# Test Results Summary for Cisco Prime Infrastructure 3.7 for Japan (Release Version 3.7.0.159 )

**First Published:** 2019-10-24

**Last Modified:** 2019-10-26

**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

## 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 3.7
- High priority scenarios and basic regression features
- Inputs from Cisco SEs/ TAC

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

The following products are covered in the test execution:

- Cisco Wireless LAN Controller 8540
- Cisco Wireless LAN Controller 5520
- Cisco Wireless LAN Controller 3504
- Cisco 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
- Cisco ISR 1100
- Cisco AP 9115
- Cisco AP 9120
- 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 |

| Acronym | Description |
|---|---|
| AP | Access Point |
| API | Application Programming Interface |
| APIC-EM | Application Policy Infrastructure Controller - Enterprise Module |
| ATF | Air-Time Fairness |
| AVC | Application Visibility and Control. |
| BGN | Bridge Group Network |
| BLE | Bluetooth Low Energy |
| BYOD | Bring Your Own Device |
| CA | Central Authentication |
| CAC | Call Admissions Control |
| CAPWAP | Control and Provisioning of Wireless Access Point |
| CCKM | Cisco Centralized Key Management |
| CCN | Channel Change Notification |
| CCX | Cisco Compatible Extensions |
| CDP | Cisco Discovery Protocol |
| CKIP | Cisco Key Integrity Protocol |
| CMX | Connected Mobile Experience |
| CVBF | Cisco Vector Beam Forming |
| CWA | Central Web Authentication |
| DCA | Dynamic Channel Assignment |
| DMZ | Demilitarized Zone |
| 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 |

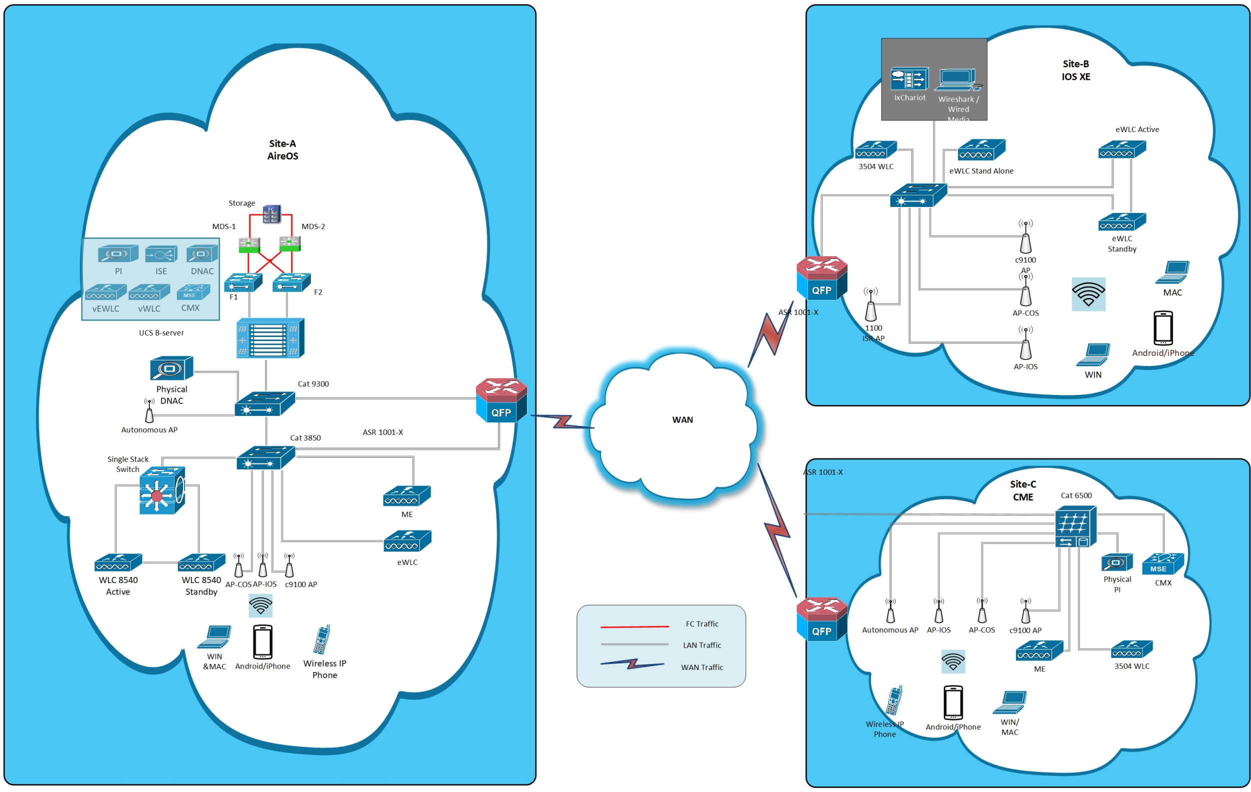
| Acronym | Description |
|---|---|
| FW | Firm Ware |
| HA | High Availability |
| H-REAP | Hybrid Remote Edge Access Point |
| IOS | Internetwork Operating System |
| ISE | Identity Service Engine |
| ISR | Integrated Services Router |
| LAG | Link Aggregation |
| LEAP | Lightweight Extensible Authentication 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 |

| Acronym | Description |
|---|---|
| RADIUS | Remote Authentication Dial-In User Service |
| RAP | Root Access Point |
| RP | Redundancy Port |
| RRM | Radio Resource Management |
| SDN | Software Defined Networking |
| SOAP | Simple Object Access Protocol |
| SFTP | Secure File Transfer Protocol |
| SNMP | Simple Network Management Protocol |
| SS | Spatial Stream |
| SSID | Service Set Identifier |
| SSO | Single Sign On |
| SSO | Stateful Switch Over |
| 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



# Component Matrix

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

| Category | Component | Version |
|---|---|---|
| Access Point | Cisco AP 4800 | 15.3 |
| | Cisco AP 3800 | 15.3 |
| | Cisco AP 2800 | 15.3 |
| | Cisco AP 3700 | 15.3 |
| | Cisco AP 2700 | 15.3 |
| | Cisco AP 1700 | 15.3 |
| | Cisco AP 1850 | 15.3 |
| | Cisco AP 1830 | 15.3 |
| | Cisco AP 1815/1815W | 15.3 |
| | Cisco AP 1810 | 15.3 |
| | Cisco AP 1570 | 15.3 |
| | Cisco AP 1562 | 15.3 |
| | Cisco AP 1542 | 15.3 |
| | Cisco AP 1532 | 15.3 |
| | Cisco AP 702I | 15.3 |
| | Catalyst 9115 AX AP | 16.12 |
| | Cisco AP 1540/1530 | 15.3 |
| | Cisco AP 9120 | 15.3 |
| | Cisco AP 9115 | 15.3 |
| | Cisco ISR 1100 AP | 16.12 |
| Switch | Cisco 3750V2 switch | 15.0(2)SE2 |
| | Cisco Cat 6509-E | 15.1(1)SY1 |
| | Cisco Cat 9300 | 16.11.1 |
| | Cisco Cat 9200L | 16.12 |
| | Cisco Cat 9800 | 16.12.2 |
| Chipset | 5300, 6300 AGN | 15.18.0.1 |
| | 7265 AC | 21.40.2 |
| | Airport Extreme | 7.9.1 |

| Category | Component | Version |
|---|---|---|
| Client | Operating System(JOS) | Windows 7 Enterprise |
| | | Windows 8 & 8.1 Enterprise |
| | | Windows XP Professional |
| | | Windows 10 |
| | Apple Mac Book Pro, Apple Mac Book Air (JP Locale) | Mac OS 10.15 |
| | iPad Pro | iOS 13.1.3 |
| | iPhone 6, 6S & 7,10 (JP Locale) | iOS 13.1.3 |
| | Samsung Galaxy S4 ,S7 & S10, Nexus 6P, Sony Xperia XZ | Android 9.0 Pie |
| | Wireless IP Phone 8821 | 11-0-5MN-102 |
| | End points | Windows 7 Enterprise |
| | | Apple Mac 10.15 |
| | | Windows 8 & 8.1 |
| | | iPhone 6,6S & 7,10 |
| | | Windows 10 |
| | | Samsung Galaxy S4, S7,S10 Nexus 6P,SonyXperia |
| | Cisco AnyConnect VPN Client | 4.8.175 |
| Active Directory | AD | Windows 2008R2 Enterprise |
| Call Control | Cisco Unified Communications Manager | 12.5.0.99832-3/12.5.0.99832-3-1(JP) |
| Browsers | IE | 11.0.11 |
| | Mozilla Firefox | 69.0 |
| | Safari | 13.0 |
| | Chrome | 77.0 |
| Antenna | Hyperlocation | NA |
| Access Point | Autonomous AP | 15.3.3-JI3 |

# What's New ?

- EWLC 16.12 Support
- Support for WPA3
- Support for OWE

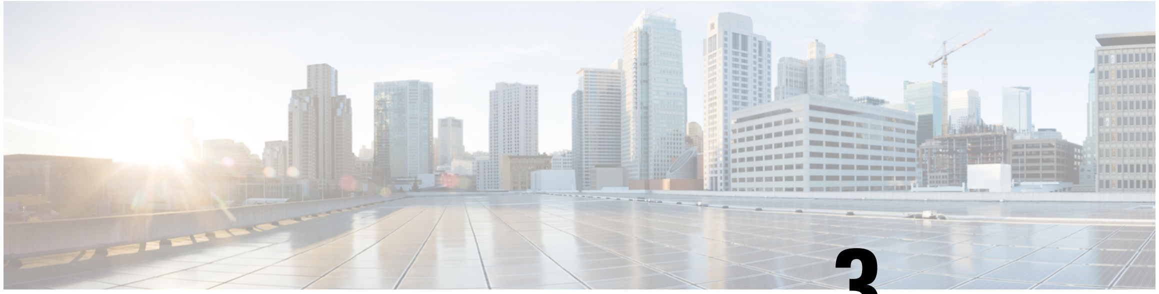
- Mesh Support for all Indoor Wave-2 AP's

# Open Caveats

| Defect ID | Title |
|---|---|
| CSCvr20453 | Not able to change the security from WPA2-psk to Static WEP by configuring the PMF as required |
| CSCvr40785 | Radius NAC State showing in RUN state for clients without selecting NAC State |
| CSCvr68893 | Port blocks gets increased when eWLC device is refreshed |
| CSCvr51021 | Getting error popup while changing Flexconnect/Local to Bridge or Flex+Bridge AP mode in PI |
| CSCvr78429 | Site Group in Device detail page of eWLC shows Undefined |
| CSCvq21727 | Default password for sxp does not get synced from eWLC to PI |

# Resolved Caveats

| Defect ID | Title |
|---|---|
| CSCvq00481 | Unable to generate custom report while login with Japanese option |
| CSCvr50970 | Fast transition not able to enable in WPA2+WPA3 mixed mode. |
| CSCvr16578 | Disabling AES in WPA2+WPA3 throws error |
| CSCvq31738 | Deploying Location template to WLC shows SNMP operation to Device failed |
| CSCvq38803 | Able to Deploy 5GHZ ATF global config to eWLC with enabling optimization in disabled mode |
| CSCvq25783 | Flex+bridge mode(AP-C9115AXI-D) should be removed from PI side |
| CSCvq35980 | ACL rule gets deleted after re-sequencing the rules |
| CSCvq56355 | Unable to deploy eogre parameters from PI to WLC |
| CSCvq57362 | Interferer data on clean Air is not showing on client and user page |
| CSCvq57674 | Unable to deploy mesh template with more than 2 PSK keys |
| CSCvq37457 | ME - WPA3 security not reflecting properly under WLAN Configuration in Prime |



CHAPTER 3

# New Features - Test Summary

## eWLC 16.12 Support

| Logical ID | Title | Description | Status | Defect ID |
|---|---|---|---|---|
| WLJPI37S_eWLC_01 | Adding the eWLC to PI | To add the eWLC in PI and check if the eWLC gets added or not | Passed | |
| WLJPI37S_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 | Passed | |
| WLJPI37S_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 | |
| WLJPI37S_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 | Failed | CSCvr68893 |

| | | | | |
|---|---|---|---|---|
| WLJPI37S_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 | |
| WLJPI37S_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 | |
| WLJPI37S_eWLC_07 | Creating WLAN in PI with Security as WPA/WPA2 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 | |
| WLJPI37S_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 | |
| WLJPI37S_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 | |
| WLJPI37S_eWLC_10 | Configuring AP credentials ,Primary Controller and Telnet parameters | To configure AP credentials ,Primary Backup controller and telnet parameters for the eWLC | Failed | CSCvr68893 |

| | | | | |
|---|---|---|---|---|
| WLJPI37S_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 | |
| WLJPI37S_eWLC_12 | Client connectivity with l2 security WLAN having different Policy weight | To verify the client connectivity with two SSID having different weight | Passed | |
| WLJPI37S_eWLC_13 | Apply ATF monitor mode 2.4GHZ/5GHz on RF group | To verify whether monitor is applied on RF group successfully | Passed | |
| WLJPI37S_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 | |
| WLJPI37S_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 | |
| WLJPI37S_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 | |
| WLJPI37S_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 templates gets deployed or not . | Passed | |
| WLJPI37S_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. | Failed | CSCvr78429 |

| | | | | |
|---|---|---|---|---|
| WLJPI37S_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 | |
| WLJPI37S_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 | |
| WLJPI37S_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 | |
| WLJPI37S_eWLC_22 | Generating a custom report for Site Summary | To check whether a custom report for Site Summary is generated or not | Passed | |
| WLJPI37S_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 | |
| WLJPI37S_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 | |
| WLJPI37S_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 | |

| | | | | |
|---|---|---|---|---|
| WLJPI37S_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 | |
| WLJPI37S_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 | |
| WLJPI37S_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 | |
| WLJPI37S_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 | |
| WLJPI37S_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 | |

| | | | | |
|---|---|---|---|---|
| WLJPI37S_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 | |
| WLJPI37S_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 | |
| WLJPI37S_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 | |
| WLJPI37S_eWLC_34 | Creating WLAN in PI with Security as WPA2/WPA3 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 . | Failed | CSCvr16578 |
| WLJPI37S_eWLC_35 | Connecting a wired client to eWLC using RLAN profile | To connect a wired client to the AP connected in eWLC using the RLAN policy created in PI . | Passed | |
| WLJPI37S_eWLC_36 | Creating a DHCP scope in eWLC to connect a client | To create a DHCP scope in eWLC through PI to check if the dhcp scope is created and check if the clients gets IP Address from the DHCP created . | Passed | |

# Support for WPA3

| Logical ID | Title | Description | Status | Defect ID |
|---|---|---|---|---|
| WLJPI37S_WPA3_01 | Checking the WPA3 configurations in PI | To check the SAE and WPA3 security support in PI. | Passed | |
| WLJPI37S_WPA3_02 | Deploy the WPA3 configurations from PI to WLC. | To verify the WPA3 configurations after deploying the WLAN template from PI to WLC. | Passed | |
| WLJPI37S_WPA3_03 | Check the WPA3 support for SAE security for the Windows client | To check the SAE and WPA3 security support for the window client | Passed | |
| WLJPI37S_WPA3_04 | Check the WPA3 support for SAE security for the Android client | To check the SAE and WPA3 security support for the Android client | Passed | |
| WLJPI37S_WPA3_05 | Check the WPA3 support for SAE security for the Mac os client | To check the SAE and WPA3 security support for the Mac os client | Passed | |
| WLJPI37S_WPA3_06 | Verifying WPA3 and dot1x support for the Windows client | To verify the dot1x Auth key support to the WPA3 security for the Window client. | Passed | |
| WLJPI37S_WPA3_07 | Verifying WPA3 and dot1x support for the Android client | To verify the dot1x Auth key support to the WPA3 security for the Android client. | Passed | |
| WLJPI37S_WPA3_08 | Verifying WPA3 and dot1x support for the Mac os client | To verify the dot1x Auth key support to the WPA3 security for the Mac os client. | Passed | |
| WLJPI37S_WPA3_09 | Verifying the WPA3 with SAE and PSK security support for the Windows client | To verify the Psk Auth key support to the WPA3 security for the Window client. | Passed | |

| | | | | |
|---|---|---|---|---|
| WLJPI37S_WPA3_10 | Verifying the WPA3 with SAE and PSK security support for the Android client | To verify the Psk Auth key support to the WPA3 security for the Android client. | Passed | |
| WLJPI37S_WPA3_11 | Verifying the WPA3 with SAE and PSK security support for the Mac os client | To verify the Psk Auth key support to the WPA3 security for the Mac os client. | Passed | |
| WLJPI37S_WPA3_12 | Verify the CCKM security key to the WPA3 for the Windows client | To verify the CCKM and WPA3 security support for the Windows client | Passed | |
| WLJPI37S_WPA3_13 | Verify the CCKM security key to the WPA3 for the Android client | To verify the CCKM and WPA3 security support for the Android client | Passed | |
| WLJPI37S_WPA3_14 | Verify the CCKM security key to the WPA3 for the Mac os client | To verify the CCKM and WPA3 security support for the Mac os client | Passed | |
| WLJPI37S_WPA3_15 | Verifying the WPA3 security support for the Ft-dot1x security | To verify the Ft-dot1x Auth key support to the WPA3 security | Passed | |
| WLJPI37S_WPA3_16 | Validate the Ft-Psk Auth key support to the WPA3 security | To validate the Ft-Psk auth key support to the WPA3 security. | Failed | CSCvr50970 |
| WLJPI37S_WPA3_17 | Validate the WPA3 support for the Layer 3 Authentication security type | To validate the Layer 3 Authentication security type support for the WPA3 security | Passed | |
| WLJPI37S_WPA3_18 | Verifying the WPA3 support for the Layer 3 Pass-through security type | To verify the Layer 3 Pass-through security type support for the WPA3 security | Passed | |
| WLJPI37S_WPA3_19 | Checking the WPA3 support for the Layer 3 Conditional web redirect security type | To check the Layer 3 Conditional web redirect security type support for the WPA3 security | Passed | |

| | | | | |
|---|---|---|---|---|
| WLJPI37S_WPA3_20 | Checking the WPA3 support for the Layer 3 Splash page web redirect security type | To check the Layer 3 Splash page web redirect security type support for the WPA3 security | Passed | |
| WLJPI37S_WPA3_21 | Checking the WPA3 support for the Layer 3 On Mac Filter Failure security type | To check the Layer 3 On Mac Filter Failure Security type support for the WPA3 security | Passed | |
| WLJPI37S_WPA3_22 | Verify the WPA3 security support for the Sleeping Client | To verify the WPA3 support for the Sleeping client | Passed | |
| WLJPI37S_WPA3_23 | Verifying the WPA3 support and SAE security with Inter WLC Roaming | To verify inter WLC Roaming between WLANs with WPA3 support and SAE support | Passed | |
| WLJPI37S_WPA3_24 | Check the WPA3 support for SAE security with Intra Roaming. | To verify intra client Roaming between APs with WPA3 support and SAE support | Passed | |

# Support for OWE

| Logical ID | Title | Description | Status | Defect ID |
|---|---|---|---|---|
| WLJPI37S_OWE_01 | Checking the OWE configurations While deploying the Template from PI to WLC | To check the OWE support by deploying the Template from PI to WLC. | Passed | |
| WLJPI37S_OWE_02 | Checking the OWE with OWE transition mode configurations While deploying the WLAN Template from PI to WLC | To check the OWE support with OWE transition mode by deploying the WLAN Template from PI to WLC. | Passed | |
| WLJPI37S_OWE_03 | Checking the OWE support for the Windows client. | To check the Client details in PI by connecting the windows client to OWE support SSID | Passed | |

| | | | | |
|---|---|---|---|---|
| WLJPI37S_OWE_04 | Checking the OWE support for the Android client. | To check the Client details in PI by connecting the Android client to OWE support SSID | Passed | |
| WLJPI37S_OWE_05 | Checking the OWE support for the Mac Os client. | To check the Client details in PI by connecting the Mac Os client to OWE support SSID | Passed | |
| WLJPI37S_OWE_06 | Verifying the OWE support with OWE transition mode for the Windows client | To verify the Client packets by connecting the windows client to OWE support SSID with OWE transition mode. | Passed | |
| WLJPI37S_OWE_07 | Verifying the OWE support with OWE transition mode for the Android client | To verify the Client packets by connecting the Android client to OWE support SSID with OWE transition mode. | Passed | |
| WLJPI37S_OWE_08 | Verifying the OWE support with OWE transition mode for the MAC OS client | To verify the Client packets by connecting the Mac os client to OWE support SSID with OWE transition mode. | Passed | |
| WLJPI37S_OWE_09 | Validate the OWE Support with Layer3 Authentication in PI | To Validate the Client details in PI by connecting the client to OWE support SSID with Layer3 Authentication | Passed | |
| WLJPI37S_OWE_10 | Checking the OWE Support with Layer3 Pass-through in PI | To check the Client details in PI by connecting the client to OWE support SSID with Layer3 Pass-through | Passed | |

| | | | | |
|---|---|---|---|---|
| WLJPI37S_OWE_11 | Validate the OWE Support with Layer3 Conditional web redirect in PI | To check the Client details in PI by connecting the client to OWE support SSID with Layer3 Conditional Web redirect. | Passed | |
| WLJPI37S_OWE_12 | Validate the OWE Support with Layer3 On MAC filter failure in PI. | To check the Client packets by connecting the client to OWE support SSID with Layer3 On MAC filter failure. | Passed | |
| WLJPI37S_OWE_13 | Validate the OWE Support with OWE transition mode and Layer3 Authentication in PI | To Validate the Client details in PI by connecting the client to OWE support SSID with OWE transition mode and Layer3 Authentication | Passed | |
| WLJPI37S_OWE_14 | Checking the OWE Support with OWE transition mode and Layer3 Pass-through | To check the Client packets by connecting the client to OWE support SSID with OWE transition mode and Layer3 Pass-through | Passed | |
| WLJPI37S_OWE_15 | Validate the OWE Support with OWE transition mode and Layer3 Conditional web redirect | To check the Client packets by connecting the client to OWE support SSID with OWE transition mode and Layer3 Conditional Web redirect. | Passed | |
| WLJPI37S_OWE_16 | Validate the OWE Support with OWE transition mode and Layer3 On MAC filter failure. | To check the Client packets by connecting the client to OWE support SSID with OWE transition mode and Layer3 On MAC filter failure. | Passed | |

| | | | | |
|---|---|---|---|---|
| WLJPI37S_OWE_17 | Verifying the OWE support with Inter WLC Roaming | To verify inter WLC Roaming between WLANs with OWE support | Passed | |
| WLJPI37S_OWE_18 | Verifying the OWE support with Client Intra Roaming | To verify client inter WLC Roaming between APs with OWE support | Passed | |

# Mesh Support for all Indoor Wave-2 AP's

| Logical ID | Title | Description | Status | Defect ID |
|---|---|---|---|---|
| WLJPI37S_MESH_01 | Verifying the Mesh template configuration in PI | Verifying whether Mesh is configured or not | Passed | |
| WLJPI37S_MESH_02 | Checking the mesh configuration by configuring RAP downlink with 2.4GhZ | To check mesh configurations are proper or not by setting RAP downlink to 2.4GhZ | Failed | CSCvr50970 |
| WLJPI37S_MESH_03 | Checking the mesh configuration by configuring RAP downlink with 5GhZ | To check mesh configurations are proper or not by setting RAP downlink to 5GhZ | Passed | |
| WLJPI37S_MESH_04 | Deploying Mesh template from PI to WLC with 2.4GHZ RAP downlink | Verifying whether the Mesh template is deploying from PI to WLC with 2.4 GhZ RAP downlink | Passed | |
| WLJPI37S_MESH_05 | Deploying Mesh template from PI to WLC with 5GHZ RAP downlink | Verifying whether the Mesh template is deploying from PI to WLC with 5 GhZ RAP downlink | Passed | |
| WLJPI37S_MESH_06 | Checking the Mac filtering configurations in WLC by deploying the template from PI. | To Check the Mac filtering configurations in WLC by deploying the template from PI. | Passed | |

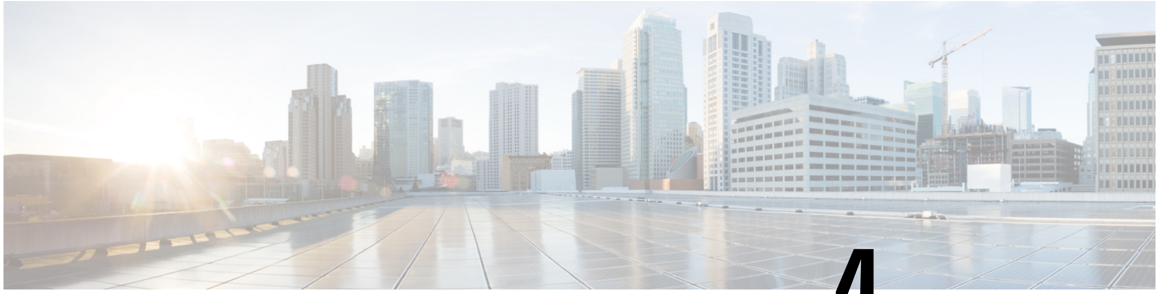
| | | | | |
|---|---|---|---|---|
| WLJPI37S_MESH_07 | Checking the Mac filtering and Mesh template configurations in WLC by deploying the template from PI. | To Check the Mac filtering and Mesh template configurations in WLC by deploying the template from PI. | Passed | |
| WLJPI37S_MESH_08 | Checking mesh configuration in PI and WLC after rebooting WLC | Verifying the mesh configuration in PI and WLC same as before after rebooting WLC | Passed | |
| WLJPI37S_MESH_09 | Checking mesh configuration in PI and WLC after upgrading/downgrading the controller | Verifying mesh configuration in PI and WLC after upgrading/downgrading the controller | Passed | |
| WLJPI37S_MESH_10 | Checking mesh configuration in PI an WLC after performing Day0 | Verifying mesh configuration exists or not after performing day0 | Passed | |
| WLJPI37S_MESH_11 | Checking the AP Mode changes reflect in PI and WLC | verifying whether the AP mode changes are reflected or not in PI and WLC | Passed | |
| WLJPI37S_MESH_12 | Checking the windows client connection for bridge mode AP's | Verifying whether the windows client is connected or not in bridge mode AP's | Passed | |
| WLJPI37S_MESH_13 | Checking the IOS client connection for bridge mode AP's | Verifying whether the IOS client is connected or not in bridge mode AP's | Passed | |
| WLJPI37S_MESH_14 | Checking the android client connection for bridge mode AP's | Verifying whether the android client is connected or not in bridge mode AP's | Passed | |
| WLJPI37S_MESH_15 | Checking the MacOS client connection for bridge mode AP's | Verifying whether the MacOS client is connected or not in bridge mode AP's | Passed | |
| WLJPI37S_MESH_16 | Checking client connection with open security in AP flex+bridge mode | Verifying client is connecting or not with open security in AP flex+bridge mode | Passed | |

| | | | | |
|---|---|---|---|---|
| WLJPI37S_MESH_17 | Checking client connection with WPA+WPA2 security in AP flex+bridge mode | Verifying client is connecting or not with WPA+WPA2 security in AP flex+bridge mode | Passed | |
| WLJPI37S_MESH_18 | Checking client connection with WPA2+WPA3 security in AP flex+bridge mode | Verifying client is connecting or not with WPA2+WPA3 security in AP flex+bridge mode | Passed | |
| WLJPI37S_MESH_19 | Checking client connection with Dot1x security in AP flex+bridge mode | Verifying client is connecting or not with Dot1x security in AP flex+bridge mode | Passed | |
| WLJPI37S_MESH_20 | Checking client connection with Static wep security in AP flex+bridge mode | Verifying client is connecting or not with Static wep security in AP flex+bridge mode | Passed | |

# CMX 10.6 Support

| Logical ID | Title | Description | Status | Defect ID |
|---|---|---|---|---|
| WLJPI37S_CMX_01 | Importing maps to CMX from prime infrastructure | To Import maps from prime infrastructure and check if the maps gets imported to the cmx | Failed | CSCvr34808 |
| WLJPI37S_CMX_02 | Importing the maps with 2 to 3 Access points from PI to CMX | To check whether MAPS is Imported or not from prime infra to CMX with 2 to 3 APs and check if the AP details are shown correctly including clients connected | Passed | |
| WLJPI37S_CMX_03 | Connect a client to the Access Point on the floor | Verify the client details are reflecting or not properly on floor MAP | Passed | |

| | | | | |
|---|---|---|---|---|
| WLJPI37S_CMX_04 | Connect the multiple clients to the multiple Aps from different location | To check whether connected client location is reflected or not properly in CMX after Importing MAPs from prime | Passed | |
| WLJPI37S_CMX_05 | Searching the client by MAC address in CMX heat map | To check whether client device can be searched by specifying its MAC address or not | Passed | |
| WLJPI37S_CMX_06 | Searching the client using its IP address in CMX heat map | To check whether client device can be searched by specifying its IP address or not | Passed | |
| WLJPI37S_CMX_07 | Searching the client using its SSID in CMX heat map | To verify whether client device can be searched by specifying the SSID or not | Passed | |
| WLJPI37S_CMX_08 | Check the number of clients visiting the building and floor in hourly basic and daily basic | Checking the the number of client visiting the building or floor on hourly and daily basic | Passed | |
| WLJPI37S_CMX_09 | Checking the number of new and repeat visitors to the building or floor. | To check whether the number of new and repeater clients/visitors reflecting or not on building or floor Map. | Passed | |



CHAPTER 4

# Regression Features - Test Summary

# Custom Reports

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

| | | | | |
|---|---|---|---|---|
| WLJPI37S_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 | |
| WLJPI37S_Reg_02 | Generating a custom report for Interface utilization | To check whether a custom report for Interface Utilization is generated or not | Passed | |
| WLJPI37S_Reg_03 | Generating a custom report for Busiest AP | To check whether a custom report for Busiest AP is generated or not | Passed | |
| WLJPI37S_Reg_04 | Generating a custom report for AP utilization | To check whether a custom report for AP utilization is generated or not | Passed | |
| WLJPI37S_Reg_05 | Creating sub report for Unique client and users summary as client summary by SSID | To check whether subreport Client summary by SSID can be customized or not | Passed | |
| WLJPI37S_Reg_06 | Creating sub report for Unique client and users summary as client summary by VLAN | To check whether subreport Client summary by VLAN can be customized or not | Passed | |
| WLJPI37S_Reg_07 | Creating sub report for rogue AP Events | To check whether subreport for rogue AP Events can be customized or not | Passed | |
| WLJPI37S_Reg_08 | Creating sub report for rogue APs(Updated) | To check whether subreport for rogue AP Events can be customized or not | Passed | |
| WLJPI37S_Reg_09 | Creating sub report for Worst RF APs | To check whether subreport for Worst RF APs can be customized or not | Passed | |
| WLJPI37S_Reg_10 | Creating sub report for AP RF Quality | To check whether subreport for AP RF Quality can be customized or not | Passed | |

| | | | | |
|---|---|---|---|---|
| WLJPI37S_Reg_11 | Creating sub report for Wireless Network Utilization | To check whether subreport for Wireless Network Utilization can be customized or not | Passed | |
| WLJPI37S_Reg_12 | Generating a custom for Busiest Client | To check whether a custom report for Client count is generated or not | Passed | |
| WLJPI37S_Reg_13 | Generating a custom for Client count | To check whether a custom report for client count is generated or not | Passed | |
| WLJPI37S_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 | |
| WLJPI37S_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 | |
| WLJPI37S_Reg_16 | Generating a custom for Rogue AP | To check whether Generate a custom report for Rogue AP | Passed | |
| WLJPI37S_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 | |
| WLJPI37S_Reg_18 | Generating a custom for Application Summary | To check whether a custom report for Application summary is generated or not | Passed | |
| WLJPI37S_Reg_19 | Generating a custom for worst RF Aps | To check whether a custom report for Worst RF Aps is generated or not | Passed | |
| WLJPI37S_Reg_20 | Generating a custom for Site Summary | To check whether a custom report for Site Summary is generated or not | Passed | |

| | | | | |
|---|---|---|---|---|
| WLJPI37S_Reg_21 | Generating a custom for AP RF Quality | To check whether a custom report for Wireless Network Utilization is generated or not | Passed | |
| WLJPI37S_Reg_22 | Generating a custom for Wireless Network Utilization | To check whether Generate a custom report for AP RF Quality | Passed | |
| WLJPI37S_Reg_23 | Creating a composite custom result for client | To check whether a composite custom report for client is generated or not | Passed | |
| WLJPI37S_Reg_24 | Creating a composite custom result for device | To check whether a composite custom report for device is generated or not | Passed | |
| WLJPI37S_Reg_25 | Creating a composite custom result for Security | To check whether a composite custom report for Security is generated or not | Passed | |
| WLJPI37S_Reg_26 | Creating a composite custom result for Performance | To check whether a composite custom report for Performance is generated or not | Passed | |
| WLJPI37S_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 | |
| WLJPI37S_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 | |
| WLJPI37S_Reg_29 | Verifying the scheduled template in composite report | To check whether the scheduled report is listed or not in the Composite Report | Passed | |

| | | | | |
|---|---|---|---|---|
| WLJPI37S_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 | |
| WLJPI37S_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 | |
| WLJPI37S_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 | |
| WLJPI37S_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 | |
| WLJPI37S_Reg_34 | Saving the report and viewing it in GUI | To check whether that saved report is available in PI GUI or not | Passed | |
| WLJPI37S_Reg_35 | Exporting the saved report | To check whether verify whether the saved report can be mailed or not | Passed | |
| WLJPI37S_Reg_36 | Saving and mailing the report | To check whether the saved report can be exported or not | Passed | |
| WLJPI37S_Reg_37 | Checking the dependency in other pages | To check whether whether the custom report page appear there or not | Passed | |
| WLJPI37S_Reg_38 | Checking th custom report in favourite icon | To check whether the custom report is listed in favourite icon | Passed | |
| WLJPI37S_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 | |

| | | | | |
|---|---|---|---|---|
| WLJPI37S_Reg_40 | Creating the report in Summary View | To check whether the view of report can be changed to summary view or not | Passed | |
| WLJPI37S_Reg_41 | Creating the report in detailed View | To check whether the view of report can be changed to detailed view or not | Passed | |
| WLJPI37S_Reg_42 | Creating the Sub report for the Top AP by client Count | To check whether Sub report can be created of not | Passed | |
| WLJPI37S_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 | |
| WLJPI37S_Reg_44 | Creating the Sub report for the Interface Utilization | To check whether Sub report for Interface utilization can be created of not | Passed | |
| WLJPI37S_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 | |
| WLJPI37S_Reg_46 | Creating Sub report for device health and applying sorting on result | To check whether the subreport for device health can be customized or not | Passed | |
| WLJPI37S_Reg_47 | Enabling the sub report for the Device Health | To check whether the subreport for device health can be created or not | Passed | |
| WLJPI37S_Reg_48 | Creating report for 802.11 a/an/ac Busiet AP | To check whether the report for 802.11a.a/an/ac can be created or not | Passed | |
| WLJPI37S_Reg_49 | Creating Sub report for 802.11a/an/ac Busiet AP and applying sorting on result | To check whether the sub report for 802.11a.a/an/ac can be created or not | Passed | |

| | | | | |
|---|---|---|---|---|
| WLJPI37S_Reg_50 | Creating report for 802.11 b/g/n Busiet AP | To check whether the report for 802.11 b/g/n can be created or not | Passed | |
| WLJPI37S_Reg_51 | Creating Sub report for 802.11a/an/ac Busiet AP and applying sorting on result | To check whether the sub report for 802.11 b/g/n can be created or not | Passed | |
| WLJPI37S_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 | |
| WLJPI37S_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 | |
| WLJPI37S_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 | |
| WLJPI37S_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 | |
| WLJPI37S_Reg_56 | Creating sub report for Busiest Client | To check whether the subreports for Busiest client can be customized or not | Passed | |
| WLJPI37S_Reg_57 | Creating sub report for Unique client and users Summary as Client User Summary | To check whether subreport Client user summary can be customized or not | Passed | |
| WLJPI37S_Reg_58 | Creating sub report for Unique client and users Summary as Client Traffic Summary | To check whether subreport Client Traffic summary can be customized or not | Passed | |

| | | | | |
|---|---|---|---|---|
| WLJPI37S_Reg_59 | Creating sub report for Unique client and users summary as client summary by protocol | To check whether subreport Client summary by protocol can be customized or not | Passed | |
| WLJPI37S_Reg_60 | Creating sub report for Unique client and users summary as client summary by Vendor | To check whether subreport Client summary by vendor can be customized or not | Passed | |
| WLJPI37S_Reg_61 | Creating sub report for Unique client and users summary as client summary by SSID | To check whether subreport Client summary by SSID can be customized or not | Passed | |
| WLJPI37S_Reg_62 | Creating sub report for Unique client and users summary as client summary by VLAN | To check whether subreport Client summary by VLAN can be customized or not | Passed | |
| WLJPI37S_Reg_63 | Creating sub report for rogue AP Events | To check whether subreport for rogue AP Events can be customized or not | Passed | |
| WLJPI37S_Reg_64 | Creating sub report for rogue APs(Updated) | To check whether subreport for rogue AP Events can be customized or not | Passed | |
| WLJPI37S_Reg_65 | Creating sub report for Worst RF APs | To check whether subreport for Worst RF APs can be customized or not | Passed | |
| WLJPI37S_Reg_66 | Creating sub report for AP RF Quality | To check whether subreport for AP RF Quality can be customized or not | Passed | |
| WLJPI37S_Reg_67 | Creating sub report for Wireless Network Utilization | To check whether subreport for Wireless Network Utilization can be customized or not | Passed | |

| | | | | |
|---|---|---|---|---|
| WLJPI37S_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 | |
| WLJPI37S_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 |
|---|---|---|---|---|
| WLJPI37S_Reg_70 | Deploying template on Aireos controller via config group and verifying the controller behaviour | Verifying that user is able to deploy template on Aireos controller via config group or not | Passed | |
| WLJPI37S_Reg_71 | Deploying multiple templates on Aireos controller via config group | Verifying that user is able to deploy multiple templates on Aireos controller | Passed | |
| WLJPI37S_Reg_72 | Deploying mutiple 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 | |
| WLJPI37S_Reg_73 | Deploying template on vWLC via config group | Verifying that user is able to deploy template on Vwlc or not | Passed | |
| WLJPI37S_Reg_74 | Deploying template on CME via config group | Verifying that user is able to deploy on CME | Passed | |
| WLJPI37S_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 | |

| | | | | |
|---|---|---|---|---|
| WLJPI37S_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 | |
| WLJPI37S_Reg_77 | Monitoring the dashboard after deploying template on controller | Verifying the dashboard after deploying the template on controller | Passed | |
| WLJPI37S_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 |
|---|---|---|---|---|
| WLJPI37S_Reg_79 | Adding a controller in PI and monitoring the clients in Network summary | Verifying the top clients by data usage | Passed | |
| WLJPI37S_Reg_80 | Monitor the top clients of different OS by by data uses | Verifying the top clients by data usage | Passed | |
| WLJPI37S_Reg_81 | 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 | |
| WLJPI37S_Reg_82 | Monitoring the signal strength of different OS client | Verifying the signal strength for different OS client | Passed | |
| WLJPI37S_Reg_83 | Verifying that Wireless Dashlets in Network Health are working for site filter and time filter or not | To check the Wireless Dashlets in Network Health are working for site filter and time filter or not | Passed | |
| WLJPI37S_Reg_84 | Monitoring the signal quality distribution of different OS client | Monitor the signal quality distribution for client | Passed | |

| | | | | |
|---|---|---|---|---|
| WLJPI37S_Reg_85 | Monitoring the network health of created campus site | To check that user can monitor the network health of created sites or not | Passed | |
| WLJPI37S_Reg_86 | Monitor the Connection rate of connected client | Monitor the Connection rate for connected client | Passed | |
| WLJPI37S_Reg_87 | Creating location group with UTF character | Verify that user can create location group with UTF for monitor network health or not | Passed | |
| WLJPI37S_Reg_88 | Monitor the Network Health of access point | Verify the Network Health of Access Point by applying time filter | Passed | |
| WLJPI37S_Reg_89 | Monitoring the client distribution by RSSI/connected protocol/SNR/End point type | Verify that user can Monitor the client distribution by RSSI/connected protocol/SNR/End point type or not | Passed | |
| WLJPI37S_Reg_90 | Monitoring the AP distribution by channel utilization/interference/client count/coverage hole | Verify that user can Monitor the AP distribution by channel utilization/interference/client count/coverage hole or not | Passed | |

# Next Generation Maps

| Logical ID | Title | Description | Status | Defect ID |
|---|---|---|---|---|
| WLJPI37S_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 | |
| WLJPI37S_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 | |
| WLJPI37S_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 | |

| | | | | |
|---|---|---|---|---|
| WLJPI37S_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 | |
| WLJPI37S_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 | |
| WLJPI37S_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 | |
| WLJPI37S_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 | |
| WLJPI37S_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 | |
| WLJPI37S_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 | |
| WLJPI37S_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 | |

| | | | | |
|---|---|---|---|---|
| WLJPI37S_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 | |
| WLJPI37S_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 | |
| WLJPI37S_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 | |
| WLJPI37S_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 | |
| WLJPI37S_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 | |
| WLJPI37S_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 | |
| WLJPI37S_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 | |
| WLJPI37S_Reg_108 | Importing MAP archive in XML format | To check Whether MAP archive can be imported or not | Passed | |

| | | | | |
|---|---|---|---|---|
| WLJPI37S_Reg_109 | Creating Group hierarchy in Maps | To check whether Group hierarchy can be created or not in PI Maps | Passed | |
| WLJPI37S_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

| | | | | |
|---|---|---|---|---|
| WLJPI37S_Reg_111 | Connect iPhone client to WLAN after creating DHCP scope | To verify that iPhone connect successfully after creating DHCP scope | Passed | |
| WLJPI37S_Reg_112 | Connect Japanese client to WLAN after creating DHCP scope | To verify that Japanese connect successfully after creating DHCP scope | Passed | |
| WLJPI37S_Reg_113 | Connect Android client to WLAN after creating DHCP scope | To verify that Android connect successfully after creating DHCP scope | Passed | |
| WLJPI37S_Reg_114 | Connect Windows client to WLAN after creating DHCP scope | To verify that Windows connect successfully after creating DHCP scope | Passed | |
| WLJPI37S_Reg_115 | Connect ios client to WLAN after creating DHCP scope | To verify that ios connect successfully after creating DHCP scope | Passed | |
| WLJPI37S_Reg_116 | Scheduling ME reboot in PI after DHCP config | To verify whether DHCP configuration are correct or not after reboot | Passed | |
| WLJPI37S_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 |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| WLJPI37S_Reg_118 | Creating a Trustsec Sxp Config Template | To Create a Trustsec Sxp config template and to deploy the the template to the controller and check if the template is deployed | Passed | |
| WLJPI37S_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 | |
| WLJPI37S_Reg_120 | Deploying Sxp configuration in WLC and synchronizing into PI | To create a Sxp Configuration in WLC GUI and deploy the same in PI and check if the configuration is identical | Passed | |
| WLJPI37S_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 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 |
|---|---|---|---|---|
| WLJPI37S_Reg_122 | MAC filtering capability for lobby ambassadors | Creating local management user with lobby access level in WLC | Passed | |
| WLJPI37S_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 | |
| WLJPI37S_Reg_124 | Enabling lobby Admin access to Wlan profile | To check whether lobby admin can access without L3 Sec wlan Profile or not | Passed | |

| | | | | |
|---|---|---|---|---|
| WLJPI37S_Reg_125 | Creating a guest user from Guest Management GUI | To check whether guest user is created or not in GUI | Passed | |
| WLJPI37S_Reg_126 | Creating auto password for user | To check whether generate a auto check whether password for guest user | Passed | |
| WLJPI37S_Reg_127 | Adding a permanent guest user from WLC Guest Management GUI | To check whether permanent guest user is added or not | Passed | |
| WLJPI37S_Reg_128 | Creating local management user with read only access level | To create local management user with read only access level | Passed | |
| WLJPI37S_Reg_129 | Creating local management user with read write access level | To create local management user with read write access level | Passed | |
| WLJPI37S_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 | |
| WLJPI37S_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 | |
| WLJPI37S_Reg_132 | Accessing guest user Management GUI | To verify Aun for a lobby user | Passed | |

# Domain based URL ACL enhancement

| Logical ID | Title | Description | Status | Defect ID |
|---|---|---|---|---|
| WLJPI37S_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 | |

| | | | | |
|---|---|---|---|---|
| WLJPI37S_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 | |
| WLJPI37S_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 | |
| WLJPI37S_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 | Passed | |
| WLJPI37S_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 | |
| WLJPI37S_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 | |
| WLJPI37S_Reg_139 | Deny cisco site for end level any connect clients by keeping black list | Blocking cisco site for end level anyconnectClients by keeping black list | Passed | |
| WLJPI37S_Reg_140 | Permit cisco site for end level MAC clients by keeping white list | Permitting cisco site for end level any connect Clients by keeping white list | Passed | |

# Autonomous to LWAPP Migration

| Logical ID | Title | Description | Status | Defect ID |
|---|---|---|---|---|
| WLJPI37S_Reg_141 | Verifying the Autonomous to LWAPP Migration | To check whether autonomous to LWAPP migrating or not | Passed | |
| WLJPI37S_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 | |

| | | | | |
|---|---|---|---|---|
| WLJPI37S_Reg_143 | Generating the migration report for the created template | To check whether migration report is generating or not for the created template | Passed | |
| WLJPI37S_Reg_144 | Verifying the current status of the Autonomous to LWAP Migration | To checking the current status of the Autonomous to LWAP Migration | Passed | |
| WLJPI37S_Reg_145 | Viewing the Migration Analysis summary for Autonomous AP to LWAP | Verifying the Migration Analysis summary for Autonomous AP to LWAP | Passed | |
| WLJPI37S_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 | |
| WLJPI37S_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 | |

# Flex AVC

| Logical ID | Title | Description | Status | Defect ID |
|---|---|---|---|---|
| WLJPI37S_Reg_148 | Dropping some application via flex avc profile | To drop some application via Flex avc profile | Passed | |
| WLJPI37S_Reg_149 | Marking the certain application and validating the same | To mark the certain application | Passed | |
| WLJPI37S_Reg_150 | Applying the rate limit on some application | To Apply the rate limit on some application | Passed | |
| WLJPI37S_Reg_151 | Trying to set rate limit out range in flex avc rule | Try to set rate limit out range in flex avc rule | Passed | |
| WLJPI37S_Reg_152 | Delete multiple flex connect avc profile | To Delete the multiple flex connect avc profile | Passed | |

| | | | | |
|---|---|---|---|---|
| WLJPI37S_Reg_153 | Try to delete applied flex connect avc profile | Try to delete applied flex connect avc profile | Passed | |
| WLJPI37S_Reg_154 | Try change the AVC rule from custom to mark/rate limit/drop | To verify whether AVC rule rule is changing from custom to mark/rate limit/drop or not | Passed | |
| WLJPI37S_Reg_155 | Checking AVC rule with more than custom value | To verify whether AVC rule is creating or not more than custom value | Passed | |
| WLJPI37S_Reg_156 | 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 | |
| WLJPI37S_Reg_157 | 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 |
|---|---|---|---|---|
| WLJPI37S_Reg_158 | Add/edit/delete APIC -EM in PI | To Add APIC -EM in PI | Passed | |
| WLJPI37S_Reg_159 | Validate the Error message | To verify the error message shown when we add the invalid APIC EM in PI | Passed | |
| WLJPI37S_Reg_160 | APIC-EM reachability history | To verify the APIC-EM reachability history once APIC-EM added | Passed | |
| WLJPI37S_Reg_161 | Creating Bootstrap template | To Create Bootstrap template | Passed | |

| | | | | |
|---|---|---|---|---|
| WLJPI37S_Reg_162 | Importing Software Images for Plug and Play Profiles | To import software images for plug and play profiles | Passed | |
| WLJPI37S_Reg_163 | Creating PnP profile for switches | To Create PnP profile for switchs | Passed | |
| WLJPI37S_Reg_164 | Creating PnP profile for wireless ap | To Create PnP profile for switchs | Passed | |
| WLJPI37S_Reg_165 | 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 | |
| WLJPI37S_Reg_166 | Adding the PI in APIC -EM | To add PI in APIC -EM | Passed | |
| WLJPI37S_Reg_167 | Plug and play Profile Activation of wireless ap | To activate plug and play profile of wireless ap | Passed | |
| WLJPI37S_Reg_168 | Plug and play Profile Activation switch | To activate plug and play profile of switch | Passed | |
| WLJPI37S_Reg_169 | Monitoring the plug and play | To monitor the plug and play | Passed | |

# SWIM Enhancement

| Logical ID | Title | Description | Status | Defect ID |
|---|---|---|---|---|
| WLJPI37S_Reg_170 | 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 | |
| WLJPI37S_Reg_171 | 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 | |
| WLJPI37S_Reg_172 | Importing the image through the URL | To import the image using URL and check if the images gets imported or not. | Passed | |

| | | | | |
|---|---|---|---|---|
| WLJPI37S_Reg_173 | Changing the image transfer protocol order . | To change the image transfer protocol order and check if the order is changed or not | Passed | |
| WLJPI37S_Reg_174 | 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 | |
| WLJPI37S_Reg_175 | Adding software image management servers | To Configure a software image management server and check if the server are added or not. | Passed | |
| WLJPI37S_Reg_176 | 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 | |
| WLJPI37S_Reg_177 | 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 | |
| WLJPI37S_Reg_178 | 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 |
|---|---|---|---|---|
| WLJPI37S_Reg_179 | HA registration of PI | To check the HA registration between primary and secondary | Passed | |
| WLJPI37S_Reg_180 | HA failback to secondary when primary is failed. | To verify the HA failback to secondary in case of primary failure. | Passed | |

| | | | | |
|---|---|---|---|---|
| WLJPI37S_Reg_181 | HA fallback to primary when primary server is restored. | To verify the HA fallback to primary in case of primary server restored. | Passed | |
| WLJPI37S_Reg_182 | Verify the HA failover messages. | To verify the HA failure messages | Passed | |
| WLJPI37S_Reg_183 | Verifying the HM with new changes. | To verify the Time zone display in Health monitor page. | Passed | |
| WLJPI37S_Reg_184 | Verifying the HA events | To verify the HA events triggered when registration and failback. | Passed | |

# Rolling AP Upgrade

| Logical ID | Title | Description | Status | Defect ID |
|---|---|---|---|---|
| WLJPI37S_Reg_185 | 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 | |
| WLJPI37S_Reg_186 | Upgrading the software image in a controller | To check whether the software image is upgraded in controller | Passed | |
| WLJPI37S_Reg_187 | Upgrading the software image into a group of AP | To check whether the software image is upgraded in group of AP | Passed | |
| WLJPI37S_Reg_188 | Upgrading the software image into existing group of AP | To check whether the software image is upgraded into existing group of AP | Passed | |
| WLJPI37S_Reg_189 | 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 | |
| WLJPI37S_Reg_190 | Upgrade the image to WLC from PI rolling AP upgrade TFTP | To check whether the WLC is upgraded using TFTP from PI | Passed | |

| | | | | |
|---|---|---|---|---|
| WLJPI37S_Reg_191 | Upgrade the image to WLC from PI rolling AP upgrade FTP | To check whether the WLC is upgraded using FTP from PI | Passed | |
| WLJPI37S_Reg_192 | 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 | |
| WLJPI37S_Reg_193 | 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 | |
| WLJPI37S_Reg_194 | 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 | |
| WLJPI37S_Reg_195 | Moving AP's back to primary controller from PI. | To verify whether the AP's are move back into primary controller. | Passed | |
| WLJPI37S_Reg_196 | Adding the AP in AP upgrade group | To verify whether the AP added into AP upgrade group | Passed | |
| WLJPI37S_Reg_197 | 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 | |

# EOGRE Profile

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

| | | | | |
|---|---|---|---|---|
| WLJPI37S_Reg_198 | 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 | |
| WLJPI37S_Reg_199 | Creating a EoGRE Profile Name in Japanese character | To verify whether the EoGRE Profile Name accepts Japanese character or not | Passed | |
| WLJPI37S_Reg_200 | Deploying the template from PI to Controller | To push the saved template from PI to controller | Passed | |
| WLJPI37S_Reg_201 | Configuring the EoGRE rule to set up the tunnel | To validate whether EoGRE rule reflects after it got saved | Passed | |
| WLJPI37S_Reg_202 | Connecting Android clients with Flex connect 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 Flex connect local switching enabled WLAN with Tunnel profile Rule followed by marking Tunnel Parameters Gateway as AAA Proxy and Accounting proxy | Passed | |
| WLJPI37S_Reg_203 | Connecting Android clients with Flex connect 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 Flex connect local switching enabled WLAN with Tunnel profile Rule followed by marking Tunnel Parameters Gateway as DHCP Option - 82 | Passed | |

| | | | | |
|---|---|---|---|---|
| WLJPI37S_Reg_204 | 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 Flex connect local switching enabled WLAN with Tunnel profile Rule followed by marking Tunnel Parameters Gateway as AAA Proxy and Accounting proxy | Passed | |
| WLJPI37S_Reg_205 | 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 Flex connect local switching enabled WLAN with Tunnel profile Rule followed by marking Tunnel Parameters Gateway as AAA Proxy and Accounting proxy | Passed | |
| WLJPI37S_Reg_206 | 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 Flex connect local switching enabled WLAN with Tunnel profile Rule followed by marking Tunnel Parameters Gateway as AAA Proxy and Accounting proxy | Passed | |
| WLJPI37S_Reg_207 | 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 Flex connect local switching enabled WLAN with Tunnel profile Rule followed by marking Tunnel Parameters as DHCP option-82 | Passed | |

| | | | | |
|---|---|---|---|---|
| WLJPI37S_Reg_208 | 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 Flex connect local switching enabled WLAN with Tunnel profile Rule followed by marking Tunnel Parameters as DHCP option-82 | Passed | |
| WLJPI37S_Reg_209 | 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 Flex connect 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 |
|---|---|---|---|---|
| WLJPI37S_Reg_210 | 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 | Failed | CSCvr34808 |
| WLJPI37S_Reg_211 | 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 | |
| WLJPI37S_Reg_212 | 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 | Failed | CSCvr40785 |
| WLJPI37S_Reg_213 | 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 | |

| | | | | |
|---|---|---|---|---|
| WLJPI37S_Reg_214 | 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 | |
| WLJPI37S_Reg_215 | 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 | |
| WLJPI37S_Reg_216 | 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 | |
| WLJPI37S_Reg_217 | 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 | |
| WLJPI37S_Reg_218 | 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 | |
| WLJPI37S_Reg_219 | 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 | |

| | | | | |
|---|---|---|---|---|
| WLJPI37S_Reg_220 | 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 | |
| WLJPI37S_Reg_221 | 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 | |
| WLJPI37S_Reg_222 | 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 |
|---|---|---|---|---|
| WLJPI37S_Reg_223 | Changing the WLAN Mode for the Created WLAN Profile Name | To Vary the WLAN Mode for the Created WLAN Profile Name | Passed | |
| WLJPI37S_Reg_224 | Mapping the Created WLAN Profile name with an AP group | To Represent the Created WLAN Profile Name with an AP Group | Passed | |
| WLJPI37S_Reg_225 | Creating the Policy Name for the Created WLAN Profile Name | To form the Policy Name for the Created WLAN Profile Name | Passed | |
| WLJPI37S_Reg_226 | 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 |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| WLJPI37S_Reg_227 | 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 | Failed | CSCvr33225 |
| WLJPI37S_Reg_228 | 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 | |
| WLJPI37S_Reg_229 | Connecting the different OS client after deploying the template of AP | Checking the client connectivity after deploying the AP template | Passed | |
| WLJPI37S_Reg_230 | 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 |
|---|---|---|---|---|
| WLJPI37S_Reg_231 | Joining the outdoor AP with WLC | Verify that user is able to join outdoor with wlc or not | Passed | |
| WLJPI37S_Reg_232 | Discovering the outdoor AP PI | Verify that outdoor ap discovering in PI or not | Passed | |
| WLJPI37S_Reg_233 | 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 | |
| WLJPI37S_Reg_234 | Locating the outdoor ap on maps | Locating the outdoor ap via GPS on map | Passed | |
| WLJPI37S_Reg_235 | Exporting the geo location of outdoor AP | Verify that user is able to exporting the AP location or not | Passed | |

| | | | | |
|---|---|---|---|---|
| WLJPI37S_Reg_236 | Importing the geo location of outdoor AP | Verify that user is able to importing the AP location or not | Passed | |
| WLJPI37S_Reg_237 | 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 | |
| WLJPI37S_Reg_238 | 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 |
|---|---|---|---|---|
| WLJPI37S_Reg_239 | 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 | |
| WLJPI37S_Reg_240 | 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 | |
| WLJPI37S_Reg_241 | 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 | |
| WLJPI37S_Reg_242 | 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 | |
| WLJPI37S_Reg_243 | 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 | |

| | | | | |
|---|---|---|---|---|
| WLJPI37S_Reg_244 | 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 | |
| WLJPI37S_Reg_245 | 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 | |
| WLJPI37S_Reg_246 | 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 | |
| WLJPI37S_Reg_247 | 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 | |
| WLJPI37S_Reg_248 | 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 | |
| WLJPI37S_Reg_249 | 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 | |
| WLJPI37S_Reg_250 | 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 | |
| WLJPI37S_Reg_251 | 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 | |

| | | | | |
|---|---|---|---|---|
| WLJPI37S_Reg_252 | 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 |
|---|---|---|---|---|
| WLJPI37S_Reg_253 | Adding ME controllers with it neighbours and check the Rx neighbour 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 neighbour functionality.. | Passed | |
| WLJPI37S_Reg_254 | Adding a ME controller with one neighbour AP in sensor mode. | To add a ME controller AP with one neighbour AP in sensor and check the details of the neighbour AP . | Passed | |
| WLJPI37S_Reg_255 | 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 | |
| WLJPI37S_Reg_256 | 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 | |
| WLJPI37S_Reg_257 | 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 | |

| | | | | |
|---|---|---|---|---|
| WLJPI37S_Reg_258 | 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 | |
| WLJPI37S_Reg_259 | 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 | |
| WLJPI37S_Reg_260 | 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 | |
| WLJPI37S_Reg_261 | 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 | |
| WLJPI37S_Reg_262 | 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 | |
| WLJPI37S_Reg_263 | 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 | |
| WLJPI37S_Reg_264 | 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 | |

| | | | | |
|---|---|---|---|---|
| WLJPI37S_Reg_265 | 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 | |
| WLJPI37S_Reg_266 | 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 |
|---|---|---|---|---|
| WLJPI37S_Reg_267 | 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 | |
| WLJPI37S_Reg_268 | 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 | |
| WLJPI37S_Reg_269 | 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 | |
| WLJPI37S_Reg_270 | 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 | |
| WLJPI37S_Reg_271 | 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 | |

| | | | | |
|---|---|---|---|---|
| WLJPI37S_Reg_272 | 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 | |
| WLJPI37S_Reg_273 | 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 | |
| WLJPI37S_Reg_274 | 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 | |
| WLJPI37S_Reg_275 | 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 | |
| WLJPI37S_Reg_276 | 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 | |
| WLJPI37S_Reg_277 | 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 | |
| WLJPI37S_Reg_278 | 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 |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| WLJPI37S_Reg_279 | Associating the ME AP to WLC and Verifying in PI. | Able to see the ME AP In PI,after associating WLC. | Passed | |
| WLJPI37S_Reg_280 | To verifying the client data rate through PI. | To check the data rate of the particular client connected to the WLAN. | Passed | |
| WLJPI37S_Reg_281 | To configure the authentication for The ME AP | To check whether the authentication is configured into ME AP | Passed | |
| WLJPI37S_Reg_282 | 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 | |
| WLJPI37S_Reg_283 | 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 | |
| WLJPI37S_Reg_284 | 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 | |
| WLJPI37S_Reg_285 | 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 | |
| WLJPI37S_Reg_286 | 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 | |
| WLJPI37S_Reg_287 | 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 | |

| | | | | |
|---|---|---|---|---|
| WLJPI37S_Reg_288 | 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 | |
| WLJPI37S_Reg_289 | 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 | |
| WLJPI37S_Reg_290 | Connect iPhone client to WLAN after creating DHCP scope | To verify that iPhone connect successfully after creating DHCP scope | Passed | |
| WLJPI37S_Reg_291 | Connect Japanese client to WLAN after creating DHCP scope | To verify that Japanese connect successfully after creating DHCP scope | Passed | |
| WLJPI37S_Reg_292 | Connect Android client to WLAN after creating DHCP scope | To verify that Android connect successfully after creating DHCP scope | Passed | |
| WLJPI37S_Reg_293 | Connect Windows client to WLAN after creating DHCP scope | To verify that Windows connect successfully after creating DHCP scope | Passed | |
| WLJPI37S_Reg_294 | Connect ios client to WLAN after creating DHCP scope | To verify that ios connect successfully after creating DHCP scope | Passed | |
| WLJPI37S_Reg_295 | Scheduled rebooting the CME from PI | To verify whether scheduled rebooting CME from PI is successful. | Passed | |
| WLJPI37S_Reg_296 | AP configuration from PI joined to CME. | To verify whether AP configuration changes from PI applies successfully in CME. | Passed | |

# SWIM Support of Mobility Express Controllers

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

| | | | | |
|---|---|---|---|---|
| WLJPI37S_Reg_297 | 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 | |
| WLJPI37S_Reg_298 | 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 | |
| WLJPI37S_Reg_299 | 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 | |
| WLJPI37S_Reg_300 | 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 | |
| WLJPI37S_Reg_301 | 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 | |
| WLJPI37S_Reg_302 | 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 | |
| WLJPI37S_Reg_303 | 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 | |
| WLJPI37S_Reg_304 | 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 |
|---|---|---|---|---|
| WLJPI37S_Reg_305 | Adding the RADIUS server in Users, Roles & AAA | Verifying whether RADIUS server is added or not in Users, Roles & AAA mode | Passed | |
| WLJPI37S_Reg_306 | Verifying the RADIUS server reachability | To check whether successfully contacted RADIUS server or not | Passed | |
| WLJPI37S_Reg_307 | Adding the TACACS+ server in Users, Roles & AAA | Verifying whether TACACS+ server is added or not in Users, Roles & AAA mode | Passed | |
| WLJPI37S_Reg_308 | Verifying the TACACS+ server reachability with ISE | To check whether successfully contacted TACACS+ server or not | Passed | |
| WLJPI37S_Reg_309 | Adding the RADIUS server with DNS name in Users, Roles & AAA | Verify whether RADIUS server is added or not with DNS name | Passed | |
| WLJPI37S_Reg_310 | Checking the RADIUS server reachability with DNS name | To check whether successfully contacted RADIUS server or not with DNS name | Passed | |
| WLJPI37S_Reg_311 | Adding the TACACS+ server with DNS name in Users, Roles & AAA | Verifying the TACACS+ server is adding or not with DNS name | Passed | |
| WLJPI37S_Reg_312 | Verifying the TACACS+ server reachability with DNS name | To check whether successfully contacted TACACS+ server or not with DNS name | Passed | |

| | | | | |
|---|---|---|---|---|
| WLJPI37S_Reg_313 | Verifying the RADIUS server reachability via PAP Authentication | To check whether RADIUS server is successfully contacted or not via PAP Authentication | Passed | |
| WLJPI37S_Reg_314 | Checking the RADIUS server reachability via CHAP Authentication | Verifying RADIUS server is successfully contacted or not via CHAP Authentication | Passed | |
| WLJPI37S_Reg_315 | Verify the RADIUS server reachability via EAP_TTLS Authentication | To check whether RADIUS server is successfully contacted or not via EAP_TTLS Authentication | Passed | |
| WLJPI37S_Reg_316 | Verifying the TACACS+ server reachability via PAP Authentication | To check whether TACACS+ server is successfully contacted or not via PAP Authentication | Passed | |
| WLJPI37S_Reg_317 | Checking the TACACS+ server reachability via CHAP Authentication | Verifying the TACACS+ server is successfully contacted or not via CHAP Authentication | Passed | |
| WLJPI37S_Reg_318 | 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 | |
| WLJPI37S_Reg_319 | 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 | |
| WLJPI37S_Reg_320 | 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 | |

| | | | | |
|---|---|---|---|---|
| WLJPI37S_Reg_321 | 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 | |
| WLJPI37S_Reg_322 | 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 | |
| WLJPI37S_Reg_323 | Verifying the Invalid RADIUS server connection via IP/DNS | To check whether RADIUS server is successfully contacted or not through IP/DNS | Passed | |
| WLJPI37S_Reg_324 | Verifying the Invalid TACACS+ server reachability via IP/DNS | To check whether TACACS+ server is successfully contacted or not through IP/DNS | Passed | |
| WLJPI37S_Reg_325 | Checking the RADIUS server reachability for invalid Secrete key | Verifying the RADIUS server reachability for invalid secrete key | Passed | |
| WLJPI37S_Reg_326 | 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 |
|---|---|---|---|---|
| WLJPI37S_Reg_327 | Adding a eWLC controller in PI | To Verify whether eWLC is added in PI | Passed | |
| WLJPI37S_Reg_328 | Create RF Profile with ATF Enforce mode in 2.4GHZ/5GHz and deploy to eWLC | To verify whether RF with Enforce mode is created successfully in 2.4GHZ/5GHz | Passed | |

| | | | | |
|---|---|---|---|---|
| WLJPI37S_Reg_329 | Enable optimization in RF profile with ATF Enforce mode in 2.4GHZ/5GHz and deploy to eWLC | To verify whether optimization in RF with Enforce mode is created successfully in 2.4GHZ/5GHz | Passed | |
| WLJPI37S_Reg_330 | Apply ATF Enforce mode 2.4GHZ/5GHz on RF group | To verify whether Enforcement mode is applied on RF group successfully | Passed | |
| WLJPI37S_Reg_331 | 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 | |
| WLJPI37S_Reg_332 | 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 | |
| WLJPI37S_Reg_333 | 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 | |
| WLJPI37S_Reg_334 | 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 | |
| WLJPI37S_Reg_335 | 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 | |
| WLJPI37S_Reg_336 | Client connectivity with L2 security WLAN having different Policy weight | To verify the client connectivity with two SSID having different weight | Passed | |

| | | | | |
|---|---|---|---|---|
| WLJPI37S_Reg_337 | Create the ATF profile and perform AP deployment and rule deployment to eWLC | To verify whether the profile is deployed to eWLC through AP deployment and rule deployment | Passed | |
| WLJPI37S_Reg_338 | Client connectivity in mesh setup with ATF profile in enforced mode | To verify whether clients gets connected in mesh setup AP | Passed | |
| WLJPI37S_Reg_339 | Create ATF profile with Weight Usage template in PI and deploy to eWLC | To verify whether ATF is created with weight usage template in PI and deployed to eWLC successfully | Passed | |
| WLJPI37S_Reg_340 | Create RF Profile with ATF disable mode in 2.4GHZ/5GHz and deploy to eWLC | To verify whether RF with disabled mode is created successfully in 2.4GHZ/5GHz and deployed to eWLC | Passed | |
| WLJPI37S_Reg_341 | Apply ATF disable mode 2.4GHZ/5GHz on RF group | To verify whether disabled is applied on RF group successfully | Passed | |
| WLJPI37S_Reg_342 | 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 | |
| WLJPI37S_Reg_343 | 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 | |
| WLJPI37S_Reg_344 | 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 | |

| | | | | |
|---|---|---|---|---|
| WLJPI37S_Reg_345 | Enable optimization in RF profile with ATF disable mode in 2.4GHZ/5GHz and deploy to eWLC | To verify whether optimization in RF with disabled mode is created successfully in 2.4GHZ/5GHz deployed to eWLC | Passed | |
| WLJPI37S_Reg_346 | Create RF Profile with ATF monitor mode in 2.4GHZ/5GHz and deploy to eWLC | To verify whether RF with monitor mode is created successfully in 2.4GHZ/5GHz | Passed | |
| WLJPI37S_Reg_347 | Enable optimization in RF profile with ATF monitor mode in 2.4GHZ/5GHz and deploy to eWLC | To verify whether optimization in RF with monitor mode is created successfully in 2.4GHZ/5GHz | Passed | |
| WLJPI37S_Reg_348 | Apply ATF monitor mode 2.4GHZ/5GHz on RF group | To verify whether monitor is applied on RF group successfully | Passed | |
| WLJPI37S_Reg_349 | 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 | |
| WLJPI37S_Reg_350 | 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 | |
| WLJPI37S_Reg_351 | 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 | |

# Manage 4800 ME controller in Prime

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

| | | | | |
|---|---|---|---|---|
| WLJPI37S_Reg_352 | 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 | |
| WLJPI37S_Reg_353 | 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 | |
| WLJPI37S_Reg_354 | 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 | |
| WLJPI37S_Reg_355 | 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 | |
| WLJPI37S_Reg_356 | Checking 4800 ME client details in CMX | Verifying 4800 ME client details are displaying correct or not in cmx | Passed | |
| WLJPI37S_Reg_357 | 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 | |
| WLJPI37S_Reg_358 | Checking AP 4800 ME config got synced in PI | To Verify ME configuration got synced in PI | Passed | |
| WLJPI37S_Reg_359 | Deploying Mac-Filter template to 4800 ME | To Verify Mac-Filter template got deployed in ME from PI | Passed | |
| WLJPI37S_Reg_360 | Deploying Apgroup template with rf-profile and WLAN to 4800 ME | To Verify Apgroup template got deployed in ME with WLAN and rf-profile configuration | Passed | |
| WLJPI37S_Reg_361 | 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 | |

| | | | | |
|---|---|---|---|---|
| WLJPI37S_Reg_362 | Creating local management user in 4800 ME from PI | To verify local management user is creating in ME from PI | Passed | |
| WLJPI37S_Reg_363 | Changing Management user priority to TACACS from PI | To verify Management user priority is able to change to tacacs or not from PI | Passed | |
| WLJPI37S_Reg_364 | Checking Android client connection with OPEN security wlan template | To verify Android client is connecting to OPEN security WLAN deployed from PI | Passed | |
| WLJPI37S_Reg_365 | 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 | |
| WLJPI37S_Reg_366 | 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 | |
| WLJPI37S_Reg_367 | 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 | |
| WLJPI37S_Reg_368 | Moving AP from one group to another | To verify AP is changing from one group to another or not | Passed | |
| WLJPI37S_Reg_369 | Detaching scheduled from scheduled WLAN | To verify schedule policy is detached or not from scheduled WLAN | Passed | |
| WLJPI37S_Reg_370 | Performing undeploy for deployed template | To verify deployed configuration got deleted after performing undeploy | Passed | |
| WLJPI37S_Reg_371 | Checking same template getting deployed twice | To verify same template is getting deployed twice or not | Passed | |

| | | | | |
|---|---|---|---|---|
| WLJPI37S_Reg_372 | Launching ME from PI | Verifying ME is launching from PI or not | Passed | |
| WLJPI37S_Reg_373 | Launching ME from PI after disabling https | Verifying ME is launching from PI or not after disabling https | Passed | |
| WLJPI37S_Reg_374 | Deploying template by adding device with different snmp communities | Verifying template is getting deployed or not with different snmp communities | Passed | |
| WLJPI37S_Reg_375 | Exporting AP 4800 CME device details to csv | Verifying CME device details are importing properly or not in csv | Passed | |
| WLJPI37S_Reg_376 | Adding AP 4800 CME device by csv file | Verifying ME device is adding successfully or not from csv file | Passed | |
| WLJPI37S_Reg_377 | Deleting AP 4800 ME device from PI | Verifying ME device is deleting from PI or not | Passed | |
| WLJPI37S_Reg_378 | 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 | |
| WLJPI37S_Reg_379 | Rebooting 4800 ME from PI | To Verify 4800 ME is rebooting from PI | Passed | |
| WLJPI37S_Reg_380 | Performing day0 for 4800 ME from PI | To Verify 4800 ME is coming to day0 or not | Passed | |
| WLJPI37S_Reg_381 | Rebooting 4800 ME controller by swapping ap image | To Verify 4800 ME is reflecting same after rebooting ME by swapping ap images | Passed | |
| WLJPI37S_Reg_382 | Rebooting 4800 ME controller without swapping ap image | To Verify 4800 ME is reflecting same after rebooting ME without swapping ap images | Passed | |
| WLJPI37S_Reg_383 | Setting 4800 CME time from PI | To verify cme device time can be set from PI to not | Passed | |

| | | | | |
|---|---|---|---|---|
| WLJPI37S_Reg_384 | Creating internal dhcp scope in 4800 ME | To verify internal dhcp scope is creating or not | Passed | |
| WLJPI37S_Reg_385 | Uploading 4800 ME config file | To verify 4800 ME config file is uploading or not | Passed | |
| WLJPI37S_Reg_386 | Downloading 4800 ME config file | To verify 4800 ME coming with same config after downloading the config file | Passed | |
| WLJPI37S_Reg_387 | 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 | |
| WLJPI37S_Reg_388 | 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 | |
| WLJPI37S_Reg_389 | Verifying syslog messages for 4800 ME are generating | To verify syslog messages are generating in PI for 4800 ME or not | Passed | |
| WLJPI37S_Reg_390 | Edit the WLAN Configuration for 4800 CME | To verify that configuration updating and reflecting to ME | Passed | |
| WLJPI37S_Reg_391 | Edit the Flex connect ACL for 4800 CME | To verify that Flex connect Acl configuration updating and reflecting to ME | Passed | |
| WLJPI37S_Reg_392 | 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 |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| WLJPI37S_CWL_05 | Not able to change the security from WPA2-psk to Static_WEP by configuring the PMF as required. | Configure and Verify the WLAN security from WPA2-PSk to Static_WEP | Failed | CSCvr20453 |

CHAPTER 5

# Related Documents

## Related Documentation

### CME 8.10 Rlease Notes

https://www.cisco.com/c/en/us/td/docs/wireless/access_point/mob_exp/810/release_notes/b_ME_RN_810.html

### WLC 8.10 Configuration Guide

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-10/config-guide/b_cg810.html

### CMX 10.6 Configuration Guide

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

### PI 3.7 User Guide

https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-7/user/guide/bk_CiscoPrimeInfrastructure_3_7_0_User_Guide.html

### ISE 2.6 Release Notes

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

### Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/16-12/config-guide/b_wl_16_12_cg.html