Test Results Summary for Cisco Prime Infrastructure 3.6 for Japan (Release Version 3.6.0.0.172)

First Published: 2019-04-26

Last Modified: 2019-05-13

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

CONTENTS

CHAPTER 1 **Overview** 1

Prime Infrastructure test 1

CHAPTER 2 **Test Topology and Environment Matrix** 7

Test Topology 7

Component Matrix 8

What's New ? 10

Open Caveats 11

Resolved Caveats 11

CHAPTER 3 **New Features - Test Summary** 13

eWLC Support in Prime 13

Support for IRCM Feature 18

CHAPTER 4 **Regression Features - Test Summary** 21

Custom Reports 22

Config Group Phase 2 29

Network Health- Wireless Client and Rogue 30

Next Generation Maps 32

DHCP Server to ME 35

TrustSec SGT/SG ACL for Wireless (WLC) 36

MAC filtering capability for lobby ambassadors 37

Domain based URL ACL enhancement 38

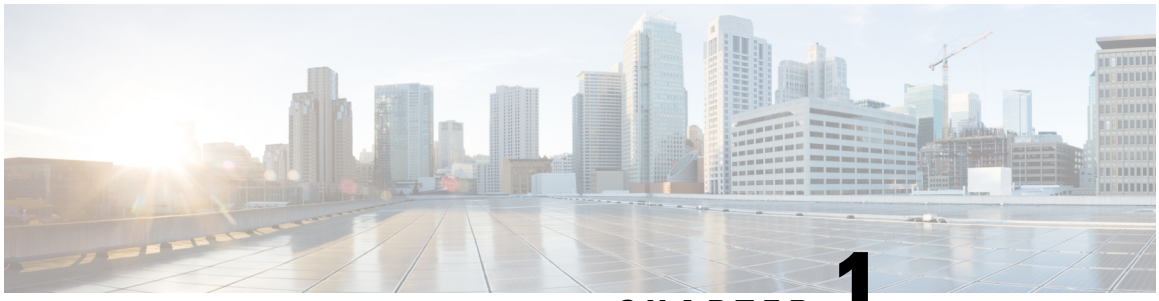
Autonomous to LWAPP Migration 39

High Availability 40

Flex AVC 41

APIC-EM Controller 42
SWIM Enhancement 44
HA Enhancements 45
End to end CMX Integration testing 45
Rolling AP Upgrade 47
Monitor Mode support in APs (1810/1815) 49
AP Health Extension 51
WLC Health Scoring 52
EOGRE Profile 55
Support Flex + Bridge mode configuration for Access points 58
Open DNS Support 60
Support hyperlocation config enhancement in Lightweight AP template 61
Outdoor AP GPS support 62
Scheduled AP upgrade 63
Support Mobility Express on Maps 65
Audit Logging for Maps/Wireless 67
Support for Zero Touch Deployment for ME-AP 69
Better HA Monitoring and Management 71
SWIM Support of Mobility Express Controllers 72
TACACS+ & RADIUS servers added without any authentication 73
eWLC Support for Airtime Entitlement 76
Support for AP 4800 in PI 80
Manage 4800 ME controller in Prime 85
Config Wireless 90

CHAPTER 5 **Related Documentation** 91



CHAPTER 1

Overview

- **Prime Infrastructure test** , on page 1

Prime Infrastructure test

Cisco Prime Infrastructure 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 Prime Infrastructure 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 PI 3.6
- High priority scenarios and basic regression features
- Inputs from Cisco SEs/ TAC

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

The following products are covered in the test execution:

- Cisco Wireless LAN Controller 8540
- Cisco Wireless LAN Controller 5520
- Cisco Wireless LAN Controller 3504
- Cisco Wireless LAN Controller 9800
- Virtual Wireless LAN Controller
- Cisco Mobility Express 1850
- Cisco Mobility Express 1830
- Cisco Mobility Express 1815I
- Cisco Mobility Express 2800
- Cisco Mobility Express 3800
- Cisco Mobility Express 4800

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

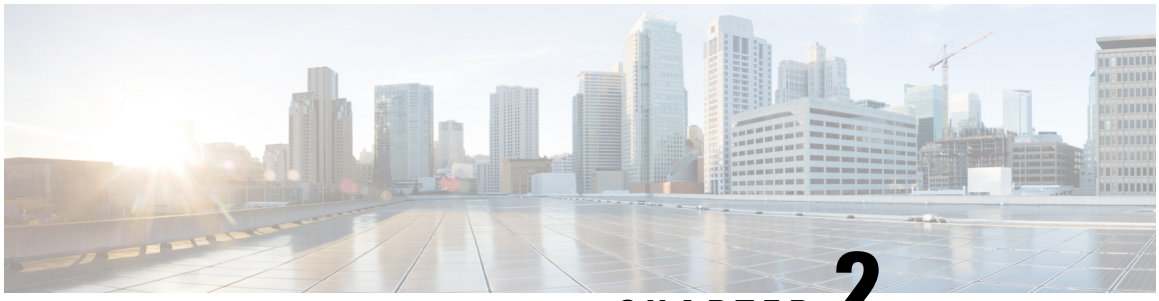
Acronyms

Acronym	Description
AAA	Authentication Authorization and Accounting
ACL	Access Control List
ACS	Access Control Server
AKM	Authentication Key Management
AP	Access Point
API	Application Programming Interface

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
DNS	Domain Name System
DTIM	Delivery Traffic Indication Map
DSCP	Differentiated Services Code Point
DTLS	Datagram Transport Layer Security
EAP	Extensible Authentication Protocol
EULA	End User Licence Agreement
EWLC	Elastic Wireless LAN Controller
FLA	Flex Local Authentication
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
ISR	Integrated Services Router
LAG	Link Aggregation
LEAP	Lightweight Extensible Authentication Protocol
LSS	Location Specific Services
LWAPP	Lightweight Access Point Protocol
MAP	Mesh Access Point
MCS	Modulation Coding Scheme
MFP	Management Frame Protection
mDNS	multicast Domain Name System
MIC	Message Integrity Check
MSE	Mobility Service Engine
MTU	Maximum Transmission Unit
NAC	Network Admission Control
NAT	Network Address Translation
NBAR	Network Based Application Recognition
NCS	Network Control System
NGWC	Next Generation Wiring closet
NMSP	Network Mobility Services Protocol
OEAP	Office Extended Access Point
PEAP	Protected Extensible Authentication Protocol
PEM	Policy Enforcement Module
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

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

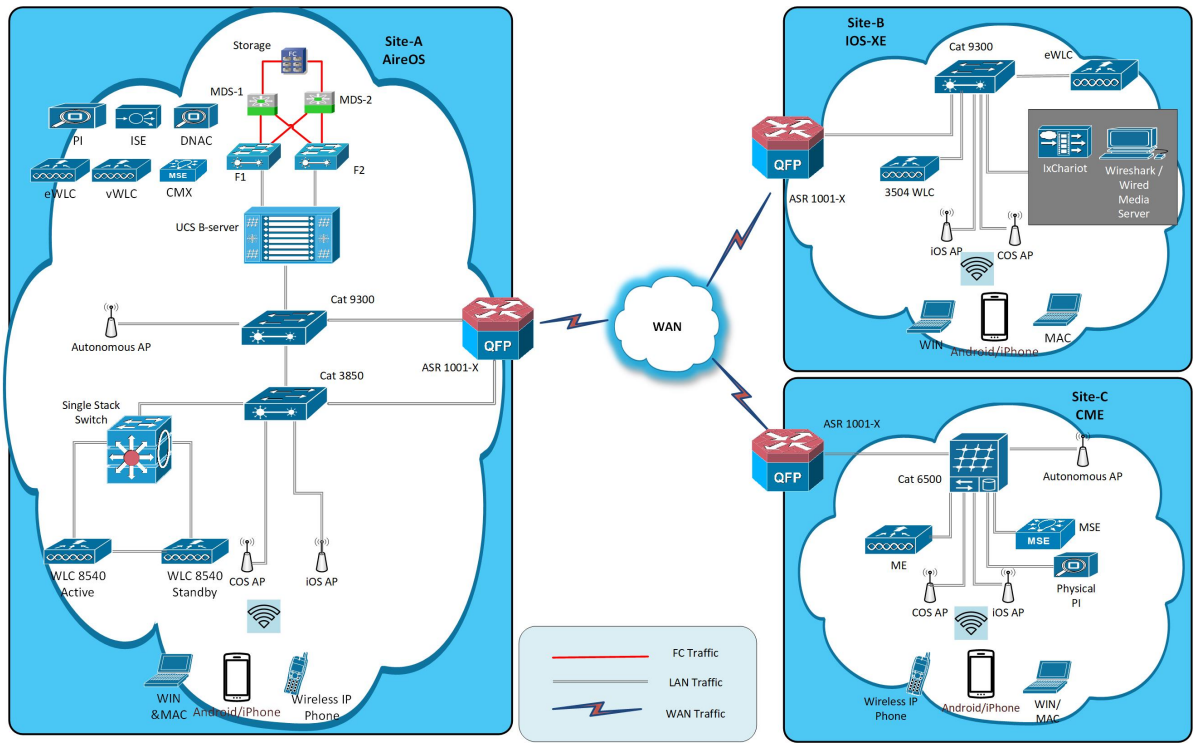


CHAPTER 2

Test Topology and Environment Matrix

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

Test Topology



Component Matrix

Category	Component	Version
Controller	Wireless LAN Controller 8540	8.9.100.0
	Wireless LAN controller 5520	8.9.100.0
	Wireless LAN controller 3504	8.9.100.0
	Wireless LAN controller 9800	16.11.1
	9800 Controller (VM)	16.11.1
	Virtual Controller	8.9.100.0
	CME 1562/1850/1830	8.9.100.0
	CME 4800/3800/2800	8.9.100.0
Applications	Prime Infrastructure (Virtual Appliance, UCS based)	3.6
	ISE(VM)	2.6
	CMX(Physical (3375), VM)	10.6
	DNAC	1.3
	MSE(Physical (3365), VM)	8.0.150.0
	APIC-EM Controller appliance	1.6
	Cisco Jabber for Windows, iPhone	12.1.0
	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
	Cisco ISR 1100	16.11
Switch	Cisco 3750V2 switch	15.0(2)SE2
	Cisco Cat 6509-E	15.1(1)SY1
	Cisco Cat 9300	16.11.1
	Cisco Cat 9200L	16.11.1
	Cisco Cat 9800	16.11.1
Chipset	5300, 6300 AGN	15.40.41.5058
	7265 AC	20.120.0
	Airport Extreme	7.7.9

Category	Component	Version
Client	Operating System(JOS)	Windows 7 Enterprise
		Windows 8 & 8.1 Enterprise
		Windows XP Professional
		Windows 10
	Apple Mac Book Pro, Apple Mac Book Air (JP Locale)	Mac OS 10.14.2
	iPad Pro	iOS 12.1.3
	iPhone 6, 6S & 7 (JP Locale)	iOS 12.1.3
	Samsung Galaxy S4 & S7, Nexus 6P, Sony Xperia XZ	Android 9.0 Pie
	Wireless IP Phone 8821	11.0.4-14
	End points	Windows 7 Enterprise
		Apple Mac 10.14.2
		Windows 8 & 8.1
		iPhone 6,6S & 7
		Windows 10
		Samsung Galaxy S4, S7, Nexus 6P, Sony Xperia
	Cisco AnyConnect VPN Client	4.6.01103
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	64.0
	Safari	11.0.2
	Chrome	71.0

What's New ?

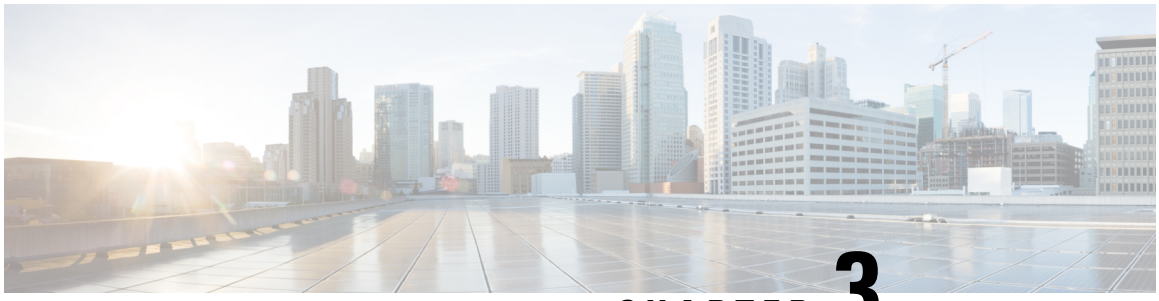
- eWLC Support in Prime
- Support for IRCM Feature

Open Caveats

Logical ID	Title
CSCvo93795	Wired client details are not showing in wired clients option in PI
CSCvp08856	Location in Clients and User Page is not clearing after deleting the Site
CSCvp16327	Unable to deploy "circuit ID " and "remote-id" parameters from PI to WLC
CSCvo87412	Flex Profile with Japanese name is not deploying to eWLC
CSCvo92083	Getting collection failure when adding vWLC in PI
CSCvo61916	WLAN template deploy got failed due to per WLAN max client range mismatch both PI and eWLC

Resolved Caveats

Logical ID	Title
CSCvo59600	Syslog host field accepting invalid inputs in PI
CSCvo80509	Invalid flexonnect ACL rules are configuring and displaying after saving continously
CSCvo82662	MultiHostMode not reflected in eWLC RLAN Policy Profile
CSCvo91527	Unable to create a new EOGRE template in PI
CSCvo88066	Mismatch in airTimeAllocation of ATF range in PI
CSCvo70289	%SNMP-3-RESPONSE_DELAYED: processing GetNext of ciscoFlashFileEntry.2



CHAPTER 3

New Features - Test Summary

- eWLC Support in Prime, on page 13
- Support for IRCM Feature, on page 18

eWLC Support in Prime

Logical ID	Title	Description	Status	Defect ID
WLJPI36S_eWLC_01	Adding the eWLC to PI	To add the eWLC in PI and check if the eWLC gets added or not	Passed	
WLJPI36S_eWLC_02	Adding eWLC with read only SNMP credentials and configuring eWLC parameters	To add eWLC in PI with read only SNMP and check if we can make configuration changes or not	Failed	CSCvo70289
WLJPI36S_eWLC_03	Checking the details of the eWLC in PI	To check the details of the eWLC in PI and check the same details are same as eWLC or not	Passed	
WLJPI36S_eWLC_04	Checking the details of the APs in eWLC through PI	To check if the Aps of eWLC details are shown in eWLC or not	Passed	
WLJPI36S_eWLC_05	Creating WLAN templates in PI and deploying it in eWLC	To create WLAN template in PI and deploying the template to eWLC and check if the WLAN is created or not.	Passed	

WLJPI36S_eWLC_06	Creating WLAN in PI with Security as None and connecting a client to it .	To check if the WLAN is created or not with none security and connecting a client to it .	Passed	
WLJPI36S_eWLC_07	Creating WLAN in PI with Security as WPA/WPA2 Enterprise and connecting a client to it .	To check if the WLAN is created or not with WPA/WPA2 Enterprise security and connecting a client to it .	Passed	
WLJPI36S_eWLC_08	Connecting a client to WLAN created with mac filtering through template created form PI .	To connect different client to a L2 Security enabled with mac filtering by creating a template in PI and check if the client gets connected to the WLAN	Passed	
WLJPI36S_eWLC_09	Creating a policy profile from PI and applying to the WLAN created and connecting a client	To create a policy profile from PI and applying it to the WLAN and check if the Policy gets applied to the clients that gets connected to the WLAN or not.	Passed	
WLJPI36S_eWLC_10	Configuring AP credentials ,Primary Controller and Telnet parameters	To configure AP credentials ,Primary Backup controller and telnet parameters for the eWLC	Passed	
WLJPI36S_eWLC_11	Create ATF profile with Weight Usage and client sharing template in PI and deploy to eWLC	To verify whether ATF Profile is created with Weight Usage and client sharing in PI and deployed to eWLC successfully	Passed	
WLJPI36S_eWLC_12	Client connectivity with l2 security WLAN having different Policy weight	To verify the client connectivity with two SSID having different weight	Passed	

WLJPI36S_eWLC_13	Apply ATF monitor mode 2.4GHZ/5GHz on RF group	To verify whether monitor is applied on RF group successfully	Passed	
WLJPI36S_eWLC_14	Adding client exclusion policies in PI for the clients in eWLC	To configure client exclusion policies in PI for the clients in eWLC	Passed	
WLJPI36S_eWLC_15	Configuring ACL rule from PI and connecting clients .	To configure ACL rules and check if the ACL rules are applied or not when a client gets connected to it .	Passed	
WLJPI36S_eWLC_16	Associating clients to Trustsec configured AP and checking the policy hit statistics in eWLC and PI	To verify the policy hit for client after Trustsec configured on AP	Passed	
WLJPI36S_eWLC_17	AP deployment using PI template for eWLC device and connecting a client	To deploy AP template from PI to eWLC and check if the d=templates gets deployed or not .	Passed	
WLJPI36S_eWLC_18	Rule Deployment using PI for the eWLC device and connecting a client	To verify if Rule deployment template from PI to eWLC is deployed and check if the clients gets the parameters mapped in that profile or not.	Passed	
WLJPI36S_eWLC_19	Adding a eWLC AP to the Maps and check the details of the AP in Maps.	To add eWLC AP to the floor map and check the details of the AP .	Passed	
WLJPI36S_eWLC_20	Connecting a client to the eWLC AP which is added to the Maps	To connect a client to the AP added on the maps and check if the clients gets connected to the AP or not.	Passed	
WLJPI36S_eWLC_21	Generating a custom report for Client count using Japanese UI	To check whether a custom report for client count is generated or not	Passed	

WLJPI36S_eWLC_22	Generating a custom report for Site Summary	To check whether a custom report for Site Summary is generated or not	Passed	
WLJPI36S_eWLC_23	Configuring trap control parameters from PI and verify the trap logs in eWLC	To configure trap control parameters from PI and check if the trap log are generated in eWLC or not.	Passed	
WLJPI36S_eWLC_24	Export the eWLC device and import the same file to add eWLC in PI	To export the eWLC device from PI and import the same back to PI and check if the devices gets added successfully.	Passed	
WLJPI36S_eWLC_25	Creating WLAN in PI with Security as WPA/WPA2 Enterprise and connecting a Windows client with PEAP method	To check if the WLAN is created or not with WPA/WPA2 Enterprise security and connecting a Windows client to it with EAP-PEAP method	Passed	
WLJPI36S_eWLC_26	Creating WLAN in PI with Security as WPA/WPA2 Enterprise and connecting a Windows client with LEAP method	To check if the WLAN is created or not with WPA/WPA2 Enterprise security and connecting a Windows client to it with EAP-LEAP method	Passed	
WLJPI36S_eWLC_27	Creating WLAN in PI with Security as WPA/WPA2 Enterprise and connecting a Windows client with PEAP method	To check if the WLAN is created or not with WPA/WPA2 Enterprise security and connecting a Windows client to it with EAP-PEAP method	Passed	

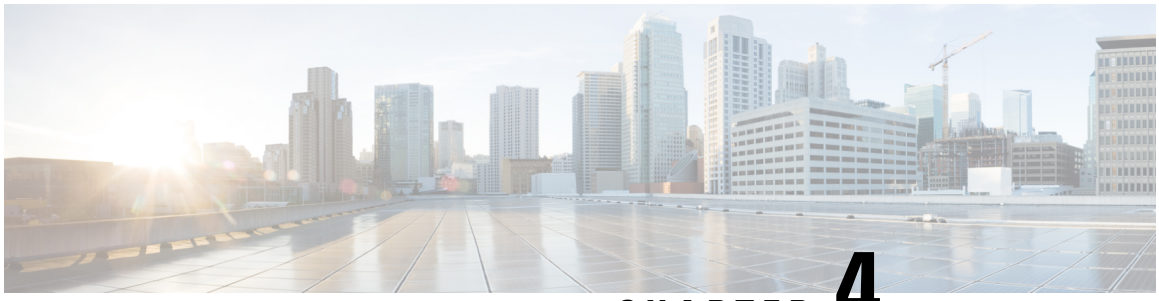
WLJPI36S_eWLC_28	Creating WLAN in PI with Security as WPA/WPA2 Enterprise and connecting a Windows client with EAP-TLS method	To check if the WLAN is created or not with WPA/WPA2 Enterprise security and connecting a Windows client to it with EAP-TLS method	Passed	
WLJPI36S_eWLC_29	Creating WLAN in PI with Security as WPA/WPA2 Enterprise and connecting a MAC OS client with PEAP method	To check if the WLAN is created or not with WPA/WPA2 Enterprise security and connecting a MAC OS client to it with EAP-PEAP method	Passed	
WLJPI36S_eWLC_30	Creating WLAN in PI with Security as WPA/WPA2 Enterprise and connecting a MAC OS client with EAP-TLS method	To check if the WLAN is created or not with WPA/WPA2 Enterprise security and connecting a MAC OS client to it with EAP-TLS method	Passed	
WLJPI36S_eWLC_31	Creating WLAN in PI with Security as WPA/WPA2 Enterprise and connecting a Android client with PEAP method	To check if the WLAN is created or not with WPA/WPA2 Enterprise security and connecting a Android client to it with EAP-PEAP method	Passed	
WLJPI36S_eWLC_32	Creating WLAN in PI with Security as WPA/WPA2 Enterprise and connecting a iOS client with PEAP method	To check if the WLAN is created or not with WPA/WPA2 Enterprise security and connecting a iOS client to it with EAP-PEAP method	Passed	

WLJPI36S_eWLC_33	Creating WLAN in PI with Security as WPA/WPA2 Enterprise and connecting a iOS client with LEAP method	To check if the WLAN is created or not with WPA/WPA2 Enterprise security and connecting a iOS client to it with EAP-LEAP method	Passed	

Support for IRCM Feature

Logical ID	Title	Description	Status	Defect ID
WLJPI36S_IRCM_01	Checking the roamed clients status in PI	To check whether clients status shown properly or not in PI for WLC's	Passed	
WLJPI36S_IRCM_02	Checking the roamed clients status in PI during HA failover	To check whether clients status shown properly or not in PI for WLC's during force failover	Passed	
WLJPI36S_IRCM_03	Creating the custom reports for the roamed clients status in PI	To check whether custom reports are created or not for roamed client status in PI	Passed	
WLJPI36S_IRCM_04	Monitoring the roamed clients between 9800 Controller and 8540 WLC with WPA2+dot1x (LEAP) in PI	To check whether clients status shown properly or not after roamed between 5520 WLC and 9800 Controller with security type WPA2+dot1x (LEAP) in PI	Passed	
WLJPI36S_IRCM_05	Monitoring the roamed clients between 9800 Controller and 3504 WLC with WPA2+dot1x (EAP-TLS) in PI	To check whether clients status shown properly or not after roamed between 5520 WLC and 9800 Controller with security type WPA2+dot1x (EAP-TLS) in PI	Passed	

WLJPI36S_IRCM_06	Monitoring the clients between 9800 Controller and 5520 WLC with WPA2+dot1x (PEAP) in PI	To check whether clients status shown properly or not after roamed between 5520 WLC and 9800 Controller with security type WPA2+dot1x (PEAP) in PI	Passed	



CHAPTER 4

Regression Features - Test Summary

- Custom Reports, on page 22
- Config Group Phase 2, on page 29
- Network Health- Wireless Client and Rogue, on page 30
- Next Generation Maps, on page 32
- DHCP Server to ME, on page 35
- TrustSec SGT/SG ACL for Wireless (WLC), on page 36
- MAC filtering capability for lobby ambassadors, on page 37
- Domain based URL ACL enhancement , on page 38
- Autonomous to LWAPP Migration, on page 39
- High Availability, on page 40
- Flex AVC, on page 41
- APIC-EM Controller, on page 42
- SWIM Enhancement, on page 44
- HA Enhancements, on page 45
- End to end CMX Integration testing, on page 45
- Rolling AP Upgrade, on page 47
- Monitor Mode support in APs (1810/1815), on page 49
- AP Health Extension, on page 51
- WLC Health Scoring, on page 52
- EOGRE Profile, on page 55
- Support Flex + Bridge mode configuration for Access points, on page 58
- Open DNS Support, on page 60
- Support hyperlocation config enhancement in Lightweight AP template, on page 61
- Outdoor AP GPS support, on page 62
- Scheduled AP upgrade, on page 63
- Support Mobility Express on Maps, on page 65
- Audit Logging for Maps/Wireless, on page 67
- Support for Zero Touch Deployment for ME-AP, on page 69
- Better HA Monitoring and Management, on page 71
- SWIM Support of Mobility Express Controllers, on page 72
- TACACS+ & RADIUS servers added without any authentication, on page 73
- eWLC Support for Airtime Entitlement, on page 76
- Support for AP 4800 in PI , on page 80

• Manage 4800 ME controller in Prime, on page 85
• Config Wireless, on page 90

Custom Reports

Logical ID	Title	Description	Status	Defect ID
WLJPI36S _Reg_01	Generating a custom report for the top AP by client count	To check whether a custom report for the top AP by client count is generated or not	Passed	
WLJPI36S _Reg_02	Generating a custom report for Interface utilization	To check whether a custom report for Interface Utilization is generated or not	Passed	
WLJPI36S _Reg_03	Generating a custom report for Busiest AP	To check whether a custom report for Busiest AP is generated or not	Passed	
WLJPI36S _Reg_04	Generating a custom report for AP utilization	To check whether a custom report for AP utilization is generated or not	Passed	
WLJPI36S _Reg_05	Creating sub report for Unique client and users summary as client summary by SSID	To check whether sub report Client summary by SSID can be customized or not	Passed	
WLJPI36S _Reg_06	Creating sub report for Unique client and users summary as client summary by VLAN	To check whether sub report Client summary by VLAN can be customized or not	Passed	
WLJPI36S _Reg_07	Creating sub report for rogue AP Events	To check whether sub report for rogue AP Events can be customized or not	Passed	
WLJPI36S _Reg_08	Creating sub report for rogue APs(Updated)	To check whether sub report for rogue AP Events can be customized or not	Passed	

WLJPI36S _Reg_09	Creating sub report for Worst RF APs	To check whether sub report for Worst RF APs can be customized or not	Passed	
WLJPI36S _Reg_10	Creating sub report for AP RF Quality	To check whether sub report for AP RF Quality can be customized or not	Passed	
WLJPI36S _Reg_11	Creating sub report for Wireless Network Utilization	To check whether sub report for Wireless Network Utilization can be customized or not	Passed	
WLJPI36S _Reg_12	Generating a custom for Busiest Client	To check whether a custom report for Client count is generated or not	Passed	
WLJPI36S _Reg_13	Generating a custom for Client count	To check whether a custom report for client count is generated or not	Passed	
WLJPI36S _Reg_14	Generating a custom for unique clients and users Summary	To check whether a custom report for unique clients and users Summary is generated or not	Passed	
WLJPI36S _Reg_15	Generating a custom for Rogue AP Events	To check whether Generate a custom report for Rogue AP events is generated or not	Passed	
WLJPI36S _Reg_16	Generating a custom for Rogue AP	To check whether Generate a custom report for Rogue AP	Passed	
WLJPI36S _Reg_17	Generating a custom for Adaptive WIPs Top 10 AP	To check whether a custom report for Adaptive WIPs Top 10 AP is generated or not	Passed	
WLJPI36S _Reg_18	Generating a custom for Application Summary	To check whether a custom report for Application summary is generated or not	Passed	

WLJPI36S _Reg_19	Generating a custom for worst RF APs	To check whether a custom report for Worst RF APs is generated or not	Passed	
WLJPI36S _Reg_20	Generating a custom for Site Summary	To check whether a custom report for Site Summary is generated or not	Passed	
WLJPI36S _Reg_21	Generating a custom for AP RF Quality	To check whether a custom report for Wireless Network Utilization is generated or not	Passed	
WLJPI36S _Reg_22	Generating a custom for Wireless Network Utilization	To check whether Generate a custom report for AP RF Quality	Passed	
WLJPI36S _Reg_23	Creating a composite custom result for client	To check whether a composite custom report for client is generated or not	Passed	
WLJPI36S _Reg_24	Creating a composite custom result for device	To check whether a composite custom report for device is generated or not	Passed	
WLJPI36S _Reg_25	Creating a composite custom result for Security	To check whether a composite custom report for Security is generated or not	Passed	
WLJPI36S _Reg_26	Creating a composite custom result for Performance	To check whether a composite custom report for Performance is generated or not	Passed	
WLJPI36S _Reg_27	Creating a composite custom reports for different groups	To check whether a composite custom report by combining template from different group is generated or not	Passed	
WLJPI36S _Reg_28	Scheduling a report on particular time through PI GUI	To check whether report can be scheduled or not on a fixed time	Passed	

WLJPI36S _Reg_29	Verifying the scheduled template in composite report	To check whether the scheduled report is listed or not in the Composite Report	Passed	
WLJPI36S _Reg_30	Verifying the scheduled template in saved report template	To check whether the scheduled report is listed or not in the saved report template	Passed	
WLJPI36S _Reg_31	Verifying that the scheduled report is running at the selected date & time selected.	To check whether the scheduled report is running at the selected date & time selected or not	Passed	
WLJPI36S _Reg_32	Verifying that the scheduled run report is shown in the Scheduled Run Results page	To verify that the scheduled run report is shown in the Scheduled Run Results page	Passed	
WLJPI36S _Reg_33	Verify the scheduled run report is shown in the Job Dashboard	To verify the scheduled run report is shown in the Job Dashboard or not	Passed	
WLJPI36S _Reg_34	Saving the report and viewing it in GUI	To check whether that saved report is available in PI GUI or not	Passed	
WLJPI36S _Reg_35	Exporting the saved report	To check whether verify whether the saved report can be mailed or not	Passed	
WLJPI36S _Reg_36	Saving and mailing the report	To check whether the saved report can be exported or not	Passed	
WLJPI36S _Reg_37	Checking the dependency in other pages	To check whether the custom report page Appear there or not	Passed	
WLJPI36S _Reg_38	Checking the custom report in favorited icon	To check whether the custom report is listed in favorited icon	Passed	
WLJPI36S _Reg_39	Verifying the Help menu for the Custom Report Page	To check whether details of custom reports in Help Page is listed or not	Passed	

WLJPI36S _Reg_40	Creating the report in Summary View	To check whether the view of report can be changed to summary view or not	Passed	
WLJPI36S _Reg_41	Creating the report in detailed View	To check whether the view of report can be changed to detailed view or not	Passed	
WLJPI36S _Reg_42	Creating the Sub report for the Top AP by client Count	To check whether Sub report can be created of not	Passed	
WLJPI36S _Reg_43	Creating the Sub report for the Top AP by client Count by Applying data filed Sorting	To check whether Sub report for Top AP Client count data can be sorted or not as per condition	Passed	
WLJPI36S _Reg_44	Creating the Sub report for the Interface Utilization	To check whether Sub report for Interface utilization can be created of not	Passed	
WLJPI36S _Reg_45	Creating the Sub report for the Interface Utilization by Applying data filed Sorting	To check whether Sub report data for Interface utilization can be sorted or not as per condition	Passed	
WLJPI36S _Reg_46	Creating Sub report for device health and Applying sorting on result	To check whether the sub report for device health can be customized or not	Passed	
WLJPI36S _Reg_47	Enabling the sub report for the Device Health	To check whether the sub report for device health can be created or not	Passed	
WLJPI36S _Reg_48	Creating report for 802.11 a/an/ac Busied AP	To check whether the report for 802.11a.a/an/ac can be created or not	Passed	

WLJPI36S _Reg_49	Creating Sub report for 802.11a/an/ac Busied AP and Applying sorting on result	To check whether the sub report for 802.11a.a/an/ac can be created or not	Passed	
WLJPI36S _Reg_50	Creating report for 802.11 b/g/n Busied AP	To check whether the report for 802.11 b/g/n can be created or not	Passed	
WLJPI36S _Reg_51	Creating Sub report for 802.11a/an/ac Busied AP and Applying sorting on result	To check whether the sub report for 802.11 b/g/n can be created or not	Passed	
WLJPI36S _Reg_52	Creating report for AP utilization for 802.11 b/g/n radio	To check whether the report for 802.11a.a/an/ac can be created or not	Passed	
WLJPI36S _Reg_53	Creating sub report for AP utilization for 802.11 a/an/ac radio	To check whether the sub report for 802.11 a/an/ac can be created or not	Passed	
WLJPI36S _Reg_54	Creating report for AP utilization for 802.11 b/g/n radio	To check whether the report for AP Utilization for radio 802.11 b/g/n can be created or not	Passed	
WLJPI36S _Reg_55	Creating sub report for AP utilization for 802.11 b/g/n radio	To check whether the sub report for AP Utilization for 802.11 b/g/n radio can be created and sorted or not	Passed	
WLJPI36S _Reg_56	Creating sub report for Busiest Client	To check whether the sub reports for Busiest client can be customized or not	Passed	
WLJPI36S _Reg_57	Creating sub report for Unique client and users Summary as Client User Summary	To check whether sub report Client user summary can be customized or not	Passed	

WLJPI36S _Reg_58	Creating sub report for Unique client and users Summary as Client Traffic Summary	To check whether sub report Client Traffic summary can be customized or not	Passed	
WLJPI36S _Reg_59	Creating sub report for Unique client and users summary as client summary by protocol	To check whether sub report Client summary by protocol can be customized or not	Passed	
WLJPI36S _Reg_60	Creating sub report for Unique client and users summary as client summary by Vendor	To check whether sub report Client summary by vendor can be customized or not	Passed	
WLJPI36S _Reg_61	Creating sub report for Unique client and users summary as client summary by SSID	To check whether sub report Client summary by SSID can be customized or not	Passed	
WLJPI36S _Reg_62	Creating sub report for Unique client and users summary as client summary by VLAN	To check whether sub report Client summary by VLAN can be customized or not	Passed	
WLJPI36S _Reg_63	Creating sub report for rogue AP Events	To check whether sub report for rogue AP Events can be customized or not	Passed	
WLJPI36S _Reg_64	Creating sub report for rogue APs(Updated)	To check whether sub report for rogue AP Events can be customized or not	Passed	
WLJPI36S _Reg_65	Creating sub report for Worst RF APs	To check whether sub report for Worst RF APs can be customized or not	Passed	
WLJPI36S _Reg_66	Creating sub report for AP RF Quality	To check whether sub report for AP RF Quality can be customized or not	Passed	

WLJPI36S _Reg_67	Creating sub report for Wireless Network Utilization	To check whether sub report for Wireless Network Utilization can be customized or not	Passed	
WLJPI36S _Reg_68	Scheduling a report on particular time through Japanese GUI	To verify whether report can be scheduled or not in Japanese GUI as in Japanese time format	Passed	
WLJPI36S _Reg_69	Verifying Saved run result in Japanese GUI for Scheduled report result	To verify whether Scheduled run result is present or not Japanese GUI for selected time Period	Passed	

Config Group Phase 2

Logical ID	Title	Description	Status	Defect ID
WLJPI36S _Reg_70	Deploying template on AireOS controller via config group and verifying the controller behavior	Verifying that user is able to deploy template on AireOS controller via config group or not	Passed	
WLJPI36S _Reg_71	Deploying multiple templates on AireOS controller via config group	Verifying that user is able to deploy multiple templates on AireOS controller	Passed	
WLJPI36S _Reg_72	Deploying multiple security type WLAN on controller via config group and connecting the client	Verifying that user is able to deploy multiple security type WLAN on controller	Passed	
WLJPI36S _Reg_73	Deploying template on vWLC via config group	Verifying that user is able to deploy template on vWLC or not	Passed	

WLJPI36S _Reg_74	Deploying template on CME via config group	Verifying that user is able to deploy on CME	Passed	
WLJPI36S _Reg_75	Deploying template on vWLC/AireOS controller/CME via config group after modify the config group	Verifying that user is able to deploy template on controller/CME/vWLC after modify the config group	Passed	
WLJPI36S _Reg_76	Try to deploy invalid template on controller via config group	Verifying that user is able to deploy invalid template on controller via config group or not	Passed	
WLJPI36S _Reg_77	Monitoring the dashboard after deploying template on controller	Verifying the dashboard after deploying the template on controller	Passed	
WLJPI36S _Reg_78	Client connectivity after deploy AVC template via config group on controller	Verifying the client connectivity after deploying AVC template on controller via config group	Passed	

Network Health- Wireless Client and Rogue

Logical ID	Title	Description	Status	Defect ID
WLJPI36S _Reg_221	To verifying the Japanese client data rate through PI.	To check the data rate of the particular Japanese client connected to the WLAN.	Passed	
WLJPI36S _Reg_222	To configure the authentication for The AP(1810/1815)	To check whether the authentication is configured into AP(1810/1815)	Passed	

WLJPI36S _Reg_223	Associating AP(1810/1815) with different country code as with WLC and check it is not joined in WLC.	To associate AP(1810/1815) with different country code and check it is not joined with WLC.	Passed	
WLJPI36S _Reg_224	Checking the AP(1810/1815) channel Utilization/Interference.	To check the timings based on Radio:802.11b/g/n Slot:0 Channel Number, AP(1810/1815) channel Utilization/Interference according to date.	Passed	
WLJPI36S _Reg_225	Connecting a window client to the AP(1810/1815)	To connect a window client to the AP and check the client gets connected or not.	Passed	
WLJPI36S _Reg_226	Connecting a Android client to the AP (1810/1815)	To connect a Android client to the AP and check the client gets connected or not.	Passed	
WLJPI36S _Reg_227	Connecting a IOS client to the AP(1810/1815)	To connect a IOS client to the AP and check the client gets connected or not.	Passed	
WLJPI36S _Reg_228	Connecting a MAC client to the AP(1810/1815)	To connect a MAC client to the AP and check if the client gets connected or not.	Passed	
WLJPI36S _Reg_229	Connecting 'Anyconnect client' to the AP(1810/1815)	To connect Anyconnect client to the AP and check if the client gets connected or not.	Passed	
WLJPI36S _Reg_230	Set the AP(1810/1815) monitor mode.	To check whether AP(1810/1815) monitor mode reflected or not in PI after AP mode changing in WLC.	Passed	

WLJPI36S _Reg_231	Deleting AP(1810/1815) from PI.	To check whether the AP(1810/1815) deleted from AP group.	Passed	
WLJPI36S _Reg_232	Monitoring the AP(1810/1815) statistics in PI.	To verify AP(1810/1815) statistics in PI.	Passed	
WLJPI36S _Reg_233	Monitoring the AP (1810/1815) Performance.	To monitor the Access point's Performance.	Passed	

Next Generation Maps

Logical ID	Title	Description	Status	Defect ID
WLJPI36S _Reg_91	Creating a New Site with/without a image	To verify whether the new site is created or not with\without any image .	Passed	
WLJPI36S _Reg_92	Creating a new building in MAP/tabular/Grid view to the site	To check whether new building is created or not in map / tabular / Grid view	Passed	
WLJPI36S _Reg_93	Performing adding / positioning / deleting operations a AP to a floor of a building	To check if the AP getting added to the floor or not	Passed	
WLJPI36S _Reg_94	Exporting a Building and the floor configuration	To export the building and floor configuration and check if the configuration is exported properly	Passed	
WLJPI36S _Reg_95	Importing a building configuration to the site map	To import a building and floor configuration and check if the configuration is imported properly or not.	Passed	

WLJPI36S _Reg_96	Exporting the floor image to a pdf	To export a floor image as a pdf and check if the image of the floor and details shown properly or not	Passed	
WLJPI36S _Reg_97	Checking the number of clients connected to each building and floor	To check the number of clients associated to each building and checking the details of the client	Passed	
WLJPI36S _Reg_98	Changing the MAP properties and enabling the next generation MAPs	To change the properties of the MAPs and enabling the next generation maps and check if the change are made to it.	Passed	
WLJPI36S _Reg_99	Connecting a JOS client to a AP positioned in the Floor	To check if the JOS client gets connected to the AP in the floor and check if the client is show in the Client and user page or not	Passed	
WLJPI36S _Reg_100	Connecting a Android client to a AP positioned in the Floor	To check if the Android client gets connected to the AP in the floor and check if the client is show in the Client and user page or not	Passed	
WLJPI36S _Reg_101	Connecting a Mac OS client to a AP positioned in the Floor	To check if the Mac OS client gets connected to the AP in the floor and check if the client is show in the Client and user page or not	Passed	

WLJPI36S _Reg_102	Connecting a IOS client to a AP positioned in the Floor	To check if the IOS client gets connected to the AP in the floor and check if the client is show in the Client and user page or not	Passed	
WLJPI36S _Reg_103	Bulk export the AP in Site MAPs page	To check whether bulk export of AP function working properly or not in Site maps page of PI	Passed	
WLJPI36S _Reg_104	Exporting the AP's for Geo MAPs	To check whether export of APs for Geo MAP is working properly or not in Site maps page of PI	Passed	
WLJPI36S _Reg_105	Exporting the MAP archive in tar format and importing the same tar file	To check whether export/import the tar file works properly or not in Site MAPs page	Passed	
WLJPI36S _Reg_106	Trying to import the bulk AP in CSV format	To check whether new CSV file can be imported or not with some AP configurations in it in Site maps page	Passed	
WLJPI36S _Reg_107	Importing AP's for Geo MAP in MAPs	To check whether AP's can be imported to Geo MAP or not from a CSV fie	Passed	
WLJPI36S _Reg_108	Importing MAP archive in XML format	To check Whether MAP archive can be imported or not	Passed	
WLJPI36S _Reg_109	Creating Group hierarchy in MAPs	To check whether Group hierarchy can be created or not in PI MAPs	Passed	

WLJPI36S _Reg_110	Filtering Available access Point on a particular floor	To check whether the access point can be filtered by name,Mac address, radio type and other avail filter or not	Passed	

DHCP Server to ME

Logical ID	Title	Description	Status	Defect ID
WLJPI36S _Reg_111	Connect IPhone client to WLAN after creating DHCP scope	To verify that IPhone connect successfully after creating DHCP scope	Passed	
WLJPI36S _Reg_112	Connect Japanese client to WLAN after creating DHCP scope	To verify that Japanese connect successfully after creating DHCP scope	Passed	
WLJPI36S _Reg_113	Connect Android client to WLAN after creating DHCP scope	To verify that Android connect successfully after creating DHCP scope	Passed	
WLJPI36S _Reg_114	Connect Windows client to WLAN after creating DHCP scope	To verify that Windows connect successfully after creating DHCP scope	Passed	
WLJPI36S _Reg_115	Connect iOS client to WLAN after creating DHCP scope	To verify that iOS connect successfully after creating DHCP scope	Passed	
WLJPI36S _Reg_116	Scheduling ME reboot in PI after DHCP config	To verify whether DHCP configuration are correct or not after reboot	Passed	

WLJPI36S _Reg_117	AP configuration from PI joined to CME.	To verify whether AP configuration changes from PI Applies successfully in CME.	Passed	

TrustSec SGT/SG ACL for Wireless (WLC)

Logical ID	Title	Description	Status	Defect ID
WLJPI36S _Reg_118	Creating a Trustsec SXP Config Template	To Create a Trustsec Sap config template and to deploy the template to the controller and check if the template is deployed	Passed	
WLJPI36S _Reg_119	Creating a WLAN with Dot1x and connect Android client	To create a WLAN with Dot1x Security and deploy it to the controller and connect Android client	Passed	
WLJPI36S _Reg_120	Deploying Sap configuration in WLC and synchronizing into PI	To create a Sap Configuration in WLC GUI and deploy the same in PI and check if the configuration is identical	Passed	
WLJPI36S _Reg_121	Creating a Trustsec CTS Config and adding SPX connection Template	To Create a Trustsec CTS config and adding SPX connection template and to deploy the template to the controller and check if the template is deployed	Passed	

MAC filtering capability for lobby ambassadors

Logical ID	Title	Description	Status	Defect ID
WLJPI36S _Reg_122	MAC filtering capability for lobby ambassadors	Creating local management user with lobby access level in WLC	Passed	
WLJPI36S _Reg_123	Creating , viewing and deleting a lobby admin user in WLC	To check whether lobby admin user is created, deleted or not in WLC	Passed	
WLJPI36S _Reg_124	Enabling lobby Admin access to WLAN profile	To check whether lobby admin can access without L3 Sec WLAN Profile or not	Passed	
WLJPI36S _Reg_125	Creating a guest user from Guest Management GUI	To check whether guest user is created or not in GUI	Passed	
WLJPI36S _Reg_126	Creating auto password for user	To check whether generate a auto check whether password for guest user	Passed	
WLJPI36S _Reg_127	Adding a permanent guest user from WLC Guest Management GUI	To check whether permanent guest user is added or not	Passed	
WLJPI36S _Reg_128	Creating local management user with read only access level	To create local management user with read only access level	Passed	
WLJPI36S _Reg_129	Creating local management user with read write access level	To create local management user with read write access level	Passed	

WLJPI36S _Reg_130	Create Template for L2 security with Static WEP and layer 3 with Authentication & Enable lobby admin	To verify that template deployed successfully and client authenticated with Static WEP enabled lobby admin access	Passed	
WLJPI36S _Reg_131	Create Template for L2 security with open configuration and layer 3 with Authentication & Enable lobby admin	To verify that template deployed successfully and client authenticated with open security enabled lobby admin access	Passed	
WLJPI36S _Reg_132	Accessing guest user Management GUI	To verify Aunthentication for lobby user	Passed	

Domain based URL ACL enhancement

Logical ID	Title	Description	Status	Defect ID
WLJPI36S _Reg_133	Deny cisco site for end level android clients by keeping black list	Blocking cisco site for end level android clients by keeping black list	Passed	
WLJPI36S _Reg_134	Permit cisco site for end level android clients by keeping white list	Permitting cisco site for end level android clients by keeping white list	Passed	
WLJPI36S _Reg_135	Deny cisco site for end level Windows clients by keeping black list	Blocking cisco site for end level Windows clients by keeping black list	Passed	
WLJPI36S _Reg_136	Permit cisco site for end level Windows clients by keeping white list	Permitting cisco site for end level Windows clients by keeping white list	Failed	CSCvo80509

WLJPI36S _Reg_137	Deny cisco site for end level MAC clients by keeping black list	Blocking cisco site for end level MAC Clients by keeping black list	Passed	
WLJPI36S _Reg_138	Permit cisco site for end level MAC clients by keeping white list	Permitting cisco site for end level MAC Clients by keeping white list	Passed	
WLJPI36S _Reg_139	Deny cisco site for end level Anyconnect clients by keeping black list	Blocking cisco site for end level Anyconnect Clients by keeping black list	Passed	
WLJPI36S _Reg_140	Permit cisco site for end level MAC clients by keeping white list	Permitting cisco site for end level Anyconnect Clients by keeping white list	Passed	

Autonomous to LWAPP Migration

Logical ID	Title	Description	Status	Defect ID
WLJPI36S _Reg_141	Verifying the Autonomous to LWAPP Migration	To check whether autonomous to LWAPP migrating or not	Passed	
WLJPI36S _Reg_142	Migrating autonomous AP to LWAPP using the “Schedule for later date/time" option	Verifying autonomous AP migrating to LWAP or not through “ Schedule for later date/time”	Passed	
WLJPI36S _Reg_143	Generating the migration report for the created template	To check whether migration report is generating or not for the created template	Passed	

WLJPI36S _Reg_144	Verifying the current status of the Autonomous to LWAP Migration	To checking the current status of the Autonomous to LWAP Migration	Passed	
WLJPI36S _Reg_145	Viewing the Migration Analysis summary for Autonomous AP to LWAP	Verifying the Migration Analysis summary for Autonomous AP to LWAP	Passed	
WLJPI36S _Reg_146	Upgrading the firmware manually for the selected AP by clicking view migration analysis summary	To renovate the firmware manually for the selected AP	Passed	
WLJPI36S _Reg_147	Upgrading the firmware automatic for the selected AP by clicking view migration analysis summary	To renovate the firmware automatic for the selected AP	Passed	

High Availability

Logical ID	Title	Description	Status	Defect ID
WLJPI36S _Reg_148	PI HA- When primary server is down(HW failure) and Failover type as "Manual"	To check whether PI has been switchover to the secondary when there is a primary server(HW) failure- failover type as "Manual"	Passed	
WLJPI36S _Reg_149	PI HA- When primary server is down(HW failure) and Failover type as "Automatic"	To check whether PI has been switchover to the secondary when there is a primary server(HW) failure- failover type as "Automatic"	Passed	

WLJPI36S _Reg_150	PI HA- When primary server is down(Network failure) and Failover type as "Manual"	To check whether PI has been switchover to the secondary when there is a primary server(NW) failure- failover type as "Manual"	Passed	
WLJPI36S _Reg_151	PI HA- When primary server is down(Network failure) and Failover type as "Manual"	To check whether PI has been switchover to the secondary when there is a primary server(NW) failure- failover type as "Automatic"	Passed	
WLJPI36S _Reg_152	PI HA- Failback to Primary server once it has been recovered from HW failure	To check whether the failback operation is successful after the primary server has been recovered from HW failure	Passed	
WLJPI36S _Reg_153	PI HA- Failback to Primary server once it has been recovered from NW failure	To check whether the failback operation is successful after the primary server has been recovered from NW failure	Passed	

Flex AVC

Logical ID	Title	Description	Status	Defect ID
WLJPI36S _Reg_154	Dropping some Application via flex AVC profile	To drop some Application via Flex AVC profile	Passed	
WLJPI36S _Reg_155	Marking the certain Application and validating the same	To mark the certain Application	Passed	
WLJPI36S _Reg_156	Applying the rate limit on some Application	To Apply the rate limit on some Application	Passed	

WLJPI36S _Reg_157	Trying to set rate limit out range in flex AVC rule	Try to set rate limit out range in flex AVC rule	Passed	
WLJPI36S _Reg_158	Delete multiple flex connect AVC profile	To Delete the multiple flex connect AVC profile	Passed	
WLJPI36S _Reg_159	Try to delete Applied flex connect AVC profile	Try to delete Applied flex connect AVC profile	Passed	
WLJPI36S _Reg_160	Try change the AVC rule from custom to mark/rate limit/drop	To verify whether AVC rule is changing from custom to mark/rate limit/drop or not	Passed	
WLJPI36S _Reg_161	Checking AVC rule with more than custom value	To verify whether AVC rule is creating or not more than custom value	Passed	
WLJPI36S _Reg_162	Create the AVC rules in one profile and check in different profile	To verify whether AVC rules are creating in one profile is reflecting in another profile or not	Passed	
WLJPI36S _Reg_163	Create the AVC profile & rule with duplicate name	To verify whether AVC rule and profile name is creating with duplicate name or not	Passed	

APIC-EM Controller

Logical ID	Title	Description	Status	Defect ID
WLJPI36S _Reg_164	Add/edit/delete APIC -EM in PI	To Add APIC -EM in PI	Passed	

WLJPI36S _Reg_165	Validate the Error message	To verify the error message shown when we add the invalid APIC EM in PI	Passed	
WLJPI36S _Reg_166	APIC-EM reachability history	To verify the APIC-EM reachability history once APIC-EM added	Passed	
WLJPI36S _Reg_167	Creating Bootstrap template	To Create Bootstrap template	Passed	
WLJPI36S _Reg_168	Importing Software Images for Plug and Play Profiles	To import software images for plug and play profiles	Passed	
WLJPI36S _Reg_169	Creating PnP profile for switches	To Create PnP profile for switch's	Passed	
WLJPI36S _Reg_170	Creating PnP profile for wireless AP	To Create PnP profile for switch's	Passed	
WLJPI36S _Reg_171	Creating PnP profile for wireless AP with controllers which name in Japanese character	To Create PnP profile for wireless AP with controllers which name in Japanese character	Passed	
WLJPI36S _Reg_172	Adding the PI in APIC -EM	To add PI in APIC -EM	Passed	
WLJPI36S _Reg_173	Plug and play Profile Activation of wireless AP	To activate plug and play profile of wireless AP	Passed	
WLJPI36S _Reg_174	Plug and play Profile Activation switch	To activate plug and play profile of switch	Passed	
WLJPI36S _Reg_175	Monitoring the plug and play	To monitor the plug and play	Passed	

SWIM Enhancement

Logical ID	Title	Description	Status	Defect ID
WLJPI36S _Reg_176	Importing a image from a device	To import a image from a device and check if the images gets imported from the device or not	Passed	
WLJPI36S _Reg_177	Importing the image through Cisco.Com using Credentials	To Import a image from Cisco.com by giving the cisco credentials and check if the image gets imported or not	Passed	
WLJPI36S _Reg_178	Importing the image through the URL	To import the image using URL and check if the images gets imported or not.	Passed	
WLJPI36S _Reg_179	Changing the image transfer protocol order .	To change the image transfer protocol order and check if the order is changed or not	Passed	
WLJPI36S _Reg_180	Checking the image imported through the Software Image Summary	To Check if the image imported is shown in the software image summary or not	Passed	
WLJPI36S _Reg_181	Adding software image management servers	To Configure a software image management server and check if the server are added or not.	Passed	
WLJPI36S _Reg_182	Collect images along with inventory collection	To collect images along with inventory Collection and check if the inventory data is successfully collected or not	Passed	

WLJPI36S _Reg_183	Importing a image through a protocol.	To import a image from a device and check if the images gets imported from the device or not	Passed	
WLJPI36S _Reg_184	Distributing the image to different devices .	To distribute different images and check if the devices selected	Passed	

HA Enhancements

Logical ID	Title	Description	Status	Defect ID
WLJPI36S _Reg_185	HA registration of PI	To check the HA registration between primary and secondary	Passed	
WLJPI36S _Reg_186	HA failback to secondary when primary is failed.	To verify the HA failback to secondary in case of primary failure.	Passed	
WLJPI36S _Reg_187	HA fallback to primary when primary server is restored.	To verify the HA fallback to primary in case of primary server restored.	Passed	
WLJPI36S _Reg_188	Verify the HA failover messages.	To verify the HA failure messages	Passed	
WLJPI36S _Reg_189	Verifying the HM with new changes.	To verify the Time zone display in Health monitor page.	Passed	
WLJPI36S _Reg_190	Verifying the HA events	To verify the HA events triggered when registration and failback.	Passed	

End to end CMX Integration testing

Logical ID	Title	Description	Status	Defect ID

WLJPI36S _Reg_191	Checking the CMX Details in PI GUI	To check whether the details for CMX is displayed correctly or not	Passed	
WLJPI36S _Reg_192	MAP Exporting from GUI	To check whether MAP page can be Exported from PI GUI or not	Passed	
WLJPI36S _Reg_193	Exporting MAP file to CMX	To check whether MAP file can be Exported to CMX from PI GUI or not	Passed	
WLJPI36S _Reg_194	Removing a MAP From PI CMX GUI	To check whether MAP can be deleted from PI CMX GUI or not	Passed	
WLJPI36S _Reg_195	Importing IOS Access points in the Floor map for CMX through PI GUI	To check whether IOS AP can be added from PI CMX	Passed	
WLJPI36S _Reg_196	Importing Cheetah Access points in the Floor map for CMX through PI GUI	To check whether cheetah AP can be added from PI CMX	Passed	
WLJPI36S _Reg_197	Associating windows client into CMX	To check whether the windows client gets associate with CMX	Passed	
WLJPI36S _Reg_198	Associating android client into CMX	To check whether the android client gets associate with CMX	Passed	
WLJPI36S _Reg_199	Associating Mac OS client into CMX	To check whether the Mac OS client gets associate with CMX	Passed	
WLJPI36S _Reg_200	Associating IOS client into CMX	To check whether the IOS client gets associate with CMX	Passed	

WLJPI36S _Reg_201	Searching Windows client by MAC address in CMX GUI	To verify whether client device can be searched by specifying its MAC address or not	Passed	
WLJPI36S _Reg_202	Searching client by IP address in CMX GUI	To verify whether client device can be searched by specifying its IP address or not	Passed	
WLJPI36S _Reg_203	Searching client by SSID in CMX GUI	To verify whether client device can be searched by specifying the SSID or not	Passed	
WLJPI36S _Reg_204	Interferers in Floor map	To verify whether interferers are displayed in the floor map or not	Passed	
WLJPI36S _Reg_205	Rogue Devices in Floor map	To verify whether rogues are displayed in the floor map or not	Passed	
WLJPI36S _Reg_206	Searching Android client by MAC address in CMX GUI	To verify whether client device can be searched by specifying its MAC address or not	Passed	
WLJPI36S _Reg_207	Searching MacOS client by MAC address in CMX GUI	To verify whether client device can be searched by specifying its MAC address or not	Passed	

Rolling AP Upgrade

Logical ID	Title	Description	Status	Defect ID

WLJPI36S _Reg_208	Providing the same controller name and IP address for primary controller and N+1 controller	To check whether the same controller name is accepted or not for primary controller and N+1 controller	Passed	
WLJPI36S _Reg_209	Upgrading the software image in a controller	To check whether the software image is upgraded in controller	Passed	
WLJPI36S _Reg_210	Upgrading the software image into a group of AP	To check whether the software image is upgraded in group of AP	Passed	
WLJPI36S _Reg_211	Upgrading the software image into existing group of AP	To check whether the software image is upgraded into existing group of AP	Passed	
WLJPI36S _Reg_212	Scheduling the time to upgrade the software image into a controller.	To check whether the software image is upgraded into a controller in scheduling time	Passed	
WLJPI36S _Reg_213	Upgrade the image to WLC from PI rolling AP upgrade TFTP	To check whether the WLC is upgraded using TFTP from PI	Passed	
WLJPI36S _Reg_214	Upgrade the image to WLC from PI rolling AP upgrade FTP	To check whether the WLC is upgraded using FTP from PI	Passed	
WLJPI36S _Reg_215	Scheduling the time "Now" to upgrade the software image into a controller.	To check whether the software image is upgraded into a controller in scheduling time "Now"	Passed	
WLJPI36S _Reg_216	Reboot trigger to WLC from PI after upgrade the software image in controller.	To check whether WLC is reloaded when triggering from PI after upgrade the software image in controller.	Passed	

WLJPI36S _Reg_217	Upgrade the wrong file name into the WLC from PI	To verify whether the error message will display when trying to upgrade wrong file into the WLC from PI	Passed	
WLJPI36S _Reg_218	Moving AP's back to primary controller from PI.	To verify whether the AP's are move back into primary controller.	Passed	
WLJPI36S _Reg_219	Adding the AP in AP upgrade group	To verify whether the AP added into AP upgrade group	Passed	
WLJPI36S _Reg_220	AP joining status to WLC's after upgrade the WLC software image and checking the JOS client connectivity.	To check whether the joined APs upgraded and verify the JOS client connectivity.	Passed	

Monitor Mode support in APs (1810/1815)

Logical ID	Title	Description	Status	Defect ID
WLJPI36S _Reg_221	To verifying the Japanese client data rate through PI.	To check the data rate of the particular Japanese client connected to the WLAN.	Passed	
WLJPI36S _Reg_222	To configure the authentication for The AP(1810/1815)	To check whether the authentication is configured into AP(1810/1815)	Passed	
WLJPI36S _Reg_223	Associating AP(1810/1815) with different country code as with WLC and check it is not joined in WLC.	To associate AP(1810/1815) with different country code and check it is not joined with WLC.	Passed	

WLJPI36S _Reg_224	Checking the AP(1810/1815) channel Utilization/Interference.	To check the timings based on Radio:802.11b/g/n Slot:0 Channel Number, AP(1810/1815) channel Utilization/Interference according to date.	Passed	
WLJPI36S _Reg_225	Connecting a window client to the AP(1810/1815)	To connect a window client to the AP and check the client gets connected or not.	Passed	
WLJPI36S _Reg_226	Connecting a Android client to the AP (1810/1815)	To connect a Android client to the AP and check the client gets connected or not.	Passed	
WLJPI36S _Reg_227	Connecting a IOS client to the AP(1810/1815)	To connect a IOS client to the AP and check the client gets connected or not.	Passed	
WLJPI36S _Reg_228	Connecting a MAC client to the AP(1810/1815)	To connect a MAC client to the AP and check if the client gets connected or not.	Passed	
WLJPI36S _Reg_229	Connecting 'Anyconnect client' to the AP(1810/1815)	To connect Anyconnect client to the AP and check if the client gets connected or not.	Passed	
WLJPI36S _Reg_230	Set the AP(1810/1815) monitor mode.	To check whether AP(1810/1815) monitor mode reflected or not in PI after AP mode changing in WLC.	Passed	
WLJPI36S _Reg_231	Deleting AP(1810/1815) from PI.	To check whether the AP(1810/1815) deleted from AP group.	Passed	
WLJPI36S _Reg_232	Monitoring the AP(1810/1815) statistics in PI.	To verify AP(1810/1815) statistics in PI.	Passed	

WLJPI36S _Reg_233	Monitoring the AP (1810/1815) Performance.	To monitor the Access point's Performance.	Passed	

AP Health Extension

Logical ID	Title	Description	Status	Defect ID
WLJPI36S _Reg_234	Monitoring the top or bottom APs by client count of different OS by data usage	Verifying the top or bottom APs clients count by data usage	Passed	
WLJPI36S _Reg_235	Validating Access point Health by Applying the time filter	Validate the Access point Health by Applying the time filter	Passed	
WLJPI36S _Reg_236	Monitoring the top clients of different OS by data uses	Verifying the top clients by data usage	Passed	
WLJPI36S _Reg_237	AP channel utilization performance after set the time frame	validate the AP channel utilization performance based on time frame setting	Passed	
WLJPI36S _Reg_238	Monitoring the associated/authenticated client count graphically through AP time frame	Verify the client count graphically through AP time frame	Failed	CSCvo93795
WLJPI36S _Reg_239	Clients with lower coverage for all OS	Verify the bad coverage of clients for ALL OS	Passed	
WLJPI36S _Reg_240	To checking the Japanese client connection rate.	Validate the Japanese client connection rate showing or not .	Passed	
WLJPI36S _Reg_241	Checking the Japanese wireless client traffic through bandwidth	Verify the Japanese wireless client traffic through bandwidth	Passed	

WLJPI36S _Reg_242	Monitoring the signal quality distribution of different OS Japanese wireless client	Validate the signal quality distribution for Japanese wireless client	Passed	
WLJPI36S _Reg_243	Checking the AP health for created campus site	Verify the user is able to monitor the AP health of created sites or not	Passed	
WLJPI36S _Reg_244	AP Critical/Generic health metrics for Japanese SSID	Validate the AP Critical/Generic health metrics showing properly or not	Passed	
WLJPI36S _Reg_245	Modify the client health rules	Verify the client health rule is able to Apply or not client after modifying	Passed	

WLC Health Scoring

Logical ID	Title	Description	Status	Defect ID
WLJPI36S _Reg_246	Checking the client coverage with the signal strength of AP less than the critical value 50.	If the client connected is less than the coverage of 50 then it indicates green color with no errors and warnings.	Passed	
WLJPI36S _Reg_247	Checking the client coverage with the signal strength of AP more than the critical value 50.	If the client connected is more than the coverage of 50 then it indicates yellow color with warnings.	Passed	

WLJPI36S _Reg_248	Checking the client coverage with the signal strength of AP more than the warning threshold value 70.	If the client connected is more than the coverage of 70 then it indicates red color with critical issues.	Passed	
WLJPI36S _Reg_249	Checking the client On boarding for the time taken to connect to the network less than 10ms and less than 50 clients.	To check whether the network gets connected with less than 10ms and with less than 50 then it indicates green color with no errors and warnings.	Passed	
WLJPI36S _Reg_250	Checking the client On boarding for the time taken to connect to the network with more than 10ms and less/more than 50 clients.	To check whether the network gets connected with more than10ms and with less/more than 50 then it indicates yellow color with warnings.	Passed	
WLJPI36S _Reg_251	Checking the client On boarding for the time taken to connect to the network with less/more than 10ms and more than 70 clients.	To check whether the network gets connected with less/more than10ms and with more than 70 then it indicates red color with critical issues.	Passed	
WLJPI36S _Reg_252	Checking the CPU utilization during the client connectivity is less than 50.	To verify during the Client connectivity the CPU utilization is less than 50 means it indicates green color with no errors and warnings.	Passed	

WLJPI36S _Reg_253	Checking the CPU utilization during the client connectivity is more than 50.	To verify during the Client connectivity the CPU utilization is less than 50 means it indicates yellow color with warnings.	Passed	
WLJPI36S _Reg_254	Checking the CPU utilization during the client connectivity is more than 70.	To verify during the Client connectivity the CPU utilization is less than 50 means it indicates red color with critical issues.	Passed	
WLJPI36S _Reg_255	Checking the memory utilization during the client connectivity is less than 50.	To verify during the Client connectivity the memory utilization is less than 50 means it indicates green color with no errors and warnings.	Passed	
WLJPI36S _Reg_256	Checking the memory utilization during the client connectivity is more than 50.	To verify during the Client connectivity the memory utilization is less than 50 means it indicates yellow color with warnings.	Passed	
WLJPI36S _Reg_257	Checking the memory utilization during the client connectivity is more than 70.	To verify during the Client connectivity the memory utilization is less than 50 means it indicates red color with critical issues.	Passed	
WLJPI36S _Reg_258	Checking the devices availability	To check whether the devices are available or not.	Passed	

WLJPI36S _Reg_259	Setting the wireless health rule and verifying that rule is working or not	Verify that user can edit the wireless health rule and Apply on device or not	Passed	
WLJPI36S _Reg_260	Connecting to Hotspot client and monitoring the health score	Connecting the client with Hotspot WLAN and monitoring the Memory & CPU utilization and the Signal Strength.	Passed	
WLJPI36S _Reg_261	Checking the client On boarding in CME	To verify the client On boarding for the time taken to connect to the network in CME and it is indicated with colors as Green-safe, Yellow-warnings & Red-Critical.	Passed	

EOGRE Profile

Logical ID	Title	Description	Status	Defect ID
WLJPI36S _Reg_262	Configuring a tunnel gateway by providing invalid IPv4 address	To check whether proper error message got displayed while creating tunnel gateway with invalid IPv4 address	Passed	
WLJPI36S _Reg_263	Creating a EoGRE Profile Name in Japanese character	To verify whether the EoGRE Profile Name accepts Japanese character or not	Failed	CSCvo91527
WLJPI36S _Reg_264	Deploying the template from PI to Controller	To push the saved template from PI to controller	Passed	

WLJPI36S _Reg_265	Configuring the EoGRE rule to set up the tunnel	To validate whether EoGRE rule reflects after it got saved	Passed	
WLJPI36S _Reg_266	Connecting Android clients with Flexconnect local switching enabled WLAN with Tunnel profile Rule followed by marking Tunnel Parameters Gateway as AAA Proxy and Accounting proxy	To check whether Android clients get associated while Flexconnect local switching enabled WLAN with Tunnel profile Rule followed by marking Tunnel Parameters Gateway as AAA Proxy and Accounting proxy	Passed	
WLJPI36S _Reg_267	Connecting Android clients with Flexconnect local switching enabled WLAN with Tunnel profile Rule followed by marking Tunnel Parameters as DHCP option-82	To check whether Android clients get associated while Flexconnect local switching enabled WLAN with Tunnel profile Rule followed by marking Tunnel Parameters Gateway as DHCP Option - 82	Passed	
WLJPI36S _Reg_268	Connecting IOS clients to a local switching enabled WLAN with Tunnel profile Rule followed by marking Tunnel Parameters Gateway as AAA Proxy and Accounting proxy	To check whether IOS clients get associated while Flexconnect local switching enabled WLAN with Tunnel profile Rule followed by marking Tunnel Parameters Gateway as AAA Proxy and Accounting proxy	Passed	

WLJPI36S _Reg_269	Connecting Windows clients to a local switching enabled WLAN with Tunnel profile Rule followed by marking Tunnel Parameters Gateway as AAA Proxy and Accounting proxy	To check whether Windows clients get associated while Flexconnect local switching enabled WLAN with Tunnel profile Rule followed by marking Tunnel Parameters Gateway as AAA Proxy and Accounting proxy	Passed	
WLJPI36S _Reg_270	Associating Apple MacBook clients to a local switching enabled WLAN with Tunnel profile Rule followed by marking Tunnel Parameters Gateway as AAA Proxy and Accounting proxy	To check whether Apple clients get associated while Flexconnect local switching enabled WLAN with Tunnel profile Rule followed by marking Tunnel Parameters Gateway as AAA Proxy and Accounting proxy	Passed	
WLJPI36S _Reg_271	Connecting IOS clients to a local switching enabled WLAN with Tunnel profile Rule followed by marking Tunnel Parameters as DHCP option-82	To check whether IOS clients get associated while Flexconnect local switching enabled WLAN with Tunnel profile Rule followed by marking Tunnel Parameters as DHCP option-82	Failed	CSCvp16327

WLJPI36S _Reg_272	Connecting Windows clients to a local switching enabled WLAN with Tunnel profile Rule followed by marking Tunnel Parameters as DHCP option-82	To check whether Windows clients get associated while Flexconnect local switching enabled WLAN with Tunnel profile Rule followed by marking Tunnel Parameters as DHCP option-82	Passed	
WLJPI36S _Reg_273	Associating Apple MacBook clients to a local switching enabled WLAN with Tunnel profile Rule followed by marking Tunnel Parameters as DHCP option-82	To check whether Apple clients get associated while Flexconnect local switching enabled WLAN with Tunnel profile Rule followed by marking Tunnel Parameters as DHCP option-82	Passed	

Support Flex + Bridge mode configuration for Access points

Logical ID	Title	Description	Status	Defect ID
WLJPI36S _Reg_274	Checking the JOS clients association with AP configured in Flex+bridge mode	To check whether JOS clients getting associated or not to AP configured in Flex+Bridge mode	Passed	
WLJPI36S _Reg_275	Checking the Android clients association with AP configured in Flex+bridge mode	To check whether Android clients getting associated or not to AP configured in Flex+Bridge mode	Passed	

WLJPI36S _Reg_276	Checking the iOS clients association with AP configured in Flex+bridge mode	To check whether iOS clients getting associated or not to AP configured in Flex+Bridge mode	Passed	
WLJPI36S _Reg_277	Checking the MAC OS clients association with AP configured in Flex+bridge mode	To check whether MAC OS clients getting associated or not to AP configured in Flex+Bridge mode	Passed	
WLJPI36S _Reg_278	Checking the Android & iOS clients associations with Flex+Bridge mode AP in local authentication	To check whether Android & iOS clients getting associated or not to Flex+bridge mode AP when Local authentication is enabled	Passed	
WLJPI36S _Reg_279	Checking the MAC & JOS clients associations with Flex+Bridge mode AP in local authentication	To check whether MAC & JOS clients getting associated or not to Flex+bridge mode AP when Local authentication is enabled	Passed	
WLJPI36S _Reg_280	Checking the Android & iOS clients associations with Flex+Bridge mode AP in RAP after Mesh setup	To check whether Android & iOS clients getting associated or not to Flex+bridge mode AP which is configured as Root AP	Passed	
WLJPI36S _Reg_281	Checking the MAC & JOS clients associations with Flex+Bridge mode AP in RAP after Mesh setup	To check whether MAC & JOS clients getting associated or not to Flex+bridge mode AP which is configured as Root AP	Passed	

WLJPI36S _Reg_282	Checking the Android & iOS clients associations with Flex+Bridge mode AP in MAP after Mesh setup	To check whether Android & iOS clients getting associated or not to Flex+bridge mode AP which is configured as Mesh AP	Passed	
WLJPI36S _Reg_283	Checking the MAC & JOS clients associations with Flex+Bridge mode AP in MAP after Mesh setup	To check whether MAC & JOS clients getting associated or not to Flex+bridge mode AP which is configured as Mesh AP	Passed	
WLJPI36S _Reg_284	Performing the Intra roaming for Android & iOS clients between 2 AP's	To check whether Android & IOS clients can be roamed between 2 AP's (mode as Flex+bridge) in a WLC	Passed	
WLJPI36S _Reg_285	Performing the Intra roaming for MAC & Windows JOS clients between 2 AP's	To check whether MAC & JOS clients can be roamed or not between 2 AP's (mode should be different) in a WLC	Passed	
WLJPI36S _Reg_286	Performing Inter roaming of all OS clients between 2 WLC's	To check whether all OS clients can be roamed or not between 2 AP's in different WLC	Passed	

Open DNS Support

Logical ID	Title	Description	Status	Defect ID
WLJPI36S _Reg_287	Changing the WLAN Mode for the Created WLAN Profile Name	To Vary the WLAN Mode for the Created WLAN Profile Name	Passed	

WLJPI36S _Reg_288	Mapping the Created WLAN Profile name with an AP group	To Represent the Created WLAN Profile Name with an AP Group	Passed	
WLJPI36S _Reg_289	Creating the Policy Name for the Created WLAN Profile Name	To form the Policy Name for the Created WLAN Profile Name	Passed	
WLJPI36S _Reg_290	Deploying the template from PI to Controller	To push the saved template from PI to controller	Passed	

Support hyperlocation config enhancement in Lightweight AP template

Logical ID	Title	Description	Status	Defect ID
WLJPI36S _Reg_291	Copying the all external antenna parameter of 802.11 a/n/ac and 802.11 b/g/n radio to other radio	Verify that user is able to copy the all antenna parameter of 802.11a/n/ac radio to other radio or not and deploying the template on AP	Passed	
WLJPI36S _Reg_292	Copying the some selected external antenna parameter of 802.11 a/n/ac and 802.11 b/g/n radio to other radio	Verify that user is able to copy the some selected antenna parameter of 802.11a/n/ac radio to other radio or not and deploying the template on AP	Passed	
WLJPI36S _Reg_293	Connecting the different OS client after deploying the template of AP	Checking the client connectivity after deploying the AP template	Passed	

WLJPI36S _Reg_294	Checking the radio status of AP after deploying the AP template	Verify the radio status of AP after deploying the AP template	Passed	

Outdoor AP GPS support

Logical ID	Title	Description	Status	Defect ID
WLJPI36S _Reg_295	Joining the outdoor AP with WLC	Verify that user is able to join outdoor with WLC or not	Passed	
WLJPI36S _Reg_296	Discovering the outdoor AP PI	Verify that outdoor AP discovering in PI or not	Passed	
WLJPI36S _Reg_297	Creating the MAPs and adding the outdoor AP	Verify that user is able to create map and add the outdoor AP in that map or not	Passed	
WLJPI36S _Reg_298	Locating the outdoor AP on maps	Locating the outdoor AP via GPS on map	Passed	
WLJPI36S _Reg_299	Exporting the geo location of outdoor AP	Verify that user is able to exporting the AP location or not	Passed	
WLJPI36S _Reg_300	Importing the geo location of outdoor AP	Verify that user is able to importing the AP location or not	Passed	
WLJPI36S _Reg_301	Locating the client on map that are associated with outdoor AP	Verify that user is able to locate client on maps after connected with outdoor AP	Passed	
WLJPI36S _Reg_302	Placing the AP of different location and locating via GPS	Verify that user is able to locate the AP after placing at different location or not	Passed	

Scheduled AP upgrade

Logical ID	Title	Description	Status	Defect ID
WLJPI36S _Reg_303	Upgrading the primary image for WLC/AP via default TFTP server on Scheduled time	To check whether WLC/AP upgrading or not via default TFTP server on Scheduled time	Passed	
WLJPI36S _Reg_304	Upgrading the primary image for WLC/AP via external TFTP server on Scheduled time	To verify the WLC/AP upgrading or not via external TFTP server on Scheduled time	Passed	
WLJPI36S _Reg_305	Upgrading the primary image for WLC/AP via default FTP server on Scheduled time	To check whether WLC/AP upgrading or not via default FTP server on Scheduled time	Passed	
WLJPI36S _Reg_306	Upgrading the primary image for WLC/AP via external ftp server on Scheduled time	To verify the WLC/AP upgrading or not via external ftp server on Scheduled time	Passed	
WLJPI36S _Reg_307	Upgrading the primary image for WLC/AP via default SFTP server on Scheduled time	To check whether WLC/AP upgrading or not via default SFTP server on Scheduled time	Passed	
WLJPI36S _Reg_308	Upgrading the primary image for WLC/AP via external SFTP server on Scheduled time	To verify the WLC/AP upgrading or not via external SFTP server on Scheduled time	Passed	
WLJPI36S _Reg_309	Upgrading the backup image for WLC/AP via default TFTP server	To check whether backup image downloading or not via default TFTP server on Scheduled time	Passed	

WLJPI36S _Reg_310	Upgrading the backup image for WLC/AP via external TFTP server on Scheduled time	Verify the WLC/AP backup image upgrading or not via external TFTP server on Scheduled time	Passed	
WLJPI36S _Reg_311	Upgrading the Backup image for WLC/AP via default FTP server on Scheduled time	To check whether WLC/AP Backup image upgrading or not via default FTP server on Scheduled time	Passed	
WLJPI36S _Reg_312	Upgrading the Backup image for WLC/AP via external FTP server on Scheduled time	To verify the WLC/AP upgrading or not via external FTP server on Scheduled time	Passed	
WLJPI36S _Reg_313	Upgrading the Backup image for WLC/AP via default SFTP server on Scheduled time	To check whether WLC/AP Backup image upgrading or not via default SFTP server on Scheduled time	Passed	
WLJPI36S _Reg_314	Upgrading the Backup image for WLC/AP via external SFTP server on Scheduled time	To verify the WLC/AP Backup image upgrading or not via external SFTP server on Scheduled time	Passed	
WLJPI36S _Reg_315	Upgrading the primary/backup image for flex connect AP's/WLC on Schedule time via default TFTP/SFTP/ftp servers	To check whether flex Connect AP's/WLC are upgrading or not on Scheduled time	Passed	
WLJPI36S _Reg_316	Upgrading the primary/backup image for flex connect AP's/WLC on Scheduled time via external TFTP/SFTP/ftp servers	To verify flex Connect AP's/WLC are upgrading or not on Scheduled time	Passed	

Support Mobility Express on Maps

Logical ID	Title	Description	Status	Defect ID
WLJPI36S _Reg_317	Adding ME controllers with it neighbors and check the Rx neighbor functionality .	To add the ME master controller to the maps with its slave AP and verify if the controller and other AP added to maps and check the Rx neighbor functionality..	Passed	
WLJPI36S _Reg_318	Adding a ME controller with one neighbor AP in sensor mode.	To add a ME controller AP with one neighbor AP in sensor and check the details of the neighbor AP .	Passed	
WLJPI36S _Reg_319	Checking the details of the ME controller placed on the floor	To check the details of the ME controller placed on the floor and compare the details and check if the details are same or not.	Passed	
WLJPI36S _Reg_320	Changing the azimuthal angle and elevation for the ME AP	To change the azimuth angle and elevation of the ME AP and check if the azimuthal angle and elevation of the AP is changed or not.	Passed	
WLJPI36S _Reg_321	Deleting ME controller AP from the floor of the building	To delete the ME controller AP from the floor of the building and check if the AP gets deleted from it or not	Passed	
WLJPI36S _Reg_322	Check the ME controller AP while searching using Search option on MAP	To check if the ME controller AP when searched in Search on MAP is shown or not.	Passed	

WLJPI36S _Reg_323	Export a MAP added with ME controller, import the same file and check the details.	To export the MAP added with ME controller and import the same file and check if the details are same.	Passed	
WLJPI36S _Reg_324	Export a MAP added with ME controller and import the same file to CMX .	To export a MAP with ME controller and import the same file to CMX and check if the file gets imported with the same	Passed	
WLJPI36S _Reg_325	Connecting a JOS window client to the ME controller in the floor map.	To connect a JOS window client to ME controller added to the floor and check if the client gets connected and the client details are shown or not.	Passed	
WLJPI36S _Reg_326	Moving the ME Controller AP from One floor to the other and check if the client moves from one floor to other.	To move the ME controller AP from one floor to the other and check if the clients move form one floor to other and verify the client detail.	Passed	
WLJPI36S _Reg_327	Check the data in top client count in particular AP in the chart and verifying it.	To verify the data in top client count in particular AP in the chart and verify the details in the chart.	Passed	
WLJPI36S _Reg_328	Check the data in top AP by interference in the chart and verifying it.	To verify the data in top AP by interference in the chart and verify the details in the chart.	Passed	
WLJPI36S _Reg_329	Creating a report for the Building which contains ME controller	To Create a scheduled report for the building which has the ME controller AP and check if the report is generated or not.	Passed	

WLJPI36S _Reg_330	Changing the parameters of the ME AP for Alarm checking.	To change the parameters of the ME AP and check if the alarm is triggered for changing corresponding parameter .	Passed	

Audit Logging for Maps/Wireless

Logical ID	Title	Description	Status	Defect ID
WLJPI36S _Reg_331	Creating a site under wireless MAP and check Audit dashboard.	To create a site in wireless maps and check if there is a log in the Audit dashboard or not.	Passed	
WLJPI36S _Reg_332	Creating a building under wireless MAP	To create a building in wireless maps and check if there is a log in the Audit dashboard or not.	Passed	
WLJPI36S _Reg_333	Creating a floor in a site MAP	To create a floor in a site map and check if the Audit dashboard shows the log for the floor created in the site maps	Passed	
WLJPI36S _Reg_334	Importing a MAP file to PI	To import a MAP file to PI and check if the Valid log is generated in Audit Dashboard	Passed	
WLJPI36S _Reg_335	Deleting a site under wireless MAP and check Audit dashboard.	To delete a site under wireless map and check if the audit dashboard generated log for the deleted site	Passed	

WLJPI36S _Reg_336	Deleting a building under wireless MAP	To delete a building in wireless map and check if the log is captured in audit dashboard or not.	Passed	
WLJPI36S _Reg_337	Delete a floor in a site MAP	To delete a floor in a map and verify if the log is generated in audit dashboard or not.	Passed	
WLJPI36S _Reg_338	Changing the parameters in the site of the map	To change the parameters in the site created in the maps and verify if the logs created in the audit dashboard.	Passed	
WLJPI36S _Reg_339	Editing the building created in the maps .	To edit the parameters of the building created in the maps and check if there is a log generated in the Audit dashboard	Passed	
WLJPI36S _Reg_340	Editing the Floor created in the maps .	To edit the parameters of the floor created in the maps and check if there is a log generated in the Audit dashboard	Passed	
WLJPI36S _Reg_341	Adding a AP to floor of the wireless map	To add a AP to the floor of the map and check if there is a log for that in the change audit dashboard .	Passed	
WLJPI36S _Reg_342	Deleting a AP from the floor of the wireless map	To delete the AP from the floor of the map and to verify if a log is generated of that in audit dashboard.	Passed	

Support for Zero Touch Deployment for ME-AP

Logical ID	Title	Description	Status	Defect ID
WLJPI36S _Reg_343	Associating the ME AP to WLC and Verifying in PI.	Able to see the ME AP In PI,after associating WLC.	Passed	
WLJPI36S _Reg_344	To verifying the client data rate through PI.	To check the data rate of the particular client connected to the WLAN.	Passed	
WLJPI36S _Reg_345	To configure the authentication for The ME AP	To check whether the authentication is configured into ME AP	Passed	
WLJPI36S _Reg_346	Associating ME AP with different country code as with WLC and check it is not joined in WLC.	To associate ME AP with different country code and check it is not joined with WLC.	Passed	
WLJPI36S _Reg_347	Configuring ME AP with duplicate IP address into WLC and verify in PI.	To configure AP with a duplicate IP address and check AP does not join the WLC	Passed	
WLJPI36S _Reg_348	Checking the ME AP channel Utilization/Interference.	To check the timings based on Radio:802.11b/g/n Slot:0 Channel Number, ME AP channel Utilization/Interference according to date.	Passed	
WLJPI36S _Reg_349	Connecting a window client to the ME AP	To connect a window client to the AP and check the client gets connected or not.	Passed	
WLJPI36S _Reg_350	Connecting a Android client to the ME AP	To connect a Android client to the AP and check the client gets connected or not.	Passed	

WLJPI36S _Reg_351	Connecting a IOS client to the ME AP	To connect a IOS client to the AP and check the client gets connected or not.	Passed	
WLJPI36S _Reg_352	Connecting a MAC client to the ME AP	To connect a MAC client to the AP and check if the client gets connected or not.	Passed	
WLJPI36S _Reg_353	Set the ME AP monitor mode.	To check whether ME AP monitor mode reflected or not in PI after AP mode changing in WLC.	Passed	
WLJPI36S _Reg_354	Connect IPhone client to WLAN after creating DHCP scope	To verify that IPhone connect successfully after creating DHCP scope	Passed	
WLJPI36S _Reg_355	Connect Japanese client to WLAN after creating DHCP scope	To verify that Japanese connect successfully after creating DHCP scope	Passed	
WLJPI36S _Reg_356	Connect Android client to WLAN after creating DHCP scope	To verify that Android connect successfully after creating DHCP scope	Passed	
WLJPI36S _Reg_357	Connect Windows client to WLAN after creating DHCP scope	To verify that Windows connect successfully after creating DHCP scope	Passed	
WLJPI36S _Reg_358	Connect iOS client to WLAN after creating DHCP scope	To verify that iOS connect successfully after creating DHCP scope	Passed	
WLJPI36S _Reg_359	Scheduled rebooting the CME from PI	To verify whether scheduled rebooting CME from PI is successful.	Passed	

WLJPI36S _Reg_360	AP configuration from PI joined to CME.	To verify whether AP configuration changes from PI Applies successfully in CME.	Passed	

Better HA Monitoring and Management

Logical ID	Title	Description	Status	Defect ID
WLJPI36S _Reg_361	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	
WLJPI36S _Reg_362	Controller HA pair with different hardware models (3504 and 8540)	To verify the role negotiation between the controllers with different hardware models	Passed	
WLJPI36S _Reg_363	Verifying the serial number of the standby controller	To check whether the serial number of the standby controller is getting or not	Passed	
WLJPI36S _Reg_364	Verifying the FAN status of the standby controller	To verify whether the FAN status of the standby controller is getting or not	Passed	
WLJPI36S _Reg_365	Configuring controller HA pair with different software versions	To verify whether controllers HA pair with different software versions	Passed	
WLJPI36S _Reg_366	Checking the controller mode when the redundancy port loses connectivity	To verify the HA pair controller mode after disconnecting the redundancy port	Passed	

WLJPI36S _Reg_367	Checking the controller modes(HA pair) after power failure	To verify the controller modes after power failure on both the controllers	Passed	
WLJPI36S _Reg_368	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	
WLJPI36S _Reg_369	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	

SWIM Support of Mobility Express Controllers

Logical ID	Title	Description	Status	Defect ID
WLJPI36S _Reg_370	Importing a ME image through a file.	To Import a ME image as a file and check if the file gets imported or not	Passed	
WLJPI36S _Reg_371	Importing a ME image from a device	To import a ME image from a device and check if the ME images gets imported from the device or not	Passed	
WLJPI36S _Reg_372	Importing the ME image through Cisco.Com using Credentials	To Import a ME image from Cisco.com by giving the cisco credentials and check if the ME image gets imported or not	Passed	
WLJPI36S _Reg_373	Importing the ME image through the URL	To import the ME image using URL and check if the ME images gets imported or not.	Passed	

WLJPI36S _Reg_374	Changing the ME image transfer protocol order .	To change the ME image transfer protocol order and check if the order is changed or not	Passed	
WLJPI36S _Reg_375	Importing a ME image through a protocol.	To import a ME image from a device and check if the images gets imported from the device or not	Passed	
WLJPI36S _Reg_376	Checking the ME image imported through the Software image Summary	To Check if the ME image imported is shown in the software image summary or not	Passed	
WLJPI36S _Reg_377	ME image is distributed with all the different devices .	To check whether the ME image is distributed among the different devices selected	Passed	

TACACS+ & RADIUS servers added without any authentication

Logical ID	Title	Description	Status	Defect ID
WLJPI36S _Reg_378	Adding the RADIUS server in Users, Roles & AAA	Verifying whether RADIUS server is added or not in Users, Roles & AAA mode	Passed	
WLJPI36S _Reg_379	Verifying the RADIUS server reachability	To check whether successfully contacted RADIUS server or not	Passed	
WLJPI36S _Reg_380	Adding the TACACS+ server in Users, Roles & AAA	Verifying whether TACACS+ server is added or not in Users, Roles & AAA mode	Passed	
WLJPI36S _Reg_381	Verifying the TACACS+ server reachability with ISE	To check whether successfully contacted TACACS+ server or not	Passed	

WLJPI36S _Reg_382	Adding the RADIUS server with DNS name in Users, Roles & AAA	Verify whether RADIUS server is added or not with DNS name	Passed	
WLJPI36S _Reg_383	Checking the RADIUS server reachability with DNS name	To check whether successfully contacted RADIUS server or not with DNS name	Passed	
WLJPI36S _Reg_384	Adding the TACACS+ server with DNS name in Users, Roles & AAA	Verifying the TACACS+ server is adding or not with DNS name	Passed	
WLJPI36S _Reg_385	Verifying the TACACS+ server reachability with DNS name	To check whether successfully contacted TACACS+ server or not with DNS name	Passed	
WLJPI36S _Reg_386	Verifying the RADIUS server reachability via PAP Authentication	To check whether RADIUS server is successfully contacted or not via PAP Authentication	Passed	
WLJPI36S _Reg_387	Checking the RADIUS server reachability via CHAP Authentication	Verifying RADIUS server is successfully contacted or not via CHAP Authentication	Passed	
WLJPI36S _Reg_388	Verify the RADIUS server reachability via EAP_TTLS Authentication	To check whether RADIUS server is successfully contacted or not via EAP_TTLS Authentication	Passed	
WLJPI36S _Reg_389	Verifying the TACACS+ server reachability via PAP Authentication	To check whether TACACS+ server is successfully contacted or not via PAP Authentication	Passed	

WLJPI36S _Reg_390	Checking the TACACS+ server reachability via CHAP Authentication	Verifying the TACACS+ server is successfully contacted or not via CHAP Authentication	Passed	
WLJPI36S _Reg_391	Add the more than 3 RADIUS server through IP address in Users, Roles & AAA	To check whether more than 3 RADIUS server is able to add or not via server IP	Passed	
WLJPI36S _Reg_392	Add the more than 3 RADIUS server through DNS name in Users, Roles & AAA	To check whether more than 3 RADIUS server is able to add or not via DNS name	Passed	
WLJPI36S _Reg_393	Add the more than 3 TACACS+ server through IP address in Users, Roles & AAA	To check whether more than 3 TACACS+ server is able to add or not via server IP	Passed	
WLJPI36S _Reg_394	Add the more than 3 TACACS+ server through DNS name in Users, Roles & AAA	To check whether more than 3 TACACS+ server is able to add or not via DNS name	Passed	
WLJPI36S _Reg_395	Verifying the popup alert message Icon for contacted TACACS+/RADIUS server	To check whether popup alert message Icon gets displayed properly or not after contacted TACACS+/RADIUS server	Passed	
WLJPI36S _Reg_396	Verifying the Invalid RADIUS server connection via IP/DNS	To check whether RADIUS server is successfully contacted or not through IP/DNS	Passed	
WLJPI36S _Reg_397	Verifying the Invalid TACACS+ server reachability via IP/DNS	To check whether TACACS+ server is successfully contacted or not through IP/DNS	Passed	

WLJPI36S _Reg_398	Checking the RADIUS server reachability for invalid Secrete key	Verifying the RADIUS server reachability for invalid secrete key	Passed	
WLJPI36S _Reg_399	Verifying the TACACS+ server reachability for invalid Secrete key	Verifying the TACACS+ server reachability for invalid secrete key	Passed	

eWLC Support for Airtime Entitlement

Logical ID	Title	Description	Status	Defect ID
WLJPI36S _Reg_400	Adding a elk controller in PI	To Verify whether elk is added in PI	Passed	
WLJPI36S _Reg_401	Create RF Profile with ATF Enforce mode in 2.4GHZ/5GHz and deploy to elk	To verify whether RF with Enforce mode is created successfully in 2.4GHZ/5GHz	Passed	
WLJPI36S _Reg_402	Enable optimization in RF profile with ATF Enforce mode in 2.4GHZ/5GHz and deploy to elk	To verify whether optimization in RF with Enforce mode is created successfully in 2.4GHZ/5GHz	Passed	
WLJPI36S _Reg_403	Apply ATF Enforce mode 2.4GHZ/5GHz on RF group	To verify whether Enforcement mode is Applied on RF group successfully	Failed	CSCvo88066
WLJPI36S _Reg_404	Client connectivity with WPA/WPA2 Personal L2 security WLAN having ATF in enforcement mode	To verify the client connectivity with WPA/WPA2 Personal having ATF in Enforcement mode	Passed	

WLJPI36S _Reg_405	Client connectivity with WPA/WPA2 Enterprise L2 security WLAN having ATF in enforcement mode	To verify the client connectivity with WPA/WPA2 Enterprise having ATF in Enforcement mode	Passed	
WLJPI36S _Reg_406	Client connectivity with WPA/WPA2 Personal L2 security and L3 webauth WLAN having ATF in enforcement mode	To verify the client connectivity with WPA/WPA2 Personal and webauth having ATF in enforced mode	Passed	
WLJPI36S _Reg_407	Connecting clients to 4800 AP in flex connect mode with ATF profile in enforced mode	To verify whether clients gets connected to 4800 AP in flex connect mode with ATF profile in enforced mode	Passed	
WLJPI36S _Reg_408	Connecting clients to 4800 AP in local mode with ATF profile in enforced mode	To verify whether clients gets connected to 4800 AP in local mode with ATF profile in enforced mode	Passed	
WLJPI36S _Reg_409	Client connectivity with L2 security WLAN having different Policy weight	To verify the client connectivity with two SSID having different weight	Passed	
WLJPI36S _Reg_410	Create the ATF profile and perform AP deployment and rule deployment to eWLC	To verify whether the profile is deployed to elk through AP deployment and rule deployment	Passed	

WLJPI36S _Reg_411	Client connectivity in mesh setup with ATF profile in enforced mode	To verify whether clients gets connected in mesh setup AP	Passed	
WLJPI36S _Reg_412	Create ATF profile with Weight Usage template in PI and deploy to elk	To verify whether ATF is created with weight usage template in PI and deployed to elk successfully	Passed	
WLJPI36S _Reg_413	Create RF Profile with ATF disable mode in 2.4GHZ/5GHz and deploy to elk	To verify whether RF with disabled mode is created successfully in 2.4GHZ/5GHz and deployed to elk	Passed	
WLJPI36S _Reg_414	Apply ATF disable mode 2.4GHZ/5GHz on RF group	To verify whether disabled is Applied on RF group successfully	Passed	
WLJPI36S _Reg_415	Client connectivity with WPA/WPA2 Personal L2 security WLAN having ATF in disable mode	To verify the client connectivity with WPA/WPA2 Personal having ATF in disabled mode	Passed	
WLJPI36S _Reg_416	Client connectivity with WPA/WPA2 Enterprise L2 security WLAN having ATF in disable mode	To verify the client connectivity with WPA/WPA2 Enterprise having ATF in disabled mode	Passed	

WLJPI36S _Reg_417	Client connectivity with WPA/WPA2 Personal L2 security and L3 as webauth WLAN having ATF in disable mode	To verify the client connectivity with WPA/WPA2 Personal and webauth having ATF in disabled mode	Passed	
WLJPI36S _Reg_418	Enable optimization in RF profile with ATF disable mode in 2.4GHZ/5GHz and deploy to elk	To verify whether optimization in RF with disabled mode is created successfully in 2.4GHZ/5GHz deployed to elk	Passed	
WLJPI36S _Reg_419	Create RF Profile with ATF monitor mode in 2.4GHZ/5GHz and deploy to elk	To verify whether RF with monitor mode is created successfully in 2.4GHZ/5GHz	Passed	
WLJPI36S _Reg_420	Enable optimization in RF profile with ATF monitor mode in 2.4GHZ/5GHz and deploy to elk	To verify whether optimization in RF with monitor mode is created successfully in 2.4GHZ/5GHz	Passed	
WLJPI36S _Reg_421	Apply ATF monitor mode 2.4GHZ/5GHz on RF group	To verify whether monitor is Applied on RF group successfully	Passed	
WLJPI36S _Reg_422	Client connectivity with WPA/WPA2 Personal L2 security WLAN having ATF in monitor mode	To verify the client connectivity with WPA/WPA2 personal having ATF in monitor mode	Passed	

WLJPI36S _Reg_423	Client connectivity with WPA/WPA2 Enterprise L2 security WLAN having ATF in monitor mode	To verify the client connectivity with WPA/WPA2 Enterprise having ATF in monitor mode	Passed	
WLJPI36S _Reg_424	Client connectivity with WPA/WPA2 Personal L2 security and L3 as webauth WLAN having ATF in monitor mode	To verify the client connectivity with WPA/WPA2 Personal and webauth having ATF in monitor mode	Passed	

Support for AP 4800 in PI

Logical ID	Title	Description	Status	Defect ID
WLJPI36S _Reg_425	Associating 4800 AP to WLC and verifying in PI	To associate the 4800 AP to WLC and check if the AP gets associated and the AP is shown in PI or not	Passed	
WLJPI36S _Reg_426	Configuring different AP parameters In WLC checking the same in PI without syncing	To configure different AP parameters in WLC and check the same in PI without syncing the controller to which the AP is connected	Passed	
WLJPI36S _Reg_427	Configuring different AP parameters In WLC checking the same in PI after syncing the controller	To configure different AP parameters in WLC and check the same in PI after syncing the controller to which the AP is connected	Passed	

WLJPI36S _Reg_428	Checking Details of 4800 AP in PI and comparing it with WLC	To view details of AP in GUI PI and Check If the detail if it's identical	Passed	
WLJPI36S _Reg_429	Restarting the 4800 AP through PI	To verify if the AP gets Restored and check if the old configuration are intact with the AP after reboot.	Passed	
WLJPI36S _Reg_430	Changing the 4800 AP mode from PI	To change the AP mode from Local to Flex connect and check if the AP from Local to flex connect or not	Passed	
WLJPI36S _Reg_431	Configure global authentication for the access point using PI	To configure username, password for the access point using PI and check if the Override Global Username Password is set without any errors and AP uses this password when opened through AP console.	Passed	
WLJPI36S _Reg_432	Configuring the 4800 AP with different country codes in PI	To configure the 4800 AP with different country codes through PI and check if the country codes are changed or not	Passed	
WLJPI36S _Reg_433	Configuring Primary Controller for the 4800 AP with different Failover Priority	To configure primary controller parameters for the AP 4800 with different AP Failover Priority.	Passed	

WLJPI36S _Reg_434	Creating a AP group in WLC UI and mapping the 4800 AP to that group from PI	To create a AP group from WLC UI and mapping the 4800 AP to the same group through PI and check if the AP moves to the AP group or not	Passed	
WLJPI36S _Reg_435	Creating a WLAN template with Open security in PI and connecting a client	To create a WLAN template in PI with Open security and check if clients gets connected to the WLAN created from PI.	Passed	
WLJPI36S _Reg_436	Creating a WLAN template with 802.1x security in PI and connecting a client	To create a WLAN template in PI with 802.1x security and check if clients gets connected to the WLAN created from PI.	Passed	
WLJPI36S _Reg_437	Creating a WLAN template with WPA+WPA2 security in PI and connecting a client	To create a WLAN template in PI with WPA+WPA2 security and check if clients gets connected to the WLAN created from PI.	Passed	
WLJPI36S _Reg_438	Creating a WLAN template with Static WEP security in PI and connecting a client	To create a WLAN template in PI with Static WEP security and check if clients gets connected to the WLAN created from PI.	Passed	
WLJPI36S _Reg_439	Adding the AP 4800 to the floor map and connecting a client	To add the AP 4800 to the floor map and check if the AP gets added to the floor and connecting a client to it .	Passed	

WLJPI36S _Reg_440	Validating the client count and channel utilization, Top N clients ,Access point details of 4800 AP .	To validate the client count , channel utilization, Top N Clients of AP 4800 and check if the give data are correct or not	Passed	
WLJPI36S _Reg_441	Connecting JOS windows client to 4800 AP through WLAN created from PI	To connect JOS Windows client to 4800 AP by using the WLAN created from PI deployed to the WLC .	Passed	
WLJPI36S _Reg_442	Connecting windows 10 client to 4800 AP through WLAN created from PI	To connect Windows 10 client to 4800 AP by using the WLAN created from PI deployed to the WLC .	Passed	
WLJPI36S _Reg_443	Connecting Android client to 4800 AP through WLAN created from PI	To connect Android client to 4800 AP by using the WLAN created from PI deployed to the WLC .	Passed	
WLJPI36S _Reg_444	Connecting IOS client to 4800 AP through WLAN created from PI	To connect IOS Windows client to 4800 AP by using the WLAN created from PI deployed to the WLC .	Passed	
WLJPI36S _Reg_445	Connecting Mac OS windows client to 4800 AP through WLAN created from PI	To connect Mac OS Windows client to 4800 AP by using the WLAN created from PI deployed to the WLC .	Passed	
WLJPI36S _Reg_446	Adding the AP 4800 to the AP group created from PI and Connecting a client	To add the AP 4800 to the AP group created from PI and check if the AP gets added to the AP group and connecting a client to it .	Passed	

WLJPI36S _Reg_447	Adding the AP 4800 to the Flex Connect AP group created from PI and Connecting a client	To add the AP 4800 to the Flex Connect AP group created from PI and check if the AP gets added to the AP group and connecting a client to it .	Passed	
WLJPI36S _Reg_448	Connecting a client to WLAN with 2.4 GHz and Validating the client data rate in PI	To connect a client to the WLAN with 2.4GHz and validating the client data rate in PI	Passed	
WLJPI36S _Reg_449	Connecting a client to WLAN with 5 GHz and Validating the client data rate in PI	To connect a client to the WLAN with 5 GHz and validating the client data rate in PI	Passed	
WLJPI36S _Reg_450	Creating a WLAN with Flexconnect Local Switching and connecting client to the 4800 AP	To create a WLAN with Flexconnect Local Switching and connecting client to the 4800 AP with the Local switched WLAN	Passed	
WLJPI36S _Reg_451	Creating a WLAN with Flexconnect Local Switching ,Local Auth and connecting client to the 4800 AP	To create a WLAN with Flexconnect Local Switching ,Local Auth and connecting client to the 4800 AP with the Local switched WLAN	Passed	
WLJPI36S _Reg_452	Configuring AVC profile and mapping it to the WLAN and connecting client to the AP 4800	To configure AVC profile and mapping it to the WLAN and connecting a client to the WLAN .	Passed	

WLJPI36S _Reg_453	Changing the modes of the AP to check the representation of modes on maps	To change the modes of the AP and check the representation of the AP modes when added to the floor maps.	Passed	
WLJPI36S _Reg_454	Creating a profile and SSID with Japanese character and connecting a client to it	To create a profile and SSID name with Japanese character and	Passed	
WLJPI36S _Reg_455	Generating Custom reports for the 4800 AP through Japanese UI	To generate a custom report for 4800 AP using Japanese UI and check if the generated reports show correct details of the AP.	Passed	
WLJPI36S _Reg_456	Check the details of the 4800 AP on performance dashboard and export the details using Japanese UI	To check the details of the 4800 AP on the performance dashboard in Japanese UI .	Passed	
WLJPI36S _Reg_457	Change the AP configuration and check if the Change audit dashboard logs in Japanese UI	To change configuration on the 4800 AP and check if the log are generated in change audit dashboard.	Passed	

Manage 4800 ME controller in Prime

Logical ID	Title	Description	Status	Defect ID
WLJPI36S _Reg_458	Adding AP 4800 ME in PI with default SNMP details	To verify AP 4800 ME is able to add in PI with default SNMP details	Passed	

WLJPI36S _Reg_459	Adding AP 4800 ME in PI with user modified SNMP details	To verify AP 4800 ME is able to add in PI with user modified SNMP details	Passed	
WLJPI36S _Reg_460	Adding AP 4800 ME in PI with invalid SNMP details	To verify AP 4800 ME is able to add in PI with invalid SNMP details	Passed	
WLJPI36S _Reg_461	Connecting a JOS client to a 4800 internal AP positioned in the Floor	To check if the JOS client gets connected to the AP in the floor and check if the client is show in the Client and user page or not	Passed	
WLJPI36S _Reg_462	Checking 4800 ME client details in CMX	Verifying 4800 ME client details are displaying correct or not in cmx	Passed	
WLJPI36S _Reg_463	Generating a custom report for Client in 4800 ME	To check whether a custom report for client in 4800 ME is generated or not	Passed	
WLJPI36S _Reg_464	Checking AP 4800 ME config got synced in PI	To Verify ME configuration got synced in PI	Passed	
WLJPI36S _Reg_465	Deploying Mac-Filter template to 4800 ME	To Verify Mac-Filter template got deployed in ME from PI	Passed	
WLJPI36S _Reg_466	Deploying AP group template with RF-profile and WLAN to 4800 ME	To Verify AP group template got deployed in ME with WLAN and RF-profile configuration	Passed	
WLJPI36S _Reg_467	Checking template is deployed to 4800 ME with read only added device	To Verify template is deploying or not if device added with read-only	Passed	

WLJPI36S _Reg_468	Creating local management user in 4800 ME from PI	To verify local management user is creating in ME from PI	Passed	
WLJPI36S _Reg_469	Changing Management user priority to TACACS from PI	To verify Management user priority is able to change to TACACS or not from PI	Passed	
WLJPI36S _Reg_470	Checking Android client connection with OPEN security WLAN template	To verify Android client is connecting to OPEN security WLAN deployed from PI	Passed	
WLJPI36S _Reg_471	Checking Windows client connection with WPA Personal security WLAN template	To Verify Windows client is connecting to WPA Personal security WLAN deployed from PI	Passed	
WLJPI36S _Reg_472	Checking IOS client connection with WPA Enterprise security WLAN template	To Verify IOS client is connecting to WPA Enterprise security WLAN deployed from PI	Passed	
WLJPI36S _Reg_473	Checking 4800 ME is coming as controller after performing reset for internal AP	To verify ME in coming as controller after resetting internal AP	Passed	
WLJPI36S _Reg_474	Moving AP from one group to another	To verify AP is changing from one group to another or not	Passed	
WLJPI36S _Reg_475	Detaching scheduled from scheduled WLAN	To verify schedule policy is detached or not from scheduled WLAN	Passed	
WLJPI36S _Reg_476	Performing undeploy for deployed template	To verify deployed configuration got deleted after performing undeploy	Passed	

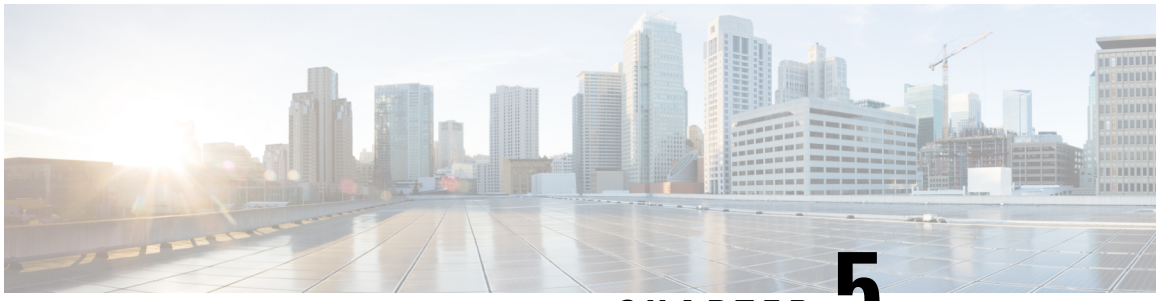
WLJPI36S _Reg_477	Checking same template getting deployed twice	To verify same template is getting deployed twice or not	Passed	
WLJPI36S _Reg_478	Launching ME from PI	Verifying ME is launching from PI or not	Passed	
WLJPI36S _Reg_479	Launching ME from PI after disabling https	Verifying ME is launching from PI or not after disabling https	Passed	
WLJPI36S _Reg_480	Deploying template by adding device with different SNMP communities	Verifying template is getting deployed or not with different SNMP communities	Passed	
WLJPI36S _Reg_481	Exporting AP 4800 CME device details to csv	Verifying CME device details are importing properly or not in csv	Passed	
WLJPI36S _Reg_482	Adding AP 4800 CME device by csv file	Verifying ME device is adding successfully or not from csv file	Passed	
WLJPI36S _Reg_483	Deleting AP 4800 ME device from PI	Verifying ME device is deleting from PI or not	Passed	
WLJPI36S _Reg_484	Verifying external AP joined to 4800 ME are syncing with PI	To verify whether external AP's joined to 4800 ME are reflecting in PI or not	Passed	
WLJPI36S _Reg_485	Rebooting 4800 ME from PI	To Verify 4800 ME is rebooting from PI	Passed	
WLJPI36S _Reg_486	Performing day0 for 4800 ME from PI	To Verify 4800 ME is coming to day0 or not	Passed	
WLJPI36S _Reg_487	Rebooting 4800 ME controller by swapping AP image	To Verify 4800 ME is reflecting same after rebooting ME by swapping AP images	Passed	

WLJPI36S _Reg_488	Rebooting 4800 ME controller without swapping AP image	To Verify 4800 ME is reflecting same after rebooting ME without swapping AP images	Passed	
WLJPI36S _Reg_489	Setting 4800 CME time from PI	To verify CME device time can be set from PI to not	Passed	
WLJPI36S _Reg_490	Creating internal DHCP scope in 4800 ME	To verify internal DHCP scope is creating or not	Passed	
WLJPI36S _Reg_491	Uploading 4800 ME config file	To verify 4800 ME config file is uploading or not	Passed	
WLJPI36S _Reg_492	Downloading 4800 ME config file	To verify 4800 ME coming with same config after downloading the config file	Passed	
WLJPI36S _Reg_493	Performing video stream and verifying in dashboard voice and video	To Verify media stream voice and video details are displaying RTP streams in dashboard	Passed	
WLJPI36S _Reg_494	Checking created media streams in 4800 ME are displayed in PI	To verify media streams in 4800 ME are displayed in PI or not	Passed	
WLJPI36S _Reg_495	Verifying syslog messages for 4800 ME are generating	To verify syslog messages are generating in PI for 4800 ME or not	Passed	
WLJPI36S _Reg_496	Edit the WLAN Configuration for 4800 CME	To verify that configuration updating and reflecting to ME	Passed	
WLJPI36S _Reg_497	Edit the Flexconnect ACL for 4800 CME	To verify that Flexconnect ACL configuration updating and reflecting to ME	Passed	

WLJPI36S _Reg_498	Change the AP mode to sensor for 4800 internal AP	To verify that AP mode changed to sensor or not	Passed	

Config Wireless

Logical ID	Title	Description	Status	Defect ID
WLJPI36S_CWL_03	Location in Clients and User Page is not clearing after deleting the Site	Cheking the client location is clearing or not in User Page after deleting the Site	Failed	CSCvp08856
WLJPI36S_CWL_06	MultiHostMode not reflected in eWLC RLAN Policy Profile	Check whether the MultiHostMode is reflecting or not in eWLC RLAN Policy Profile	Failed	CSCvo82662
WLJPI36S_CWL_09	Syslog host field accepting invalid inputs in PI	Check Whether the Syslog host field accepts invalid inputs or not in PI	Failed	CSCvo59600
WLJPI36S_CWL_10	Flex Profile with Japanese name is not deploying to eWLC	To check whether the user is able to deploy Flex profile or not with Japanese name in eWLC	Failed	CSCvo87412
WLJPI36S_CWL_11	WLAN template deploy got failed due to per WLAN max client range mismatch both PI and eWLC	Checking whether the WLAN template gets deployed or not with WLAN max client range mismatch in both PI and eWLC	Failed	CSCvo61916
WLJPI36S_CWL_14	Getting collection failure when adding vWLC in PI	Checking whether the user gets collection failure or not while adding vWLC in PI	Failed	CSCvo92083



CHAPTER 5

Related Documentation

CME 8.9 Rlease Notes

https://www.cisco.com/c/en/us/td/docs/wireless/controller/release/notes/crn89.html

WLC 8.9 Configuration Guide

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-9/config-guide/b_cg89/monitoring_cisco_wlc.html

CMX 10.6 Configuration Guide

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

PI 3.6 User Guide

https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-6/quickstart/guide/bk_Cisco_Prime_Infrastructure_3_6_0_Quick_Start_guide.html

ACS 5.8 User Guide

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

ISE 2.6 Release Notes

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