	
WLJ88S_REG_217	Configuring the DHCP with maximum & minimum timeout	To verify whether DHCP maximum & minimum values are configured successfully	Passed	

Monitor Mode support in APs(1810/1815)

Logical ID	Title	Description	Status	Defect ID
WLJ88S_REG_218	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	

WLJ88S_REG_219	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	
WLJ88S_REG_220	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	
WLJ88S_REG_221	Detecting the interfering devices via 5GHZ band	Verifying that AP 1815/1810 able to detect interfering device via 5GHZ band or not	Passed	
WLJ88S_REG_222	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	
WLJ88S_REG_223	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	
WLJ88S_REG_224	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	
WLJ88S_REG_225	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	

WLJ88S_REG_226	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	
WLJ88S_REG_227	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
WLJ88S_REG_228	Roaming the Windows JOS clients between 5520/8540 WLC's after enabling New mobility converged access	To check whether Windows JOS clients gets roamed successfully or not between 5520 & 8540 WLC's after enabling New mobility converged access	Passed	
WLJ88S_REG_229	Roaming the Apple iOS clients between 5520\8540 WLC's after enabling New mobility converged access	To check whether Apple iOS clients gets roamed successfully or not between 5520 & 8540 WLC's after enabling New mobility converged access	Passed	
WLJ88S_REG_230	Roaming the MAC OS clients between 5520\8540 WLC's after enabling New mobility converged access	To check whether MAC OS clients gets roamed successfully or not between 5520 & 8540 WLC's after enabling New mobility converged access	Passed	

WLJ88S_REG_231	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	
WLJ88S_REG_232	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	
WLJ88S_REG_233	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	
WLJ88S_REG_234	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	
WLJ88S_REG_235	Roaming the Android clients between 3504\8540 WLC's after enabling New mobility converged access	To check whether Android clients gets roamed successfully or not between 3504 & 8540 WLC's after enabling New mobility converged access	Passed	

WLJ88S_REG_236	Configuring Multicast IP in mobility groups and checking the roaming of Windows JOS clients	To check whether Windows JOS clients gets roamed successfully or not between WLC's with multicast IP configured in mobility groups	Passed	
WLJ88S_REG_237	Configuring Multicast IP in mobility groups and checking the roaming of Apple iOS clients	To check whether Apple iOS clients gets roamed successfully or not between WLC's with multicast IP configured in mobility groups	Passed	
WLJ88S_REG_238	Configuring Multicast IP in mobility groups and checking the roaming of MAC OS clients	To check whether MAC OS clients gets roamed successfully or not between WLC's with multicast IP configured in mobility groups	Passed	
WLJ88S_REG_239	Configuring Multicast IP in mobility groups and checking the roaming of Android clients	To check whether Android clients gets roamed successfully or not between WLC's with multicast IP configured in mobility groups	Passed	
WLJ88S_REG_240	Checking the configuration of mobility converged access after upload/download the config file via TFTP	To check whether mobility converged access configurations gets retained or not after upload/download the config file via TFTP in all WLC's	Passed	
WLJ88S_REG_241	Enabling mobility converged access for WLC from PI	To check whether mobility converged access can be configured or not from PI for 5520/8540/3504 WLC's.	Passed	

HA WLC Auth/Authz

Logical ID	Title	Description	Status	Defect ID
WLJ88S_REG_242	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	
WLJ88S_REG_243	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	
WLJ88S_REG_244	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	
WLJ88S_REG_245	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	
WLJ88S_REG_246	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	

WLJ88S_REG_247	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	
WLJ88S_REG_248	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	
WLJ88S_REG_249	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	
WLJ88S_REG_250	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

WLJ88S_REG_251	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	
WLJ88S_REG_252	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	
WLJ88S_REG_253	Enable/disable the DHCP Proxy through CLI	To verify whether DHCP proxy server enable/disable through CLI or not	Passed	
WLJ88S_REG_254	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	
WLJ88S_REG_255	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	
WLJ88S_REG_256	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	
WLJ88S_REG_257	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	
WLJ88S_REG_258	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	

WLJ88S_REG_259	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	
WLJ88S_REG_260	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	
WLJ88S_REG_261	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	
WLJ88S_REG_262	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	
WLJ88S_REG_263	Configuring the DHCP option 82 through PI	To verify whether DHCP option 82 is enabling through PI or not	Passed	

Client Auth Failures(AAA Failures/WLC Failures)

Logical ID	Title	Description	Status	Defect ID
WLJ88S_REG_264	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	
WLJ88S_REG_265	Applying access control list to the WLAN and check if the ACL rule works to deny the client .	To check whether the ACL apllied to WLAN works and check if the client get denied or not.	Passed	

WLJ88S_REG_266	Configuring maxium allowed clients for the WLAN and check if the specified clients alone gets connected	To connect a specified number of clients to a specific WLAN and check if client more than the specified value does not authenticated or not	Passed	
WLJ88S_REG_267	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	
WLJ88S_REG_268	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	
WLJ88S_REG_269	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	
WLJ88S_REG_270	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	

WLJ88S_REG_271	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	
WLJ88S_REG_272	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	
WLJ88S_REG_273	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	

Roaming

Logical ID	Title	Description	Status	Defect ID
WLJ88S_REG_83	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	
WLJ88S_REG_84	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	

WLJ88S_REG_85	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	
WLJ88S_REG_86	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	
WLJ88S_REG_274	L2 Security Roaming between WLANs with differenet security	To verify whether Mobility Management can be successfully configured between two controllers or not	Passed	
WLJ88S_REG_275	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	
WLJ88S_REG_276	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	
WLJ88S_REG_277	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	
WLJ88S_REG_278	Monitoring the Client details before/after Roaming	To verify whether Client details are showing properly or not in Monitoring page	Passed	

WLJ88S_REG_279	L3 Roaming between WLANs with Differenet security	To verify whether Client is Moving between Controllers with Different sercurity or not with L3 Roaming	Passed	
WLJ88S_REG_280	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	
WLJ88S_REG_281	L3 Roaming between Controllers with Differenet Radio type	To verify whether Client is Roaming between the Controllers with differenet Radio type or not	Passed	
WLJ88S_REG_282	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	
WLJ88S_REG_283	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	
WLJ88S_REG_284	debuging the Client details	To verify whether Client details are shoing or not at the time of Roaming	Passed	
WLJ88S_REG_285	Enabling the New Converged Access	To verify whether New Converged Access and Mobility parameters are enabling or not	Passed	

WLJ88S_REG_286	Roaming the Client with Different QOS details	To verify whether Client is roaming or not with different QOS details	Passed	
WLJ88S_REG_287	Roaming the Client with AVC rules	To verify whether after client Roaming the AVC rules will apply or not	Passed	
WLJ88S_REG_288	Roaming the Client with ACL rules	To verify whether after Client Roam the ACL rules are applying or not	Passed	
WLJ88S_REG_289	Roaming the Client with HA mode	To verify whether Client is connecting or not after Active controller is down	Passed	
WLJ88S_REG_290	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	
WLJ88S_REG_291	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	
WLJ88S_REG_292	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

WLJ88S_REG_293	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	
WLJ88S_REG_294	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	
WLJ88S_REG_295	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	
WLJ88S_REG_296	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	
WLJ88S_REG_297	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	
WLJ88S_REG_298	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	

WLJ88S_REG_299	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	
WLJ88S_REG_300	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	

Flexconnect IOS Parity: Ethernet fallback

Logical ID	Title	Description	Status	Defect ID
WLJ88S_REG_301	Enable/Disable Ethernet fall-back in WLC UI	To verify whether Ethernet fall-back is enable/disable successfully or not from WLC UI	Passed	
WLJ88S_REG_302	Enable/Disable Ethernet fall-back in WLC CLI	To verify whether Ethernet fall-back is enable/disable successfully or not from WLC CLI	Passed	
WLJ88S_REG_303	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	
WLJ88S_REG_304	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	
WLJ88S_REG_305	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	

WLJ88S_REG_306	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	
WLJ88S_REG_307	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	
WLJ88S_REG_308	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	
WLJ88S_REG_309	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	
WLJ88S_REG_310	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	
WLJ88S_REG_311	Verifying the fall back details from CLI for read only	To verify whether Ethernet fall-back details are showing or not	Passed	
WLJ88S_REG_312	Reloading the AP after Ethernet fall-back configuring	To verify whether Ethernet fall-back details are showing properly or not after reload	Passed	
WLJ88S_REG_313	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	
WLJ88S_REG_314	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
WLJ88S_REG_315	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	
WLJ88S_REG_316	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	
WLJ88S_REG_317	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	
WLJ88S_REG_318	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	
WLJ88S_REG_319	Reseting the WLC after configure the Client and SSID values	To verify whether Client and SSID values are proper or not	Passed	
WLJ88S_REG_320	Clearing the values after AAA override enable	To verify whether values are clearing or not	Passed	
WLJ88S_REG_321	Checking the roaming scenario	To verify whether after client roam between controllers client accessing proper bandwidth or not	Passed	

WLJ88S_REG_322	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
WLJ88S_REG_323	Creating the VLAN Template	To verify whether VLAN Template is creating or not	Passed	
WLJ88S_REG_324	Assigning the flexconnect VLAN to Flexconnect group	To verify whether VLAN Template is assigning successfully or not to Flexconnect group	Passed	
WLJ88S_REG_325	Checking the AAA override for VLAN name id	To verify whether AAA overriding happening or not with VLAN name	Passed	
WLJ88S_REG_326	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	
WLJ88S_REG_327	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	
WLJ88S_REG_328	Checking the details in AP after VLAN name id Exchage	To verify details are showing in AP cli or not	Passed	
WLJ88S_REG_329	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	

WLJ88S_REG_330	Rebooting the WLC after AAA overide with VLAN name ID	To verify whether Client are getting AAA override details or not after reboot	Passed	
WLJ88S_REG_331	Checking the client details at the time of standalone mode	To verify whether clients are serving or not in standalone mode	Passed	
WLJ88S_REG_332	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
WLJ88S_REG_333	Configuring the DHCP Option 60 in router	To verify whether DHCP Option 60 is configuring successfully or not	Passed	
WLJ88S_REG_334	Checking DHCP option 63 is matching with AP	To verify whether DHCP Option 60 details are matching with AP or not	Passed	
WLJ88S_REG_335	Connecting the andriod client without adding VCI	To verify whether android is getting the IP address or not	Passed	
WLJ88S_REG_336	Connecting the IOS client without adding VCI	To verify whether IOS client is getting the IP address or not	Passed	
WLJ88S_REG_337	Connecting the Japanese client without adding VCI	To verify whether Japanese is getting the IP address or not	Passed	

High Availability & Monitoring HA

Logical ID	Title	Description	Status	Defect ID

WLJ88S_REG_338	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	
WLJ88S_REG_339	Controller HA pair with different hardware models (3504 and 8540)	To verify the role negotiation between the controllers with different hardware models	Passed	
WLJ88S_REG_340	Verifying the serial number of the standby controller	To check whether the serial number of the standby controller is getting or not	Passed	
WLJ88S_REG_341	Verifying the FAN status of the standby controller	To verify whether the FAN status of the standby controller is getting or not	Passed	
WLJ88S_REG_342	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	
WLJ88S_REG_343	Configuring controller HA pair with different software versions	To verify whether controllers HA pair with different software versions	Passed	
WLJ88S_REG_344	Checking the controller mode when the redundancy port loses connectivity	To verify the HA pair controller mode after disconnecting the redundancy port	Passed	
WLJ88S_REG_345	Checking the controller modes(HA pair) after power failure	To verify the controller modes after power failure on both the controllers	Passed	
WLJ88S_REG_346	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	

WLJ88S_REG_347	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	
WLJ88S_REG_348	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	
WLJ88S_REG_349	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	
WLJ88S_REG_350	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	
WLJ88S_REG_351	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	

Limit clients per Radio

Logical ID	Title	Description	Status	Defect ID
WLJ88S_REG_352	Confiuring maximum Allowed Clients Per AP Radio with radio policy as 2.4 GHz and connecting client with different security policy.	To configure maxium allowed client Per AP radio with radio policy as 2.4GHz and connecting a client.	Passed	

WLJ88S_REG_353	Confiuring maximum Allowed Clients Per AP Radio with radio policy as 5 GHz and connecting client with different security policy.	To configure maxium allowed client Per AP radio with radio policy as 5 GHz and connecting a client.	Passed	
WLJ88S_REG_354	Confiuring 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	
WLJ88S_REG_355	Confiuring 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	
WLJ88S_REG_356	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	
WLJ88S_REG_357	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	

WLJ88S_REG_358	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	
WLJ88S_REG_359	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	
WLJ88S_REG_360	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	
WLJ88S_REG_361	Configuring maximum allowed client Per AP radio as 5 GHz with local switcing 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	
WLJ88S_REG_362	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	

WLJ88S_REG_363	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	
WLJ88S_REG_364	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	
WLJ88S_REG_365	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	
WLJ88S_REG_366	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	

WLJ88S_REG_367	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	
WLJ88S_REG_368	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	

MFP support

Logical ID	Title	Description	Status	Defect ID
WLJ88S_REG_369	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	
WLJ88S_REG_370	Checking if IMIC IE value in MFP is appended in 3800 AP	To check if the IMIC IE value in MFP is appeneded in 3800 AP or not after enabling MFP globally.	Passed	
WLJ88S_REG_371	Checking if IMIC IE value in MFP is appended in 2800 AP	To check if the IMIC IE value in MFP is appeneded in 2800 AP or not after enabling MFP globally.	Passed	

WLJ88S_REG_372	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	
WLJ88S_REG_373	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	
WLJ88S_REG_374	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	
WLJ88S_REG_375	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	
WLJ88S_REG_376	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	
WLJ88S_REG_377	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	

IPv4 DNS Filtering for BYOD

Logical ID	Title	Description	Status	Defect ID
WLJ88S_REG_388	Connecting Android client with single ssid BYOD network	Verify that Android client is getting connected or not with single SSID	Passed	
WLJ88S_REG_389	Connecting ios client with single ssid BYOD network	Verify that IOS client is getting connected or not with single SSID	Passed	
WLJ88S_REG_390	Connecting windows client with single ssid BYOD network	Verify that windows client is getting connected or not with single SSID	Passed	
WLJ88S_REG_391	Connecting android client with dual ssid BYOD network	Verify that android client is getting connected or not with dual SSID	Passed	
WLJ88S_REG_392	Connecting ios client with dual ssid BYOD network	Verify that IOS client is getting connected or not with dual SSID	Passed	
WLJ88S_REG_393	Connecting windows client with dual ssid BYOD network	Verify that windows client is getting connected or not with dual SSID	Passed	
WLJ88S_REG_394	Debugging the BYOD client connection	Verify that user is able to take debug the BYOD Client or not	Passed	
WLJ88S_REG_395	Connecting JOS client with single ssid BYOD network	Verify that JOS client is connected with single ssid BYOD network or not	Passed	
WLJ88S_REG_396	Connecting JOS client with dual ssid BYOD network	Verify that JOS client is connected with dual ssid BYOD network or not	Passed	
WLJ88S_REG_397	Configuring the maximum URL ACL via GUI/CLI/PI	Verify that user is able to configure maximum url acl or not	Passed	

Aging Cases

Logical ID	Title	Description	Status	Defect ID
WLJ88S_REG_398	Connecting a JOS client to a 1815I AP and enable debug log and check RSSI value for the client for 2 to 3 hours.	To connect JOS client to 1815I and check the debug log for the client and check the RSSI value for 2 to 3 hours.	Passed	
WLJ88S_REG_399	Connecting a Window client to a 1815I AP and enable debug log and check RSSI value for the client for 2 to 3 hours.	To connect Window client to 1815I and check the debug log for the client and check the RSSI value for 2 to 3 hours.	Passed	
WLJ88S_REG_400	Connecting a Android client to a 1815I AP and enable debug log and check RSSI value for the client for 2 to 3 hours.	To connect Android client to 1815I and check the debug log for the client and check the RSSI value for 2 to 3 hours.	Passed	
WLJ88S_REG_401	Connecting a IOS client to a 1815I AP and enable debug log and check RSSI value for the client for 2 to 3 hours.	To connect IOS client to 1815I and check the debug log for the client and check the RSSI value for 2 to 3 hours.	Passed	
WLJ88S_REG_402	Connecting a MAC OS client to a 1815I AP and enable debug log and check RSSI value for the client for 2 to 3 hours.	To connect MAC OS client to 1815I and check the debug log for the client and check the RSSI value for 2 to 3 hours.	Passed	
WLJ88S_REG_403	Checking the JOS Client details when the client is connected to 2802/3802 AP and check the Average rate for the client for more than 2 hours	To check the JOS Client details when the client is connected to 2802/3802 AP and check the Average rate for the client for more than 2 hours	Passed	

WLJ88S_REG_404	Checking the Android Client details when the client is connected to 2802/3802 AP and check the Average rate for the client for more than 2 hours	To check the Android Client details when the client is connected to 2802/3802 AP and check the Average rate for the client for more than 2 hours	Passed	
WLJ88S_REG_405	Checking the Window Client details when the client is connected to 2802/3802 AP and check the Average rate for the client for more than 2 hours	To check the Window Client details when the client is connected to 2802/3802 AP and check the Average rate for the client for more than 2 hours	Passed	
WLJ88S_REG_406	Checking the IOS Client details when the client is connected to 2802/3802 AP and check the Average rate for the client for more than 2 hours	To check the IOS Client details when the client is connected to 2802/3802 AP and check the Average rate for the client for more than 2 hours	Passed	
WLJ88S_REG_407	Checking the Air Quality data for different AP with JOS client and check the health of the AP in a regular interval.	To check the Air quality data for different AP with JOS client and check the health of the particular AP in a regular interval	Passed	

Config Wireless

Logical ID	Title	Description	Status	Defect ID
WLJ88S_config_01	Checking Multicast group client details can be filtered in Monitor page	Verfying Multicast group details can be filtered in Monitor Page	Passed	
WLJ88S_config_02	Configuring Monitor mode for AP 1542	Checking 1542 AP can be configured with Monitor mode	Failed	CSCvj74163

WLJ88S_config_03	Changing IOS AP to sensor mode from AP CLI without WSA configured in WLC	Verfying AP mode can be changed to sensor without WSA	Failed	CSCvj93292
WLJ88S_config_04	Checking URL-ACL client details in AP CLI using command "show flex client url-acl" output	Checking the output of "show flex client url-acl" in AP CLI	Failed	CSCvk23585
WLJ88S_config_05	Configuring OEAP ACL from CLI	Verfying controller is crashing or not by configuring OEAP ACL	Failed	CSCvk26217
WLJ88S_config_06	Creating OEAP ACL rule with invalid subnet mask.	To Verify OEAP ACL rule can be created with invalid mask or not	Failed	CSCvk26409
WLJ88S_config_07	Configuring TGW list with TACACS controller user in WLC UI	Verfying TGW can be configured with TACACS controller user	Failed	CSCvk52187

SR Cases

Logical ID	Title	Description	Status	Defect ID
WLJ88S_SR_01	Associating IP phones from one AP to another between 2 WLC's with Local Switching	To check whether IP phones gets associated successfully or not to one AP from another with locally switching enabled WLAN between 2 WLC's	Passed	

WLJ88S_SR_02	Associating IP phones from one AP to another between 2 WLC's with Central Switching	To check whether IP phones gets associated successfully or not to one AP from another with central switching enabled WLAN between 2 WLC's	Passed	
WLJ88S_SR_03	Checking the association of IP phones when AP moves to Standalone mode	To check whether IP phones gets associated successfully or not to AP when it moves to Standalone from Connected	Passed	
WLJ88S_SR_04	Checking the association of windows clients when AP moves to Standalone mode	To check whether windows clients gets associated successfully or not to AP when it moves to Standalone from Connected	Passed	
WLJ88S_SR_05	Checking the association of Mac OS clients when AP moves to Standalone mode	To check whether Mac OS clients gets associated successfully or not to AP when it moves to Standalone from Connected	Passed	
WLJ88S_SR_06	Checking the association of android clients when AP moves to Standalone mode	To check whether android clients gets associated successfully or not to AP when it moves to Standalone from Connected	Passed	

WLJ88S_SR_07	Checking the association of iOS clients when AP moves to Standalone mode	To check whether iOS clients gets associated successfully or not to AP when it moves to Standalone from Connected	Passed	
WLJ88S_SR_08	Checking the association of eogre clients when AP moves to Standalone mode	To check whether eogre clients gets associated successfully or not to AP when it moves to Standalone from Connected	Passed	
WLJ88S_SR_09	Monitoring the memory utilization of CMX by adding multiple WLC's	To check whether memory utilization goes up or not in CMX while adding many WLC's in it	Passed	
WLJ88S_SR_10	Checking the channel utilization of IOS APs in WLC CLI/UI	To check whether channel utilization displayed or not for IOS AP's after associating multiple OS clients in WLC	Passed	
WLJ88S_SR_11	Checking the channel utilization of COS APs in WLC CLI/UI	To check whether channel utilization displayed or not for COS AP's after associating multiple OS clients in WLC	Passed	
WLJ88S_SR_12	Checking the channel utilization of IOS APs in ME CLI/UI	To check whether channel utilization displayed or not for IOS AP's after associating multiple OS clients in ME	Passed	
WLJ88S_SR_13	Checking the channel utilization of COS APs in ME CLI/UI	To check whether channel utilization displayed or not for COS AP's after associating multiple OS clients in ME	Passed	

WLJ88S_SR_14	Verifying the AP failover functionality between same model WLC's having same version and same Flexgroup name	To check whether flex AP join to same flex group or not when WLC have the same Image and platform/model	Passed	
WLJ88S_SR_15	Verifying the AP failover functionality between different model WLC's having same version and same Flexgroup name	To check whether flex AP join to same flex group or not when WLC have the same Image and different platform/model	Passed	
WLJ88S_SR_16	Verifying the AP failover functionality between same model WLC's having different version and same Flexgroup name	To check whether flex AP join to same flex group or not when WLC have the different Image and same model	Passed	
WLJ88S_SR_17	Verifying the AP failover functionality between different model WLC's having same version and same Flexgroup name	To check whether flex AP join to same flex group or not when WLC have the different Image and different model	Passed	
WLJ88S_SR_18	Verifying the AP failover functionality between the WLC having different AP group	To verify the selection of flexconnect group when flex AP moves from Controller A to B.	Passed	
WLJ88S_SR_19	Verifying Addition of Flex AP to flexgroup containing spaces in its Name	To verify whether the AP added successfully or not to flexconnect group having spaces in name	Passed	
WLJ88S_SR_20	Verifying syncing of CMX to WLC	To check whether CMX successfully got sync with WLC or not	Passed	

WLJ88S_SR_21	Verifying syncing of CMX to WLC after rebooting of WLC	To check whether CMX successfully got sync with WLC or not after rebooting of WLC	Passed	
WLJ88S_SR_22	Verifying Rx Sop configuration at RF profile level with 2.4 GHZ with Client Connectivity with Wave2 AP(2802)	To verify whether the clients got connected or not when Rx sop has been enabled at RF profile level	Passed	
WLJ88S_SR_23	Verifying Rx Sop configuration at AP group with 5 GHZ with Client Connectivity with Wave2 AP(3802)	To verify whether the clients got connected or not when Rx sop has been enabled at AP group level	Passed	
WLJ88S_SR_24	Verifying Rx Sop configuration at RF profile level with 2.4 GHZ and 5 GHZ Client Connectivity with Wave2 AP(1852)	To verify whether the clients got connected or not when Rx sop has been enabled at AP level	Passed	
WLJ88S_SR_25	Check the client count per AP after associated/diassociated window client	To verify that client count showing as expected when client associated/diassocited	Passed	
WLJ88S_SR_26	Check the client count per SSID after associated/diassociated Android client	To verify that client count showing as expected when client associated/diassocited	Passed	
WLJ88S_SR_27	Check the client count per SSID with Lauer 3 security	To verify that client count showing as expected when client associated/diassocited with l3 web auth security	Passed	
WLJ88S_SR_28	Add and edit mac address of iOS client in Identify unknown user list	To add and edit ios client mac address in Identify unknown user list	Passed	

WLJ88S_SR_29	Remove added multiple entry in Identify Unkown Users	To verify that multiple entry able to delete or not in Identify Unkown Users	Passed	
WLJ88S_SR_30	Add partial match mac address of window client and connect same client	To verify that username is showing or not after connecting client with partial match mac address in Identify unknown user	Passed	
WLJ88S_SR_31	Config/edit/delete WLAN template in PI and push in WLC	To verify that WLAN template able to config/edit/delete in PI and push in WLC	Passed	
WLJ88S_SR_32	Config/delete Mac filtering tempalte and deploy in WLC	To verify that Mac filtering Template able to config/delete or not	Passed	
WLJ88S_SR_33	Continous ping test to 1815 ME	To verify that continous ping from wired and Wireless to ME AP	Passed	
WLJ88S_SR_34	Continous ping test to 1542 AP	To verify that continous ping from wired and Wireless to 1542 AP	Passed	
WLJ88S_SR_35	Create AP group with max character in primary controller and check that it synced to standby controller or not	To verify that AP group config got synced in standby Controller	Passed	
WLJ88S_SR_36	Config ATF in primary Controller and check config in StandBy Controller	To verfiy that ATF configuration got synced in Standby Controller	Passed	
WLJ88S_SR_37	Upgrade/Downgrade iOS AP and check that its going to boot mode or not	To verify that after upgrading/downgrading iOS AP going to boot mode or not	Passed	

WLJ88S_SR_38	Upgrade/Downgrade COS AP and check that its going to boot mode or not	To verify that after upgrading/downgrading COS AP going to boot mode or not	Passed	
WLJ88S_SR_39	Down/UP the switch connectivity while downloading image from WLC	To verify that AP going in to boot mode or not after down/UP the switch connectivity	Passed	
WLJ88S_SR_40	checking 2.4 GHZ rf-profiles are syncing in HA	veryfing 2.4 GHZ rf-profiles are displaying propoerly in stand by controller	Passed	
WLJ88S_SR_41	checking 5 GHZ rf-profiles are syncing in HA	veryfing 5 GHZ rf-profiles are displaying propoerly in stand by controller	Passed	
WLJ88S_SR_42	checking rf-profile config in config file	verfying rf-profile config is same in both primary and standBy	Passed	
WLJ88S_SR_43	checking rfprofile config in AP group	Verfying rfprofile in AP group for client	Passed	
WLJ88S_SR_44	Checking vlan mode for 3702 AP after upgrading the wlc	Verfying vlan mode is enabled or not after upgrading WLC	Passed	
WLJ88S_SR_45	Checking vlan mode for 1542 AP after Downgrading the wlc	Verfying vlan mode is enabled or not after downgrading WLC	Passed	
WLJ88S_SR_46	Checking 1815 AP can able to join to controller after enabling VLAN tagging	Verfying 1815 AP is joining to controller with VLAN tagging	Passed	
WLJ88S_SR_47	Checking 1542 AP can able to join to controller after enabling VLAN tagging	Verfying 1542 AP is joining to controller with VLAN tagging	Passed	

WLJ88S_SR_48	Checking 2800 AP can able to join different controller after enabling VLAN tagging	Verfying 2800 AP is joining to controller with VLAN tagging	Passed	
WLJ88S_SR_49	Checking 3702 AP can able to join different controller after enabling VLAN tagging	Verfying 3700 AP is joining to controller with VLAN tagging	Passed	
WLJ88S_SR_50	Checking any duplex mismatch error in 9300 switch when connecting 2800 AP	Verifying any duplex mismatch error is generating in switch when connecting 2800AP	Passed	
WLJ88S_SR_51	Checking any duplex mismatch error in 3650 switch when connecting 1852 AP after changing port to full duplex	Verifying any duplex mismatch error is generating in switch when connecting 1852AP after changing port to ful duplex	Passed	
WLJ88S_SR_52	Checking any duplex mismatch error in 3650 switch when connecting 1702AP after changing port to full duplex	Verifying any duplex mismatch error is generating in switch when connecting 1702AP after changing port to ful duplex	Passed	
WLJ88S_SR_53	Checking 2702 AP state when max clients reached for WLAN	Verify 2702 AP state when max clients reached for WLAN	Passed	
WLJ88S_SR_54	Checking 1852 AP state when max clients reached for WLAN in ME	Verify 1852 AP state when max clients reached for WLAN in ME	Passed	
WLJ88S_SR_55	Checking 1810 AP state when max clients reached for WLAN in ME	Verify 1810 AP state when max clients reached for WLAN in ME	Passed	
WLJ88S_SR_56	Creating rsync user as management user in WLC	Verify rsync user is creating as management user or not in WLC	Passed	

WLJ88S_SR_57	Creating rsync user as management user in ME	Verify rsync user is creating as management user or not in ME	Passed	
WLJ88S_SR_58	Checking config is getting cleared after clear config in ME	Verifyng ME config gets cleared after clear config	Passed	
WLJ88S_SR_59	Checking 1542AP is joining to 5520 controller after configuring DHCP option 43	Verifying 1542AP is joining to 5520 controller after configuring DHCP option 43	Passed	
WLJ88S_SR_60	Checking 1702AP is joining to 3540 controller after configuring DHCP option 43	Verifying 1702AP is joining to 3540 controller after configuring DHCP option 43	Passed	
WLJ88S_SR_61	Checking 3800AP is joining to 8540 controller after configuring DHCP option 43	Verifying 3800AP is joining to 8540 controller after configuring DHCP option 43	Passed	
WLJ88S_SR_62	Checking AP is joining to ME after configuring DHCP option 43	Verifying AP is joining to ME after configuring DHCP option 43	Passed	
WLJ88S_SR_63	Exporting Maps from PI and import maps to the CMX and connect the Android clients	To verify whether Maps exported and imported in CMX succesfully	Passed	
WLJ88S_SR_64	Adding 1542/2800/3800 AP to floor and export maps from PI and Import to CMX	To verify whether AP added to floor and imported to CMX successfully	Passed	
WLJ88S_SR_65	Exporting 2 campus sites from PI and importing it to CMX	To verify whether 2 campus building can export from PI and import to CMX	Passed	
WLJ88S_SR_66	Joining 1700/2700/3700 AP to the 8540 controller keeping mode in local	To verify whether AP joined to WLC successfully	Passed	

WLJ88S_SR_67	Changing 1700/2700/3700 AP from 8540 controller to 3504 controller with mode local and submode WIPS	To verify whether 1700/2700/3700 AP joined from 8504 controller to 3504 controller	Passed	
WLJ88S_SR_68	Changing 1700/2700/3700 AP from 3504 controller to 5520 controller with mode flexconnect and submode PPPOE	To verify whether 1700/2700/3700 AP joined from 3504 controller to 5520 controller	Passed	
WLJ88S_SR_69	Changing 1700/2700/3700 AP from 8540 controller to 3504 controller with mode local and changing country code	To verify whether 1700/2700/3700 AP joined from 8504 controller to 3504 controller	Passed	
WLJ88S_SR_70	Joining IOS AP to the 8540 controller and check DTLS state	To verify whether AP joined to WLC successfully	Passed	
WLJ88S_SR_71	Installing CMX using web interface	To check whether CMX installed sucessfully	Passed	
WLJ88S_SR_72	Installing CMX using web interface and upgrading it	To check whether CMX installed and upgraded sucessfully	Passed	
WLJ88S_SR_73	Verifying AP becon frames on 3800AP with 5ghz radios	To check whether AP is broadcasting becons for 3800AP with 5ghz radios	Passed	
WLJ88S_SR_74	Verifying AP becon frames on 3800AP with 2.4 ghz radios	To check whether AP is broadcasting becons for 3800AP with 5ghz radios	Passed	
WLJ88S_SR_75	Join 3800/2800 Aps to the controller and connect multiple clients	To check whether multiple clients gets connected and broadcasting even after certain time	Passed	

WLJ88S_SR_76	Configuring full duplex value on the switch by joining wave 2 Aps	Checking the duplex value when wave 2 AP connected to switch	Passed	
WLJ88S_SR_77	Configuring half duplex value on the switch by joining wave 2 Aps	Checking the duplex value when wave 2 AP connected to switch	Passed	
WLJ88S_SR_78	Check whether UI getting stuck while uploading config file	To verify whether UI is working fine	Passed	
WLJ88S_SR_79	Check whether UI getting stuck while uploading Peer config file	To verify whether UI and CLI is working fine	Passed	
WLJ88S_SR_80	Check whether UI getting stuck while uploading config file	To verify whether CLI is working fine	Passed	
WLJ88S_SR_81	Disbaling slave AP and Enabling Master AP and connectING the clients	To verify client can access GUI /SSH to the connected SSID	Passed	
WLJ88S_SR_82	Disabling Master AP and Enabling slave AP and connecting clients	To verify client can access GUI /SSH to the connected SSID	Passed	
WLJ88S_SR_83	Verifying the SSID is brodcasting or not after AP1852 roam from WLC1 to WLC2	Validate the SSID is brocasting or not after moved the AP1852 WLC1 to WLC2	Passed	
WLJ88S_SR_84	Configure the WLAN in AP group	To check whether the SSID is brodcasting or not after AP removed from AP group	Passed	
WLJ88S_SR_85	Verifying deleted/Disabled SSID on AP2700/8540WLC	Validate the disabled/deleted SSID is brodcasting or not on AP2700/8540WLC	Passed	
WLJ88S_SR_86	Verifying the fan failure error after upgrading 3504WLC	To check whether fan failure error is showing or not after upgrading the wlc3504	Passed	

WLJ88S_SR_87	Verifying the client is SSH or not on Wave2 AP3802E	To check whether client is able to SSH or not on AP3802E when directly connected to it.	Passed	
WLJ88S_SR_88	Checking the client SSH connection on Wave2 AP1852	Validate the client SSH connection on 1852 AP	Passed	
WLJ88S_SR_89	Verifying the wireless client SSH/telnet on Wave2 2800i AP	Validate the wireless client is able to SSH/telnet on Wave2 AP2800i	Passed	
WLJ88S_SR_90	Verifying the duplex value on switch for AP2800/3700	To checking the duplex value when AP2800/3700 connected to switch	Passed	
WLJ88S_SR_91	Configure the WLAN with AP group in 3504WLC	Verifying whether disabled SSID is brodcasting or not in 3504 wlc	Passed	
WLJ88S_SR_92	Verifying the SSID status when AP moved from 3504WLC to 5520WLC	To check whether from old wlc SSID is brodcasting or not after AP moved 3504wlc to 5520wlc	Passed	
WLJ88S_SR_93	Roaming multicast wireless clients in Flex connect mode.	To check for the successful and roaming of multicast clients in Flex connect mode.	Passed	
WLJ88S_SR_94	Roaming multicast wireless clients in Local mode.	To check for the successful and roaming of multicast clients in Local mode.	Passed	
WLJ88S_SR_95	Roaming multicast wireless clients in Local mode and Flex connect.	To check for the successful and roaming of multicast clients in Local mode and Flex connect mode.	Passed	

WLJ88S_SR_96	Configuring roaming with Fast Transition.	To check for the successful and seamless roaming of wireless clients between Aps.	Passed	
WLJ88S_SR_97	Verifying clients payload can able to roam with same model WLCs.	To check for the successful and seamless roaming of wireless clients between same model WLCs.	Passed	
WLJ88S_SR_98	Verifying clients payload can able to roam with same model APs.	To check for the successful and seamless roaming of wireless clients between same model APs.	Passed	
WLJ88S_SR_99	Limits Clients should not get same AIDs.	To check Clients should not get same AIDs.	Passed	
WLJ88S_SR_100	Limit the clients in AP Radio(2.4GHZ) and clients should not get same AIDs.	To check Clients should not get same AIDs AP Radio(2.4 GHZ).	Passed	
WLJ88S_SR_101	Limit the clients in AP Radio(5GHZ) and clients should not get same AIDs.	To check Clients should not get same AIDs AP Radio(5 GHZ).	Passed	
WLJ88S_SR_102	Limit the clients AIDs in Flex connect Local switching and local Auth.	To check the clients AIDs in Flex connect Local switching and local Auth.	Passed	
WLJ88S_SR_103	Limit the clients AIDs in Flex connect Central switching.	To check the clients AIDs in Flex connect cental switching.	Passed	
WLJ88S_SR_104	Limit the clients AIDs in Flexconnect group.	To check Limit the clients AIDs in Flexconnect group.	Passed	
WLJ88S_SR_105	Limit the clients AIDs in local mode.	To check Limit the clients AIDs in local mode.	Passed	

WLJ88S_SR_106	Limit the clients AIDs and Vlan ID should be same in client and WLC in Flex connect mode.	To check Limit the clients AIDs and Vlan ID should be same in client and WLC in Flex connect mode.	Passed	
WLJ88S_SR_107	Clients should not connect more than Maximum clients allowed.	To check Clients should not connect more than maximum clients allowed.	Passed	
WLJ88S_SR_108	saving AVC profile configuration AP should not get crash.	To check whether AP crashes or not while saving the AVC profile configuration.	Passed	
WLJ88S_SR_109	Saving AP configuration without crash.	To check Saving AP configuration without crash.	Passed	
WLJ88S_SR_110	Configuring 1815 AP with Different LAN speeds	To configure 1815 AP with diffreent LAN speed and check if the AP works fine or not.	Passed	
WLJ88S_SR_111	Configuring 3800 AP with Different LAN speeds	To configure 3800 AP with diffreent LAN speed and check if the AP works fine or not.	Passed	
WLJ88S_SR_112	Configuring 3700 AP with LAN speed as auto	To configure 3700 AP with LAN speed as Auto and check if the AP works fine or not.	Passed	
WLJ88S_SR_113	Checking client connectivity to 2800 AP by changing the DCA channel	To verify client connectivity to 2800 AP by changing the DCA channel of particular radio	Passed	
WLJ88S_SR_114	Checking client connectivity to 3800 AP by changing the DCA channel	To verify client connectivity to 3800 AP by changing the DCA channel of particular radio	Passed	

WLJ88S_SR_115	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	
WLJ88S_SR_116	Configuring DCA channels in different WLC 3504,5520 and connecting a client	To configure DCA channel in different WLC 5520,3504 and making back and restoring the same back and check if the details are same or not.	Passed	
WLJ88S_SR_117	Checking the DFS when a AP is joining to the controller	To check the DFS when a AP is joining the controller	Passed	
WLJ88S_SR_118	Configure smart DFC and check the DFS status of the mesh AP	To check the DFS status of the Mesh AP and check the details of the DFS is shown correctly or not.	Passed	
WLJ88S_SR_119	Roaming between the 1572 Mesh Aps with RAP and MAP	To verify whether roaming is happening between 1572 mesh aps with Rap and Map	Passed	
WLJ88S_SR_120	Roaming between the 1572 Mesh Aps with MAP and MAP	To verify whether roaming is happening between 1572 mesh aps with Map and Map	Passed	
WLJ88S_SR_121	Roaming between 1572 RAP and other Aps	To verify whether Roaming happneing between 1572 RAP and other Aps or not	Passed	
WLJ88S_SR_122	Connecting the client to WLAN with PSK security after import and export the config	To verify whether after import and export client is connecting or not to WLAN with PSK	Passed	

WLJ88S_SR_123	Connecting the client to WLAN with PSK security after image upgrade	To verify whether Client is connecting to the WLAN with PSK security after image Upgrade	Passed	
WLJ88S_SR_124	Connecting the client to WLAN with PSK security after image downgrade	To verify whether Client is connecting to the WLAN with PSK security after image Downgrade	Passed	
WLJ88S_SR_125	Rejoining the AP to AP-group created with special characters	To verify whether after failover AP is joining back to the same Ap group created with special characters or not	Passed	
WLJ88S_SR_126	Moving the AP between different Ap groups created with special characters	To verify whether AP is moving between different AP groups created with special characters	Passed	
WLJ88S_SR_127	Rejoining the AP to Flexconnect AP-group created with special characters	To verify whether after failover AP is joining back to the same Flexconnect Ap group created with special characters or not	Passed	
WLJ88S_SR_128	Moving the AP between different Flexconnect Ap groups created with special characters	To verify whether AP is moving between different Flexconnect AP groups created with special characters	Passed	
WLJ88S_SR_129	Checking WLAN details after Flexconnect AP reboot with android/Windows clients connect	To verify whether WLAN details are showing properly or not after flexconnect Ap reboot with Andriod/Windows clients connect	Passed	

WLJ88S_SR_130	Checking WLAN details after Flexconnect AP reboot with ios/mac clients connect	To verify whether WLAN details are showing properly or not after flexconnect Ap reboot with ios/MAC clients	Passed	
WLJ88S_SR_131	Adding the WLC in CMX and checking the details after 1 week	To verify whether WLC is working fine in CMX or not	Passed	
WLJ88S_SR_132	Checking the rouges details in CMX from WLC	To verify whether Rouge details are showing in CMX or not	Passed	
WLJ88S_SR_133	Checking the rouges details in CMX after import the maps from PI	To verify whether rouge details are showing properly or not after import the maps from PI	Passed	
WLJ88S_SR_134	Upload/Download the Configuration file after coredump enable	To verify whether all configurations are showing poperly or not after coredump enable and import/export the configurations	Passed	
WLJ88S_SR_135	Checking the WLC crash after executing the basic commands	To verify whether WLC getting crash after executing the basic commands	Passed	
WLJ88S_SR_136	Checking the Controller Count and AP limit after adding device to PI	To check the controller count and AP limit in the Licence Summary Page after adding the controller to PI and check if the details are same in WLC and PI	Failed	CSCvk47809

CME

Captive Portal with Email address and Web Consent

Logical ID	Title	Description	Status	Defect ID
MEJ88PH2S_Reg_337	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	
MEJ88PH2S_Reg_338	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	
MEJ88PH2S_Reg_339	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	
MEJ88PH2S_Reg_340	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	

MEJ88PH2S_Reg_341	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	
MEJ88S_Reg_01	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	
MEJ88S_Reg_02	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	
MEJ88S_Reg_03	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	

MEJ88S_Reg_04	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	
MEJ88S_Reg_05	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	

TACACS

Logical ID	Title	Description	Status	Defect ID
MEJ88PH2S_Reg_239	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	
MEJ88PH2S_Reg_240	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	
MEJ88PH2S_Reg_241	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	
MEJ88PH2S_Reg_242	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	

MEJ88PH2S_Reg_243	Verifying the augh server TACACS through CME CLI	To check whether augh server added or not to the TACACS from CME CLI.	Passed	
MEJ88PH2S_Reg_244	Providing the user for selected access to the CME via TACACS	To check whether user can able to have access with the selected checkbox's like "WLAN" and "Controller" checkboxes.	Passed	
MEJ88PH2S_Reg_245	Providing the user for selected access to the CME via TACACS	To check whether user can able to have access with the selected checkbox's like "Wireless" and "Security" checkboxes.	Passed	
MEJ88PH2S_Reg_246	Providing the user for selected access to the CME via TACACS	To check whether user can able to have access with the selected checkbox's like "Command" and "Management" checkboxes.	Passed	
MEJ88PH2S_Reg_247	Providing the user for selected access to the CME via TACACS	To check whether user can able to have access with the selected checkbox's like"WLAN, Controller, Wireless, Security, Command and "Management" checkboxes.	Passed	
MEJ88PH2S_Reg_248	Trying to login CME network via TACACS with Invalid credentials.	To verify whether user can able to login or not in CME via TACACS with invalid credentials	Passed	
MEJ88S_Reg_06	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	

MEJ88S_Reg_07	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	
MEJ88S_Reg_08	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	
MEJ88S_Reg_09	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
MEJ88PH2S_Reg_249	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	
MEJ88PH2S_Reg_250	Connecting IOS Client via hotspot 2.0	Verifying that user is able to connect IOS Client via hotspot 2.0 or not	Passed	
MEJ88PH2S_Reg_251	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	
MEJ88PH2S_Reg_252	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	

MEJ88PH2S_Reg_253	Try to disable WPA on Hotspot enabled WLAN	Verifying that user is able to disable WPA on Hotspot enabled WLAN or not	Passed	
MEJ88PH2S_Reg_254	Trying to config Passpoint on guest-LAN	Verifying that user is able to config Passpoint on guest-LAN or not	Passed	
MEJ88PH2S_Reg_255	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	
MEJ88PH2S_Reg_256	Try to enable hotspot on open/Guest network	Verifying that user is able to enable hotspot on open network or not	Passed	
MEJ88PH2S_Reg_257	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	
MEJ88PH2S_Reg_258	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	
MEJ88PH2S_Reg_259	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	
MEJ88S_Reg_10	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	
MEJ88S_Reg_11	Connecting IOS Client via hotspot 2.0	Verifying that user is able to connect IOS Client via hotspot 2.0 or not	Passed	

MEJ88S_Reg_12	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	
MEJ88S_Reg_13	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	Failed	CSCvk41500
MEJ88S_Reg_14	Try to disable WPA on Hotspot enabled WLAN	Verifying that user is able to disable WPA on Hotspot enabled WLAN or not	Passed	
MEJ88S_Reg_15	Trying to config pass point on guest-LAN	Verifying that user is able to config Passpoint on guest-LAN or not	Passed	
MEJ88S_Reg_16	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	
MEJ88S_Reg_17	Try to enable hotspot on open/Guest network	Verifying that user is able to enable hotspot on open network or not	Passed	
MEJ88S_Reg_18	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	
MEJ88S_Reg_19	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	
MEJ88S_Reg_20	Assigning the venue group and venue type for the specific AP on 802.11u	Providing the venue group and venue type for the specific AP on 802.11u	Passed	

MAC Filtering (for L2 security)

Logical ID	Title	Description	Status	Defect ID
MEJ88PH2S_Reg_70	Adding Windows (7,10) Client mac address in CME and checking the connection of Clients in 1800 Series ME	To add the windows Client mac address in mac filtering in CME and checking whether Clients gets associated or not successfully in 1800 Series ME	Passed	
MEJ88PH2S_Reg_71	Uploading the empty CSV file in ME UI	To check whether an blank CSV file could be uploaded in ME UI	Passed	
MEJ88PH2S_Reg_72	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	
MEJ88PH2S_Reg_73	Connecting the Client with wan security mac filtering + WPA personal	To Connect the Client with wan security mac filtering + WPA personal	Passed	
MEJ88PH2S_Reg_74	Connecting the Client with wan security mac filtering + WPA enterprise	To Connect the Client with wan security mac filtering + WPA enterprise	Passed	
MEJ88PH2S_Reg_75	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	

MEJ88PH2S_Reg_76	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	
MEJ88PH2S_Reg_77	Connecting the Client after Client identity account expired in ISE	To Connect the Client after Client identity account expired in ISE	Passed	
MEJ88PH2S_Reg_78	Connecting the Client and then moving it to block using MAC address	To Connect the Client and then blocking it using the MAC address	Passed	
MEJ88S_Reg_21	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	
MEJ88S_Reg_22	Uploading the empty CSV file in ME UI	To check whether an blank CSV file could be uploaded in ME UI	Passed	
MEJ88S_Reg_23	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	
MEJ88S_Reg_24	Connecting the Client with wan security mac filtering + WPA personal	To Connect the Client with wan security mac filtering + WPA personal	Passed	

MEJ88S_Reg_25	Connecting the Client with wan security mac filtering + WPA enterprise	To Connect the Client with wan security mac filtering + WPA enterprise	Passed	
MEJ88S_Reg_26	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	
MEJ88S_Reg_27	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	
MEJ88S_Reg_28	Connecting the Client after Client identity account expired in ISE	To Connect the Client after Client identity account expired in ISE	Passed	

AVC

Logical ID	Title	Description	Status	Defect ID
MEJ88PH2S_Reg_260	Drop/mark the different types of social Application for the connected Clients to the created AVC profile	To confirm whether the particular Facebook Application is been dropped/marked	Passed	
MEJ88PH2S_Reg_261	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	

MEJ88PH2S_Reg_262	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	
MEJ88PH2S_Reg_263	Configuring the custom value for Gmail Application with JSSID MAC OS	verify whether custom value is assigned or not for Gmail Application	Passed	
MEJ88PH2S_Reg_264	Drop/mark the cisco-jabber-in Application for the MAC OS to the created AVC profile	To confirm whether the particular cisco-jabber-in Application is been dropped/marked	Passed	
MEJ88PH2S_Reg_265	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	
MEJ88PH2S_Reg_266	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	
MEJ88PH2S_Reg_267	configure the custom value with mark action for Apple-services with JSSID	Verify whether customer value is configured or not for Apple-services	Passed	
MEJ88PH2S_Reg_268	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	
MEJ88PH2S_Reg_269	Drop/mark the amazon-instant-video Application for JSSID to the created AVC profile	Validating the amazon-instant-video Application is dropped/marked or not after connecting JSSID with different OS Clients	Passed	

MEJ88PH2S_Reg_270	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	
MEJ88PH2S_Reg_271	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	
MEJ88PH2S_Reg_272	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	
MEJ88PH2S_Reg_273	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	
MEJ88PH2S_Reg_274	Drop/mark then-daily-news Application for JSSID to the created AVC profile	Validating the my-daily-news Application is dropped/marked or not after connecting JSSID with different OS Clients	Passed	
MEJ88S_Reg_29	Drop/mark the different types of social Application for the connected Clients to the created AVC profile	To confirm whether the particular Facebook Application is been dropped/marked	Failed	CSCvm41862
MEJ88S_Reg_30	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	

MEJ88S_Reg_31	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	
MEJ88S_Reg_32	Configuring the custom value for Gmail Application with JSSID MAC OS	verify whether custom value is assigned or not for Gmail Application	Passed	
MEJ88S_Reg_33	Drop/mark the cisco-jabber-in Application for the MAC OS to the created AVC profile	To confirm whether the particular cisco-jabber-in Application is been dropped/marked	Passed	
MEJ88S_Reg_34	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	
MEJ88S_Reg_35	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	
MEJ88S_Reg_36	configure the custom value with mark action for Apple-services with JSSID	Verify whether customer value is configured or not for Apple-services	Passed	
MEJ88S_Reg_37	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	
MEJ88S_Reg_38	Drop/mark the amazon-instant-video Application for JSSID to the created AVC profile	Validating the amazon-instant-video Application is dropped/marked or not after connecting JSSID with different OS Clients	Passed	

MEJ88S_Reg_39	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	
MEJ88S_Reg_40	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	
MEJ88S_Reg_41	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	
MEJ88S_Reg_42	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	
MEJ88S_Reg_43	Drop/mark then-daily-news Application for JSSID to the created AVC profile	Validating the my-daily-news Application is dropped/marked or not after connecting JSSID with different OS Clients	Passed	

Lobby Ambassador

Logical ID	Title	Description	Status	Defect ID
MEJ88PH2S_Reg_287	Creating a Lobby Admin in CME GUI/CLI	To check whether lobby admin user is created or not in CME GUI/CLI	Passed	
MEJ88PH2S_Reg_288	Creating /deleting a management guest User	To check whether a guest user can be added /deleted or not in CME guest management GUI	Passed	

MEJ88PH2S_Reg_289	Deleting a management guest user	To check whether guest user can be deleted or not in CME GUI	Passed	
MEJ88PH2S_Reg_290	Generating auto Password for management guest user	To check whether Password is generated or not for management guest user	Passed	
MEJ88PH2S_Reg_291	Generating Password manually for management guest user	To check whether manually Password is generating or not for management guest user	Passed	
MEJ88PH2S_Reg_292	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	
MEJ88PH2S_Reg_293	Configuring Guest WLAN with default login Page	To check whether a default page can be configured or not for guest login	Passed	
MEJ88PH2S_Reg_294	Configuring Guest WLAN with customized login Page	To check whether a customized page can be configured or not for guest login	Passed	
MEJ88S_Reg_44	Creating a Lobby Admin in CME GUI/CLI	To check whether lobby admin user is created or not in CME GUI/CLI	Passed	
MEJ88S_Reg_45	Creating a management guest User	To check whether a guest user can be added or not in CME guest management GUI	Passed	
MEJ88S_Reg_46	Deleting a management guest user	To check whether guest user can be deleted or not in CME GUI	Passed	
MEJ88S_Reg_47	Generating auto password for management guest user	To check whether password is generated or not for management guest user	Failed	CSCvm36109

MEJ88S_Reg_48	Generating password manually for management guest user	To check whether manually password is generating or not for management guest user	Passed	
MEJ88S_Reg_49	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	Failed	CSCvm44422
MEJ88S_Reg_50	Configuring Guest WLAN with default login Page	To check whether a default page can be configured or not for guest login	Passed	
MEJ88S_Reg_51	Configuring Guest WLAN with customized login Page	To check whether a customized page can be configured or not for guest login	Passed	

CME Guest Login

Logical ID	Title	Description	Status	Defect ID
MEJ88PH2S_Reg_342	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	
MEJ88PH2S_Reg_343	Associating Windows Client to a WLAN in which security web-augh 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	
MEJ88PH2S_Reg_344	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	

MEJ88PH2S_Reg_345	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	
MEJ88PH2S_Reg_346	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	
MEJ88PH2S_Reg_347	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	
MEJ88PH2S_Reg_348	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	
MEJ88PH2S_Reg_349	Creating a default login page for guest WLANs after Client connect to SSID	To verify whether the default login page is created or not for guest WLANs	Passed	
MEJ88PH2S_Reg_350	Creating a customized login page for guest WLANs after associate the SSID	To verify whether the customized login page is created or not for guest WLANs	Passed	
MEJ88S_Reg_52	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	

MEJ88S_Reg_53	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	
MEJ88S_Reg_54	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	
MEJ88S_Reg_55	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	
MEJ88S_Reg_56	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	
MEJ88S_Reg_57	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	

MEJ88S_Reg_58	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	
MEJ88S_Reg_59	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	
MEJ88S_Reg_60	Creating a default login page for guest WLANs after Client connect to SSID	To verify whether the default login page is created or not for guest WLANs	Passed	
MEJ88S_Reg_61	Creating a customized login page for guest WLANs after associate the SSID	To verify whether the customized login page is created or not for guest WLANs	Passed	
MEJ88S_Reg_62	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	Title	Description	Status	Defect ID
MEJ88PH2S_Reg_295	Validating deployed WLANs from PI in CME	To check whether Mobility Express WLANs or reflecting or not in PI	Passed	
MEJ88PH2S_Reg_296	Creating WLAN in PI with open security and connecting a Client	To check Client connectivity to created WLAN with open security	Passed	

MEJ88PH2S_Reg_297	Creating WLAN in PI with WPA2 personal security and connecting a Client	To check Client connectivity to created WLAN with WPA2 personal security	Passed	
MEJ88PH2S_Reg_298	Creating WLAN in PI with WPA2 enterprise security and connecting a Client	To check Client connectivity to created WLAN with WPA2 enterprise security	Passed	
MEJ88PH2S_Reg_299	Connecting a Window Client to the created WLAN and validate the same in PI	To Check whether windows Client connecting or not to WLAN	Passed	
MEJ88PH2S_Reg_300	Connecting a android Client to the created WLAN and validate the same in PI	To Check whether android Client connecting or not to WLAN	Passed	
MEJ88PH2S_Reg_301	Connecting a IOS Client to the created WLAN and validate the same in PI	To Check whether IOS Client connecting or not to WLAN	Passed	
MEJ88PH2S_Reg_302	Connecting a MAC Client to the created WLAN and validate the same in PI	To Check whether MAC Client connecting or not to WLAN	Passed	
MEJ88PH2S_Reg_303	Creating flex connect AVC profiles in PI and validating in CME CLI	To Check created flex connect AVC profiles from PI reflecting in CME CLI or not	Passed	
MEJ88PH2S_Reg_304	Creating flex connect AVC ACL profiles in PI and validating in CME CLI	Checking in PI created flex connect AVC ACL in CME CLI	Passed	
MEJ88S_Reg_63	Adding Mobility Express of general parameters into Prime Infrastructure.	To check whether Mobility Express of general parameters added into Prime.	Passed	
MEJ88S_Reg_64	Adding Mobility Express of SNMP parameters into Prime Infrastructure.	To check whether Mobility Express of SNMP parameters added into Prime.	Passed	

MEJ88S_Reg_65	Adding Mobility Express into Prime Infrastructure.	To check whether Mobility Express added into Prime.	Passed	
MEJ88S_Reg_66	Adding into group Mobility Express into Prime Infrastructure.	To check whether Mobility Express added into Prime Infrastructure group.	Passed	
MEJ88S_Reg_67	Sync Mobility Express into Prime Infrastructure.	To check whether Mobility Express sync or not in Prime Infrastructure.	Passed	
MEJ88S_Reg_68	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	
MEJ88S_Reg_69	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	
MEJ88S_Reg_70	Creating WLANs from Prime on CME	To check whether WLANs from Prime on CME created or not.	Passed	
MEJ88S_Reg_71	Configuring WLANs template from Prime on CME	To check whether WLAN template from Prime on CME configured or not.	Passed	
MEJ88S_Reg_72	Deploying the WLAN template to CME	To check whether WLAN template to CME deployed or not	Passed	
MEJ88S_Reg_73	Viewing the job status to CME	To check whether job status to CME deployed or not	Passed	
MEJ88S_Reg_74	Validating the CME device details from PI	To check the CME device details from PI	Passed	
MEJ88S_Reg_75	Verifying the Client details in PI	To check the Client details shown or not in PI	Passed	

Syslog

Logical ID	Title	Description	Status	Defect ID
MEJ88PH2S_Reg_79	Enabling logging for Errors in CME	To check whether log can be generated or not for Error Message in CME GUI	Passed	
MEJ88PH2S_Reg_80	Disabling logging for Errors in CME	To check whether logging for Errors disabled or not in CME	Passed	
MEJ88PH2S_Reg_81	Enabling logging for Debugging in CME	To check whether log can be generated or not for Debug Message in CME GUI	Passed	
MEJ88PH2S_Reg_82	Enabling logging server for Emergencies	To check whether log can be generated or not for Emergencies in CME GUI	Passed	
MEJ88PH2S_Reg_83	Enabling logging for Alerts	To check whether log can be generated or not for alerts in CME GUI	Passed	
MEJ88PH2S_Reg_84	Enabling logging for Warning	To check whether log can be generated or not for warning in CME GUI	Passed	
MEJ88PH2S_Reg_85	Enabling logging for Critical	To check whether log can be generated or not for critical events in CME GUI	Passed	
MEJ88PH2S_Reg_86	Enabling logging for Notification	To check whether log can be generated or not for notification in CME GUI	Failed	CSCvj89220
MEJ88PH2S_Reg_87	Enabling logging for Information message	To check whether log can be generated or not for Informational message in CME GUI	Passed	

MEJ88PH2S_Reg_88	Checking the validation of syslog errors in PI	To check whether the syslog errors are displayed in PI	Passed	
MEJ88PH2S_Reg_89	Checking the validation of syslog information in PI	To check whether the syslog information are displayed in PI	Passed	
MEJ88PH2S_Reg_90	Checking the historic information about syslog in PI	To check whether the historic information about syslog in PI	Passed	
MEJ88PH2S_Reg_91	Validating the syslog warning message in PI	To check whether the syslog warning message in PI	Passed	
MEJ88PH2S_Reg_92	Validating the syslog notification in PI	To check whether syslog notification in PI	Passed	
MEJ88PH2S_Reg_93	Verifying the severity filtering for syslog in PI	To verify the severity filtering for syslog in PI	Passed	
MEJ88PH2S_Reg_94	Verifying the Device IP address filtering for syslog in PI	To verify the Device IP address filtering for syslog in PI	Passed	
MEJ88S_Reg_76	Enabling logging for Errors in CME	To check whether log can be generated or not for Error Message in CME GUI	Passed	
MEJ88S_Reg_77	Disabling logging for Errors in CME	To check whether logging for Errors disabled or not in CME	Passed	
MEJ88S_Reg_78	Enabling logging for Debugging in CME	To check whether log can be generated or not for Debug Message in CME GUI	Passed	
MEJ88S_Reg_79	Enabling logging server for Emergencies	To check whether log can be generated or not for Emergencies in CME GUI	Passed	

MEJ88S_Reg_80	Enabling logging for Alerts	To check whether log can be generated or not for alerts in CME GUI	Passed	
MEJ88S_Reg_81	Enabling logging for Warning	To check whether log can be generated or not for warning in CME GUI	Passed	
MEJ88S_Reg_82	Enabling logging for Critical	To check whether log can be generated or not for critical events in CME GUI	Passed	
MEJ88S_Reg_83	Enabling logging for Notification	To check whether log can be generated or not for notification in CME GUI	Passed	
MEJ88S_Reg_84	Enabling logging for Information message	To check whether log can be generated or not for Informational message in CME GUI	Passed	
MEJ88S_Reg_85	Checking the validation of syslog errors in PI	To check whether the syslog errors are displayed in PI	Passed	
MEJ88S_Reg_86	Checking the validation of syslog information in PI	To check whether the syslog information are displayed in PI	Passed	
MEJ88S_Reg_87	Checking the historic information about syslog in PI	To check whether the historic information about syslog in PI	Passed	
MEJ88S_Reg_88	Validating the syslog warning message in PI	To check whether the syslog warning message in PI	Passed	
MEJ88S_Reg_89	Validating the syslog notification in PI	To check whether syslog notification in PI	Passed	
MEJ88S_Reg_90	Verifying the severity filtering for syslog in PI	To verify the severity filtering for syslog in PI	Passed	

MEJ88S_Reg_91	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
MEJ88PH2S_Reg_305	Configuring the Central-NAT configuration at DHCP Scope level	To verify whether Central-NAT Configuration Applied successfully or not	Passed	
MEJ88PH2S_Reg_306	Associating the DHCP Scope to WLAN	To verify whether DHCP Scope is associate the WLAN or not	Passed	
MEJ88PH2S_Reg_307	Peer-to-peer blocking the configuration on DHCP through CLI	To verify whether Peer-to-peer blocking Applied successfully or not	Passed	
MEJ88PH2S_Reg_308	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	
MEJ88PH2S_Reg_309	Configuring the NAT functionality in radio 5GHZ band AP	To verify whether NATing working or not in 5 GHZ radio band	Passed	
MEJ88PH2S_Reg_310	Choking Client performance in Monitoring page after Client connect	To verify whether Client performance is showing or not in monitoring page	Passed	
MEJ88PH2S_Reg_311	Checking the Connection and event log after Client connect	To verify whether Connection showing properly or not	Passed	
MEJ88PH2S_Reg_312	Checking the NAT configuration with invalid DHCP parameters	To verify whether NAT configured for invalid DHCP scope	Passed	

MEJ88S_Reg_92	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	
MEJ88S_Reg_93	Client IP Management with Mobility express controller	To verify whether Client IP Management creating or not with mobility express controller	Passed	
MEJ88S_Reg_94	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	
MEJ88S_Reg_95	Configuring the Central-NAT configuration at DHCP Scope level	To verify whether Central-NAT Configuration Applied successfully or not	Passed	
MEJ88S_Reg_96	NATing enabling in Client	To verify whether NATing Applying to the Client or not	Passed	
MEJ88S_Reg_97	Associating the DHCP Scope to WLAN	To verify whether DHCP Scope is associate the WLAN or not	Passed	
MEJ88S_Reg_98	Peer-to-peer blocking the configuration on DHCP through CLI	To verify whether Peer-to-peer blocking Applied successfully or not	Passed	
MEJ88S_Reg_99	Choking the lease period after Client connect	To verify whether lease period is showing properly or not after Client connect	Passed	
MEJ88S_Reg_100	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	
MEJ88S_Reg_101	Configuring the NAT functionality in radio 5GHZ band AP	To verify whether NATing working or not in 5 GHZ radio band	Passed	

MEJ88S_Reg_102	Choking Client performance in Monitoring page after Client connect	To verify whether Client performance is showing or not in monitoring page	Passed	
MEJ88S_Reg_103	Performing the PING test for Client	To verify whether PING performing successfully or not	Passed	
MEJ88S_Reg_104	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
MEJ88PH2S_Reg_218	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	
MEJ88PH2S_Reg_219	Enabling/disabling rogue detection on CME CLI	To verify that user is able to enable/disable rogue detection on CME or not	Passed	
MEJ88PH2S_Reg_220	Classifying the rogue Client on CME after Client connect	To verify that user is able to classify rogue Client on CME or not	Passed	
MEJ88PH2S_Reg_221	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	
MEJ88PH2S_Reg_222	Verifying the special character names rogue devices	To verifying that special character names rogue devices are Appearing under rogue AP or not	Passed	
MEJ88PH2S_Reg_223	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	

MEJ88PH2S_Reg_224	Manual mitigation of rogue device	Verify that user is able to manually mitigate the rogue AP or not	Passed	
MEJ88PH2S_Reg_225	Auto mitigation of rogue device	Verify that user is able to auto mitigate the rogue AP or not	Passed	
MEJ88PH2S_Reg_226	Classifying the rogue Adhoc on CME	Verify that user is able to classify rogue Adhoc on CME or not	Passed	
MEJ88PH2S_Reg_227	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	
MEJ88S_Reg_105	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	
MEJ88S_Reg_106	Enabling/disabling rogue detection on CME CLI	To verify that user is able to enable/disable rogue detection on CME or not	Passed	
MEJ88S_Reg_107	Classifying the rogue Client on CME after Client connect	To verify that user is able to classify rogue Client on CME or not	Passed	
MEJ88S_Reg_108	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	
MEJ88S_Reg_109	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	
MEJ88S_Reg_110	Verifying the special character names rogue devices	To verifying that special character names rogue devices are Appearing under rogue AP or not	Passed	

MEJ88S_Reg_111	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	
MEJ88S_Reg_112	Manual mitigation of rogue device	Verify that user is able to manually mitigate the rogue AP or not	Passed	
MEJ88S_Reg_113	Auto mitigation of rogue device	Verify that user is able to auto mitigate the rogue AP or not	Passed	
MEJ88S_Reg_114	Classifying the rogue ado on CME	Verify that user is able to classify rogue ado on CME or not	Passed	
MEJ88S_Reg_115	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	
MEJ88S_Reg_116	Verifying the CME is detecting the different OS rogue devices	To verifying that CME is able to detect the different OS rogue devices or not	Passed	

ACL

Logical ID	Title	Description	Status	Defect ID
MEJ88PH2S_Reg_275	Creating the ACL name with Duplicate name	To verify whether ACL name is created with existing name or not	Passed	
MEJ88PH2S_Reg_276	Applying the ACL rule with Ingress and egress values	To verify whether ingress and Egress rule is Applied to ACL or not	Passed	
MEJ88PH2S_Reg_277	Creating the ACL rule for Specified source address with Permit/Deny action	To verify whether ACL rule is Applied to the specified source address with Permit/Deny action or not	Failed	CSCvm67040

MEJ88PH2S_Reg_278	Creating the ACL rule for Specified destination address with Permit/Deny action	To verify whether ACL rule is Applied to the specified destination address with Permit/Deny action or not	Passed	
MEJ88PH2S_Reg_279	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	
MEJ88PH2S_Reg_280	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	
MEJ88PH2S_Reg_281	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	
MEJ88PH2S_Reg_282	Creating the ACL name with special characters through CLI	To verify whether ACL name is creating with special characters or not	Passed	
MEJ88PH2S_Reg_283	Adding the action to the ACL rule through CLI	To verify whether ACL action is Applied successfully or not through CLI	Passed	
MEJ88PH2S_Reg_284	Changing the Protocol from one to another	To verify whether Protocols are changing from one to another or not	Passed	
MEJ88PH2S_Reg_285	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	Failed	CSCvm34269
MEJ88PH2S_Reg_286	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	

MEJ88S_Reg_117	Creating the ACL name with Duplicate name	To verify whether ACL name is created with existing name or not	Passed	
MEJ88S_Reg_118	Applying the ACL rule with Engross values	To verify whether Egress rule is Applied to ACL or not	Passed	
MEJ88S_Reg_119	Applying the ACL rule with Ingress values	To verify whether Ingress rule is Applied to ACL or not	Passed	
MEJ88S_Reg_120	Applying the ACL rule with Ingress and egress values	To verify whether ingress and Egress rule is Applied to ACL or not	Passed	
MEJ88S_Reg_121	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	
MEJ88S_Reg_122	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	
MEJ88S_Reg_123	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	
MEJ88S_Reg_124	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	
MEJ88S_Reg_125	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	Failed	CSCvj37172

MEJ88S_Reg_126	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	
MEJ88S_Reg_127	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	
MEJ88S_Reg_128	Creating the ACL name with special characters through CLI	To verify whether ACL name is creating with special characters or not	Passed	
MEJ88S_Reg_129	Adding the action to the ACL rule through CLI	To verify whether ACL action is Applied successfully or not through CLI	Passed	
MEJ88S_Reg_130	Changing the Protocol from one to another	To verify whether Protocols are changing from one to another or not	Passed	
MEJ88S_Reg_131	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	
MEJ88S_Reg_132	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
MEJ88PH2S_Reg_410	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	

MEJ88PH2S_Reg_411	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	
MEJ88PH2S_Reg_412	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	
MEJ88PH2S_Reg_413	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	
MEJ88PH2S_Reg_414	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	
MEJ88S_Reg_133	Mapping a Internal DHCP pool to WLAN and verifying Windows Client IP Address and VLAN id	To verify whether a window Client get IP address and VLAN id from a specified DHCP pool or not	Passed	
MEJ88S_Reg_134	Mapping a Internal DHCP pool to WLAN and verifying Android Client IP Address and VLAN id	To verify whether a Android Client get IP address and VLAN id from a specified DHCP pool or not	Passed	
MEJ88S_Reg_135	Mapping a Internal DHCP pool to WLAN and verifying MAC Client IP Address and VLAN id	To verify whether a MAC OS Client get IP address and VLAN id from a specified DHCP pool or not	Passed	

MEJ88S_Reg_136	Mapping a Internal DHCP pool to WLAN and verifying iOS Client IP Address and VLAN id	To verify whether a iOS Client get IP address and VLAN id from a specified DHCP pool or not	Passed	
MEJ88S_Reg_137	Checking lease period for connected Client through a DHCP pool	To verify whether DHCP release a particular IP address or not after a certain lease period for Client	Passed	

Video Streaming

Logical ID	Title	Description	Status	Defect Id
MEJ88S_Reg_138	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	
MEJ88S_Reg_139	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	
MEJ88S_Reg_140	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	
MEJ88S_Reg_141	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	

MEJ88S_Reg_142	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	
MEJ88S_Reg_143	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	
MEJ88S_Reg_144	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	
MEJ88S_Reg_145	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	
MEJ88S_Reg_146	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	
MEJ88S_Reg_147	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	
MEJ88S_Reg_148	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	

MEJ88S_Reg_149	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
MEJ88PH2S_Reg_176	Create URL ACL rule with guest network WLAN	To verify that URL ACL created with guest network	Passed	
MEJ88PH2S_Reg_177	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	
MEJ88PH2S_Reg_178	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	
MEJ88PH2S_Reg_179	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	

MEJ88PH2S_Reg_180	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	
MEJ88PH2S_Reg_181	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	
MEJ88PH2S_Reg_182	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	
MEJ88PH2S_Reg_183	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	
MEJ88PH2S_Reg_184	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	

MEJ88PH2S_Reg_185	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	
MEJ88PH2S_Reg_186	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	
MEJ88PH2S_Reg_187	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	
MEJ88S_Reg_150	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	
MEJ88S_Reg_151	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	

MEJ88S_Reg_152	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	
MEJ88S_Reg_153	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	
MEJ88S_Reg_154	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	
MEJ88S_Reg_155	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	
MEJ88S_Reg_156	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	

MEJ88S_Reg_157	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	
MEJ88S_Reg_158	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	

OpenDNS

Logical ID	Title	Description	Status	Defect ID
MEJ88PH2S_Reg_235	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	
MEJ88PH2S_Reg_236	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	
MEJ88PH2S_Reg_237	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	

MEJ88PH2S_Reg_238	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	
MEJ88S_Reg_159	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	
MEJ88S_Reg_160	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	
MEJ88S_Reg_161	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	
MEJ88S_Reg_162	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 Groups

Logical ID	Title	Description	Status	Defect ID

MEJ88PH2S_Reg_415	Adding the wan 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	
MEJ88PH2S_Reg_416	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	
MEJ88PH2S_Reg_417	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	
MEJ88PH2S_Reg_418	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	
MEJ88PH2S_Reg_419	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	
MEJ88PH2S_Reg_420	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	
MEJ88PH2S_Reg_421	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	
MEJ88PH2S_Reg_422	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	

MEJ88S_Reg_163	Adding the wan 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	
MEJ88S_Reg_164	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	
MEJ88S_Reg_165	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	
MEJ88S_Reg_166	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	
MEJ88S_Reg_167	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	
MEJ88S_Reg_168	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	
MEJ88S_Reg_169	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	
MEJ88S_Reg_170	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	

CME Crashes(DHCP/Troubleshootings)

Logical ID	Title	Description	Status	Defect ID
MEJ88PH2S_Reg_01	Creating the DHCP scope form CLI with invalid IP address	To verify whether DHCP scope is created or not with invalid IP address form CLI	Passed	
MEJ88PH2S_Reg_02	Changing the DHCP scope default gateway from Network to Mobility Express	To verify whether DHCP scope default gateway changing from Network to Mobility Express or not	Passed	
MEJ88PH2S_Reg_03	Changing the RRM details after Client connected to WLAN	To verify whether DHCP going to Crash or not after changing the RRM details	Passed	
MEJ88PH2S_Reg_04	Enabling/Disabling the Central NAT	To verify whether Central NAT enabling/Disabling without any issues or not	Passed	
MEJ88PH2S_Reg_05	Creating more than 10 DHCP scopes and assign to different WLANs	To verify whether more than 10 DHCP scopes are created and assigned to WLAN without any issues or not	Passed	
MEJ88PH2S_Reg_06	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	
MEJ88PH2S_Reg_07	Clearing the Controller Configurations	To verify whether Controller Configurations are clearing or not	Passed	
MEJ88PH2S_Reg_08	Export/Import the Controller Configurations	To verify whether Controller Configurations are Exporting/Importing or not	Passed	

MEJ88PH2S_Reg_09	Migrate the Cisco Mobility express deployment	To verify whether AP can be migrating to new controller or not	Passed	
MEJ88PH2S_Reg_10	Downloading the support bundle from Controller	To verify whether Support bundle downloading successfully or not	Passed	
MEJ88PH2S_Reg_11	Invalid DNS server IP address configuration	To verify whether DNS IP address field accepting the Invalid IP address or not	Passed	
MEJ88PH2S_Reg_12	Checking the Radius/ping response	To verify whether Radius/ping response is Applying successfully or not	Passed	
MEJ88PH2S_Reg_13	Performing the all tests	To verify whether all tests are performing or not	Passed	
MEJ88S_Reg_171	Creating the DHCP Scope with valid IP address	To verify whether DHCP scope is creating or not with valid details	Passed	
MEJ88S_Reg_172	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	
MEJ88S_Reg_173	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	
MEJ88S_Reg_174	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	
MEJ88S_Reg_175	Changing the RRM details after Client connected to WLAN	To verify whether DHCP going to Crash or not after changing the RRM details	Passed	

MEJ88S_Reg_176	Enabling/Disabling the Central NAT	To verify whether Central NAT enabling/Disabling without any issues or not	Passed	
MEJ88S_Reg_177	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	
MEJ88S_Reg_178	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	
MEJ88S_Reg_179	Assigning the DHCP scope to WLAN with network	To verify whether DHCP scope assigned to the WLAN or not with Network DHCP	Passed	
MEJ88S_Reg_180	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	
MEJ88S_Reg_181	Restarting the Controller	To verify whether Controller is restarting or not	Passed	
MEJ88S_Reg_182	Clearing the Controller Configurations	To verify whether Controller Configurations are clearing or not	Passed	
MEJ88S_Reg_183	Export the Controller Configurations	To verify whether Controller Configurations are Exporting or not	Passed	
MEJ88S_Reg_184	Import the Controller Configurations	To verify whether Controller Configurations are importing or not	Passed	
MEJ88S_Reg_185	Migrate the Cisco Mobility express deployment	To verify whether AP can be migrating to new controller or not	Passed	

MEJ88S_Reg_186	Downloading the support bundle from Controller	To verify whether Support bundle downloading successfully or not	Passed	
MEJ88S_Reg_187	Invalid DNS server IP address configuration	To verify whether DNS IP address field accepting the Invalid IP address or not	Passed	
MEJ88S_Reg_188	Performing the PING test with valid/invalid IP	To verify whether PING test is performing with valid/invalid IP address successfully or not	Passed	
MEJ88S_Reg_189	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	
MEJ88S_Reg_190	Checking the Radius response	To verify whether Radius response is Applying successfully or not	Passed	
MEJ88S_Reg_191	Performing the all tests	To verify whether all tests are performing or not	Passed	
MEJ88S_Reg_192	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
MEJ88PH2S_Reg_369	Client connectivity with WPA2 personal security with Wrong credentials .	To verify if the Client connects to WLAN with WPA2 personal security or not with the Wrong credentials.	Passed	

MEJ88PH2S_Reg_370	Configuring Client Idle timeout/Session timeout for a particular WLAN and check if the timeout works properly.	To configure Client ideal Timeout/Session timeout and check if the timeout for the Client works .	Passed	
MEJ88PH2S_Reg_371	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	
MEJ88PH2S_Reg_372	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	
MEJ88PH2S_Reg_373	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	
MEJ88PH2S_Reg_374	Connecting a JOS/Android/MAC Client with WPA2 enterprises security and debugging the Client for errors .	To verify that JOS/Android/MAC Client connect successfully with WPA2 enterprises or not	Passed	
MEJ88PH2S_Reg_375	Connecting 2 different Android Client with WPA2 enterprises security and debugging the Client for errors and performing the PING test	To verify that 2 different Android Clients connected and pinging each other with different WPA2 enterprises or not	Passed	

MEJ88PH2S_Reg_376	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	
MEJ88PH2S_Reg_377	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	
MEJ88PH2S_Reg_378	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	
MEJ88PH2S_Reg_379	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	
MEJ88PH2S_Reg_380	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	
MEJ88S_Reg_193	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	
MEJ88S_Reg_194	Client connectivity with WPA2 personal security with Wrong credentials .	To verify if the Client connects to WLAN with WPA2 personal security or not with the Wrong credentials.	Passed	

MEJ88S_Reg_195	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	
MEJ88S_Reg_196	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	
MEJ88S_Reg_197	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	
MEJ88S_Reg_198	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	
MEJ88S_Reg_199	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	
MEJ88S_Reg_200	Connecting a JOS Client with WPA2 enterprises security and debugging the Client for errors .	To verify that JOS Client connect successfully with WPA2 enterprises or not	Passed	
MEJ88S_Reg_201	Connecting 3 Window Client with WPA2 enterprises security and debugging the Client for errors .	To verify that Window Client connect successfully with WPA2 enterprises or not	Passed	

MEJ88S_Reg_202	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 successfully with WPA2 enterprises or not	Passed	
MEJ88S_Reg_203	Connecting a IOS Client with WPA2 enterprises security and debugging the Client for errors .	To verify that IOS Client connect successfully with WPA2 enterprises or not	Passed	
MEJ88S_Reg_204	Connecting a MAC OS Client with WPA2 enterprises security and debugging the Client for errors .	To verify that MAC OS Client connect successfully with WPA2 enterprises or not	Passed	
MEJ88S_Reg_205	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	
MEJ88S_Reg_206	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	
MEJ88S_Reg_207	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	
MEJ88S_Reg_208	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	

MEJ88S_Reg_209	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	
MEJ88S_Reg_210	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 WLC Roaming Failures(Ping Pong Issues)

Logical ID	Title	Description	Status	Defect ID
MEJ88PH2S_Reg_14	Intra Controller Roaming with Open Security	To verify whether Client is Roaming with Open Security or not between APs	Passed	
MEJ88PH2S_Reg_15	Intra Controller Roaming with WPA2 Security	To verify whether Client is Roaming with WPA2 Security or not between APs	Passed	
MEJ88PH2S_Reg_16	Intra Controller Roaming with WPA Enterprise + Radius server Security	To verify whether Client is Roaming with WPA Enterprise + Radios Security or not between APs	Passed	
MEJ88PH2S_Reg_17	Intra Controller Roaming with WPA Enterprise + AP Security	To verify whether Client is Roaming with WPA Enterprise + AP Security or not between APs	Passed	
MEJ88PH2S_Reg_18	Intra Controller Roaming with WPA2+Mac-filtering	To verify whether Client is Roaming with WPA2+ Mac-filtering security or not between APs	Passed	

MEJ88PH2S_Reg_19	Intra Controller Roaming with Guest Network+Mac-filtering	To verify whether Client is Roaming with Guest Network+Mac-filtering security or not between APs	Passed	
MEJ88PH2S_Reg_20	Intra Controller Roaming with Guest Network in Internal splash page+Local user account	To verify whether Client is Roaming in Guest Network with Internal splash page+Local user account or not	Passed	
MEJ88PH2S_Reg_21	Intra Controller Roaming with Guest Network in Internal splash page+Web consent	To verify whether Client is Roaming in Guest Network with Internal splash page+Web consent	Passed	
MEJ88PH2S_Reg_22	Intra Controller Roaming with Guest Network in Internal splash page+Email address	To verify whether Client is Roaming in Guest Network with Internal splash page+Email address	Passed	
MEJ88PH2S_Reg_23	Intra Controller Roaming with Guest Network in Internal splash page+Radius server	To verify whether Client is Roaming in Guest Network with Internal splash page+Radius server	Passed	
MEJ88PH2S_Reg_24	Intra Controller Roaming with Guest Network in Internal splash page+WPA2 personal	To verify whether Client is Roaming in Guest Network with Internal splash page+WPA2 personal	Passed	
MEJ88PH2S_Reg_25	Intra Controller Roaming with Guest Network in CMX Connect	To verify whether Client is Roaming in Guest Network with CMX Connect or not	Passed	
MEJ88PH2S_Reg_26	Intra Controller Roaming with Guest Network in External splash page+Local user account	To verify whether Client is Roaming in Guest Network with External splash page+Local user account	Passed	

MEJ88PH2S_Reg_27	Intra Controller Roaming with Guest Network in External splash page+Web consent	To verify whether Client is Roaming in Guest Network with External splash page+Web consent	Passed	
MEJ88PH2S_Reg_28	Intra Controller Roaming with Guest Network in External splash page+Email address	To verify whether Client is Roaming in Guest Network with External splash page+Email address	Passed	
MEJ88PH2S_Reg_29	Intra Controller Roaming with Guest Network in External splash page+Radius server	To verify whether Client is Roaming in Guest Network with External splash page+Radius server	Passed	
MEJ88PH2S_Reg_30	Intra Controller Roaming with Guest Network in External splash page+WPA personal	To verify whether Client is Roaming in Guest Network with External splash page+WPA2 personal	Passed	
MEJ88S_Reg_211	Intra Controller Roaming with Open Security	To verify whether Client is Roaming with Open Security or not between APs	Passed	
MEJ88S_Reg_212	Intra Controller Roaming with WPA2 Security	To verify whether Client is Roaming with WPA2 Security or not between APs	Passed	
MEJ88S_Reg_213	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	
MEJ88S_Reg_214	Intra Controller Roaming with WPA Enterprise + AP Security	To verify whether Client is Roaming with WPA Enterprise + AP Security or not between APs	Passed	
MEJ88S_Reg_215	Intra Controller Roaming with WPA2+Mac-filtering	To verify whether Client is Roaming with WPA2+ Mac-filtering security or not between APs	Passed	

MEJ88S_Reg_216	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	
MEJ88S_Reg_217	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	
MEJ88S_Reg_218	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	
MEJ88S_Reg_219	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	
MEJ88S_Reg_220	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	
MEJ88S_Reg_221	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	
MEJ88S_Reg_222	Intra Controller Roaming with Guest Network in CMX Connect	To verify whether Client is Roaming in Guest Network with CMX Connect or not	Passed	
MEJ88S_Reg_223	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	

MEJ88S_Reg_224	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	
MEJ88S_Reg_225	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	
MEJ88S_Reg_226	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	
MEJ88S_Reg_227	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 Failover Issues

Logical ID	Title	Description	Status	Defect ID
MEJ88PH2S_Reg_31	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	
MEJ88PH2S_Reg_32	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	
MEJ88PH2S_Reg_33	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	
MEJ88PH2S_Reg_34	Deleting the Master Prepared AP from CLI	To verify whether Master preferred AP is deleting from CLI or not	Passed	

MEJ88PH2S_Reg_35	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	
MEJ88PH2S_Reg_36	Assigning the Global AP Configurations	To verify whether Global AP Configurations authenticate to the AP or not	Passed	
MEJ88S_Reg_228	CAPWAP AP to ME Capable AP	To verify whether CAPWAP can be changed to ME capable AP or not	Passed	
MEJ88S_Reg_229	Making the ME Capable AP to Preferred master AP	To verify whether ME AP is changing the Preferred Master AP or not	Passed	
MEJ88S_Reg_230	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	
MEJ88S_Reg_231	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	
MEJ88S_Reg_232	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	Failed	CSCvk21890
MEJ88S_Reg_233	Deleting the Master Prepared AP from CLI	To verify whether Master preferred AP is deleting from CLI or not	Passed	
MEJ88S_Reg_234	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	

MEJ88S_Reg_235	Changing the CAPWAP to CAPWAP	To verify whether proper error showing or not at the time of CAPWAP changing to CAPWAP	Passed	
MEJ88S_Reg_236	Assigning the Global AP Configurations	To verify whether Global AP Configurations authenticate to the AP or not	Passed	
MEJ88S_Reg_237	Exporting the Configurations after Next master AP Configurations	To verify whether Export Configurations are showing properly or not after next master AP select	Passed	
MEJ88S_Reg_238	Importing the Configurations after Next master AP Configurations	To verify whether Import Configurations are showing properly or not after next master AP select	Passed	
MEJ88S_Reg_239	802.1x Configurations to AP in CME	To verify whether 802.1x Configurations are Applying to the AP in CME or not	Passed	
MEJ88S_Reg_240	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
MEJ88PH2S_Reg_101	Associating Windows JOS Client with WPA2-dot1x using ISE server in cloud via TLS Tunnel	To verify whether Windows JOS Client associated successfully or not with WPA2-dot1x via ISE server configured in cloud	Passed	

MEJ88PH2S_Reg_102	Associating iOS Client with WPA2-dot1x using ISE server in cloud via TLS Tunnel	To verify whether Apple iOS Client associated successfully or not with WPA2-dot1x via ISE server configured in cloud	Passed	
MEJ88PH2S_Reg_103	Associating MAC OS Client with WPA2-dot1x using ISE server in cloud via TLS Tunnel	To verify whether MAC OS Client associated successfully or not with WPA2-dot1x via ISE server configured in cloud	Passed	
MEJ88PH2S_Reg_104	Associating Android Client with WPA2-dot1x using ISE server in cloud via TLS Tunnel	To verify whether Android Client associated successfully or not with WPA2-dot1x via ISE server configured in cloud	Passed	
MEJ88PH2S_Reg_105	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	
MEJ88PH2S_Reg_106	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	
MEJ88PH2S_Reg_107	Setting up the tunnel configurations in CME	To check whether tunnel status get UP or not after configuring in CME	Passed	
MEJ88PH2S_Reg_108	Checking the ME association with PI after establishing TLS tunnel	To check whether ME is getting synchronized or not with PI	Passed	

MEJ88PH2S_Reg_109	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	
MEJ88PH2S_Reg_110	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	
MEJ88S_Reg_241	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	
MEJ88S_Reg_242	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	
MEJ88S_Reg_243	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	
MEJ88S_Reg_244	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	

MEJ88S_Reg_245	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	
MEJ88S_Reg_246	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	
MEJ88S_Reg_247	Setting up the tunnel configurations in CME	To check whether tunnel status get UP or not after configuring in CME	Passed	
MEJ88S_Reg_248	Checking the ME association with PI	To check whether ME is getting synchronized or not with PI	Passed	
MEJ88S_Reg_249	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	
MEJ88S_Reg_250	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	

Maximum number of clients per WLAN/radio

Logical ID	Title	Description	Status	Defect ID

MEJ88PH2S_Reg_423	Configuring maximum Allowed Clients Per AP Radio as 4 and connecting Client with WPA 2 Personal security.	To configure maximum allowed Client Per AP radio as 4 and connecting 5 different Client with radio policy as ALL and checking if the number of Client that is configured alone gets connected to the WLAN	Passed	
MEJ88PH2S_Reg_424	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	
MEJ88PH2S_Reg_425	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	
MEJ88PH2S_Reg_426	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	

MEJ88PH2S_Reg_427	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	
MEJ88PH2S_Reg_428	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	
MEJ88S_Reg_251	Configuring maximum Allowed Clients Per AP Radio as 4 and connecting Client with WPA 2 Personal security.	To configure maximum allowed Client Per AP radio as 4 and connecting 5 different Client with radio policy as ALL and checking if the number of Client that is configured alone gets connected to the WLAN	Passed	
MEJ88S_Reg_252	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	

MEJ88S_Reg_253	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	
MEJ88S_Reg_254	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	
MEJ88S_Reg_255	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	
MEJ88S_Reg_256	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	

Passive client-ARP

Logical ID	Title	Description	Status	Defect ID

MEJ88PH2S_Reg_351	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	
MEJ88PH2S_Reg_352	Roaming Clients between AP with Arp and Passive Clients in ME	To verify whether Clients are roaming or not with ARP and Passive Client	Passed	
MEJ88PH2S_Reg_353	Enabling proxy and disabling Passive Client for WLAN profile in ME	To verify whether ARP details are transferring to the router or not when proxy is in enable and passive Client disable state	Passed	
MEJ88PH2S_Reg_354	Disabling proxy and enabling Passive Client for WLAN profile in ME	To verify whether ARP details are transferring to the router or not when proxy is in disable and passive Client enable state	Passed	
MEJ88PH2S_Reg_355	Verifying the Client connectivity of a wan profile when Passive Client & proxy are disabled/enabled	To verify whether ARP details are transferring to the router or not when proxy is in enable and passive Client enable state	Passed	
MEJ88S_Reg_257	Enable/Disable Passive Client with multicast IP address	To verify whether Passive Client with multicast enable/disable or not	Passed	
MEJ88S_Reg_258	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	
MEJ88S_Reg_259	Roaming Clients between AP with Arp and passive Clients	To verify whether Clients are roaming or not with ARP and passive Client	Passed	

MEJ88S_Reg_260	Enabling proxy and disabling passive Client for WLAN profile	To verify whether ARP details are transferring to the router or not when proxy is in enable and passive Client disable state	Passed	
MEJ88S_Reg_261	Disabling proxy and enabling passive Client for WLAN profile	To verify whether ARP details are transferring to the router or not when proxy is in disable and passive Client enable state	Passed	
MEJ88S_Reg_262	Verifying the Client connectivity of a wan profile when passive Client and proxy both are disabled or enabled	To verify whether ARP details are transferring to the router or not when proxy is in enable and passive Client enable state	Passed	

SNMP trap receivers

Logical ID	Title	Description	Status	Defect ID
MEJ88PH2S_Reg_95	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	
MEJ88PH2S_Reg_96	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	
MEJ88PH2S_Reg_97	Checking the validation of SNMP trap receiver information.	To check whether the SNMP trap receiver is received the information or not.	Passed	
MEJ88PH2S_Reg_98	Verifying the severity filtering for SNMP trap receiver information.	To verify the severity filtering for SNMP trap receiver information.	Passed	

MEJ88PH2S_Reg_99	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	
MEJ88PH2S_Reg_100	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	
MEJ88S_Reg_263	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	
MEJ88S_Reg_264	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	
MEJ88S_Reg_265	Checking the validation of SNMP trap receiver information.	To check whether the SNMP trap receiver is received the information or not.	Passed	
MEJ88S_Reg_266	Verifying the severity filtering for SNMP trap receiver information.	To verify the severity filtering for SNMP trap receiver information.	Passed	
MEJ88S_Reg_267	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	
MEJ88S_Reg_268	Create the SNMP trap receiver by using the invalid IP address in CME CLI.	To check whether the SNMP trap receiver is created or not in CME CLI	Passed	

CWA (Central Web Authentication)

Logical ID	Title	Description	Status	Defect ID

MEJ88PH2S_Reg_140	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	
MEJ88PH2S_Reg_141	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	
MEJ88PH2S_Reg_142	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	Failed	CSCvk74100
MEJ88PH2S_Reg_143	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	
MEJ88PH2S_Reg_144	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	
MEJ88PH2S_Reg_145	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	
MEJ88PH2S_Reg_146	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	

MEJ88PH2S_Reg_147	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	
MEJ88PH2S_Reg_148	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	
MEJ88PH2S_Reg_149	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	
MEJ88PH2S_Reg_150	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	
MEJ88PH2S_Reg_151	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	
MEJ88PH2S_Reg_152	Validate whether CME is switch between configured Radius servers	To verify whether AAA authentication is occurring when one radius server goes down	Passed	
MEJ88PH2S_Reg_153	Reboot the Controller after CWA enabling	To verify whether Configurations are showing same or different after controller reboot	Passed	

MEJ88PH2S_Reg_154	Creating a CWA along with ACL Configuration through CLI	To verify whether ACL rule is created or not through CLI	Passed	
MEJ88PH2S_Reg_155	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	CSCvm65289
MEJ88PH2S_Reg_156	Exporting/Importing configuration of CWA	To verify whether export and import is done successfully	Passed	
MEJ88S_Reg_269	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	
MEJ88S_Reg_270	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	
MEJ88S_Reg_271	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	
MEJ88S_Reg_272	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	
MEJ88S_Reg_273	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	
MEJ88S_Reg_274	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	

MEJ88S_Reg_275	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	
MEJ88S_Reg_276	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	
MEJ88S_Reg_277	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	
MEJ88S_Reg_278	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	
MEJ88S_Reg_279	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	
MEJ88S_Reg_280	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	
MEJ88S_Reg_281	Validate whether CME is switch between configured Radius servers	To verify whether AAA authentication is occurring when one radius server goes down	Passed	

MEJ88S_Reg_282	Reboot the Controller after CWA enabling	To verify whether Configurations are showing same or different after controller reboot	Passed	
MEJ88S_Reg_283	Creating a CWA along with ACL Configuration through CLI	To verify whether ACL rule is created or not through CLI	Passed	
MEJ88S_Reg_284	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	

Bidirectional rate limit per client

Logical ID	Title	Description	Status	Defect ID
MEJ88PH2S_Reg_332	Configuring rate limit for per Client for different types of Client with WPA 2 Personal security with QOS as Silver	To configure rate limit for JOS Client with open security and QOS as silver and check if the Client gets the rate that is been configured or not.	Passed	
MEJ88PH2S_Reg_333	Configuring rate limit for per Client with QOS as Gold for different types of Client with WPA 2 Enterprise security	To configure rate limit per Client with QOS as Gold and connecting a JOS Client with WPA 2 Enterprise security and check if the rate limit is Applied or not.	Passed	

MEJ88PH2S_Reg_334	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	
MEJ88PH2S_Reg_335	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	
MEJ88PH2S_Reg_336	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	
MEJ88S_Reg_285	Configuring rate limit for per Client for different types of Client with WPA 2 Personal security with QOS as Silver	To configure rate limit for JOS Client with open security and QOS as silver and check if the Client gets the rate that is been configured or not.	Passed	
MEJ88S_Reg_286	Configuring rate limit for per Client with QOS as Gold for different types of Client with WPA 2 Enterprise security	To configure rate limit per Client with QOS as Gold and connecting a JOS Client with WPA 2 Enterprise security and check if the rate limit is Applied or not.	Passed	

MEJ88S_Reg_287	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	
MEJ88S_Reg_288	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	
MEJ88S_Reg_289	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
MEJ88PH2S_Reg_62	To check connectivity of Clients to RLAN configured with Open security	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 the AP and there is flow in traffic	Passed	

MEJ88PH2S_Reg_63	To check connectivity of Client to RLAN configured with Open security and Mac filtering enabled	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 the AP and there is flow in traffic.	Passed	
MEJ88PH2S_Reg_64	To check connectivity of Clients to a RLAN profile configured with 802.1X security with mac filtering Option	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 the AP and there is flow in traffic.	Passed	
MEJ88PH2S_Reg_65	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 .	Passed	
MEJ88PH2S_Reg_66	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 .	Passed	

MEJ88PH2S_Reg_67	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	
MEJ88PH2S_Reg_68	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	
MEJ88PH2S_Reg_69	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	
MEJ88S_Reg_290	To check connectivity of Clients to RLAN configured with Open security	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 the AP and there is flow in traffic	Passed	

MEJ88S_Reg_291	To check connectivity of Client to RLAN configured with Open security and Mac filtering enabled	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 the AP and there is flow in traffic.	Passed	
MEJ88S_Reg_292	To check connectivity of Clients to a RLAN profile configured with 802.1X security with mac filtering Option	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 the AP and there is flow in traffic.	Passed	
MEJ88S_Reg_293	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 .	Passed	
MEJ88S_Reg_294	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 .	Passed	

MEJ88S_Reg_295	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	
MEJ88S_Reg_296	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	
MEJ88S_Reg_297	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	

AAA Override of VLAN Name / VLAN Name-id template

Logical ID	Title	Description	Status	Defect ID
MEJ88PH2S_Reg_167	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	

MEJ88PH2S_Reg_168	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	
MEJ88PH2S_Reg_169	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	
MEJ88PH2S_Reg_170	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	
MEJ88PH2S_Reg_171	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	

MEJ88PH2S_Reg_172	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	
MEJ88PH2S_Reg_173	Connecting a IOS Client to the AAA override enabled WLAN with WPA 2 Enterprise security enabled with AAA override .	To connect a IOS Client to AAA override enabled WLAN with WPA 2 Enterprise security and check if the Native VLAN is overridden or not.	Passed	
MEJ88PH2S_Reg_174	Connecting a MacOS Client to the AAA override enabled WLAN with WPA 2 Enterprise security enabled with AAA override .	To connect a Mac OS Client to AAA override enabled WLAN with WPA 2 Enterprise security and check if the Native VLAN is overridden or not.	Passed	
MEJ88PH2S_Reg_175	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	
MEJ88S_Reg_298	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	

MEJ88S_Reg_299	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	
MEJ88S_Reg_300	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	
MEJ88S_Reg_301	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	
MEJ88S_Reg_302	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	

MEJ88S_Reg_303	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	
MEJ88S_Reg_304	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	
MEJ88S_Reg_305	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	
MEJ88S_Reg_306	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	

P2P Blocking

Logical ID	Title	Description	Status	Defect ID
MEJ88PH2S_Reg_228	Connecting any two different OS Client to a open security WLAN enabling Peer to Peer Block	To connect two JOS Client to a open security WLAN enabling Peer to Peer Block and check if there is a traffic flow between two Clients or not	Passed	

MEJ88PH2S_Reg_229	Connecting two different OS Client to a WPA 2 Personal security WLAN enabling Peer to Peer Block	To connect two JOS Client to a WPA 2 Personal security WLAN enabling Peer to Peer Block and check if there is a traffic flow between two Clients or not	Passed	
MEJ88PH2S_Reg_230	Connecting two different OS Client to a WPA 2 Enterprise security WLAN enabling Peer to Peer Block	To connect two JOS Client to a WPA 2 Enterprise security WLAN enabling Peer to Peer Block and check if there is a traffic flow between two Clients or not	Passed	
MEJ88PH2S_Reg_231	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	
MEJ88PH2S_Reg_232	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	
MEJ88PH2S_Reg_233	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	

MEJ88PH2S_Reg_234	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	
MEJ88S_Reg_307	Connecting any two different OS Client to a open security WLAN enabling Peer to Peer Block	To connect two JOS Client to a open security wan enabling Peer to Peer Block and check if there is a traffic flow between two Clients or not	Passed	
MEJ88S_Reg_308	Connecting two different OS Client to a WPA 2 Personal security WLAN enabling Peer to Peer Block	To connect two JOS Client to a WPA 2 Personal security wan enabling Peer to Peer Block and check if there is a traffic flow between two Clients or not	Passed	
MEJ88S_Reg_309	Connecting two different OS Client to a WPA 2 Enterprise security WLAN enabling Peer to Peer Block	To connect two JOS Client to a WPA 2 Enterprise security wan enabling Peer to Peer Block and check if there is a traffic flow between two Clients or not	Passed	
MEJ88S_Reg_310	Connecting four different Client to a open security WLAN enabling Peer to Peer Block	To connect four different Client to a open security wan enabling Peer to Peer Block and check if there is a traffic flow between two Clients or not	Passed	
MEJ88S_Reg_311	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 wan enabling Peer to Peer Block and check if there is a traffic flow between two Clients or not	Passed	

MEJ88S_Reg_312	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 wan enabling Peer to Peer Block and check if there is a traffic flow between two Clients or not	Passed	
MEJ88S_Reg_313	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	

Global AP configuration & 802.1x support with EAP-TLS and EAP-PEAP

Logical ID	Title	Description	Status	Defect ID
MEJ88PH2S_Reg_356	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	
MEJ88PH2S_Reg_357	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	
MEJ88PH2S_Reg_358	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	
MEJ88PH2S_Reg_359	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	

MEJ88PH2S_Reg_360	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	
MEJ88PH2S_Reg_361	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	
MEJ88PH2S_Reg_362	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	
MEJ88PH2S_Reg_363	Enabling dot1x auth for AP in 3850 Switch	Configuring the 3850 Switch for Dot1x authentication by mapping the identity profiles to a port.	Passed	
MEJ88PH2S_Reg_364	Checking the configuration of 802.1x authentication parameters after export/import the config file	To check whether 802.1x auth parameters restores or not after export/import the config file in ME UI via TFTP	Passed	
MEJ88PH2S_Reg_365	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	
MEJ88PH2S_Reg_366	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	

MEJ88PH2S_Reg_367	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	
MEJ88PH2S_Reg_368	Trying to configure of 802.1x authentication parameters via Read-only User	To check whether Read only user can be able to configure or not the 802.1x auth parameters in ME UI	Passed	
MEJ88S_Reg_314	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	
MEJ88S_Reg_315	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	
MEJ88S_Reg_316	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	
MEJ88S_Reg_317	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	
MEJ88S_Reg_318	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	

MEJ88S_Reg_319	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	
MEJ88S_Reg_320	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	
MEJ88S_Reg_321	Enabling dot1x auth for AP in 3850 Switch	Configuring the 3850 Switch for Dot1x authentication by mapping the identity profiles to a port.	Passed	
MEJ88S_Reg_322	Checking the configuration of 802.1x authentication parameters after export/import the config file	To check whether 802.1x auth parameters restores or not after export/import the config file in ME UI via TFTP	Passed	
MEJ88S_Reg_323	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	
MEJ88S_Reg_324	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	
MEJ88S_Reg_325	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	

MEJ88S_Reg_326	Trying to configure of 802.1x authentication parameters via Read-only User	To check whether Read only user can be able to configure or not the 802.1x auth parameters in ME UI	Passed	

Ethernet Fallback

Logical ID	Title	Description	Status	Defect ID
MEJ88PH2S_Reg_111	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	
MEJ88PH2S_Reg_112	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	
MEJ88PH2S_Reg_113	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	
MEJ88PH2S_Reg_114	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	
MEJ88PH2S_Reg_115	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	

MEJ88PH2S_Reg_116	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	
MEJ88PH2S_Reg_117	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	
MEJ88PH2S_Reg_118	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	
MEJ88S_Reg_327	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	
MEJ88S_Reg_328	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	
MEJ88S_Reg_329	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	
MEJ88S_Reg_330	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	

MEJ88S_Reg_331	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	
MEJ88S_Reg_332	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	
MEJ88S_Reg_333	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	
MEJ88S_Reg_334	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	

Dynamic OUI update

Logical ID	Title	Description	Status	Defect ID
MEJ88PH2S_Reg_119	OUI file uploading via TFTP server In ME UI	To check whether OUI file is uploading or not via TFTP server	Passed	
MEJ88PH2S_Reg_120	OUI file uploading via TFTP server In ME CLI	Validate the OUI file is uploading or not in ME CLI	Passed	
MEJ88PH2S_Reg_121	Uploading the invalid OUI file through via TFTP server	Verify Invalid OUI file is uploading or not via TFTP sever	Passed	
MEJ88PH2S_Reg_122	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	

MEJ88PH2S_Reg_123	OUI file uploading via HTTP server in ME CLI	validate via http server OUI file is uploading or not in ME CLI	Passed	
MEJ88PH2S_Reg_124	Invalid OUI File uploading via HTTP sever	Validate Invalid OUI file is uploading or not via HTTP server	Passed	
MEJ88PH2S_Reg_125	Uploading the OUI file via FTP server in ME UI	To check whether OUI file is uploading or not	Passed	
MEJ88PH2S_Reg_126	Uploading the OUI file via FTP server in ME CLI	Validate the OUI file is uploading via ftp server in ME CLI	Passed	
MEJ88PH2S_Reg_127	Invalid OUI File uploading via FTP sever	To check whether Invalid OUI file is uploading or not via FTP server	Passed	
MEJ88S_Reg_335	OUI file uploading via TFTP server In ME UI	To check whether OUI file is uploading or not via TFTP server	Passed	
MEJ88S_Reg_336	OUI file uploading via TFTP server In ME CLI	Validate the OUI file is uploading or not in ME CLI	Passed	
MEJ88S_Reg_337	Uploading the invalid OUI file through via TFTP server	Verify Invalid OUI file is uploading or not via TFTP sever	Passed	
MEJ88S_Reg_338	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	
MEJ88S_Reg_339	OUI file uploading via HTTP server in ME CLI	validate via http server OUI file is uploading or not in ME CLI	Passed	
MEJ88S_Reg_340	Invalid OUI File uploading via HTTP sever	Validate Invalid OUI file is uploading or not via HTTP server	Passed	

MEJ88S_Reg_341	Uploading the OUI file via FTP server in ME UI	To check whether OUI file is uploading or not	Passed	
MEJ88S_Reg_342	Uploading the OUI file via FTP server in ME CLI	Validate the OUI file is uploading via ftp server in ME CLI	Passed	
MEJ88S_Reg_343	Invalid OUI File uploading via FTP sever	To check whether Invalid OUI file is uploading or not via FTP server	Passed	

Software update using SFTP

Logical ID	Title	Description	Status	Defect ID
MEJ88PH2S_Reg_128	ME AP1815 Software updating via SFTP server	Verifying AP 1815 ME software updating or not via SFTP server	Passed	
MEJ88PH2S_Reg_129	Invalid software updating via SFTP server for ME AP 1815	To check whether Invalid software updating or not via SFTP server	Passed	
MEJ88PH2S_Reg_130	Software Schedule Update on ME AP 1830 via SFTP server	Validate the software Schedule Update on ME AP1830 via SFTP server	Passed	
MEJ88PH2S_Reg_131	Software Update on ME AP 1850 via SFTP server	Verifying AP 1850 ME software updating or not via SFTP server	Passed	
MEJ88PH2S_Reg_132	Invalid software updating via SFTP server on ME AP 1850	Verifying whether Invalid software updating or not on ME AP 1850	Passed	
MEJ88PH2S_Reg_133	Schedule the Software update on 1850 ME AP	Verifying on schedule time ME software is updating or not	Passed	
MEJ88PH2S_Reg_134	Software updating via SFTP server on ME 2800AP	To check whether software is updating or not via SFTP server on 2800AP	Passed	

MEJ88PH2S_Reg_135	Invalid software updating on ME 2800AP via SFTP software	Verifying whether Invalid software updating or not on ME AP2800	Passed	
MEJ88PH2S_Reg_136	Software Update Schedule on ME AP2800 via SFTP server	Validate the software Schedule Update on ME AP2800 via SFTP server	Passed	
MEJ88PH2S_Reg_137	Software updating via SFTP server on ME 3800AP	To check whether software is updating or not via SFTP server on 3800AP	Passed	
MEJ88PH2S_Reg_138	Invalid software updating on ME 3800AP via SFTP software	Verifying whether Invalid software updating or not on ME AP3800	Passed	
MEJ88PH2S_Reg_139	Software Update Schedule on ME AP3800 via SFTP server	Validate the software Schedule Update on ME AP3800 via SFTP server	Passed	
MEJ88S_Reg_344	ME AP1830 Software updating via SFTP server	Verifying AP 1830 ME software updating or not via SFTP server	Passed	
MEJ88S_Reg_345	Invalid software updating via SFTP server for ME AP 1830	To check whether Invalid software updating or not via SFTP server	Passed	
MEJ88S_Reg_346	Software Schedule Update on ME AP 1830 via SFTP server	Validate the software Schedule Update on ME AP1830 via SFTP server	Passed	
MEJ88S_Reg_347	Software Update on ME AP 1850 via SFTP server	Verifying AP 1850 ME software updating or not via SFTP server	Passed	
MEJ88S_Reg_348	Invalid software updating via SFTP server on ME AP 1850	Verifying whether Invalid software updating or not on ME AP 1850	Passed	

MEJ88S_Reg_349	Schedule the Software update on 1850 ME AP	Verifying on schedule time ME software is updating or not	Passed	
MEJ88S_Reg_350	Software updating via SFTP server on ME 2800AP	To check whether software is updating or not via SFTP server on 2800AP	Passed	
MEJ88S_Reg_351	Invalid software updating on ME 2800AP via SFTP software	Verifying whether Invalid software updating or not on ME AP2800	Passed	
MEJ88S_Reg_352	Software Update Schedule on ME AP2800 via SFTP server	Validate the software Schedule Update on ME AP2800 via SFTP server	Passed	
MEJ88S_Reg_353	Software updating via SFTP server on ME 3800AP	To check whether software is updating or not via SFTP server on 3800AP	Passed	
MEJ88S_Reg_354	Invalid software updating on ME 3800AP via SFTP software	Verifying whether Invalid software updating or not on ME AP3800	Passed	
MEJ88S_Reg_355	Software Update Schedule on ME AP3800 via SFTP server	Validate the software Schedule Update on ME AP3800 via SFTP server	Passed	

Import EAP certificate

Logical ID	Title	Description	Status	Defect ID
MEJ88PH2S_Reg_313	Downloading the EAP device certificate through HTTP	To verify whether EAP device certificate is downloading or not through HTTP mode	Passed	
MEJ88PH2S_Reg_314	downloading the EAP device certificate via SFTP	To verify whether EAP device certificate is downloading or not through SFTP	Passed	

MEJ88PH2S_Reg_315	Downloading the EAP device certificate through FTP	To verify whether EAP device certificate is downloading or not through FTP mode	Passed	
MEJ88PH2S_Reg_316	Downloading the EAP device certificate through TFTP	To verify whether EAP device certificate is downloading or not through TFTP mode	Passed	
MEJ88PH2S_Reg_317	Downloading the EAP CA certificate through HTTP	To verify whether EAP CA certificate is downloading or not through HTTP mode	Passed	
MEJ88PH2S_Reg_318	Downloading the EAP CA certificate through FTP	To verify whether EAP CA certificate is downloading or not through FTP mode	Passed	
MEJ88PH2S_Reg_319	Downloading the EAP CA certificate through SFTP	To check whether EAP CA certificate is downloading or not through SFTP server	Passed	
MEJ88PH2S_Reg_320	Downloading the EAP CA certificate through TFTP	To verify whether EAP CA certificate is downloading or not through TFTP mode	Passed	
MEJ88PH2S_Reg_321	Downloading the NA SERV CA Certificate through HTTP	To verify whether NA SERV CA Certificate is downloading or not through HTTP mode	Passed	
MEJ88PH2S_Reg_322	Downloading the NA SERV CA Certificate through FTP	To verify whether NA SERV CA Certificate is downloading or not through FTP mode	Passed	
MEJ88PH2S_Reg_323	Downloading the NA SERV CA Certificate through SFTP	To check whether NA SERV CA Certificate is downloading or not through SFTP mode	Passed	

MEJ88PH2S_Reg_324	Downloading the NA SERV CA Certificate through TFTP	To verify whether NA SERV CA Certificate is downloading or not through TFTP mode	Passed	
MEJ88PH2S_Reg_325	Initiate the download with read-only mode	To verify whether image download initiating or not for read-only user or not	Passed	
MEJ88PH2S_Reg_326	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	
MEJ88PH2S_Reg_327	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	
MEJ88PH2S_Reg_328	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	
MEJ88PH2S_Reg_329	Initiating the certificates(EAP,EAP CA,NA SEV) download through SFTP from CLI	To verify whether certificate is downloading or not from SFTP mode through CLI	Passed	
MEJ88PH2S_Reg_330	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	
MEJ88PH2S_Reg_331	Initiating the download through read-only mode	To verify whether certificate are downloading or not read-only user	Passed	
MEJ88S_Reg_356	Downloading the EAP device certificate through HTTP	To verify whether EAP device certificate is downloading or not through HTTP mode	Passed	

MEJ88S_Reg_357	Downloading the EAP device certificate through FTP	To verify whether EAP device certificate is downloading or not through FTP mode	Passed	
MEJ88S_Reg_358	Downloading the EAP device certificate through TFTP	To verify whether EAP device certificate is downloading or not through TFTP mode	Passed	
MEJ88S_Reg_359	Downloading the EAP CA certificate through HTTP	To verify whether EAP CA certificate is downloading or not through HTTP mode	Passed	
MEJ88S_Reg_360	Downloading the EAP CA certificate through FTP	To verify whether EAP CA certificate is downloading or not through FTP mode	Passed	
MEJ88S_Reg_361	Downloading the EAP CA certificate through TFTP	To verify whether EAP CA certificate is downloading or not through TFTP mode	Passed	
MEJ88S_Reg_362	Downloading the NA SERV CA Certificate through HTTP	To verify whether NA SERV CA Certificate is downloading or not through HTTP mode	Passed	
MEJ88S_Reg_363	Downloading the NA SERV CA Certificate through FTP	To verify whether NA SERV CA Certificate is downloading or not through FTP mode	Passed	
MEJ88S_Reg_364	Downloading the NA SERV CA Certificate through TFTP	To verify whether NA SERV CA Certificate is downloading or not through TFTP mode	Passed	
MEJ88S_Reg_365	Changing the OUI String values	To verify whether OUI sting values are changing or not	Passed	
MEJ88S_Reg_366	Initiating the download with invalid file name	To verify whether Invalid file name is accepting or not	Passed	

MEJ88S_Reg_367	Initiate the download with read-only mode	To verify whether image download initiating or not for read-only user or not	Passed	
MEJ88S_Reg_368	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	
MEJ88S_Reg_369	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	
MEJ88S_Reg_370	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	
MEJ88S_Reg_371	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	
MEJ88S_Reg_372	Checking the certification details through CLI for read-only users	To verify whether certificate details are showing properly or not for read-only users	Passed	
MEJ88S_Reg_373	Initiating the download through read-only mode	To verify whether certificate are downloading or not read-only user	Passed	
MEJ88S_Reg_374	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
MEJ88PH2S_Reg_157	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	

MEJ88PH2S_Reg_158	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	
MEJ88PH2S_Reg_159	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 calming the device in day2	Passed	
MEJ88PH2S_Reg_160	Provisioning the1815 ME in day0 via claiming the device	Verify that user is able to Provisioned the 1815 ME in day0 via calming the device in day3	Passed	
MEJ88PH2S_Reg_161	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	
MEJ88PH2S_Reg_162	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	
MEJ88PH2S_Reg_163	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	
MEJ88PH2S_Reg_164	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	
MEJ88PH2S_Reg_165	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	
MEJ88PH2S_Reg_166	Applying the config after image download	Verify that user can Apply the config file on provisioned device image download or not	Passed	

MEJ88S_Reg_375	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	
MEJ88S_Reg_376	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	
MEJ88S_Reg_377	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 calming the device in day2	Passed	
MEJ88S_Reg_378	Provisioning the1815 ME in day0 via claiming the device	Verify that user is able to Provisioned the 1815 ME in day0 via calming the device in day3	Passed	
MEJ88S_Reg_379	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	
MEJ88S_Reg_380	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	
MEJ88S_Reg_381	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	
MEJ88S_Reg_382	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	
MEJ88S_Reg_383	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	

MEJ88S_Reg_384	Applying the config after image download	Verify that user can Apply the config file on provisioned device image download or not	Passed	

Conversion of AP type default configuration from CAPWAP to Cisco Mobility Express

Logical ID	Title	Description	Status	Defect ID
MEJ88PH2S_Reg_37	Joining the AP image with less than other than ME and checking the details	To verify whether AP join to the CME and downloading the image or not	Passed	
MEJ88PH2S_Reg_38	Joining the AP after Efficient join enable/Disable state	To verify whether AP is joining & downloading image from ME or not after efficient join enable state	Passed	
MEJ88PH2S_Reg_39	COS AP with CAPWAP image joins to ME WLC with	To verify whether COS AP is joining to the ME with ME capable or not	Failed	CSCvm17349
MEJ88PH2S_Reg_40	IOS AP with CAPWAP image joins to ME WLC	To verify whether IOS AP is joining to the ME with AP & ME different version and not downloading the image	Passed	
MEJ88PH2S_Reg_41	Upgrading the ME image and making the CAPWAP APs to ME capable	To verify whether APs converting the ME capable or not after upgrade the ME image	Passed	
MEJ88PH2S_Reg_42	Downgrading the ME image and making the CAPWAP APs to ME capable	To verify whether APs converting the ME capable or not after downgrade the ME image	Passed	

MEJ88PH2S_Reg_43	Removing the Master AP at the time of AP downloading the image	To verify whether it is possible to remove the Master AP at the time of AP downloading the image	Passed	
MEJ88PH2S_Reg_44	Changing the ME time and trying to join the AP	To verify whether AP joining to the ME or not with AP and ME times are different	Passed	
MEJ88PH2S_Reg_45	Performing the Master AP failover	To verify whether after Master AP failover, AP is again downloading the images or not	Passed	
MEJ88PH2S_Reg_46	Interchanging the ME image	To verify whether after image interchange ME coming as changed version or not	Passed	
MEJ88PH2S_Reg_47	Interchanging the AP image and making as ME Controller	To verify whether after AP interchange, AP is coming as changed image with ME capable controller or not	Passed	

AP does not reboot when it joins an AP group

Logical ID	Title	Description	Status	Defect ID
MEJ88PH2S_Reg_48	Creating the AP group with Japanese Language and assigning the COS AP	To verify whether AP associating to the AP group or not	Passed	
MEJ88PH2S_Reg_49	Moving the 1852/1832 COS AP between different Groups in CME(1800/2800/3800/1500)	To verify whether 1852/1832 COS AP Changing the groups or not without reboot in 1800/2800/3800/1500 CME models	Passed	
MEJ88PH2S_Reg_50	Moving the 1542/1562 COS AP between different AP Groups in CME(1800/2800/3800/1500)	To verify whether 1542/1562 COS AP moving between different groups or not without reboot in CME(1800/2800/3800/1500)	Passed	

MEJ88PH2S_Reg_51	Moving the 2802I COS AP between different AP Groups in CME(1800/2800/3800/1500)	To verify whether 2802I2 COS AP moving between different groups or not without reboot in CME(1800/2800/3800/1500)	Passed	
MEJ88PH2S_Reg_52	Moving the 3802I/3802E COS AP between different AP Groups in CME(1800/2800/3800/1500)	To verify whether 3802I/3802E COS AP moving between different groups or not without reboot in CME(1800/2800/3800/1500)	Passed	
MEJ88PH2S_Reg_53	Moving the 1815I/1810 COS AP between different AP Groups in CME(1800/2800/3800/1500)	To verify whether 1815I/1810 COS AP moving between different groups or not without reboot in CME(1800/2800/3800/1500)	Passed	
MEJ88PH2S_Reg_54	Changing the AP between groups at the time of software upgrade/downgrade	To verify whether it is possible to change the AP group or not at the time upgrading the image	Passed	
MEJ88PH2S_Reg_55	Master/Next-preferred AP Changing between different groups at the time of software upgrade/downgrade	To verify whether after AP group change Master/Next-preferred AP downloading the image or not	Passed	
MEJ88PH2S_Reg_56	Changing the AP between different AP group in read-only mode	To verify whether AP is Changing the Groups or not in read-only mode	Passed	
MEJ88PH2S_Reg_57	Moving the 702/3700/2700 IOS AP between different AP Groups in CME(1800/2800/3800/1500)	To verify whether 702/3700/2700 COS AP moving between different groups or not without reboot in CME(1800/2800/3800/1500)	Passed	
MEJ88PH2S_Reg_58	Assigning the default RF-Profile to AP group from PI	To verify whether default RF-Profile is Applying to the AP-group or not	Failed	CSCvm78435
MEJ88PH2S_Reg_59	Assigning the user defined RF-Profile with 2.4/5 GHZ to AP group from PI	To verify whether user defined RF-profile with 2.4/5GHZ is Applying to the AP-group or not	Passed	
MEJ88PH2S_Reg_60	Changing the COS APs between different AP-groups from PI	To verify whether COS APS are changing successfully between AP groups without reboot or not	Passed	
MEJ88PH2S_Reg_61	Changing the IOS APs between different AP-groups from PI	To verify whether IOS APS are changing successfully between AP groups without reboot or not	Passed	

ME AP convert to CAPWAP via DHCP Option

Logical ID	Title	Description	Status	Defect ID
MEJ88PH2S_Reg_399	Change the 1852 ME AP type to CAPWAP using DHCP 43	To change the AP type to CAPWAP using DHCP 43	Passed	
MEJ88PH2S_Reg_400	Change the 2800 ME AP type to CAPWAP using DHCP 43	To change the AP type to CAPWAP using DHCP 43	Passed	
MEJ88PH2S_Reg_401	Change the 1542 ME AP type to CAPWAP using DHCP 43	To change the AP type to CAPWAP using DHCP 43	Passed	
MEJ88PH2S_Reg_402	Change the 1815i ME AP type to CAPWAP using DHCP 43	To change the AP type to CAPWAP using DHCP 43	Passed	
MEJ88PH2S_Reg_403	Change the AP mode after converting in to CAPWAP	To change the AP mode after converting in to CAPWAP	Passed	
MEJ88PH2S_Reg_404	Connect iOS Client to CAPWAP converted AP from ME with WPA2-PSK security	To connect the iOS Client to CAPWAP converted AP from ME with WPA2-PSK security	Passed	
MEJ88PH2S_Reg_405	Connect Android Client to CAPWAP converted AP from ME with WPA2-PSK security	To connect the Android Client to CAPWAP converted AP from ME with WPA2-PSK security	Passed	
MEJ88PH2S_Reg_406	Config primary, secondary controller in AP and reload ME controller	To verify that ME changed to CAPWAP and send join request to controller that configured using DHCP option 43	Passed	
MEJ88PH2S_Reg_407	Config two controller IP in DHCP option 43 and first should be wrong IP	To verify that AP joined to second controller if first IP is wrong in DHCP	Passed	

MEJ88PH2S_Reg_408	Change the 1815i ME AP type to CAPWAP using DHCP 43 and join in to awl	To change the AP type to CAPWAP using DHCP 43and join in to awl	Passed	
MEJ88PH2S_Reg_409	Make the Preferred Master one ME capable AP and reload ME Controller	To verify that ME Controller changed to CAPWAP after make Preferred master as another ME capable AP	Passed	

Cisco DNA Center Support for ME

Logical ID	Title	Description	Status	Defect ID
MEJ88PH2S_Reg_188	Adding the ME in Cisco DNA Center via inventory method	Verify that user is able to add ME in Cisco DNA Center via inventory method or not	Passed	
MEJ88PH2S_Reg_189	Exporting the CSV file of CME from Cisco DNA Center using Credential export type	To check whether the exported CSV file using Credential export type has correct information of CME	Passed	
MEJ88PH2S_Reg_190	Adding CME to Cisco DNA Center by Importing CSV file using Credential export type	To check whether the user is able to add CME device in Cisco DNA Center by importing CSV file exported using Credential export type	Passed	
MEJ88PH2S_Reg_191	Exporting the CSV file of CME from Cisco DNA Center using data export type	To check whether the exported CSV file using data export type has correct information of CME	Passed	
MEJ88PH2S_Reg_192	Adding CME to Cisco DNA Center by Importing CSV file using data export type	To check whether user is able to import the CSV file or not	Passed	

MEJ88PH2S_Reg_193	Creating WLAN through Enterprise Wireless with different level of security type and with advanced security types like MAC Filtering & Fast Transition	Checking whether SSID is created or not with the selected security type	Passed	
MEJ88PH2S_Reg_194	Creating Guest Wireless for adding ISE or any other External Authentication	Verifying whether user can add ISE or another External authentic an in Guest Wireless network	Passed	
MEJ88PH2S_Reg_195	Creating Wireless Interface and Wireless Radio Frequency Profile	To check whether Wireless interface are created or not and modifying radio frequency to our requirements.	Passed	
MEJ88PH2S_Reg_196	Creating Sensor SSID with WPA2 Enterprise, WPA2 Personal, Open with anyone of the security type	Checking whether Sensor SSID is created or not with the selected security type	Passed	
MEJ88PH2S_Reg_197	Adding CMX in Cisco DNA Center	To check whether the user is able to add CMX in Cisco DNA Center or not	Passed	
MEJ88PH2S_Reg_198	Provisioning ME via Cisco DNA Center	Verify that user is able to add ME in Cisco DNA Center via provisioning method or not	Passed	
MEJ88PH2S_Reg_199	Importing maps from Cisco DNA Center	To import maps from Cisco DNA Center and check if the maps gets imported to the cmx .	Passed	
MEJ88PH2S_Reg_200	Adding Access Points from CME to the imported maps from Cisco DNA Center to CMX	To check whether the imported Access Points are shown correctly in CMX or not	Passed	

MEJ88PH2S_Reg_201	Checking the Client details by connecting to the Access Points	Connecting the Client to the Access Points and checking the connectivity	Passed	
MEJ88PH2S_Reg_202	Discovering CME device IP in Cisco DNA Center	To check whether the added CME device IP is discovered in Cisco DNA Center or not	Passed	
MEJ88PH2S_Reg_203	Updating the credentials, in CME and checking the same in Cisco DNA Center	Verifying whether the updated credentials are reflected in Cisco DNA Center or not	Passed	
MEJ88PH2S_Reg_204	Updating the management IP in CME and checking the same in Cisco DNA Center	Connecting the Client to the Access Points and checking the connectivity	Passed	
MEJ88PH2S_Reg_205	Resync CME in Cisco DNA Center after updating the management IP and check the resync interval	Verifying whether CME resyncs with Cisco DNA Center successfully or not after updating management IP	Passed	
MEJ88PH2S_Reg_206	Using Launch Command Runner we can execute the CLI commands for selected device from the inventory	Verifying whether CLI commands are executed successfully or not for selected the device from the inventory	Passed	
MEJ88PH2S_Reg_207	Upgrading CME OS image from Cisco DNA Center	Upgrading the OS image for CME through Cisco DNA Center and checking whether CME is upgraded or not from CME GUI.	Passed	

CMX 10.5 Support

Logical ID	Title	Description	Status	Defect ID

MEJ88PH2S_Reg_208	Adding Cisco CME to CMX	To add a Cisco CME to CMX and check if the CME gets added to the CMX with the CME status showing	Passed	
MEJ88PH2S_Reg_209	Importing maps from prime infrastructure	To import maps from prime infrastructure and check if the maps gets imported to the cmx .	Passed	
MEJ88PH2S_Reg_210	Importing the maps with Access points from PI to CMX	To import the maps from prime infra to CMX with Access points and check if the access point details are shown correctly including Clients connected .	Passed	
MEJ88PH2S_Reg_211	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	
MEJ88PH2S_Reg_212	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	
MEJ88PH2S_Reg_213	Using MAC address the Client devices are searched	To check whether Client device can be searched by specifying its MAC address or not	Passed	
MEJ88PH2S_Reg_214	Using IP address the Client devices are searched	To check whether Client device can be searched by specifying its IP address or not	Passed	

MEJ88PH2S_Reg_215	Using SSID the Client devices are searched	To verify whether Client device can be searched by specifying the SSID or not	Passed	
MEJ88PH2S_Reg_216	Number of Clients visiting the building and floor in hourly and daily basis	Verifying the number of Clients visiting the building or floor on hourly and daily basis	Passed	
MEJ88PH2S_Reg_217	Number of Client visits to the building and the floor	To check the number of new Clients and repeated Clients to the building or floor .	Passed	

Aging Test Cases

Logical ID	Title	Description	Status	Defect ID
MEJ88PH2S_Reg_381	Trasfering the data via http between IOS client with fastlane enabled app	Transfering the traffic between two IOS client with fastlane coverage	Passed	
MEJ88PH2S_Reg_382	Validate the Application library scenarios by adding applications in the Ixchariot	To validate the Application in the Ixchariot library and check the output of each library	Passed	
MEJ88PH2S_Reg_383	Transfering the data via UDP and measure the throughput between Windows and IOS client with fastlane enabled wlan	Verify that user is able to transfer the data via UDP and measure the throughput between IOS and non IOS client with fastlane enabled wlan	Passed	
MEJ88PH2S_Reg_384	Measuring the throughput of TCP packets between client	To mesure throughput of TCP packet tranfer between client	Passed	

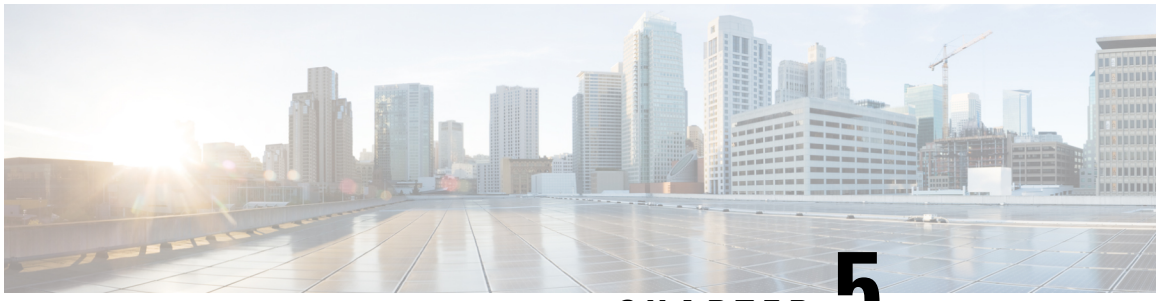
MEJ88PH2S_Reg_385	Connecting the IOS and android/windows/mac client with flexconnect mode ap and performe UDP perfomance test	Testing the UDP performance between different client that associated with flexconnect mode ap	Passed	
MEJ88PH2S_Reg_386	Connecting the client with flexconnect mode ap and perform the measeue the TCP perfomance	Testing the TCP performance between different client that associated with flexconnect mode ap	Passed	
MEJ88PH2S_Reg_387	Connecting the IOS client with fast lane coverage wlan and test the facetime app througput	Measure the performance of factime app with fastlane coverage	Passed	
MEJ88PH2S_Reg_388	Connecting a client and stream a video file and check the performance of the client using IXchariot	To stream a video from the client and check if the streaming occurs without any lag in performance using the IX chariot	Passed	
MEJ88PH2S_Reg_389	Connecting a client continueously to the same WLAN by disconnecting and connecting	To connect the same client to the same WLAN by connecting and disconnecting contineously and check the behaviour .	Passed	
MEJ88PH2S_Reg_390	Throughput test using the 5 GHz radio using Ixchariot for 2 to 3 hours	To test the throughput of the 5 GHz radio using Ixchariot for a period of 2 to 3 hours	Passed	
MEJ88PH2S_Reg_391	Throughput test using the 2.4 GHz radio using Ixchariot for 2 to 3 hours	To test the throughput of the 2.4 GHz radio using Ixchariot for a period of 2 to 3 hours	Passed	

MEJ88PH2S_Reg_392	Configuring session timeout for the client and monitoring the client activity	To configure the session timeout for the clients and monitoring the client activity .	Passed	
MEJ88PH2S_Reg_393	Checking the RSSI values after client connect to the WLAN near to AP	To verify whether RSSI values are showing properly or not after client connected to the WLAN	Passed	
MEJ88PH2S_Reg_394	Checking the RSSI values after client connect to the WLAN with certain range	To verify whether Client is showing the proper RSSI details or not	Passed	
MEJ88PH2S_Reg_395	Perfoming the PING test after client connect	To verify whether PING test is performing or not after client connect	Passed	
MEJ88PH2S_Reg_396	Capturing the TCP Packets after Client connected to WLAN	To verify whether TCP Packets are transfering or not after client connect	Passed	
MEJ88PH2S_Reg_397	Capturing the UDP Packets after client connect to WLAN	To verify whether UDP packets are transfering or not	Passed	
MEJ88PH2S_Reg_398	Performing the FTP operation after client connected to WLAN	To verify whether FTP operation is performing or not	Passed	

Mobexp

Logical ID	Title	Description	Status	Defect Id
MEJ88S_mobexp_01	Changing AP details for sensor mode AP in ME	Verfying AP details can be changed after changing to sensor mode	Passed	
MEJ88S_mobexp_02	configuring RRC parameters under media-stream from UI and CLI	Verfying RRC parameters can be configured same in CLI & UI or not	Passed	

MEJ88S_mobexp_03	Verfying system details by the command "show system slabtop command"	Verfying " show system slabtop" command is executing properly or not	Failed	CSCvj70836
MEJ88S_mobexp_04	Verfying the ME CLI commands under mob-exp	Checking mob-exp CLI commands are executing properly or nor every time	Passed	
MEJ88S_mobexp_05	Changing WLAN admin status during Schedule interval from current state	Verifying whether WLAN admin status changing to expected hours during scheduled interval	Failed	CSCvk05680
MEJ88S_mobexp_06	Checking Radius server status admin accounts and WLAN page.	Checking both admin account and WLAN page displaying same radius server status in UI.	Failed	CSCvk25119
MEJ88S_mobexp_07	Checking WLAN admin state by creating WLAn after scheduled hours	Checking whether admin status is working as expected after scheduled hours.	Failed	CSCvk32119
MEJ88S_mobexp_08	Creating Pre-auth acl's for RLAN in ME UI	Checking whether pre-auth acl is displaying for RLAN in ME UI	Failed	CSCvk47740



CHAPTER 5

Related Documents

Related Documentation

CME 8.8 release Notes

https://www.cisco.com/c/en/us/td/docs/wireless/access_point/mob_exp/88/release_notes/b_ME_RN_88.html

WLC 8.8 Configuration Guide

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-8/config-guide/b_cg88/monitoring_cisco_wlc.html

CMX 10.5 Configuration Guide

https://www.cisco.com/c/en/us/td/docs/wireless/mse/10-5/cmx_config/b_cg_cmx105/getting_started_with_cisco_cmx.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.html

ISE 2.4 Release Notes

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