Test Results Summary for Catalyst 9800 Series Wireless Controller and EWC 17.6 for Japan (Release Version 17.6)

First Published: 2021-08-16

Last Modified: 2021-08-19

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

CONTENTS

Overview

Catalyst 9800 and EWC test

Cisco Catalyst 9800 and EWC 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 Catalyst 9800 and EWC 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 Catalyst 9800 and EWC 17.6
- High priority scenarios and basic regression features
- Inputs from Cisco SEs/ TAC

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

The following products are covered in the test execution:

- Cisco Catalyst 9800 Series Wireless Controller
- Cisco Catalyst 9800-CL Wireless Controller for Cloud
- Cisco Embedded Wireless Controller on Catalyst Access Points
- Cisco DNA Spaces
- Cisco DNA Connector
- ISE(VM)
- Cisco ISR 1100
- Cisco AP c9115
- Cisco AP c9120
- Cisco AP c9130
- Cisco AP c9105
- Access Point 4800
- Access Point 1810

Acronyms

Acronym	Description
AAA	Authentication Authorization and Accounting
ACL	Access Control List
ACS	Access Control Server
AKM	Authentication Key Management

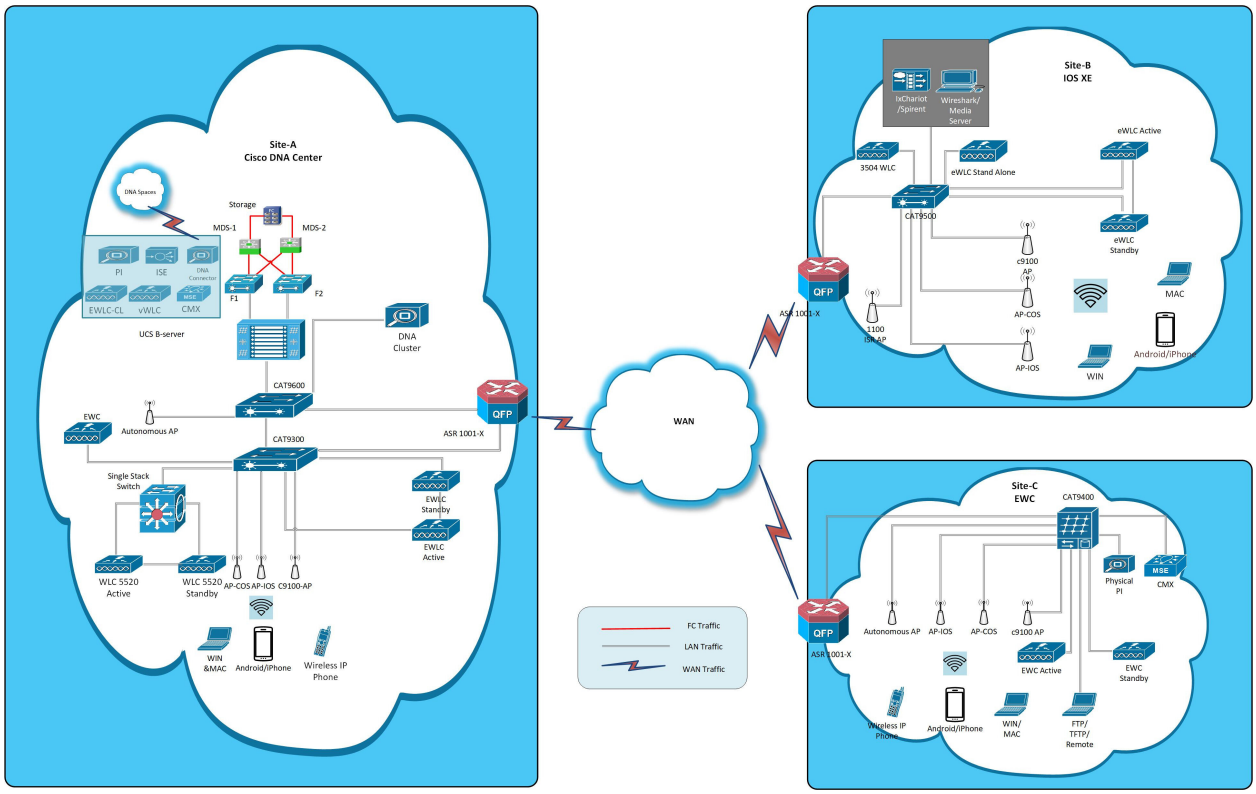
Acronym	Description
AP	Access Point
API	Application Programming Interface
APIC-EM	Application Policy Infrastructure Controller - Enterprise Module
ATF	Air-Time Fairness
AVC	Application Visibility and Control.
BGN	Bridge Group Network
BLE	Bluetooth Low Energy
BYOD	Bring Your Own Device
CA	Central Authentication
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
DNA-C	Digital Network Architecture Center
DTIM	Delivery Traffic Indication Map
DSCP	Differentiated Services Code Point
DTLS	Datagram Transport Layer Security
EAP	Extensible Authentication Protocol
EULA	End User Licence Agreement
EWC	Embedded Wireless Controller
FLA	Flex Local Authentication
FLS	Flex Local Switching
FT	Fast Transition

Acronym	Description
FTP	File Transfer Protocol
FW	Firm Ware
HA	High Availability
H-REAP	Hybrid Remote Edge Access Point
IOS	Internetwork Operating System
ISE	Identity Service Engine
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

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

Test Topology and Environment Matrix

Test Topology



Component Matrix

Category	Component	Version
Controller	Cisco Catalyst 9800-40 Wireless Controller	17.6
	Cisco Catalyst 9800-80 Wireless Controller	17.6
	Cisco Catalyst 9800-CL Wireless Controller for Cloud	17.6
	Cisco Catalyst 9800-L Wireless Controller	17.6
	Cisco Embedded Wireless Controller on Catalyst Access Points	17.6
	Virtual Controller	8.10.121.0
Applications	Cisco DNA Center	2.2.3
	Cisco DNA Spaces	Cloud (Jul 2021)
	Cisco DNA Spaces Connector	2.3.1
	Prime Infrastructure (Virtual Appliance, UCS based)	3.9.0.0
	ISE(VM)	3.0.0.393
	Cisco Jabber for Windows, iPhone	12.8
	Cisco Air Provisioning App	1.4
	Cisco Wireless App	1.0.228
Access Point	Cisco AP 9115	17.6
	Cisco AP 9120	17.6
	Cisco AP 9130	17.6
	Cisco AP 9105	17.6
	Cisco 1100 ISR	17.6
	Cisco AP 4800	15.3
	Cisco AP 1810	15.3

Category	Component	Version
Switch	Cisco Cat 9300	17.6
	Cisco Cat 9200L	17.6
	Cisco Cat 9800	17.6
	Cisco 3750V2 switch	15.0(2)SE2
	Cisco Cat 6509-E	15.1(1)SY1
Chipset	5300, 6300 AGN	15.40.41.5058
	7265 AC	21.40.2
	Airport Extreme	7.9.1
Client	Operating System(JOS)	Windows 8 & 8.1 Enterprise
		Windows XP Professional
		Windows 10
	Apple Mac Book Pro, Apple Mac Book Air (JP Locale)	Mac OS 11.5
	iPad Pro	iOS 14.7
	iPhone 6, 6S ,7 & 11 (JP Locale)	iOS 14.7
	Samsung Galaxy S7,S10, Nexus 6P, Sony Xperia XZ	Android 10.0
	Wireless IP Phone 8821	11.0.4-14
	End points	Windows 7 Enterprise
		Apple Mac 11.2.1
		Windows 8 & 8.1
		iPhone 6,6S ,7 & 11
		Windows 10
		Samsung Galaxy S4, S7,S10, Nexus 6P, Sony Xperia
	Cisco AnyConnect VPN Client	4.9.01095
	MS surface GO	Windows 10
Module	Hyper location Module	NA
Active Directory	AD	Windows server 2019
Call Control	Cisco Unified Communications Manager	12.5.0.99832-3/12.5.0.99832-3-1(JP)

Category	Component	Version
Browsers	IE	11.0
	Mozilla Firefox	90.0.2
	Safari	14.1
	Chrome	92.0.4515.107

What's New ?

Cisco Catalyst 9800 Series Wireless Controller

- Link local bridging support
- Knob to disable Random MAC Clients
- C9105 AP Support
- To share Client, Delete reason code at AP to controller
- 4800: 3rd Radio in Monitor Mode (IOS-XE)
- SSID per radio on Dual 5G
- Per AP Group NTP Server Config
- Adaptive Load EDCA Parameter (Giga School)
- Regulatory Domain Reduction
- WebUI: WLAN/AAA/ACL Simplication
- HA Management - Interface Status of the Stndby through the Active using SNMP
- MAC Address Consistency
- AP Tags needs to be Preserved
- Parallel Mode support in Image download feature
- Enhanced PnP for workflow support (AP dependency)

EWC

- C9105 EWC AP Support
- Knob to disable Random MAC Clients
- To share Client, Delete reason code at AP to controller
- Regulatory Domain Reduction
- MAC Address Consistency
- Enhanced PnP for workflow support (AP dependency)
- Parallel Mode support in Image download feature

Open Caveats

Defect	Title
CSCvx73022	Able to configure wpa2 security with 6 GHZ radio policy
CSCvy01415	Controller reloads repeatedly after giving upgrade - Critical process crash generated
CSCvx65348	Access Points count is shown incorrectly for 5Ghz radios
CSCvx88789	AccessPoints page is not loading after changingFlash duration value to 3601
CSCvx41202	Show version command output missing
CSCvx32288	Attack Detected and Cleared messages on AIR-CAP3702I-Q-K9 AP console - (No Config)
CSCvy09070	6ghz Low Data Rates option needs to remove from Best Practices - (No Config)
CSCvx69538	6 GHZ Radio Policy wlan should not configure for EWC Platforms
CSCvx98966	Not able to start or stop AP Neighborhood timer in eWC
CSCvx34344	Wlan Id and Transition Mode Wlan id should not configure same id
CSCvx38809	Unable to create/update ap join profile
CSCvx51898	EWC - Client is connecting to Protocol : 802.11n - 5 GHz even when 11n is disabled
CSCvy39499	Once Location is created, AP Join Profile should not delete
CSCvy90626	9800 HA - Able to access standby via WebUI with empty dashboard page
CSCvy89875	Transition Mode WLAN Id values needs to be update for Help guide
CSCvz09499	eWLC Wireless AP option shows "Unrecognized command' in CLI Mode
CSCvz07838	Able to configure WPA3 security without any Auth Key Mgmt parameters
CSCvy79837	Transition Mode WLAN Id valid input should be 1 to 16 - eWC
CSCvy81617	Able to configure Policy profile vlan id as more than boundary values

CSCvy29806	Unable to disable configured Regulatory Domain Country through CLI
CSCvy92385	Layer 2 Security Mode WPA3 needs to be documented in Help guide

Resolved Caveats

Defect	Title
CSCvx65392	Access Points - Unable to enable Clean air for dual band radio slot 2 AP 4800
CSCvx86103	Edit AP - Flash duration field allows input more than boundary value leading to unexpected results
CSCvx44081	Hyperlocation NTPServer IPdetails are not showing in UI dashboard
CSCvy09143	Refresh/Scrollbar button missed in Monitoring ->System page in Dark Mode
CSCvx28625	Eye Icon is not properly allocated in ewlc
CSCvx72977	Unable to delete created AP Join profile in UI dashboard
CSCvx84590	Enabled status not shown correctly for data rates in Best Practice in Japanese
CSCvx91066	AP Certificate Policy Serial Number should not configure if it doesn't match the requirements
CSCvx89610	Password Policy page is not loading after performing wrong configuration
CSCvy09686	Exported data is not properly aligned in AP Statistics
CSCvx41349	Wrong indication is showing in UI dashboard
CSCvx44999	Unable to upload CSV file and webpage loading issues observed for Flex Profile
CSCvx43702	Wireless Setup->Basic Profile creation gets failed in UI dashboard
CSCvx42701	No success pop up after click on Fix it Now
CSCvx70145	Basic wlan profile creation gets failed via WLAN Wizard
CSCvy05131	5ghz band DTPC Support redirection needs to be modified
CSCvy12668	6ghz band DFS Network is redirecting to 5ghz band network
CSCvx94077	Telnet support for newer AP models to be updated - No Config
CSCvx68495	Max RF Bandwidth cannot be configured due to Pop-up overlap
CSCvx84448	Multi BSSID profile are duplicated on clicking refresh twice

CSCvx51493	Wlan creation gets failed via WLAN Wizard - eWC Platforms
CSCvx88559	To hide non applicable attributes for Hyperlocation in EWC webUI
CSCvx26327	EWC - Unable to create location
CSCvy05454	Once configured 24ghz network through CLI, the changes not effected in UI dashboard
CSCvx46901	downgrade and upgrade impact
CSCvx86095	Data Rates are showing as blank for 2.4 GHZ - EWC Platforms
CSCvx52243	Webpage loading issues observed in RRM page - EWC Platforms
CSCvy11277	Dark Mode background issues observed stealthwatch page
CSCvx42676	Remove client allowed and blocklist feature from EWC webUI
CSCvy34239	When empty csv file uploaded, location creation gets failed
CSCvy89157	Wireless Setup -Basic ->Unable to Import Bulk AP MAC addresses using AP Provisioning
CSCvy46412	Transition Mode WLAN ID error message needs to be modified
CSCvy35505	Unnecessary scroll bars needs to be remove
CSCvy27162	Dashboard ->Interferers is not properly alligned
CSCvy36350	Warning message is not displayed properly in services in UI
CSCvy34614	Redirection name should be modified as Manual Configuration
CSCvy34145	AAA Advanced ->Device Authentication page is not loading after uploading CSV file
CSCvx64102	WLAN List shown empty after refresh button is hit continuously - (No Config)
CSCvy02731	Add radius server Pop Up cannot be closed - (No Config)
CSCvz12570	EWLC: unable to disable mac address-table aging process
CSCvz01396	Cancel button not working in file uploading option
CSCvy36282	Pop-up is appearing when configuring the interface status in controller

CSCvy27990	eWLC : General - Local EAP timers some values are not accurate & not matching
CSCvy29392	Hidden/Not displayed properly ACL in controller
CSCvy83045	Able to configure Transition Mode WLAN Id more than 16 - eWC
CSCvy34218	Able to save configuration with the new password, even if Current Password is wrong
CSCvy79693	Getting success pop up while deleting default-mesh-profile
CSCvy96687	JP Locale: Unable to create custom new-aaa-policy & unable to map NAS-ID Options for AAA Policy
CSCvy24458	JP locale : Unable to see month selection and week days in dark mode (background issue)

New Features

Link local bridging support

Logical ID	Title	Description	Status	Defect ID
EWLCJ176S_LLBS_1	Configure Link Local Bridging policy profile configuration via CLI	To configure Link Local Bridging policy profile configuration via CLI	Passed	
EWLCJ176S_LLBS_2	Checking the status of the LL bridging after creating the policy profile	To check the status of the LL bridging in policy profile	Passed	
EWLCJ176S_LLBS_3	Enabling Link Local Bridging policy profile configuration via UI	To enabling Link Local Bridging policy profile configuration via UI	Passed	
EWLCJ176S_LLBS_4	Configuring LL bridging policy profile with different VLAN id and connecting a client	To configure Link Local Bridging policy profile with different VLAN id and check if the clients gets connected or not	Passed	
EWLCJ176S_LLBS_5	Connecting a Window client to the LL bridging policy profile configured with VLAN	To connect a Window client to the LL bridging policy profile configured with VLAN and check if the client connected and the VLAN given in policy profile is used by the client for traffic	Passed	
EWLCJ176S_LLBS_6	Connecting a Android client to the LL bridging policy profile configured with VLAN	To connect a Android client to the LL bridging policy profile configured with VLAN and check if the client connected and the VLAN given in policy profile is used by the client for traffic	Passed	

EWLCJ176S_LLBS_7	Connecting a IOS client to the LL bridging policy profile configured with VLAN	To connect a IOS client to the LL bridging policy profile configured with VLAN and check if the client connected and the VLAN given in policy profile is used by the client for traffic	Passed	
EWLCJ176S_LLBS_8	Connecting a Mac OS client to the LL bridging policy profile configured with VLAN	To connect a Mac OS client to the LL bridging policy profile configured with VLAN and check if the client connected and the VLAN given in policy profile is used by the client for traffic	Passed	
EWLCJ176S_LLBS_9	Enable link local bridging in an inter controller scenario, with a different VLAN set on first eWLC than on second eWLC. Roam the Window client from first to second controller.	To roam the Window client front one eWLC to another eWLC enabling link local bridging in an inter controller scenario, with a different VLAN set on first eWLC than on second eWLC.	Passed	
EWLCJ176S_LLBS_10	Enable link local bridging in an inter controller scenario, with a different VLAN set on first eWLC than on second eWLC. Roam the Android client from first to second controller.	To roam the Android client front one eWLC to another eWLC enabling link local bridging in an inter controller scenario, with a different VLAN set on first eWLC than on second eWLC.	Passed	

EWLCJ176S_LLBS_11	Enable link local bridging in an inter controller scenario, with a different VLAN set on first eWLC than on second eWLC. Roam the IOS client from first to second controller.	To roam the IOS client front one eWLC to another eWLC enabling link local bridging in an inter controller scenario, with a different VLAN set on first eWLC than on second eWLC.	Passed	
EWLCJ176S_LLBS_12	Enable link local bridging in an inter controller scenario, with a different VLAN set on first eWLC than on second eWLC. Roam the Window client from first to second controller.	To roam the Mac OS client front one eWLC to another eWLC enabling link local bridging in an inter controller scenario, with a different VLAN set on first eWLC than on second eWLC.	Passed	
EWLCJ176S_LLBS_13	Enabling link local bridging in policy profile in a HA setup and verifying the same after switchover	To verify the link local bridging in policy profile in a HA setup and check the configuration after the switchover	Passed	
EWLCJ176S_LLBS_14	Enable link local bridging in policy profile in a HA setup and Join a window client to try Switch over.	To enable link local bridging in policy profile in a HA setup and Join a window client to try Switch over.	Passed	
EWLCJ176S_LLBS_15	Enable link local bridging in policy profile in a HA setup and Join a Android client to try Switch over.	To enable link local bridging in policy profile in a HA setup and Join a window client to try Switch over.	Passed	
EWLCJ176S_LLBS_16	Enable link local bridging in policy profile in a HA setup and Join a IOS client to try Switch over.	To enable link local bridging in policy profile in a HA setup and Join a IOS client to try Switch over.	Passed	

EWLCJ176S_LLBS_17	Enable link local bridging in policy profile in a HA setup and Join a Mac OS client to try Switch over.	To enable link local bridging in policy profile in a HA setup and Join a Mac OS client to try Switch over.	Passed	
EWLCJ176S_LLBS_18	Enable link local bridging in policy profile in a HA setup and Join a window Surface client to try Switch over.	To enable link local bridging in policy profile in a HA setup and Join a window Surface client to try Switch over.	Passed	
EWLCJ176_2S_Reg_01	Configure Link Local Bridging policy profile configuration via CLI	To configure Link Local Bridging policy profile configuration via CLI	Passed	
EWLCJ176_2S_Reg_02	Checking the status of the LL bridging after creating the policy profile	To check the status of the LL bridging in policy profile	Passed	
EWLCJ176_2S_Reg_03	Enabling Link Local Bridging policy profile configuration via UI	To enabling Link Local Bridging policy profile configuration via UI	Passed	
EWLCJ176_2S_Reg_04	Configuring LL bridging policy profile with different VLAN id and connecting a client	To configure Link Local Bridging policy profile with different VLAN id and check if the clients gets connected or not	Passed	
EWLCJ176_2S_Reg_05	Connecting a Window client to the LL bridging policy profile configured with VLAN	To connect a Window client to the LL bridging policy profile configured with VLAN and check if the client connected and the VLAN given in policy profile is used by the client for traffic	Passed	CSCvy46412

EWLCJ176_2S_Reg_06	Connecting a Android client to the LL bridging policy profile configured with VLAN	To connect a Android client to the LL bridging policy profile configured with VLAN and check if the client connected and the VLAN given in policy profile is used by the client for traffic	Passed	
EWLCJ176_2S_Reg_07	Connecting a IOS client to the LL bridging policy profile configured with VLAN	To connect a IOS client to the LL bridging policy profile configured with VLAN and check if the client connected and the VLAN given in policy profile is used by the client for traffic	Passed	
EWLCJ176_2S_Reg_08	Connecting a Mac OS client to the LL bridging policy profile configured with VLAN	To connect a Mac OS client to the LL bridging policy profile configured with VLAN and check if the client connected and the VLAN given in policy profile is used by the client for traffic	Passed	
EWLCJ176_2S_Reg_09	Enable link local bridging in an inter controller scenario, with a different VLAN set on first eWLC than on second eWLC. Roam the Window client from first to second controller.	To roam the Window client front one eWLC to another eWLC enabling link local bridging in an inter controller scenario, with a different VLAN set on first eWLC than on second eWLC.	Passed	

EWLCJ176_2S_Reg_10	Enable link local bridging in an inter controller scenario, with a different VLAN set on first eWLC than on second eWLC. Roam the Android client from first to second controller.	To roam the Android client front one eWLC to another eWLC enabling link local bridging in an inter controller scenario, with a different VLAN set on first eWLC than on second eWLC.	Passed	
EWLCJ176_2S_Reg_11	Enable link local bridging in an inter controller scenario, with a different VLAN set on first eWLC than on second eWLC. Roam the IOS client from first to second controller.	To roam the IOS client front one eWLC to another eWLC enabling link local bridging in an inter controller scenario, with a different VLAN set on first eWLC than on second eWLC.	Passed	
EWLCJ176_2S_Reg_12	Enable link local bridging in an inter controller scenario, with a different VLAN set on first eWLC than on second eWLC. Roam the Window client from first to second controller.	To roam the Mac OS client front one eWLC to another eWLC enabling link local bridging in an inter controller scenario, with a different VLAN set on first eWLC than on second eWLC.	Passed	
EWLCJ176_2S_Reg_13	Enabling link local bridging in policy profile in a HA setup and verifying the same after switchover	To verify the link local bridging in policy profile in a HA setup and check the configuration after the switchover	Passed	
EWLCJ176_2S_Reg_14	Enable link local bridging in policy profile in a HA setup and Join a window client to try Switch over.	To enable link local bridging in policy profile in a HA setup and Join a window client to try Switch over.	Passed	

EWLCJ176_2S_Reg_15	Enable link local bridging in policy profile in a HA setup and Join a Android client to try Switch over.	To enable link local bridging in policy profile in a HA setup and Join a window client to try Switch over.	Passed	
EWLCJ176_2S_Reg_16	Enable link local bridging in policy profile in a HA setup and Join a IOS client to try Switch over.	To enable link local bridging in policy profile in a HA setup and Join a IOS client to try Switch over.	Passed	
EWLCJ176_2S_Reg_17	Enable link local bridging in policy profile in a HA setup and Join a Mac OS client to try Switch over.	To enable link local bridging in policy profile in a HA setup and Join a Mac OS client to try Switch over.	Passed	
EWLCJ176_2S_Reg_18	Enable link local bridging in policy profile in a HA setup and Join a window Surface client to try Switch over.	To enable link local bridging in policy profile in a HA setup and Join a window Surface client to try Switch over.	Passed	

Knob to disable Random MAC Clients

Logical ID	Title	Description	Status	Defect ID
EWLCJ176S_KDRM_1	Configure a WLAN and verify LAA default setting	To Configure a WLAN and verify LAA default setting	Passed	
EWLCJ176S_KDRM_2	Enable LAA in WLAN and connect iPhone with burned in mac	To verify connectivity after enabling LAA in WLAN and connect iPhone with burned in mac	Passed	
EWLCJ176S_KDRM_3	Enable LAA in WLAN and connect Windows with burned in mac	To verify connectivity after enabling LAA in WLAN and connect Windows with burned in mac / WIFI adapter mac	Passed	
EWLCJ176S_KDRM_4	Enable LAA in WLAN and connect Android with burned in mac	To verify connectivity after enabling LAA in WLAN and connect Android with burned in mac	Passed	
EWLCJ176S_KDRM_5	Enable LAA in WLAN and connect iPhone with LAA	To verify connectivity after enabling LAA in WLAN and connect iPhone with LAA	Passed	
EWLCJ176S_KDRM_6	Enable LAA in WLAN and connect Windows with LAA	To verify connectivity after enabling LAA in WLAN and connect Windows with LAA	Passed	

EWLCJ176S_KDRM_7	Enable LAA in WLAN and connect Android with LAA	To verify connectivity after enabling LAA in WLAN and connect Android with LAA	Passed	
EWLCJ176S_KDRM_8	Connect iPhone without LAA and after joining enable LAA device in WLAN and verify client connectivity.	To verify connectivity after connecting iPhone without LAA and after joining enable LAA device in WLAN and verify client connectivity.	Passed	
EWLCJ176S_KDRM_9	Connect windows without LAA and after joining enable LAA device in WLAN and verify client connectivity.	To verify connectivity after connecting windows without LAA and after joining enable LAA device in WLAN and verify client connectivity.	Passed	
EWLCJ176S_KDRM_10	Connect android without LAA and after joining enable LAA device in WLAN and verify client connectivity.	To verify connectivity after connecting android without LAA and after joining enable LAA device in WLAN and verify client connectivity.	Passed	
EWLCJ176S_KDRM_11	Connect iPhone without LAA and after joining enable LAA in WLAN, disconnect and reconnect the device to different SSID without LAA	To verify connectivity after connecting iPhone without LAA and after joining enable LAA device disconnect and reconnect the device to different SSID without LAA	Passed	

EWLCJ176S_KDRM_12	Connect windows without LAA and after joining enable LAA in WLAN device disconnect and reconnect the device to different SSID without LAA	To verify connectivity after connecting connect windows without LAA and after joining enable LAA device disconnect and reconnect the device to different SSID without LAA	Passed	
EWLCJ176S_KDRM_13	Connect android without LAA and after joining enable LAA in WLAN, disconnect and reconnect the device to different SSID without LAA	To verify connectivity after connecting connect android without LAA and after joining enable LAA device disconnect and reconnect the device to different SSID without LAA	Passed	
EWLCJ176S_KDRM_14	Connect one device in random mac and other with burned-in mac to WLAN profile with LAA enabled	To verify connectivity after connecting one device in random mac and other with burned-in mac to WLAN profile with LAA enabled	Passed	
EWLCJ176S_KDRM_15	Add LAA address of in iPhone client and Create a DHCP pool in ewlc and give LAA of windows as client identifier and use LAA deny profile, connect client then check client gets denied or not	To verify connectivity after adding LAA mac address of iPhone client and Create a DHCP pool in ewlc and give private mac address as client identifier and use LAA deny profile, connect client then check client gets denied or not	Passed	

EWLCJ176S_KDRM_16	Add LAA address of in windows client and Create a DHCP pool in ewlc and give LAA of windows as client identifier and use LAA deny profile, connect client then check client gets denied or not	To verify connectivity after adding LAA mac address of Windows client and Create a DHCP pool in ewlc and give private mac address as client identifier and use LAA deny profile, connect client then check client gets denied or not	Passed	
EWLCJ176S_KDRM_17	functionality of Non random mac Client with default config and verify client details in DNAC	To verify functionality of Non random mac Client with default config and verify client details in DNAC	Passed	
EWLCJ176S_KDRM_18	functionality of Non random mac Client with default config and verify client details in DNA Spaces Behaviour metrics	To verify functionality of Non random mac Client with default config and verify client details in DNAS Behaviour metrics	Passed	
EWLCJ176S_KDRM_19	functionality of Non random mac Client with default config and verify client details in DNA Spaces location metrics	To verify functionality of Non random mac Client with default config and verify client details in DNAS location metrics	Passed	
EWLCJ176S_KDRM_20	client connectivity to WLAN enabled with LAA deny after ewlc reload	To verify client connectivity to WLAN enabled with LAA deny after ewlc reload	Passed	
EWCJ176S_KDRM_01	Creating WLAN with "deny LAA Clients" disable	To Create a WLAN with "deny LAA clients" disable	Passed	

EWCJ176S_KDRM_02	Creating WLAN with " deny LAA Clients" enable	To Create a WLAN with "deny LLA clients" enable	Passed	
EWCJ176S_KDRM_03	Enable LAA in WLAN and connect Windows with burned in mac	To verify connectivity after enabling LAA in WLAN and connect Windows with burned in mac / WIFI adapter mac	Passed	
EWCJ176S_KDRM_04	Enable LAA in WLAN and connect Samsung S10 with burned in mac	To verify connectivity after enabling LAA in WLAN and connect Samsung S10 with burned in mac	Passed	
EWCJ176S_KDRM_05	Enable LAA in WLAN and connect iPhone with burned in mac	To verify connectivity after enabling LAA in WLAN and connect iPhone with burned in mac	Passed	
EWCJ176S_KDRM_06	Enable LAA in WLAN and connect iPhone with LAA	To verify connectivity after enabling LAA in WLAN and connect iPhone with LAA	Passed	
EWCJ176S_KDRM_07	Enable LAA in WLAN and connect Windows with LAA	To verify connectivity after enabling LAA in WLAN and connect Windows with LAA	Passed	
EWCJ176S_KDRM_08	Enable LAA in WLAN and connect Android with LAA	To verify connectivity after enabling LAA in WLAN and connect Android with LAA	Passed	

EWCJ176S_KDRM_09	Connect iPhone without LAA and after joining enable LAA device in WLAN and verify client connectivity.	To verify connectivity after connecting iPhone without LAA and after joining enable LAA device in WLAN and verify client connectivity.	Passed	
EWCJ176S_KDRM_10	Connect windows without LAA and after joining enable LAA device in WLAN and verify client connectivity.	To verify connectivity after connecting windows without LAA and after joining enable LAA device in WLAN and verify client connectivity.	Passed	
EWCJ176S_KDRM_11	Connect android without LAA and after joining enable LAA device in WLAN and verify client connectivity.	To verify connectivity after connecting android without LAA and after joining enable LAA device in WLAN and verify client connectivity.	Passed	
EWCJ176S_KDRM_12	Connect iPhone without LAA and after joining enable LAA in WLAN, disconnect and reconnect the device to different SSID without LAA	To verify connectivity after connecting iPhone without LAA and after joining enable LAA device disconnect and reconnect the device to different SSID without LAA	Passed	

EWCJ176S_KDRM_13	Connect windows without LAA and after joining enable LAA in WLAN device disconnect and reconnect the device to different SSID without LAA	To verify connectivity after connecting connect windows without LAA and after joining enable LAA device disconnect and reconnect the device to different SSID without LAA	Passed	
EWCJ176S_KDRM_14	Connect android without LAA and after joining enable LAA in WLAN, disconnect and reconnect the device to different SSID without LAA	To verify connectivity after connecting connect android without LAA and after joining enable LAA device disconnect and reconnect the device to different SSID without LAA	Passed	
EWCJ176S_KDRM_15	Connect one device in random mac and other with burned-in mac to WLAN profile with LAA enabled	To verify connectivity after connecting one device in random mac and other with burned-in mac to WLAN profile with LAA enabled	Passed	
EWCJ176S_KDRM_16	Add LAA address of in iPhone client and Create a DHCP pool in EWC and give LAA of windows as client identifier and use LAA deny profile, connect client then check client gets denied or not	To verify connectivity after adding LAA mac address of iPhone client and Create a DHCP pool in EWC and give private mac address as client identifier and use LAA deny profile, connect client then check client gets denied or not	Passed	

EWCJ176S_KDRM_17	Add LAA address of in windows client and Create a DHCP pool in EWC and give LAA of windows as client identifier and use LAA deny profile, connect client then check client gets denied or not	To verify connectivity after adding LAA mac address of Windows client and Create a DHCP pool in EWC and give private mac address as client identifier and use LAA deny profile, connect client then check client gets denied or not	Passed	
EWCJ176S_KDRM_18	functionality of Non random mac Client with default config and verify client details in DNAC	To verify functionality of Non random mac Client with default config and verify client details in DNAC	Passed	
EWCJ176S_KDRM_19	functionality of Non random mac Client with default config and verify client details in DNA Spaces Behaviour metrics	To verify functionality of Non random mac Client with default config and verify client details in DNAS Behaviour metrics	Passed	
EWCJ176S_KDRM_20	functionality of Non random mac Client with default config and verify client details in DNA Spaces location metrics	To verify functionality of Non random mac Client with default config and verify client details in DNAS location metrics	Passed	
EWCJ176S_KDRM_21	client connectivity to WLAN enabled with LAA deny after EWC reload	To verify client connectivity to WLAN enabled with LAA deny after EWC reload	Passed	
EWCJ176S_KDRM_22	Checking the Intra roaming concepts with enabled LAA	To verify the intra roaming concepts with enabled LAA	Passed	

EWCJ176S_KDRM_23	Checking the Intra roaming concepts with enabled LAA using different end points	To verify the intra roaming concepts with enabled LAA using different end points	Passed	
EWLCJ176_2S_R_MAC_1	Configure a WLAN and verify LAA default setting	To Configure a WLAN and verify LAA default setting	Passed	
EWLCJ176_2S_R_MAC_2	Enable Deny LAA in WLAN and connect iPhone with burned in mac	To verify connectivity after enabling LAA in WLAN and connect iPhone with burned in mac	Passed	
EWLCJ176_2S_R_MAC_3	Enable Deny LAA in WLAN and connect Windows with burned in mac	To verify connectivity after enabling LAA in WLAN and connect Windows with burned in mac / WIFI adapter mac	Passed	
EWLCJ176_2S_R_MAC_4	Enable Deny LAA in WLAN and connect Android with burned in mac	To verify connectivity after enabling LAA in WLAN and connect Android with burned in mac	Passed	
EWLCJ176_2S_R_MAC_5	Enable Deny LAA in WLAN and connect iPhone with LAA	To verify connectivity after enabling LAA in WLAN and connect iPhone with LAA	Passed	
EWLCJ176_2S_R_MAC_6	Enable Deny LAA in WLAN and connect Windows with LAA	To verify connectivity after enabling LAA in WLAN and connect Windows with LAA	Passed	

EWLCJ176_2S_R_MAC_7	Enable Deny LAA in WLAN and connect Android with LAA	To verify connectivity after enabling LAA in WLAN and connect Android with LAA	Passed	
EWLCJ176_2S_R_MAC_8	Connect iPhone without deny LAA in WLAN and after joining enable LAA device in WLAN and verify client connectivity.	To verify connectivity after connecting iPhone without LAA and after joining enable LAA device in WLAN and verify client connectivity.	Passed	
EWLCJ176_2S_R_MAC_9	Connect windows without deny LAA in WLAN and after joining enable deny LAA device in WLAN and verify client connectivity.	To verify connectivity after connecting windows without LAA and after joining enable LAA device in WLAN and verify client connectivity.	Passed	
EWLCJ176_2S_R_MAC_10	Connect android without deny LAA in WLAN and after joining enable deny LAA device in WLAN and verify client connectivity.	To verify connectivity after connecting android without LAA and after joining enable LAA device in WLAN and verify client connectivity.	Passed	
EWLCJ176_2S_R_MAC_11	Connect iPhone without deny LAA in WLAN and after joining enable deny LAA in WLAN, disconnect and reconnect the device to different SSID without LAA	To verify connectivity after connecting iPhone without LAA and after joining enable LAA device disconnect and reconnect the device to different SSID without LAA	Passed	

EWLCJ176_2S_R_MAC_12	Connect windows without deny LAA in WLAN and after joining enable deny LAA in WLAN device disconnect and reconnect the device to different SSID without LAA	To verify connectivity after connecting connect windows without LAA and after joining enable LAA device disconnect and reconnect the device to different SSID without LAA	Passed	
EWLCJ176_2S_R_MAC_13	Connect android without deny LAA in WLAN and after joining enable deny LAA in WLAN, disconnect and reconnect the device to different SSID without LAA	To verify connectivity after connecting connect android without LAA and after joining enable LAA device disconnect and reconnect the device to different SSID without LAA	Passed	
EWLCJ176_2S_R_MAC_14	Connect one device in random mac and other with burned-in mac to WLAN profile with LAA enabled	To verify connectivity after connecting one device in random mac and other with burned-in mac to WLAN profile with LAA enabled	Passed	
EWLCJ176_2S_R_MAC_15	Add LAA address of in iPhone client and Create a DHCP pool in ewlc and give LAA of windows as client identifier and use LAA deny profile, connect client then check client gets denied or not	To verify connectivity after adding LAA mac address of iPhone client and Create a DHCP pool in ewlc and give private mac address as client identifier and use LAA deny profile, connect client then check client gets denied or not	Passed	

EWLCJ176_2S_R_MAC_16	Add LAA address of in windows client and Create a DHCP pool in ewlc and give LAA of windows as client identifier and use LAA deny profile, connect client then check client gets denied or not	To verify connectivity after adding LAA mac address of Windows client and Create a DHCP pool in ewlc and give private mac address as client identifier and use LAA deny profile, connect client then check client gets denied or not	Passed	
EWLCJ176_2S_R_MAC_17	functionality of Non random mac Client with default config and verify client details in DNAC	To verify functionality of Non random mac Client with default config and verify client details in DNAC	Passed	
EWLCJ176_2S_R_MAC_18	client connectivity to WLAN enabled with LAA deny after ewlc reload	To verify client connectivity to WLAN enabled with LAA deny after ewlc reload	Passed	
EWCJ176_2S_R_MAC_1	Configure a WLAN and verify LAA default setting	To Configure a WLAN and verify LAA default setting	Passed	
EWCJ176_2S_R_MAC_2	Enable LAA in WLAN and connect iPhone with burned in mac	To verify connectivity after enabling LAA in WLAN and connect iPhone with burned in mac	Passed	
EWCJ176_2S_R_MAC_3	Enable LAA in WLAN and connect Windows with burned in mac	To verify connectivity after enabling LAA in WLAN and connect Windows with burned in mac / WIFI adapter mac	Passed	

EWCJ176_2S_R_MAC_4	Enable LAA in WLAN and connect Android with burned in mac	To verify connectivity after enabling LAA in WLAN and connect Android with burned in mac	Passed	
EWCJ176_2S_R_MAC_5	Enable LAA in WLAN and connect iPhone with LAA	To verify connectivity after enabling LAA in WLAN and connect iPhone with LAA	Passed	
EWCJ176_2S_R_MAC_6	Enable LAA in WLAN and connect Windows with LAA	To verify connectivity after enabling LAA in WLAN and connect Windows with LAA	Failed	CSCvy83045
EWCJ176_2S_R_MAC_7	Enable LAA in WLAN and connect Android with LAA	To verify connectivity after enabling LAA in WLAN and connect Android with LAA	Passed	
EWCJ176_2S_R_MAC_8	Connect iPhone without LAA and after joining enable LAA device in WLAN and verify client connectivity.	To verify connectivity after connecting iPhone without LAA and after joining enable LAA device in WLAN and verify client connectivity.	Passed	
EWCJ176_2S_R_MAC_9	Connect windows without LAA and after joining enable LAA device in WLAN and verify client connectivity.	To verify connectivity after connecting windows without LAA and after joining enable LAA device in WLAN and verify client connectivity.	Passed	

EWCJ176_2S_R_MAC_10	Connect android without LAA and after joining enable LAA device in WLAN and verify client connectivity.	To verify connectivity after connecting android without LAA and after joining enable LAA device in WLAN and verify client connectivity.	Passed	
EWCJ176_2S_R_MAC_11	Connect iPhone without LAA and after joining enable LAA in WLAN, disconnect and reconnect the device to different SSID without LAA	To verify connectivity after connecting iPhone without LAA and after joining enable LAA device disconnect and reconnect the device to different SSID without LAA	Passed	
EWCJ176_2S_R_MAC_12	Connect windows without LAA and after joining enable LAA in WLAN device disconnect and reconnect the device to different SSID without LAA	To verify connectivity after connecting connect windows without LAA and after joining enable LAA device disconnect and reconnect the device to different SSID without LAA	Passed	
EWCJ176_2S_R_MAC_13	Connect android without LAA and after joining enable LAA in WLAN, disconnect and reconnect the device to different SSID without LAA	To verify connectivity after connecting connect android without LAA and after joining enable LAA device disconnect and reconnect the device to different SSID without LAA	Passed	

EWCJ176_2S_R_MAC_14	Connect one device in random mac and other with burned-in mac to WLAN profile with LAA enabled	To verify connectivity after connecting one device in random mac and other with burned-in mac to WLAN profile with LAA enabled	Passed	
EWCJ176_2S_R_MAC_15	Add LAA address of in iPhone client and Create a DHCP pool in ewlc and give LAA of windows as client identifier and use LAA deny profile, connect client then check client gets denied or not	To verify connectivity after adding LAA mac address of iPhone client and Create a DHCP pool in ewlc and give private mac address as client identifier and use LAA deny profile, connect client then check client gets denied or not	Passed	
EWCJ176_2S_R_MAC_16	Add LAA address of in windows client and Create a DHCP pool in ewlc and give LAA of windows as client identifier and use LAA deny profile, connect client then check client gets denied or not	To verify connectivity after adding LAA mac address of Windows client and Create a DHCP pool in ewlc and give private mac address as client identifier and use LAA deny profile, connect client then check client gets denied or not	Passed	
EWCJ176_2S_R_MAC_17	functionality of Non random mac Client with default config and verify client details in DNAC	To verify functionality of Non random mac Client with default config and verify client details in DNAC	Passed	

EWCJ176_2S_R_MAC_18	functionality of Non random mac Client with default config and verify client details in DNA Spaces Behaviour metrics	To verify functionality of Non random mac Client with default config and verify client details in DNAS Behaviour metrics	Passed	
EWCJ176_2S_R_MAC_19	functionality of Non random mac Client with default config and verify client details in DNA Spaces location metrics	To verify functionality of Non random mac Client with default config and verify client details in DNAS location metrics	Passed	
EWCJ176_2S_R_MAC_20	client connectivity to WLAN enabled with LAA deny after ewlc reload	To verify client connectivity to WLAN enabled with LAA deny after ewlc reload	Passed	

C9105 AP Support

Logical ID	Title	Description	Status	Defect ID
EWLCJ176S_C9105AP_1	Association of 9105 AP with different eWLC model	To associate 9105 AP to eWLC with latest image and check if the AP gets associated or not	Passed	
EWLCJ176S_C9105AP_2	Associating 9105 AP with different country code as with eWLC	To associate 9105 AP with different country code and check if the AP does not get joined to eWLC	Passed	
EWLCJ176S_C9105AP_3	Configuring AP with duplicate IP	To configure AP with a duplicate IP address and check if the AP shows error message and AP does not join the eWLC	Passed	
EWLCJ176S_C9105AP_4	Rebooting the 9105 AP	To check if the AP gets Rebooted or not and check if the AP joins the controller again.	Passed	
EWLCJ176S_C9105AP_5	Rebooting the AP with primary controller given in High Availability	To reboot the AP by giving the primary controller IP using high availability and check if the AP joins the primary controller	Passed	
EWLCJ176S_C9105AP_6	Checking the details of the AP through the CLI	To check the details of the AP using CLI and check if the details are correctly shown or not	Passed	
EWLCJ176S_C9105AP_7	Connecting a Window client to the 9105 AP	To connect a window client to the AP and check if the client gets connected to the AP without any errors.	Passed	

EWLCJ176S_C9105AP_8	Connecting a Android client to the 9105 AP	To connect a Android client to the AP and check if the client gets connected to the AP without any errors.	Passed	
EWLCJ176S_C9105AP_9	Connecting a IOS client to the 9105 AP	To connect a IOS client to the AP and check if the client gets connected to the AP without any errors.	Passed	
EWLCJ176S_C9105AP_10	Connecting a MAC client to the 9105 AP	To connect a MAC client to the AP and check if the client gets connected to the AP without any errors.	Passed	
EWLCJ176S_C9105AP_11	AP failover priority with critical	To check AP failover priority with critical and check if the AP gets connected to the next controller .	Passed	
EWLCJ176S_C9105AP_12	AP failover priority with High priority	To check AP failover priority with critical and check if the AP gets connected to the next controller .	Passed	
EWLCJ176S_C9105AP_13	Moving AP from 9800-40 eWLC to 9800-80 through High availability	To check if the AP moves from 9800-40 eWLC to 9800-80 eWLC through high availability.	Passed	
EWLCJ176S_C9105AP_14	Reassociation of client to the AP after reboot	To verify if the client gets reassociated to the to the AP .	Passed	

EWLCJ176S_C9105AP_15	Checking if the client do not connect to the AP after rebooting and joining the primary controller	To check if the client gets connected to the AP after rebooting the AP and AP joining the primary controller .where there is no same WLAN	Passed	
EWLCJ176S_C9105AP_16	Performing Intra controller roaming of Android client	To check whether intra controller roaming of Android clients works properly or not	Passed	
EWLCJ176S_C9105AP_17	Performing Intra controller roaming of IOS client	To check whether intra controller roaming of IOS clients works properly or not in eWLC	Passed	
EWLCJ176S_C9105AP_18	Performing Intra controller roaming of Mac OS client	To check whether intra controller roaming of MacOS clients works properly or not	Passed	
EWLCJ176S_C9105AP_19	Performing Inter controller roaming of Windows OS client	To check whether inter controller roaming of windows clients works properly or not	Passed	
EWLCJ176S_C9105AP_20	Performing Inter controller roaming of Android client	To check whether inter controller roaming of Android clients works properly or not	Passed	
EWLCJ176S_C9105AP_21	Performing Inter controller roaming of IOS client	To check whether inter controller roaming of IOS clients works properly or not	Passed	
EWLCJ176S_C9105AP_22	Performing Inter controller roaming of Mac OS client	To check whether inter controller roaming of Mac OS clients works properly or not	Passed	

EWLCJ176S_C9105AP_23	Change AP mode from local to Flex connect in 9105 AP.	To change the mode of AP from local mode to Flex connect mode and check if the AP does not reboot.	Passed	
EWLCJ176S_C9105AP_24	Changing the AP from Flex connect to Local mode and check if the AP reboot	To check if the AP reboots when AP mode is changed from flex connect to Local mode .	Passed	
EWLCJ176S_C9105AP_25	Adding two 9105 AP in the AP group and connecting a client to the AP with specific WLAN	To add two 9105 AP in AP group and map a WLAN to group and connect a client to the WLAN and check the client connectivity	Passed	
EWLCJ176S_C9105AP_26	Configuring different Syslog facility for 9115 11ax AP in eWLC and checking the same in the APs	To configure different syslog facility for 9115 AP in eWLC AP join profile and validating the same in the AP	Passed	
EWLCJ176S_C9105AP_27	Packet capture of client when the client is connected to 9115/9120 AP with 2.4 GHz	To capture the Packet of the client when the client is connected to AP with radio as 2.4GHz	Passed	
EWLCJ176S_C9105AP_28	Verify details by connecting client to 2.4Ghz radio of 9105 AP.	To verify OFDMA details by connecting client to 2.4 Ghz radio.	Passed	
EWLCJ176S_C9105AP_29	Verify details by connecting client to 5 Ghz radio of 9105 AP	To verify OFDMA details by connecting client to 5 Ghz radio.	Passed	
EWLCJ176S_C9105AP_30	Verify 9105AP MU-MIMO details with client connecting to WPA2 configured WLAN	To verify 11ax MU-MIMO details of 9105 AP with client connecting to WPA2 configured WLAN	Passed	

EWLCJ176S_C9105AP_31	Verify 9105AP MU-MIMO details with client connecting to WPA 3 configured WLAN	To verify 11ax MU-MIMO details of 9105 AP with client connecting to WPA 3 configured WLAN	Passed	
EWLCJ176_2S_Reg_19	Association of 9105 AP with different eWLC model	To associate 9105 AP to eWLC with latest image and check if the AP gets associated or not	Passed	
EWLCJ176_2S_Reg_20	Associating 9105 AP with different country code as with eWLC	To associate 9105 AP with different country code and check if the AP does not get joined to eWLC	Passed	
EWLCJ176_2S_Reg_21	Configuring AP with duplicate IP	To configure AP with a duplicate IP address and check if the AP shows error message and AP does not join the eWLC	Passed	
EWLCJ176_2S_Reg_22	Rebooting the 9105 AP	To check if the AP gets Rebooted or not and check if the AP joins the controller again.	Passed	
EWLCJ176_2S_Reg_23	Rebooting the AP with primary controller given in High Availability	To reboot the AP by giving the primary controller IP using high availability and check if the AP joins the primary controller	Passed	
EWLCJ176_2S_Reg_24	Checking the details of the AP through the CLI	To check the details of the AP using CLI and check if the details are correctly shown or not	Failed	CSCvz01396
EWLCJ176_2S_Reg_25	Connecting a Window client to the 9105 AP	To connect a window client to the AP and check if the client gets connected to the AP without any errors.	Passed	

EWLCJ176_2S_Reg_26	Connecting a Android client to the 9105 AP	To connect a Android client to the AP and check if the client gets connected to the AP without any errors.	Passed	
EWLCJ176_2S_Reg_27	Connecting a IOS client to the 9105 AP	To connect a IOS client to the AP and check if the client gets connected to the AP without any errors.	Passed	CSCvy35505
EWLCJ176_2S_Reg_28	Connecting a MAC client to the 9105 AP	To connect a MAC client to the AP and check if the client gets connected to the AP without any errors.	Passed	
EWLCJ176_2S_Reg_29	AP failover priority with critical	To check AP failover priority with critical and check if the AP gets connected to the next controller .	Passed	
EWLCJ176_2S_Reg_30	AP failover priority with High priority	To check AP failover priority with critical and check if the AP gets connected to the next controller .	Passed	
EWLCJ176_2S_Reg_31	Moving AP from 9800-40 eWLC to 9800-80 through High availability	To check if the AP moves from 9800-40 eWLC to 9800-80 eWLC through high availability.	Passed	
EWLCJ176_2S_Reg_32	Reassociation of client to the AP after reboot	To verify if the client gets reassociated to the to the AP .	Passed	

EWLCJ176_2S_Reg_33	Checking if the client do not connect to the AP after rebooting and joining the primary controller	To check if the client gets connected to the AP after rebooting the AP and AP joining the primary controller .where there is no same WLAN	Passed	
EWLCJ176_2S_Reg_34	Performing Intra controller roaming of Android client	To check whether intra controller roaming of Android clients works properly or not	Passed	
EWLCJ176_2S_Reg_35	Performing Intra controller roaming of IOS client	To check whether intra controller roaming of IOS clients works properly or not in eWLC	Passed	
EWLCJ176_2S_Reg_36	Performing Intra controller roaming of Mac OS client	To check whether intra controller roaming of MacOS clients works properly or not	Passed	
EWLCJ176_2S_Reg_37	Performing Inter controller roaming of Windows OS client	To check whether inter controller roaming of windows clients works properly or not	Passed	
EWLCJ176_2S_Reg_38	Performing Inter controller roaming of Android client	To check whether inter controller roaming of Android clients works properly or not	Passed	
EWLCJ176_2S_Reg_39	Performing Inter controller roaming of IOS client	To check whether inter controller roaming of IOS clients works properly or not	Passed	
EWLCJ176_2S_Reg_40	Performing Inter controller roaming of Mac OS client	To check whether inter controller roaming of Mac OS clients works properly or not	Passed	

EWLCJ176_2S_Reg_41	Change AP mode from local to Flex connect in 9105 AP.	To change the mode of AP from local mode to Flex connect mode and check if the AP does not reboot.	Passed	
EWLCJ176_2S_Reg_42	Changing the AP from Flex connect to Local mode and check if the AP reboot	To check if the AP reboots when AP mode is changed from flex connect to Local mode .	Passed	
EWLCJ176_2S_Reg_43	Adding two 9105 AP in the AP group and connecting a client to the AP with specific WLAN	To add two 9105 AP in AP group and map a WLAN to group and connect a client to the WLAN and check the client connectivity	Passed	
EWLCJ176_2S_Reg_44	Configuring different Syslog facility for 9115 11ax AP in eWLC and checking the same in the APs	To configure different syslog facility for 9115 AP in eWLC AP join profile and validating the same in the AP	Passed	
EWLCJ176_2S_Reg_45	Packet capture of client when the client is connected to 9115/9120 AP with 2.4 GHz	To capture the Packet of the client when the client is connected to AP with radio as 2.4GHz	Passed	
EWLCJ176_2S_Reg_46	Verify details by connecting client to 2.4Ghz radio of 9105 AP.	To verify OFDMA details by connecting client to 2.4 Ghz radio.	Failed	CSCvy36282
EWLCJ176_2S_Reg_47	Verify details by connecting client to 5 Ghz radio of 9105 AP	To verify OFDMA details by connecting client to 5 Ghz radio.	Passed	
EWLCJ176_2S_Reg_48	Verify 9105AP MU-MIMO details with client connecting to WPA2 configured WLAN	To verify 11ax MU-MIMO details of 9105 AP with client connecting to WPA2 configured WLAN	Passed	

EWLCJ176_2S_Reg_49	Verify 9105AP MU-MIMO details with client connecting to WPA 3 configured WLAN	To verify 11ax MU-MIMO details of 9105 AP with client connecting to WPA 3 configured WLAN	Passed	

To share Client Delete reason code at AP to controller

Logical ID	Title	Description	Status	Defect ID
EWLCJ176S_CDR_1	Verify Client delete reason code for Webauth timer expiry when AP is in Local mode	LWA webauth timer expire	Passed	
EWLCJ176S_CDR_2	Verify Client delete reason code for Webauth timer expiry when AP is in Flex mode	LWA webauth timer expire	Passed	
EWLCJ176S_CDR_3	Verify Client delete reason code for Mac filtering	MAB authentication failed for Wireless client	Passed	
EWLCJ176S_CDR_4	Verify Client delete reason code for Mac filtering when AP is in Flex mode	MAB authentication failed for Wireless client	Passed	
EWLCJ176S_CDR_5	Verify Client delete reason code for Wrong PSK	To verify Client delete reason code for Wrong PSK	Passed	
EWLCJ176S_CDR_6	Verify Client delete reason code for Wrong PSK when AP is in Flex mode	To verify Client delete reason code for Wrong PSK	Passed	
EWLCJ176S_CDR_7	Verify Client delete reason code for dot1x timer expired	Deleting the client due to the expiry dot1x timer	Passed	
EWLCJ176S_CDR_8	Verify Client Manually Excluded with reason code	To verify Client Manually Excluded with reason code	Passed	
EWLCJ176S_CDR_9	Verify Client delete reason code for VLAN mismatch	To verify Client delete reason code for VLAN mismatch	Passed	
EWLCJ176S_CDR_10	Verify Android client delete reason code for dot1x authentication failure	Deleting the Android client due to the dot1x authentication failure	Passed	

EWLCJ176S_CDR_11	Verify Windows client delete reason code for dot1x authentication failure	Deleting the Windows client due to dot1x authentication failure	Passed	
EWLCJ176S_CDR_12	Verify IOS client delete reason code for dot1x authentication failure	Deleting the IOS client due to dot1x authentication failure	Passed	
EWLCJ176S_CDR_13	Verify Surface client delete reason code for dot1x authentication failure	Deleting the Surface client due to dot1x authentication failure	Passed	
EWLCJ176S_CDR_14	Verify client delete reason code for dot1x authentication failure when AP is in Flex mode	Deleting the client due to dot1x authentication failure	Passed	
EWLCJ176S_CDR_15	Verify syslog when client connected with run state	To verify syslog when client connected with run state	Passed	
EWLCJ176S_CDR_16	Verify Client delete reason code for IP learn state	To verify Client delete reason code for IP learn state	Passed	
EWLCJ176S_CDR_17	Checking the client delete reason when Client using wrong bssid while associating	To check the client delete reason when client using wrong BSSID while associating	Passed	
EWLCJ176S_CDR_18	Configure Roaming between controllers and verify client delete reason	To configure Roaming between controllers and verify client delete reason	Passed	
EWLCJ176S_CDR_19	Verify Client delete reason due to FT roaming failure	To verify Client delete reason due to FT roaming failure	Passed	
EWLCJ176S_CDR_20	Using DNAC verify Client delete reason WEBAUTH TIMER EXPIRED	Using DNAC, to verify Client delete reason WEBAUTH TIMER EXPIRED	Passed	
EWLCJ176S_CDR_21	Verify Client delete reason IPLEARN	Client failed to get IP within this period	Passed	

EWLCJ176S_CDR_22	Verify Client delete reason code for Wired LAN	Deleting the clients connected to a port	Passed	
EWLCJ176S_CDR_23	Verify Client delete reason code for Webauth timer expiry when AP is in Flex mode	LWA webauth timer expire	Passed	
EWCJ176S_CDR_1	Validate the client delete reason after changing AP mode	To validate the client delete reason after changing AP mode	Passed	
EWCJ176S_CDR_2	Checking the client delete reason when Client is disconnected in run State	To verify the client delete reason when client is disconnected in run state	Passed	
EWCJ176S_CDR_3	Checking the client delete reason when Client using wrong bssid while associating	To check the client delete reason when client using wrong BSSID while associating	Passed	
EWCJ176S_CDR_4	Checking the client delete reason after expire the webauth timer	To validate the client delete reason after expire the webauth timer	Passed	
EWCJ176S_CDR_5	Checking the client delete reason when AP moves from standalone mode to connected mode	To validate the client delete reason when AP moves from standalone mode to connected mode	Passed	
EWCJ176S_CDR_6	Validate the client delete reason after MAB authentication failed	To validate the client delete reason after MAB authentication failed	Passed	
EWCJ176S_CDR_7	Checking the client delete reason after expire dot1x timer	To check the client delete reason after expire dot1x timer	Passed	
EWCJ176S_CDR_8	Validate the client delete reason after client failed to get IP	To validate the client delete reason after client failed to get IP	Passed	CSCvx51493

EWCJ176S_CDR_9	Verifying the Android client delete reason after eap timer expires	To validate the Android client delete reason after eap timer expires	Passed	
EWCJ176S_CDR_10	Verifying the Windows client delete reason after eap timer expires	To validate the windows client delete reason after eap timer expires	Passed	
EWCJ176S_CDR_11	Validating the client delete reason when Authentication response rejected	To verify the client delete reason when Authentication response rejected	Passed	
EWCJ176S_CDR_12	Validating the client delete reason when Failing to send the Association response message to the wireless client	To validate the client delete reason when Failing to send the Association response message to the wireless client	Passed	CSCvx88559
EWCJ176S_CDR_13	Checking the client delete reason when Deleting client due to de-authentication	To Check the client delete reason when Deleting client due to de-authentication	Passed	
EWCJ176S_CDR_14	Verifying the Samsung S10 client delete reason after eap timer expires	To validate the Samsung S10 client delete reason after eap timer expires	Passed	
EWCJ176S_CDR_15	Verifying the iPhone client delete reason after eap timer expires	To validate the iPhone client delete reason after eap timer expires	Passed	
EWCJ176S_CDR_16	Verifying the Surface Go client delete reason after eap timer expires	To validate the Surface Go client delete reason after eap timer expires	Passed	
EWCJ176S_CDR_17	Verifying the IOS client delete reason after eap timer expires	To validate the IOS client delete reason after eap timer expires	Passed	
EWCJ176S_CDR_18	Verifying the Client delete reason due to FT roaming failure	To verify the Client delete reason due to FT roaming failure	Passed	
EWCJ176S_CDR_19	Verify alert triggered in Alarms & Events in PI	To verify alert triggered in Alarms & Events in PI	Passed	

EWCJ176S_CDR_20	Verify alert triggered for Webauth failure in Alarms & Events Prime Infra	To verify alert triggered for Webauth failure in Alarms & Events Prime Infra	Passed	
EWLCJ176_2S_Reg_50	Verify Client delete reason code for Webauth timer expiry when AP is in Local mode	LWA webauth timer expire	Passed	
EWLCJ176_2S_Reg_51	Verify Client delete reason code for Webauth timer expiry when AP is in Flex mode	LWA webauth timer expire	Passed	
EWLCJ176_2S_Reg_52	Verify Client delete reason code for Mac filtering	MAB authentication failed for Wireless client	Passed	
EWLCJ176_2S_Reg_53	Verify Client delete reason code for Mac filtering when AP is in Flex mode	MAB authentication failed for Wireless client	Passed	
EWLCJ176_2S_Reg_54	Verify Client delete reason code for Wrong PSK	To verify Client delete reason code for Wrong PSK	Passed	
EWLCJ176_2S_Reg_55	Verify Client delete reason code for Wrong PSK when AP is in Flex mode	To verify Client delete reason code for Wrong PSK	Passed	
EWLCJ176_2S_Reg_56	Verify Client delete reason code for dot1x timer expired	Deleting the client due to the expiry dot1x timer	Passed	
EWLCJ176_2S_Reg_57	Verify Client Manually Excluded with reason code	To verify Client Manually Excluded with reason code	Passed	
EWLCJ176_2S_Reg_58	Verify Client delete reason code for VLAN mismatch	To verify Client delete reason code for VLAN mismatch	Passed	
EWLCJ176_2S_Reg_59	Verify Android client delete reason code for dot1x authentication failure	Deleting the Android client due to the dot1x authentication failure	Passed	

EWLCJ176_2S_Reg_60	Verify Windows client delete reason code for dot1x authentication failure	Deleting the Windows client due to dot1x authentication failure	Passed	
EWLCJ176_2S_Reg_61	Verify IOS client delete reason code for dot1x authentication failure	Deleting the IOS client due to dot1x authentication failure	Passed	
EWLCJ176_2S_Reg_62	Verify Surface client delete reason code for dot1x authentication failure	Deleting the Surface client due to dot1x authentication failure	Passed	
EWLCJ176_2S_Reg_63	Verify client delete reason code for dot1x authentication failure when AP is in Flex mode	Deleting the client due to dot1x authentication failure	Passed	
EWLCJ176_2S_Reg_64	Verify syslog when client connected with run state	To verify syslog when client connected with run state	Passed	
EWLCJ176_2S_Reg_65	Verify Client delete reason code for IP learn state	To verify Client delete reason code for IP learn state	Passed	
EWLCJ176_2S_Reg_66	Checking the client delete reason when Client using wrong bssid while associating	To check the client delete reason when client using wrong BSSID while associating	Passed	
EWLCJ176_2S_Reg_67	Configure Roaming between controllers and verify client delete reason	To configure Roaming between controllers and verify client delete reason	Passed	
EWLCJ176_2S_Reg_68	Verify Client delete reason CO_CLIENT_ DELETE_REASON_MN_ AP_FLEX_FT_ FAILURE due to FT roaming failure	To verify Client delete reason due to FT roaming failure	Passed	

EWLCJ176_2S_Reg_69	Using DNAC verify Client delete reason CO_CLIENT_ DELETE_REASON_ MN_AP_CLSM_ WEBAUTH_TIMER_ EXPIRED	Using DNAC, to verify Client delete reason CO_CLIENT_ DELETE_REASON_ MN_AP_CLSM_ WEBAUTH_TIMER_ EXPIRED	Passed	
EWLCJ176_2S_Reg_70	Verify Client delete reason CO_CLIENT_ DELETE_ REASON_ MN_AP_IPLEARN_ TIMEOUT	Client failed to get IP within this period	Passed	
EWLCJ176_2S_Reg_71	Verify Client delete reason code for Wired LAN	Deleting the clients connected to a port	Passed	
EWCJ176_2S_Reg_1	Validate the client delete reason after changing AP mode	To validate the client delete reason after changing AP mode	Passed	
EWCJ176_2S_Reg_2	Checking the client delete reason when Client is disconnected in run State	To verify the client delete reason when client is disconnected in run state	Passed	
EWCJ176_2S_Reg_3	Checking the client delete reason when Client using wrong bssid while associating	To check the client delete reason when client using wrong BSSID while associating	Passed	
EWCJ176_2S_Reg_4	Checking the client delete reason after expire the webauth timer	To validate the client delete reason after expire the webauth timer	Passed	
EWCJ176_2S_Reg_5	Checking the client delete reason when AP moves from standalone mode to connected mode	To validate the client delete reason when AP moves from standalone mode to connected mode	Passed	
EWCJ176_2S_Reg_6	Validate the client delete reason after MAB authentication failed	To validate the client delete reason after MAB authentication failed	Passed	

EWCJ176_2S_Reg_7	Checking the client delete reason after expire dot1x timer	To check the client delete reason after expire dot1x timer	Passed	
EWCJ176_2S_Reg_8	Validate the client delete reason after client failed to get IP	To validate the client delete reason after client failed to get IP	Passed	
EWCJ176_2S_Reg_9	Verifying the Android client delete reason after eap timer expires	To validate the Android client delete reason after eap timer expires	Passed	
EWCJ176_2S_Reg_10	Verifying the Windows client delete reason after eap timer expires	To validate the windows client delete reason after eap timer expires	Passed	
EWCJ176_2S_Reg_11	Validating the client delete reason when Authentication response rejected	To verify the client delete reason when Authentication response rejected	Passed	
EWCJ176_2S_Reg_12	Validating the client delete reason when Failing to send the Association response message to the wireless client	To validate the client delete reason when Failing to send the Association response message to the wireless client	Passed	
EWCJ176_2S_Reg_13	Checking the client delete reason when Deleting client due to de-authentication	To Check the client delete reason when Deleting client due to de-authentication	Passed	
EWCJ176_2S_Reg_14	Verifying the Samsung S10 client delete reason after eap timer expires	To validate the Samsung S10 client delete reason after eap timer expires	Passed	
EWCJ176_2S_Reg_15	Verifying the iPhone client delete reason after eap timer expires	To validate the iPhone client delete reason after eap timer expires	Passed	
EWCJ176_2S_Reg_16	Verifying the Surface Go client delete reason after eap timer expires	To validate the Surface Go client delete reason after eap timer expires	Passed	

EWCJ176_2S_Reg_17	Verifying the IOS client delete reason after eap timer expires	To validate the IOS client delete reason after eap timer expires	Passed	
EWCJ176_2S_Reg_18	Verifying the Client delete reason due to FT roaming failure	To verify the Client delete reason due to FT roaming failure	Passed	
EWCJ176_2S_Reg_19	Verify alert triggered in Alarms & Events in PI	To verify alert triggered in Alarms & Events in PI	Passed	
EWCJ176_2S_Reg_20	Verify alert triggered for Webauth failure in Alarms & Events Prime Infra	To verify alert triggered for Webauth failure in Alarms & Events Prime Infra	Passed	

4800: 3rd Radio in Monitor Mode (IOS-XE)

Logical ID	Title	Description	Status	Defect ID
EWLCJ176S_4800_1	Check if AP profile configuration is done and pushed to AP from controller	To check if AP profile configuration is done and pushed to AP from controller	Passed	
EWLCJ176S_4800_2	Verify operation with AP mode as local and sub mode as AWIPS	To verify operation with AP mode as local and sub mode as AWIPS	Passed	CSCvx65392
EWLCJ176S_4800_3	Verify operation with AP mode as flex and sub mode as AWIPS	To verify operation with AP mode as flex and sub mode as AWIPS	Passed	
EWLCJ176S_4800_4	Verify operation with AP mode as local/flex and sub mode as none	To verify operation with AP mode as local/flex and sub mode as none	Passed	
EWLCJ176S_4800_5	Verify operation with AP mode as local and different combinations of slot sub modes	To verify operation with AP mode as local and different combinations of slot sub modes	Passed	
EWLCJ176S_4800_6	Verify operation with AP mode as local and different combinations of slot sub modes	To verify operation with AP mode as local and different combinations of slot sub modes	Passed	
EWLCJ176S_4800_7	Verify operation with AP mode as monitor and different combinations of slot sub modes	To verify operation with AP mode as monitor and different combinations of slot sub modes	Passed	
EWLCJ176S_4800_8	Connect client with each combination of AP mode/sub mode and monitor the status	To connect client with each combination of AP mode/sub mode and monitor the status	Passed	

EWLCJ176S_4800_9	Connect android client with each combination of AP mode/sub mode and monitor the status	To connect android client with each combination of AP mode/sub mode and monitor the status	Passed	
EWLCJ176S_4800_10	Connect MAC client with each combination of AP mode/sub mode and monitor the status	To connect MAC client with each combination of AP mode/sub mode and monitor the status	Passed	
EWLCJ176S_4800_11	Connect Surface client with each combination of AP mode/sub mode and monitor the status	To connect Surface client with each combination of AP mode/sub mode and monitor the status	Passed	
EWLCJ176S_4800_12	Verify catalyst 9120 AP operation with AP mode as local/flex/monitor and different combinations of slot sub modes	Verify catalyst 9120 AP operation with AP mode as local/flex/monitor and different combinations of slot sub modes	Passed	
EWLCJ176S_4800_13	Verify catalyst 9130 AP operation with AP mode as local/flex/monitor and different combinations of slot sub modes	Verify catalyst 9130 AP operation with AP mode as local/flex/monitor and different combinations of slot sub modes	Passed	CSCvx86103
EWLCJ176S_4800_14	Verify catalyst 9105 AP operation with AP mode as local/flex/monitor and different combinations of slot sub modes	Verify catalyst 9105 AP operation with AP mode as local/flex/monitor and different combinations of slot sub modes	Passed	
EWLCJ176S_4800_15	Verify EWC Internal AP operation with AP mode as local/flex/monitor and different combinations of slot sub modes	Verify EWC Internal AP operation with AP mode as local/flex/monitor and different combinations of slot sub modes	Passed	

EWLCJ176S_4800_16	Verify EWC & 4800 AP operation with AP mode as local/flex/monitor and different combinations of slot sub modes	Verify EWC & 4800 AP operation with AP mode as local/flex/monitor and different combinations of slot sub modes	Passed	
EWLCJ176S_4800_17	Verify EWC & 9100 AP operation with AP mode as local/flex/monitor and different combinations of slot sub modes	Verify EWC & 9100 AP operation with AP mode as local/flex/monitor and different combinations of slot sub modes	Passed	
EWLCJ176S_4800_18	Verify 4800 operation with DNAC & AP mode as local and sub mode as AWIPS	To verify 4800 operation with DNAC & AP mode as local and sub mode as AWIPS	Passed	
EWLCJ176S_4800_19	Verify 9105 operation with DNAC & AP mode as local and sub mode as AWIPS	To verify 9105 operation with DNAC & AP mode as local and sub mode as AWIPS	Passed	
EWLCJ176S_4800_20	Verify 9120 operation with DNAC & AP mode as local and sub mode as AWIPS	To verify 9120 operation with DNAC & AP mode as local and sub mode as AWIPS	Passed	
EWLCJ176S_4800_21	Verify 9130 operation with DNAC & AP mode as local and sub mode as AWIPS	To verify 9130 operation with DNAC & AP mode as local and sub mode as AWIPS	Passed	
EWLCJ176S_4800_22	Import maps to PI and check if AP details are shown in the dashboard analytics	To import maps to PI and check if AP details are shown in the dashboard analytics	Passed	
EWLCJ176_2S_Reg_72	Check if AP profile configuration is done and pushed to AP from controller	To check if AP profile configuration is done and pushed to AP from controller	Passed	

EWLCJ176_2S_Reg_73	Verify operation with AP mode as local and submode as AWIPS	To verify operation with AP mode as local and submode as AWIPS	Passed	
EWLCJ176_2S_Reg_74	Verify operation with AP mode as flex and submode as AWIPS	To verify operation with AP mode as flex and submode as AWIPS	Passed	
EWLCJ176_2S_Reg_75	Verify operation with AP mode as local/flex and submode as none	To verify operation with AP mode as local/flex and submode as none	Passed	
EWLCJ176_2S_Reg_76	Verify operation with AP mode as local and different combinations of slot submodes	To verify operation with AP mode as local and different combinations of slot submodes	Passed	
EWLCJ176_2S_Reg_77	Verify operation with AP mode as local and different combinations of slot submodes	To verify operation with AP mode as local and different combinations of slot submodes	Passed	
EWLCJ176_2S_Reg_78	Verify operation with AP mode as monitor and different combinations of slot submodes	To verify operation with AP mode as monitor and different combinations of slot submodes	Passed	
EWLCJ176_2S_Reg_79	Connect client with each combination of AP mode/submode and monitor the status	To connect client with each combination of AP mode/submode and monitor the status	Passed	
EWLCJ176_2S_Reg_80	Connect android client with each combination of AP mode/submode and monitor the status	To connect android client with each combination of AP mode/submode and monitor the status	Passed	
EWLCJ176_2S_Reg_81	Connect MAC client with each combination of AP mode/submode and monitor the status	To connect MAC client with each combination of AP mode/submode and monitor the status	Passed	

EWLCJ176_2S_Reg_82	Connect Surface client with each combination of AP mode/submode and monitor the status	To connect Surface client with each combination of AP mode/submode and monitor the status	Passed	
EWLCJ176_2S_Reg_83	Verify catalyst 9120 AP operation with AP mode as local/flex/monitor and different combinations of slot submodes	Verify catalyst 9120 AP operation with AP mode as local/flex/monitor and different combinations of slot submodes	Passed	
EWLCJ176_2S_Reg_84	Verify catalyst 9130 AP operation with AP mode as local/flex/monitor and different combinations of slot submodes	Verify catalyst 9130 AP operation with AP mode as local/flex/monitor and different combinations of slot submodes	Passed	
EWLCJ176_2S_Reg_85	Verify catalyst 9105 AP operation with AP mode as local/flex/monitor and different combinations of slot submodes	Verify catalyst 9105 AP operation with AP mode as local/flex/monitor and different combinations of slot submodes	Passed	
EWLCJ176_2S_Reg_86	Verify EWC Internal AP operation with AP mode as local/flex/monitor and different combinations of slot submodes	Verify EWC Internal AP operation with AP mode as local/flex/monitor and different combinations of slot submodes	Passed	
EWLCJ176_2S_Reg_87	Verify EWC & 4800 AP operation with AP mode as local/flex/monitor and different combinations of slot submodes	Verify EWC & 4800 AP operation with AP mode as local/flex/monitor and different combinations of slot submodes	Passed	
EWLCJ176_2S_Reg_88	Verify EWC & 9100 AP operation with AP mode as local/flex/monitor and different combinations of slot submodes	Verify EWC & 9100 AP operation with AP mode as local/flex/monitor and different combinations of slot submodes	Passed	

SSID per radio on Dual 5G

Logical ID	Title	Description	Status	Defect ID
EWLCJ176S_SSID5G_1	Associate client to 5 GHz radio policy with slot 0	To verify slot details shown or not	Passed	
EWLCJ176S_SSID5G_2	Associate client to 5 GHz radio policy with slot 1	To verify slot details shown or not	Passed	
EWLCJ176S_SSID5G_3	Associate client to 5 GHz radio policy with slot 2	To verify slot details shown or not	Passed	
EWLCJ176S_SSID5G_4	Creating WLAN with 6 GHz radio policy	To Validate client details with 6 GHz radio	Passed	
EWLCJ176S_SSID5G_5	Associating windows client to 9115 Ap with WPA2 security type for 2.4GHz radio policy	To Verify Windows client associate to 2.4 GHz radio with WPA2 security type or not	Passed	
EWLCJ176S_SSID5G_6	Associating Android client to 9120 Ap with WPA2 security type for 5GHz radio policy	To Verify android client associate to 5 GHz radio with WPA2 security type or not	Passed	
EWLCJ176S_SSID5G_7	Associating iOS client to 9130 Ap with WPA2 security type for 6GHz radio policy	To Verify iOS client associate to 6 GHz radio with WPA2 security type or not	Passed	
EWLCJ176S_SSID5G_8	Associating Mac client to 9105 Ap with WPA3 security type for 2.4GHz radio policy	To Verify mac client associate to 2.4 GHz radio with WPA3 security type or not	Passed	
EWLCJ176S_SSID5G_9	Associating Ms-go client to 9115 Ap with WPA3 security type for 5GHz radio policy	To associate the client and verifying EDCA parameter	Passed	

EWLCJ176S_SSID5G_10	Associating MS-GO2 client to 9120 Ap with WPA3 + AES cipher + OWE AKM security type for 6GHz radio policy	To Verify MS-GO2 client associate to 6 GHz radio with WPA3 + AES cipher + OWE AKM security type or not	Passed	
EWLCJ176S_SSID5G_11	Associating client with WPA3 + AES cipher + 802.1x-SHA256 AKM security type for 6GHz radio policy	To Verify Windows client associate to 6 GHz radio with WPA3 security type or not	Passed	
EWLCJ176S_SSID5G_12	Associating client with WPA3 + AES cipher + SAE AKM security type for 6GHz radio policy	To Verify client associate to 6 GHz radio with WPA3 + AES cipher + SAE AKM security type or not	Passed	
EWLCJ176S_SSID5G_13	Associating client with WPA3 + CCMP256 cipher + SUITEB192-1X AKM security type for 6GHz radio policy	To Verify client associate to 6 GHz radio with WPA3 + CCMP256 cipher + SUITEB192-1X AKM security type or not	Passed	
EWLCJ176S_SSID5G_14	Associating client with WPA3 + GCMP256 cipher + SUITEB-1X AKM security type for 6GHz radio policy	To Verify client associate to 6 GHz radio with WPA3 + GCMP256 cipher + SUITEB-1X AKM security type or not	Passed	
EWLCJ176S_SSID5G_15	Associating client with WPA3 + GCMP128 cipher + SUITEB192-1X AKM security type for 6GHz radio policy	To Verify client associate to 6 GHz radio with WPA3 + GCMP128 cipher + SUITEB192-1X AKM security type or not	Passed	
EWLCJ176S_SSID5G_16	Associating client with WPA3 + adaptive WPA2 security type for 6GHz radio policy	To Verify client associate to 6 GHz radio with WPA3 + adaptive WPA2 security type or not	Passed	

EWLCJ176S_SSID5G_17	Perform inter roaming across different radio policy	To verify radio policy details after inter roaming	Passed	
EWLCJ176S_SSID5G_18	Perform intra roaming across different radio policy	To verify radio policy details after intra roaming	Passed	
EWLCJ176S_SSID5G_19	Perform IRCM across different radio policy	To verify radio policy details after IRCM	Passed	
EWLCJ176S_SSID5G_20	Validate radio policy details in PI	To verify radio policy details after config pushed to PI	Passed	
EWLCJ176S_SSID5G_21	Validate 2.4 GHz radio policy details in DNAC	To verify 2.4 GHz radio policy details after config pushed to DNAC	Passed	
EWLCJ176S_SSID5G_22	Validate 5 GHz radio policy details in DNAC	To verify 5 GHz radio policy details after config pushed to DNAC	Passed	
EWLCJ176S_SSID5G_23	Validate 6 GHz radio policy details in DNAC	To verify 6 GHz radio policy details after config pushed to DNAC	Passed	
EWLCJ176S_SSID5G_24	Validate stots of radio policy in CMX	To verify 5 GHz radio slots difference in CMX	Passed	
EWLCJ176S_SSID5G_25	Limit the client by radio policy	To verify the no of client associate with particular radio policy	Passed	
EWLCJ176_2S_Reg_89	Associate client to 5 GHz radio policy with slot 0	To verify slot details shown or not	Passed	
EWLCJ176_2S_Reg_90	Associate client to 5 GHz radio policy with slot 1	To verify slot details shown or not	Passed	
EWLCJ176_2S_Reg_91	Associate client to 5 GHz radio policy with slot 2	To verify slot details shown or not	Passed	

EWLCJ176_2S_Reg_92	Creating WLAN with 6 GHz radio policy	To Validate client details with 6 GHz radio	Passed	
EWLCJ176_2S_Reg_93	Associating windows client to 9115 Ap with WPA2 security type for 2.4GHz radio policy	To Verify Windows client associate to 2.4 GHz radio with WPA2 security type or not	Passed	
EWLCJ176_2S_Reg_94	Associating Android client to 9120 Ap with WPA2 security type for 5GHz radio policy	To Verify android client associate to 5 GHz radio with WPA2 security type or not	Passed	
EWLCJ176_2S_Reg_95	Associating iOS client to 9130 Ap with WPA2 security type for 6GHz radio policy	To Verify iOS client associate to 6 GHz radio with WPA2 security type or not	Passed	
EWLCJ176_2S_Reg_96	Associating Mac client to 9105 Ap with WPA3 security type for 2.4GHz radio policy	To Verify mac client associate to 2.4 GHz radio with WPA3 security type or not	Passed	
EWLCJ176_2S_Reg_97	Associating Ms-go client to 9115 Ap with WPA3 security type for 5GHz radio policy	To associate the client and verifying EDCA parameter	Passed	
EWLCJ176_2S_Reg_98	Associating MS-GO2 client to 9120 Ap with WPA3 + AES cipher + OWE AKM security type for 6GHz radio policy	To Verify MS-GO2 client associate to 6 GHz radio with WPA3 + AES cipher + OWE AKM security type or not	Passed	
EWLCJ176_2S_Reg_99	Associating client with WPA3 + AES cipher + 802.1x-SHA256 AKM security type for 6GHz radio policy	To Verify Windows client associate to 6 GHz radio with WPA3 security type or not	Passed	

EWLCJ176_2S_Reg_100	Associating client with WPA3 + AES cipher + SAE AKM security type for 6GHz radio policy	To Verify client associate to 6 GHz radio with WPA3 + AES cipher + SAE AKM security type or not	Passed	
EWLCJ176_2S_Reg_101	Associating client with WPA3 + CCMP256 cipher + SUITEB192-1X AKM security type for 6GHz radio policy	To Verify client associate to 6 GHz radio with WPA3 + CCMP256 cipher + SUITEB192-1X AKM security type or not	Passed	
EWLCJ176_2S_Reg_102	Associating client with WPA3 + GCMP256 cipher + SUITEB-1X AKM security type for 6GHz radio policy	To Verify client associate to 6 GHz radio with WPA3 + GCMP256 cipher + SUITEB-1X AKM security type or not	Passed	
EWLCJ176_2S_Reg_103	Associating client with WPA3 + GCMP128 cipher + SUITEB192-1X AKM security type for 6GHz radio policy	To Verify client associate to 6 GHz radio with WPA3 + GCMP128 cipher + SUITEB192-1X AKM security type or not	Passed	
EWLCJ176_2S_Reg_104	Associating client with WPA3 + adaptive WPA2 security type for 6GHz radio policy	To Verify client associate to 6 GHz radio with WPA3 + adaptive WPA2 security type or not	Passed	
EWLCJ176_2S_Reg_105	Perform inter roaming across different radio policy	To verify radio policy details after inter roaming	Passed	
EWLCJ176_2S_Reg_106	Perform intra roaming across different radio policy	To verify radio policy details after intra roaming	Passed	
EWLCJ176_2S_Reg_107	Perform IRCM across different radio policy	To verify radio policy details after IRCM	Passed	
EWLCJ176_2S_Reg_108	Validate radio policy details in PI	To verify radio policy details after config pushed to PI	Passed	

EWLCJ176_2S_Reg_109	Validate 2.4 GHz radio policy details in DNAC	To verify 2.4 GHz radio policy details after config pushed to DNAC	Passed	
EWLCJ176_2S_Reg_110	Validate 5 GHz radio policy details in DNAC	To verify 5 GHz radio policy details after config pushed to DNAC	Passed	
EWLCJ176_2S_Reg_111	Validate 6 GHz radio policy details in DNAC	To verify 6 GHz radio policy details after config pushed to DNAC	Passed	
EWLCJ176_2S_Reg_112	Validate stots of radio policy in CMX	To verify 5 GHz radio slots difference in CMX	Passed	
EWLCJ176_2S_Reg_113	Limit the client by radio policy	To verify the no of client associate with particular radio policy	Passed	
EWCJ176_2S_Reg_387	Associate client to 5 GHz radio policy with slot 0	To verify slot details shown or not	Passed	
EWCJ176_2S_Reg_388	Associate client to 5 GHz radio policy with slot 1	To verify slot details shown or not	Passed	
EWCJ176_2S_Reg_389	Associate client to 5 GHz radio policy with slot 2	To verify slot details shown or not	Passed	
EWCJ176_2S_Reg_390	Creating WLAN with 6 GHz radio policy	To Validate client details with 6 GHz radio	Passed	
EWCJ176_2S_Reg_391	Associating windows client to 9115 Ap with WPA2 security type for 2.4GHz radio policy	To Verify Windows client associate to 2.4 GHz radio with WPA2 security type or not	Passed	
EWCJ176_2S_Reg_392	Associating Android client to 9120 Ap with WPA2 security type for 5GHz radio policy	To Verify android client associate to 5 GHz radio with WPA2 security type or not	Passed	

EWCJ176_2S_Reg_393	Associating iOS client to 9130 Ap with WPA2 security type for 6GHz radio policy	To Verify iOS client associate to 6 GHz radio with WPA2 security type or not	Passed	
EWCJ176_2S_Reg_394	Associating Mac client to 9105 Ap with WPA3 security type for 2.4GHz radio policy	To Verify mac client associate to 2.4 GHz radio with WPA3 security type or not	Passed	
EWCJ176_2S_Reg_395	Associating Ms-go client to 9115 Ap with WPA3 security type for 5GHz radio policy	To associate the client and verifying EDCA parameter	Passed	
EWCJ176_2S_Reg_396	Associating MS-GO2 client to 9120 Ap with WPA3 + AES cipher + OWE AKM security type for 6GHz radio policy	To Verify MS-GO2 client associate to 6 GHz radio with WPA3 + AES cipher + OWE AKM security type or not	Passed	
EWCJ176_2S_Reg_397	Associating client with WPA3 + AES cipher + 802.1x-SHA256 AKM security type for 6GHz radio policy	To Verify Windows client associate to 6 GHz radio with WPA3 security type or not	Passed	
EWCJ176_2S_Reg_398	Associating client with WPA3 + AES cipher + SAE AKM security type for 6GHz radio policy	To Verify client associate to 6 GHz radio with WPA3 + AES cipher + SAE AKM security type or not	Passed	
EWCJ176_2S_Reg_399	Associating client with WPA3 + CCMP256 cipher + SUITEB192-1X AKM security type for 6GHz radio policy	To Verify client associate to 6 GHz radio with WPA3 + CCMP256 cipher + SUITEB192-1X AKM security type or not	Passed	

EWCJ176_2S_Reg_400	Associating client with WPA3 + GCMP256 cipher + SUITEB-1X AKM security type for 6GHz radio policy	To Verify client associate to 6 GHz radio with WPA3 + GCMP256 cipher + SUITEB-1X AKM security type or not	Passed	
EWCJ176_2S_Reg_401	Associating client with WPA3 + GCMP128 cipher + SUITEB192-1X AKM security type for 6GHz radio policy	To Verify client associate to 6 GHz radio with WPA3 + GCMP128 cipher + SUITEB192-1X AKM security type or not	Passed	
EWCJ176_2S_Reg_402	Associating client with WPA3 + adaptive WPA2 security type for 6GHz radio policy	To Verify client associate to 6 GHz radio with WPA3 + adaptive WPA2 security type or not	Passed	
EWCJ176_2S_Reg_403	Perform inter roaming across different radio policy	To verify radio policy details after inter roaming	Passed	
EWCJ176_2S_Reg_404	Perform intra roaming across different radio policy	To verify radio policy details after intra roaming	Passed	
EWCJ176_2S_Reg_405	Perform IRCM across different radio policy	To verify radio policy details after IRCM	Passed	
EWCJ176_2S_Reg_406	Validate radio policy details in PI	To verify radio policy details after config pushed to PI	Passed	
EWCJ176_2S_Reg_407	Validate 2.4 GHz radio policy details in DNAC	To verify 2.4 GHz radio policy details after config pushed to DNAC	Passed	
EWCJ176_2S_Reg_408	Validate 5 GHz radio policy details in DNAC	To verify 5 GHz radio policy details after config pushed to DNAC	Passed	
EWCJ176_2S_Reg_409	Validate 6 GHz radio policy details in DNAC	To verify 6 GHz radio policy details after config pushed to DNAC	Passed	

EWCJ176_2S_Reg_410	Validate stots of radio policy in CMX	To verify 5 GHz radio slots difference in CMX	Passed	
EWCJ176_2S_Reg_411	Limit the client by radio policy	To verify the no of client associate with particular radio policy	Passed	

Per AP Group NTP Server Config

Logical ID	Title	Description	Status	Defect ID
EWLCJ176S_APNTP_1	Configure AP Group NTP Server in CMX and verify NTP status in Console	To configure AP Group NTP Server in CMX and verify NTP status in Console	Passed	
EWLCJ176S_APNTP_2	Remove NTP Server from CMX and verify NTP status in Console	To remove NTP Server from CMX and verify NTP status in Console	Passed	
EWLCJ176S_APNTP_3	Add NTP IPv4/IPV6 address for AP profile through CLI and verify TLV logs	To add NTP IPv4/IPV6 address for AP profile through CLI and verify TLV logs	Passed	CSCvx44081
EWLCJ176S_APNTP_4	Remove NTP IPv4/IPV6 address for AP profile through CLI and verify TLV logs	To remove NTP IPv4/IPV6 address for AP profile through CLI and verify TLV logs	Passed	
EWLCJ176S_APNTP_5	Verify whether AP is getting ntpd is up and running or not after configuring NTP IPV4/IPV6 address through GUI	To verify whether AP is getting ntpd is up and running or not after configuring NTP IPV4/IPV6 address through GUI	Passed	
EWLCJ176S_APNTP_6	Verify whether AP is getting ntpd is not running or not after removing NTP IPV4/IPV6 address through GUI	To verify whether AP is getting ntpd is not running or not after removing NTP IPV4/IPV6 address through GUI	Passed	
EWLCJ176S_APNTP_7	Modify AP Time zone using Controller	To modify AP Time zone using Controller	Passed	
EWLCJ176S_APNTP_8	Check warning message when Hyper location enabled, but NTP server is not configured	To check warning message when Hyper location enabled, but NTP server is not configured	Passed	

EWLCJ176S_APNTP_9	Check memory leaks after configuring NTP Server and Authentication Key through CLI	To check memory leaks after configuring NTP Server and Authentication Key	Passed	
EWLCJ176S_APNTP_10	Check memory leaks after configuring NTP Server and Authentication Key through GUI	To check memory leaks after configuring NTP Server and Authentication Key	Passed	
EWLCJ176S_APNTP_11	Configure Authentication key in CLI and remove configured key through GUI	To configure Authentication key in CLI and to remove configured key through GUI	Passed	
EWLCJ176S_APNTP_12	Verify whether 9105 AP is getting ntpd is up and running or not after configuring NTP IPV4/IPV6 address	To verify whether 9105 AP is getting ntpd is up and running or not after configuring NTP IPV4/IPV6 address	Passed	
EWLCJ176S_APNTP_13	Verify whether 9115 AP is getting ntpd is up and running or not after configuring NTP IPV4/IPV6 address	To verify whether 9115 AP is getting ntpd is up and running or not after configuring NTP IPV4/IPV6 address	Passed	
EWLCJ176S_APNTP_14	Verify whether 9120 AP is getting ntpd is up and running or not after configuring NTP IPV4/IPV6 address	To verify whether 9120 AP is getting ntpd is up and running or not after configuring NTP IPV4/IPV6 address	Passed	
EWLCJ176S_APNTP_15	Connect multiple Aps and check ntpd is up and running or not after configuring NTP IPV4/IPV6 address in AP Join page	To connect multiple Aps and check ntpd is up and running or not after configuring NTP IPV4/IPV6 address in AP Join page	Passed	

EWLCJ176S_APNTP_16	Configure Authentication key through Best Practices and check whether AP is getting ntpd is up and running or not	To configure Authentication key through Best Practices and check whether AP is getting ntpd is up and running or not	Passed	
EWLCJ176S_APNTP_17	Check UI is getting error message or not if trusted-key is invalid	To check UI is getting error message or not if trusted-key is invalid	Passed	
EWLCJ176S_APNTP_18	Check any errors messages triggered or not after configuring trusted key	To check any errors messages triggered or not after configuring trusted key	Passed	
EWLCJ176S_APNTP_19	Configure 9103 AP Group NTP Server in CMX and verify NTP status in Console	To configure 9103 AP Group NTP Server in CMX and verify NTP status in Console	Passed	
EWLCJ176_2S_Reg_114	Configure AP Group NTP Server in CMX and verify NTP status in Console	To configure AP Group NTP Server in CMX and verify NTP status in Console	Passed	
EWLCJ176_2S_Reg_115	Remove NTP Server from CMX and verify NTP status in Console	To remove NTP Server from CMX and verify NTP status in Console	Passed	
EWLCJ176_2S_Reg_116	Add NTP IPv4/IPV6 address for AP profile through CLI and verify TLV logs	To add NTP IPv4/IPV6 address for AP profile through CLI and verify TLV logs	Passed	
EWLCJ176_2S_Reg_117	Remove NTP IPv4/IPV6 address for AP profile through CLI and verify TLV logs	To remove NTP IPv4/IPV6 address for AP profile through CLI and verify TLV logs	Passed	

EWLCJ176_2S_Reg_118	Verify whether AP is getting ntp is up and running or not after configuring NTP IPV4/IPV6 address through GUI	To verify whether AP is getting ntp is up and running or not after configuring NTP IPV4/IPV6 address through GUI	Passed	
EWLCJ176_2S_Reg_119	Verify whether AP is getting ntp is not running or not after removing NTP IPV4/IPV6 address through GUI	To verify whether AP is getting ntp is not running or not after removing NTP IPV4/IPV6 address through GUI	Passed	
EWLCJ176_2S_Reg_120	Modify AP Time zone using Controller	To modify AP Time zone using Controller	Passed	
EWLCJ176_2S_Reg_121	Check warning message when Hyper location enabled, but NTP server is not configured	To check warning message when Hyper location enabled, but NTP server is not configured	Passed	
EWLCJ176_2S_Reg_122	Check memory leaks after configuring NTP Server and Authentication Key through CLI	To check memory leaks after configuring NTP Server and Authentication Key	Passed	
EWLCJ176_2S_Reg_123	Check memory leaks after configuring NTP Server and Authentication Key through GUI	To check memory leaks after configuring NTP Server and Authentication Key	Passed	
EWLCJ176_2S_Reg_124	Configure Authentication key in CLI and remove configured key through GUI	To configure Authentication key in CLI and to remove configured key through GUI	Passed	
EWLCJ176_2S_Reg_125	Verify whether 9105 AP is getting ntp is up and running or not after configuring NTP IPV4/IPV6 address	To verify whether 9105 AP is getting ntp is up and running or not after configuring NTP IPV4/IPV6 address	Passed	

EWLCJ176_2S_Reg_126	Verify whether 9115 AP is getting ntp is up and running or not after configuring NTP IPV4/IPV6 address	To verify whether 9115 AP is getting ntp is up and running or not after configuring NTP IPV4/IPV6 address	Passed	
EWLCJ176_2S_Reg_127	Verify whether 9120 AP is getting ntp is up and running or not after configuring NTP IPV4/IPV6 address	To verify whether 9120 AP is getting ntp is up and running or not after configuring NTP IPV4/IPV6 address	Passed	
EWLCJ176_2S_Reg_128	Connect multiple Aps and check ntp is up and running or not after configuring NTP IPV4/IPV6 address in AP Join page	To connect multiple Aps and check ntp is up and running or not after configuring NTP IPV4/IPV6 address in AP Join page	Passed	
EWLCJ176_2S_Reg_129	Configure Authentication key through Best Practices and check whether AP is getting ntp is up and running or not	To configure Authentication key through Best Practices and check whether AP is getting ntp is up and running or not	Passed	
EWLCJ176_2S_Reg_130	Check UI is getting error message or not if trusted-key is invalid	To check UI is getting error message or not if trusted-key is invalid	Passed	
EWLCJ176_2S_Reg_131	Check any errors messages triggered or not after configuring trusted key	To check any errors messages triggered or not after configuring trusted key	Passed	
EWLCJ176_2S_Reg_132	Configure 9103 AP Group NTP Server in CMX and verify NTP status in Console	To configure 9103 AP Group NTP Server in CMX and verify NTP status in Console	Passed	

Adapative Load EDCA Parameter(Giga School)

Logical ID	Title	Description	Status	Defect ID
EWLCJ176S_EDCA_1	Validate the EDCA parameter with wmm-default profile	To associate the client and verifying EDCA parameter in wmm-default profile	Passed	
EWLCJ176S_EDCA_2	Validate the EDCA parameter with custom-voice profile	To associate the client and verifying EDCA parameter in custom-voice profile	Passed	
EWLCJ176S_EDCA_3	Validate the EDCA parameter with optimized-video-voice profile	To associate the client and verifying EDCA parameter in optimized-video-voice profile	Passed	
EWLCJ176S_EDCA_4	Validate the EDCA parameter with optimized-voice profile	To associate the client and verifying EDCA parameter in optimized-voice profile	Passed	
EWLCJ176S_EDCA_5	Validate the EDCA parameter with svp-voice profile	To associate the client and verifying EDCA parameter in svp-voice profile	Passed	
EWLCJ176S_EDCA_6	Validate the EDCA parameter with Fastlane profile	To associate the client and verifying EDCA parameter in Fastlane profile	Passed	
EWLCJ176S_EDCA_7	Associate the windows client and verify the EDCA parameter in 9120 AP	To associate the client and verifying EDCA parameter	Passed	
EWLCJ176S_EDCA_8	Associate the Android client and verify the EDCA parameter in 9130 AP	To associate the client and verifying EDCA parameter	Passed	

EWLCJ176S_EDCA_9	Associate the MAC client and verify the EDCA parameter in 9120 AP	To associate the client and verifying EDCA parameter	Passed	
EWLCJ176S_EDCA_10	Validate the EDCA parameter with different profile in 2.4GHz frequency	To associate the client and verifying EDCA parameter for 2.4GHZ frequency	Passed	
EWLCJ176S_EDCA_11	Validate the EDCA parameter with different profile in 6GHz frequency	To associate the client and verifying EDCA parameter for 6GHZ frequency	Passed	
EWLCJ176S_EDCA_12	Validate the EDCA parameter with different profile in 5GHz frequency	To associate the client and verifying EDCA parameter for 5GHZ frequency	Passed	
EWLCJ176S_EDCA_13	Validate the EDCA parameter with single client	To associate the client and verifying EDCA parameter.	Passed	
EWLCJ176S_EDCA_14	Perform Inter roaming and validate the load balancing	To associate the client and verifying EDCA parameter for 5GHZ frequency	Passed	
EWLCJ176S_EDCA_15	Perform Intra roaming and validate the load balancing	To associate the client and verifying EDCA parameter for 5GHZ frequency	Passed	
EWLCJ176S_EDCA_16	Perform controller reload and validate the load balancing	To associate the client and verifying EDCA parameter for 5GHZ frequency	Passed	
EWLCJ176S_EDCA_17	Associate the MS-GO client with SSID and validate the EDCA parameter	To associate the client and verifying EDCA parameter.	Passed	
EWLCJ176S_EDCA_18	Associate the MS-GO2 client with SSID and validate the EDCA parameter	To associate the client and verifying EDCA parameter.	Passed	

EWLCJ176_2S_Reg_345	Validate the EDCA parameter with wmm-default profile	To associate the client and verifying EDCA parameter in wmm-default profile	Passed	
EWLCJ176_2S_Reg_346	Validate the EDCA parameter with custom-voice profile	To associate the client and verifying EDCA parameter in custom-voice profile	Passed	
EWLCJ176_2S_Reg_347	Validate the EDCA parameter with optimized-video-voice profile	To associate the client and verifying EDCA parameter in optimized-video-voice profile	Passed	
EWLCJ176_2S_Reg_348	Validate the EDCA parameter with optimized-voice profile	To associate the client and verifying EDCA parameter in optimized-voice profile	Passed	
EWLCJ176_2S_Reg_349	Validate the EDCA parameter with svp-voice profile	To associate the client and verifying EDCA parameter in svp-voice profile	Passed	
EWLCJ176_2S_Reg_350	Validate the EDCA parameter with Fastlane profile	To associate the client and verifying EDCA parameter in Fastlane profile	Passed	
EWLCJ176_2S_Reg_351	Associate the windows client and verify the EDCA parameter in 9120 AP	To associate the client and verifying EDCA parameter	Passed	
EWLCJ176_2S_Reg_352	Associate the Android client and verify the EDCA parameter in 9130 AP	To associate the client and verifying EDCA parameter	Passed	
EWLCJ176_2S_Reg_353	Associate the MAC client and verify the EDCA parameter in 9120 AP	To associate the client and verifying EDCA parameter	Passed	

EWLCJ176_2S_Reg_354	Validate the EDCA parameter with different profile in 2.4GHz frequency	To associate the client and verifying EDCA parameter for 2.4GHZ frequency	Passed	
EWLCJ176_2S_Reg_355	Validate the EDCA parameter with different profile in 6GHz frequency	To associate the client and verifying EDCA parameter for 6GHZ frequency	Passed	
EWLCJ176_2S_Reg_356	Validate the EDCA parameter with different profile in 5GHz frequency	To associate the client and verifying EDCA parameter for 5GHZ frequency	Passed	
EWLCJ176_2S_Reg_357	Validate the EDCA parameter with single client	To associate the client and verifying EDCA parameter.	Passed	
EWLCJ176_2S_Reg_358	Perform Inter roaming and validate the load balancing	To associate the client and verifying EDCA parameter for 5GHZ frequency	Passed	
EWLCJ176_2S_Reg_359	Perform Intra roaming and validate the load balancing	To associate the client and verifying EDCA parameter for 5GHZ frequency	Passed	
EWLCJ176_2S_Reg_360	Perform controller reload and validate the load balancing	To associate the client and verifying EDCA parameter for 5GHZ frequency	Passed	
EWLCJ176_2S_Reg_361	Associate the MS-GO client with SSID and validate the EDCA parameter	To associate the client and verifying EDCA parameter.	Passed	
EWLCJ176_2S_Reg_362	Associate the MS-GO2 client with SSID and validate the EDCA parameter	To associate the client and verifying EDCA parameter.	Passed	

Regulatory Domain Reduction

Logical ID	Title	Description	Status	Defect ID
EWLCJ176_2S_RegDom_1	Verify whether supported countries are showing properly or not	To verify whether supported countries are showing properly or not	Passed	
EWLCJ176_2S_RegDom_2	Verify whether configured countries are showing properly or not	To verify whether configured countries are showing properly or not	Passed	
EWLCJ176_2S_RegDom_3	Configure Regulatory Domain Country code	To configure Regulatory Domain Country code	Passed	
EWLCJ176_2S_RegDom_4	Configure multiple Countries and assign country code to access point	To configure multiple Countries and assign country code to access point	Passed	
EWLCJ176_2S_RegDom_5	Verify country code is changed for access point	To verify country code is changed for access point	Passed	
EWLCJ176_2S_RegDom_6	Verify Syslog is generated or not after configuring non-regulatory country code to the Access Point	To verify Syslog is generated or not after configuring non-regulatory country code to the Access Point	Passed	
EWLCJ176_2S_RegDom_7	Configure multiple countries through UI dashboard and disable same countries through CLI	To configure multiple countries through UI dashboard and disable same countries through CLI	Passed	
EWLCJ176_2S_RegDom_8	Verify AP joins to other eWLC with another country code supported	To verify AP joins to other eWLC with another country code supported	Passed	

EWLCJ176_2S_RegDom_9	Verify eWLC reboot to retain the country code	To verify eWLC reboot to retain the country code	Passed	
EWLCJ176_2S_RegDom_10	Verify non-regulatory country code change	To verify non-regulatory country code change	Passed	
EWLCJ176_2S_RegDom_11	Verify atleast one Regulatory Domain is configured or not	To verify atleast one Regulatory Domain is configured or not	Passed	
EWLCJ176_2S_RegDom_12	Associate Windows client to AP with Regulatory country code	To associate Windows client to AP with Regulatory country code	Passed	
EWLCJ176_2S_RegDom_13	Associate Android client to AP with Regulatory country code	To associate Android client to AP with Regulatory country code	Passed	
EWLCJ176_2S_RegDom_14	Associate MAC client to AP with Regulatory country code	To associate MAC client to AP with Regulatory country code	Passed	
EWLCJ176_2S_RegDom_15	Associate IOS client to AP with Regulatory country code	To associate IOS client to AP with Regulatory country code	Passed	
EWLCJ176_2S_RegDom_16	Associate Surface client to AP with Regulatory country code	To associate Surface client to AP with Regulatory country code	Passed	
EWLCJ176_2S_RegDom_17	Verify PID values once configured Regulatory Domain	To verify PID values once configured Regulatory Domain	Passed	
EWLCJ176_2S_RegDom_18	Verify Packet Capture, Ping and Traffic after configuring Regulatory Domain	To verify Packet Capture, Ping and Traffic after configuring Regulatory Domain	Passed	

EWLCJ176_2S_RegDom_19	Verify Radio Operation status of AP	To verify Radio Operation status of AP	Passed	
EWLCJ176_2S_RegDom_20	Day 0 configuration when no country code configured	To do Day 0 configuration when no country code configured	Passed	
EWLCJ176_2S_RegDom_21	Verify list of access point models and protocols are supported per country and regulatory domain	To verify list of access point models and protocols are supported per country and regulatory domain	Passed	
EWLCJ176_2S_RegDom_22	Verify Prime Infrastructure Syslog alert is generated or not for non-regulatory domain	To verify Prime Infrastructure Syslog alert is generated or not for non-regulatory domain	Passed	
EWCJ176_2S_RegDom_1	Verify whether supported countries are showing properly or not	To verify whether supported countries are showing properly or not	Passed	
EWCJ176_2S_RegDom_2	Verify whether configured countries are showing properly or not	To verify whether configured countries are showing properly or not	Passed	
EWCJ176_2S_RegDom_3	Configure Regulatory Domain Country code	To configure Regulatory Domain Country code	Passed	
EWCJ176_2S_RegDom_4	Configure multiple Countries and assign country code to access point	To configure multiple Countries and assign country code to access point	Passed	
EWCJ176_2S_RegDom_5	Verify country code is changed for access point	To verify country code is changed for access point	Passed	

EWCJ176_2S_RegDom_6	Verify Syslog is generated or not after configuring non-regulatory country code to the Access Point	To verify Syslog is generated or not after configuring non-regulatory country code to the Access Point	Passed	
EWCJ176_2S_RegDom_7	Configure multiple countries through UI dashboard and disable same countries through CLI	To configure multiple countries through UI dashboard and disable same countries through CLI	Failed	CSCvy29806
EWCJ176_2S_RegDom_8	Verify AP joins to other eWLC with another country code supported	To verify AP joins to other eWLC with another country code supported	Passed	
EWCJ176_2S_RegDom_9	Verify eWLC reboot to retain the country code	To verify eWLC reboot to retain the country code	Passed	
EWCJ176_2S_RegDom_10	Verify non-regulatory country code change	To verify non-regulatory country code change	Passed	
EWCJ176_2S_RegDom_11	Verify atleast one Regulatory Domain is configured or not	To verify atleast one Regulatory Domain is configured or not	Passed	
EWCJ176_2S_RegDom_12	Associate Windows client to AP with Regulatory country code	To associate Windows client to AP with Regulatory country code	Failed	CSCvy92385
EWCJ176_2S_RegDom_13	Associate Android client to AP with Regulatory country code	To associate Android client to AP with Regulatory country code	Passed	
EWCJ176_2S_RegDom_14	Associate MAC client to AP with Regulatory country code	To associate MAC client to AP with Regulatory country code	Passed	

EWCJ176_2S_RegDom_15	Associate IOS client to AP with Regulatory country code	To associate IOS client to AP with Regulatory country code	Passed	
EWCJ176_2S_RegDom_16	Associate Surface client to AP with Regulatory country code	To associate Surface client to AP with Regulatory country code	Passed	
EWCJ176_2S_RegDom_17	Verify PID values once configured Regulatory Domain	To verify PID values once configured Regulatory Domain	Passed	
EWCJ176_2S_RegDom_18	Verify Packet Capture, Ping and Traffic after configuring Regulatory Domain	To verify Packet Capture, Ping and Traffic after configuring Regulatory Domain	Passed	
EWCJ176_2S_RegDom_19	Verify Radio Operation status of AP	To verify Radio Operation status of AP	Passed	
EWCJ176_2S_RegDom_20	Day 0 configuration when no country code configured	To do Day 0 configuration when no country code configured	Passed	
EWCJ176_2S_RegDom_21	Verify list of access point models and protocols are supported per country and regulatory domain	To verify list of access point models and protocols are supported per country and regulatory domain	Passed	
EWCJ176_2S_RegDom_22	Verify Prime Infrastructure Syslog alert is generated or not for non-regulatory domain	To verify Prime Infrastructure Syslog alert is generated or not for non-regulatory domain	Passed	

WebUI: WLAN/AAA/ACL Simplication

Logical ID	Title	Description	Status	Defect ID
EWLCJ176_2S_aaa_acl_1	Connecting Android client to 9105 AP with Local mode PSK.	To verify whether the android client connect to 9105 AP with local mode PSK or not	Passed	
EWLCJ176_2S_aaa_acl_2	Connecting Windows client to 9115 AP with Local mode Dot1x	To verify whether the windows client connect to 9115 AP with local mode Dot1x or not	Passed	
EWLCJ176_2S_aaa_acl_3	Configuring Dot1x Security & checking the Authentication list via CLI	To configure Dot1x Security & validate the Authentication list via CLI	Passed	
EWLCJ176_2S_aaa_acl_4	Connecting mac client to 9130 AP with Local mode LWA	To verify Whether the MAC client to 9130 Ap with local mode LWA	Passed	
EWLCJ176_2S_aaa_acl_5	Validating AAA parameters in Local mode LWA	To Validate the AAA parameters in Local mode LWA	Passed	
EWLCJ176_2S_aaa_acl_6	Checking the client connectivity for Local mode EWA	To check the client connectivity for local mode EWA	Failed	CSCvy27990
EWLCJ176_2S_aaa_acl_7	Checking the parameter Map for Local mode EWA	To check the parameter map for local mode EWA	Passed	
EWLCJ176_2S_aaa_acl_8	Connect the windows client with local mode CWA	To check the windows client connectivity for local mode CWA	Passed	
EWLCJ176_2S_aaa_acl_9	Creating user group for Local mode CWA	To create User group for Local mode CWA	Passed	

EWLCJ176_2S_aaa_acl_10	Checking the client connectivity for flex connect LWA	To check whether the client connected with flex connect LWA or not	Passed	
EWLCJ176_2S_aaa_acl_11	Validate the client connectivity for flex connect EWA	To validate whether the client connected with flex connect EWA or not	Passed	
EWLCJ176_2S_aaa_acl_12	Mapping ACL policy in Flex connect EWA	To map the ACL policy in flex connect EWA	Passed	
EWLCJ176_2S_aaa_acl_13	Monitor the client connectivity for flex connect CWA	To monitor whether the client connect with flex connect CWA or not	Passed	
EWLCJ176_2S_aaa_acl_14	Checking the client connectivity for Guest Foreign CWA	To check the client connectivity for Guest foreign CWA	Passed	
EWLCJ176_2S_aaa_acl_15	validating radius server details in Guest foreign CWA	To validate the radius server details	Passed	
EWLCJ176_2S_aaa_acl_16	Monitor the client connectivity for Guest CWA Anchor	To monitor whether the client connect with Guest CWA anchor or not	Passed	

HA Management - Interface Status of the Standby through the Active using SNMP

Logical ID	Title	Description	Status	Defect ID
EWLCJ176_2S_HA_1	Check if standby interface status details are shown on bootup in active	To check if standby interface status details are shown on bootup in active	Passed	
EWLCJ176_2S_HA_2	Check if standby interface status details are shown on moving to SSO mode in active	To check if standby interface status details are shown on moving to SSO mode in active	Passed	
EWLCJ176_2S_HA_3	Check if standby interface status details are updated on adding interface in active	To check if standby interface status details are updated on adding interface in active	Failed	CSCvy90626
EWLCJ176_2S_HA_4	Check if standby interface status details are updated on adding VLAN interface in active	To check if standby interface status details are updated on adding VLAN interface in active	Passed	
EWLCJ176_2S_HA_5	Check if standby interface status details are updated on removing rmi cable/breaking the HA connectivity	To check if standby interface status details are updated on removing rmi cable/breaking the HA connectivity	Passed	
EWLCJ176_2S_HA_6	Check if standby interface status details changes upon AP addition	To check if standby interface status details changes upon AP addition	Passed	
EWLCJ176_2S_HA_7	Check if standby interface status details are updated on removing VLAN interface in active	To check if standby interface status details are updated on removing VLAN interface in active	Passed	

EWLCJ176_2S_HA_8	Check if standby interface status details are updated on shutting VLAN interface in active	To check if standby interface status details are updated on shutting VLAN interface in active	Passed	
EWLCJ176_2S_HA_9	Check if standby interface status details are shown in active chassis on standby reload	To check if standby interface status details are shown in active chassis on standby reload	Passed	
EWLCJ176_2S_HA_10	Check if standby interface status details are shown on active chassis for different SNMP protocols/privileges	To check if standby interface status details are shown on active chassis for different SNMP protocols/privileges	Passed	
EWLCJ176_2S_HA_11	Check if standby interface status details are shown without loopback/null address	To check if standby interface status details are shown without loopback/null address	Passed	

MAC Address Consistency

Logical ID	Title	Description	Status	Defect ID
EWLCJ176_2S_MacAdd_1	Configuring the Mobility Peer Mac Address with different formats to verify the consistency	To configure the Mobility Peer Mac Address with different formats to verify the consistency	Passed	
EWLCJ176_2S_MacAdd_2	Configure AP Provisioning to check MAC Address consistency	To Configure Ap Provisioning to check MAC Address consistency	Passed	
EWLCJ176_2S_MacAdd_3	Configure Ap tag to check MAC Address consistency	To Configure Ap tag to check MAC Address consistency	Passed	
EWLCJ176_2S_MacAdd_4	Configure Policy Map to check MAC Address consistency	To Configure Policy Map to check MAC Address consistency	Passed	
EWLCJ176_2S_MacAdd_5	Configure Device authentication to check MAC Address consistency	To Configure Device authentication to check MAC Address consistency	Passed	
EWLCJ176_2S_MacAdd_6	Configure Device authentication through CSV file to check MAC Address consistency	To Configure Device authentication through CSV file to check MAC Address consistency	Passed	
EWLCJ176_2S_MacAdd_7	Configure Excluded clients to check MAC Address consistency	To configure Excluded clients to check MAC Address consistency	Passed	

EWLCJ176_2S_MacAdd_8	Configure Radioactive trace to check MAC Address consistency	To configure Radioactive trace to check MAC Address consistency	Passed	
EWLCJ176_2S_MacAdd_9	Configure packet tracer to check MAC Address consistency	To configure Packet tracer to check MAC Address consistency	Passed	
EWLCJ176_2S_MacAdd_10	Configure Ap Join to check MAC Address consistency	To Configure Ap Join to check MAC Address consistency	Passed	
EWLCJ176_2S_MacAdd_11	Configure Mac filtering windows client connection to check MAC Address consistency	To Configure Mac filtering windows client connection to check MAC Address consistency	Failed	CSCvz12570
EWLCJ176_2S_MacAdd_12	Configure Mac filtering MAC/Android client connection to check MAC Address consistency	To Configure Mac filtering MAC/Android client connection to check MAC Address consistency	Passed	
EWLCJ176_2S_MacAdd_13	Configure client whitelisting to check MAC Address consistency	To Configure client whitelisting to check MAC Address consistency	Passed	
EWLCJ176_2S_MacAdd_14	Deleting a Whitelisted User & client MAC Address in UI	To check whether a guest user & MAC Address consistency can be deleted or not in EWLC UI	Passed	
EWLCJ176_2S_MacAdd_15	Associating Window client with Mac filter enabled L3-Web auth SSID & Web login with guest user	To check that Window 10 client got associated with Mac filter enabled L3-Web auth SSID & Login with guest user credentials	Passed	

EWLCJ176_2S_MacAdd_16	Configure when eWC1 is down AP should join to eWC2	To Configure when eWC1 is down AP should join to eWC2	Passed	
EWLCJ176_2S_MacAdd_17	Verify client delete reason (mac-address) code is generated or not to check MAC Address consistency	To Verify client delete reason (mac-address) code is generated or not to check MAC Address consistency	Passed	
EWLCJ176_2S_MacAdd_18	Verify whether your able to add APs MAC Address to LSC Provision List	To Verify whether your able to add APs MAC Address to LSC Provision List	Passed	
EWLCJ176_2S_MacAdd_19	Verify whether you are able to add APs MAC Address through CSV file to LSC Provision List	To Verify whether you are able to add APs MAC Address through CSV file to LSC Provision List	Passed	
EWLCJ176_2S_MacAdd_20	Verify whether you are able to add MAC Address in Ap certificate policy	To Verify whether you are able to add MAC Address in Ap certificate policy	Passed	
EWLCJ176_2S_MacAdd_21	Verify whether you are able to add MAC Address through CSC file in Ap certificate policy	To Verify whether you are able to add MAC Address through CSC file in Ap certificate policy	Passed	
EWLCJ176_2S_MacAdd_22	Verifying whether you are able to get RA logs to check MAC Address consistency	To Verify whether you are able to get RA logs to check MAC Address consistency	Passed	
EWLCJ176_2S_MacAdd_23	Verify mac filtering client connection in WLC to check MAC Address consistency	To Verify mac filtering client connection in WLC to check MAC Address consistency	Passed	

EWCJ176_2S_MacAdd_01	Configure Excluded clients by using mac_address consistency	To Configure Excluded clients by using mac_address consistency	Passed	
EWCJ176_2S_MacAdd_02	Configure Radioactive trace by using mac_address consistency	To Configure Radioactive trace by using mac_address consistency	Passed	
EWCJ176_2S_MacAdd_03	Configure packet tracer by using mac_address consistency	To Configure Packet tracer by using mac_address consistency	Passed	
EWCJ176_2S_MacAdd_04	Configure Ap Provisioning by using mac_address consistency	To Configure Ap Provisioning by using mac_address consistency	Passed	
EWCJ176_2S_MacAdd_05	Configure Ap tag by using mac_address consistency	To Configure Ap tag by using mac_address consistency	Passed	
EWCJ176_2S_MacAdd_06	Configure Policy Map by using mac_address consistency	To Configure Policy Map by using mac_address consistency	Passed	
EWCJ176_2S_MacAdd_07	Configure Device authentication by using mac_address consistency	To Configure Device authentication by using mac_address consistency	Passed	
EWCJ176_2S_MacAdd_08	Configure Device authentication through CSV file by using mac_address consistency	To Configure Device authentication through CSV file by using mac_address consistency	Passed	
EWCJ176_2S_MacAdd_09	Configure Ap Join by using mac_address consistency	To Configure Ap Join by using mac_address consistency	Passed	

EWCJ176_2S_MacAdd_10	Configure Mac filtering windows client connection by using mac_address consistency	To Configure Mac filtering windows client connection by using mac_address consistency	Passed	
EWCJ176_2S_MacAdd_11	Configure Mac filtering MAC/Android client connection by using mac_address consistency	To Configure Mac filtering MAC/Android client connection by using mac_address consistency	Passed	
EWCJ176_2S_MacAdd_12	Configure client whitelisting by using mac_address consistency	To Configure client whitelisting by using mac_address consistency	Passed	
EWCJ176_2S_MacAdd_13	Deleting a Whitelisted User & client mac address in UI	To check whether a guest user & mac address consistency can be deleted or not in EWLC UI	Passed	
EWCJ176_2S_MacAdd_14	Associating Window client with Mac filter enabled L3-Web auth SSID & Web login with guest user	To check that Window 10 client got associated with Mac filter enabled L3-Web auth SSID & Login with guest user credentials	Passed	
EWCJ176_2S_MacAdd_15	Configure when eWC1 is down AP should join to eWC2	To Configure when eWC1 is down AP should join to eWC2	Passed	
EWCJ176_2S_MacAdd_16	Verify client delete reason (mac-address) code is generated or not by using mac_address consistency	To Verify client delete reason (mac-address) code is generated or not by using mac_address consistency	Passed	

EWCJ176_2S_MacAdd_17	Verify whether your able to add APs MAC address to LSC Provision List	To Verify whether your able to add APs MAC address to LSC Provision List	Passed	
EWCJ176_2S_MacAdd_18	Verify whether you are able to add APs MAC address through CSV file to LSC Provision List	To Verify whether you are able to add APs MAC address through CSV file to LSC Provision List	Passed	
EWCJ176_2S_MacAdd_19	Verify whether you are able to add MAC address in Ap certificate policy	To Verify whether you are able to add MAC address in Ap certificate policy	Passed	
EWCJ176_2S_MacAdd_20	Verify whether you are able to add MAC address through CSC file in Ap certificate policy	To Verify whether you are able to add MAC address through CSC file in Ap certificate policy	Passed	
EWCJ176_2S_MacAdd_21	Verify whether you are able to get RA logs by using Mac_address consistency	To Verify whether you are able to get RA logs by using Mac_address consistency	Passed	
EWCJ176_2S_MacAdd_22	Verify mac filtering client connection in WLC by using mac_address consistency	To Verify mac filtering client connection in WLC by using mac_address consistency	Passed	

AP Tags needs to be Preserved

Logical ID	Title	Description	Status	Defect ID
EWLCJ176_2S_APTag_1	Verify whether your able to execute tag persistency command or not	To verify whether your able to execute tag persistency command or not	Passed	
EWLCJ176_2S_APTag_2	Verify whether your able to configure AP Join Profile, Policy tag, Site tag, RF tag	To verify whether your able to configure AP Join Profile, Policy tag, Site tag, RF tag	Failed	CSCvy39499
EWLCJ176_2S_APTag_3	Map tagX profile to Access Point	To map tagX profile to Access Point	Passed	
EWLCJ176_2S_APTag_4	Test tag source priority is followed by AP tags persistency	To test tag source priority is followed by AP tags persistency	Passed	
EWLCJ176_2S_APTag_5	Upload multiple AP MAC addresses, tagX through CSV file	To upload multiple AP MAC addresses, tagX through CSV file	Passed	
EWLCJ176_2S_APTag_6	Verify Tag Source Priority	To verify Tag Source Priority	Passed	
EWLCJ176_2S_APTag_7	Move Access Point from eWLC1 to eWLC2 with Preserved tags	To move Access Point from eWLC1 to eWLC2 with Preserved tags	Passed	
EWLCJ176_2S_APTag_8	Move Access Point from eWLC1 to eWLC2 without Preserved tags and verify automatic default tagX parameters	To move Access Point from eWLC1 to eWLC2 without Preserved tags and to verify automatic default tagX parameters	Passed	
EWLCJ176_2S_APTag_9	Move Access Point to other controller on Priority base	To move Access Point to other controller on Priority base	Passed	

EWLCJ176_2S_APTag_10	Verify Syslog's after moving AP from eWLC1 to eWLC2	To verify Syslog's after moving AP from eWLC1 to eWLC2	Passed	
EWLCJ176_2S_APTag_11	Move AP from eWLC1 to eWLC2 using Basic Profile with Preserved tags	To move AP from eWLC1 to eWLC2 using Basic Profile with Preserved tags	Passed	
EWLCJ176_2S_APTag_12	Connect Windows client when AP tags are Preserved and verify client status	To connect Windows client when AP tags are Preserved and to verify client status	Passed	
EWLCJ176_2S_APTag_13	Connect Android client when AP tags are Preserved and verify client status	To connect Android client when AP tags are Preserved and verify client status	Passed	
EWLCJ176_2S_APTag_14	Connect IOS client when AP tags are Preserved and verify client status	To connect IOS client when AP tags are Preserved and verify client status	Passed	
EWLCJ176_2S_APTag_15	Connect MAC client when AP tags are Preserved and verify client status	To connect MAC client when AP tags are Preserved and verify client status	Passed	
EWLCJ176_2S_APTag_16	Connect Surface client when AP tags are Preserved and verify client status	To connect Surface client when AP tags are Preserved and verify client status	Passed	
EWLCJ176_2S_APTag_17	Create AP tags needs to be Preserved using Basic Profile and check Joined APs and Clients count	To create AP tags needs to be Preserved using Basic Profile and check Joined APs and Clients count	Passed	
EWLCJ176_2S_APTag_18	Verify AP disjoined alert is triggered or not in Prime Infrastructure	To verify AP disjoined alert is triggered or not in Prime Infrastructure	Passed	

EWLCJ176_2S_APTag_19	Verify AP moved alert is triggered or not in Prime Infrastructure	To verify AP moved alert is triggered or not in Prime Infrastructure	Passed	
EWLCJ176_2S_APTag_20	Create Location and upload empty csv file	To create Location and upload empty csv file	Passed	CSCvy34239
EWLCJ176_2S_APTag_21	Create Location, upload bulk csv file and check AP Joined status	To create Location, upload bulk csv file and check AP Joined status	Passed	CSCvy89157

Parallel Mode support in Image download feature

Logical ID	Title	Description	Status	Defect ID
EWLCJ176_2S_ImgDown_1	Verify parallel mode image download using TFTP in EWC 9130	To Verify parallel mode image download using TFTP in EWC 9130	Passed	
EWLCJ176_2S_ImgDown_2	Verify parallel mode image download using SFTP in EWC 9130	To Verify parallel mode image download using SFTP in EWC 9130	Passed	
EWLCJ176_2S_ImgDown_3	Verify parallel mode image download using TFTP in EWC HA setup	To Verify parallel mode image download using TFTP in EWC HA setup	Passed	
EWLCJ176_2S_ImgDown_4	Verify parallel mode image download using SFTP in EWC HA setup	To Verify parallel mode image download using SFTP in EWC HA setup	Passed	
EWLCJ176_2S_ImgDown_5	Verify parallel mode image download using TFTP in EWC 9120	To Verify parallel mode image download using TFTP in EWC 9120	Passed	
EWLCJ176_2S_ImgDown_6	Verify parallel mode image download using SFTP in EWC 9120	To Verify parallel mode image download using SFTP in EWC 9120	Passed	
EWLCJ176_2S_ImgDown_7	Verify parallel mode image download using TFTP in EWC 9115	To Verify parallel mode image download using TFTP in EWC 9115	Passed	
EWLCJ176_2S_ImgDown_8	Verify parallel mode image download using SFTP in EWC 9115	To Verify parallel mode image download using SFTP in EWC 9115	Passed	

EWLCJ176_2S_ImgDown_9	Verify parallel mode image download using TFTP in EWC 9105	To Verify parallel mode image download using TFTP in EWC 9105	Passed	
EWLCJ176_2S_ImgDown_10	Verify parallel mode image download using SFTP in EWC 9105	To Verify parallel mode image download using SFTP in EWC 9105	Passed	
EWLCJ176_2S_ImgDown_11	Cancel Image TFTP download process after predownloaded completion and upgrade with another version	To verify Image downloaded based on latest version	Passed	
EWLCJ176_2S_ImgDown_12	Cancel Image SFTP download process after predownloaded completion and upgrade with another version	To verify Image downloaded based on latest version	Passed	
EWLCJ176_2S_ImgDown_13	Upgrade using TFTP without parallel image support	To verify Upgrade using TFTP without parallel image support	Passed	
EWLCJ176_2S_ImgDown_14	Upgrade using SFTP without parallel image support	To verify Upgrade using SFTP without parallel image support	Passed	
EWLCJ176_2S_ImgDown_15	Verify Image upgrade using http method	To Verify Image upgrade using http method	Passed	
EWCJ176_2S_ImgDown_1	Verify parallel mode image download using TFTP in EWC 9130	To Verify parallel mode image download using TFTP in EWC 9130	Passed	
EWCJ176_2S_ImgDown_2	Verify parallel mode image download using SFTP in EWC 9130	To Verify parallel mode image download using SFTP in EWC 9130	Passed	

EWCJ176_2S_ImgDown_3	Verify parallel mode image download using TFTP in EWC HA setup	To Verify parallel mode image download using TFTP in EWC HA setup	Passed	
EWCJ176_2S_ImgDown_4	Verify parallel mode image download using SFTP in EWC HA setup	To Verify parallel mode image download using SFTP in EWC HA setup	Passed	
EWCJ176_2S_ImgDown_5	Verify parallel mode image download using TFTP in EWC 9120	To Verify parallel mode image download using TFTP in EWC 9120	Passed	
EWCJ176_2S_ImgDown_6	Verify parallel mode image download using SFTP in EWC 9120	To Verify parallel mode image download using SFTP in EWC 9120	Passed	
EWCJ176_2S_ImgDown_7	Verify parallel mode image download using TFTP in EWC 9115	To Verify parallel mode image download using TFTP in EWC 9115	Passed	
EWCJ176_2S_ImgDown_8	Verify parallel mode image download using SFTP in EWC 9115	To Verify parallel mode image download using SFTP in EWC 9115	Passed	
EWCJ176_2S_ImgDown_9	Verify parallel mode image download using TFTP in EWC 9105	To Verify parallel mode image download using TFTP in EWC 9105	Passed	
EWCJ176_2S_ImgDown_10	Verify parallel mode image download using SFTP in EWC 9105	To Verify parallel mode image download using SFTP in EWC 9105	Passed	
EWCJ176_2S_ImgDown_11	Cancel Image TFTP download process after predownloaded completion and upgrade with another version	To verify Image downloaded based on latest version	Passed	

EWCJ176_2S_ImgDown_12	Cancel Image SFTP download process after predownloaded completion and upgrade with another version	To verify Image downloaded based on latest version	Passed	
EWCJ176_2S_ImgDown_13	Upgrade using TFTP without parallel image support	To verify Upgrade using TFTP without parallel image support	Passed	
EWCJ176_2S_ImgDown_14	Upgrade using SFTP without parallel image support	To verify Upgrade using SFTP without parallel image support	Passed	
EWCJ176_2S_ImgDown_15	Verify Image upgrade using http method	To Verify Image upgrade using http method	Passed	

Enhanced PnP for workflow support -AP dependency

Logical ID	Title	Description	Status	Defect ID
EWLCJ176_2S_PnP_1	Configure AP via PNP workflow using EAP-TLS authentication	To configure AP via PNP workflow using EAP-TLS authentication	Passed	
EWLCJ176_2S_PnP_2	Configure AP via PNP workflow using EAP-PEAP authentication	To configure AP via PNP workflow using EAP-PEAP authentication	Passed	
EWLCJ176_2S_PnP_3	Configure AP via PNP workflow using EAP-FAST authentication	To configure AP via PNP workflow using EAP-FAST authentication	Passed	
EWLCJ176_2S_PnP_4	Configure 4800 AP via PNP workflow using EAP authentication	To configure 4800 AP via PNP workflow using EAP authentication	Passed	
EWLCJ176_2S_PnP_5	Configure 9120 AP via PNP workflow using EAP authentication	To configure 9120 AP via PNP workflow using EAP authentication	Passed	
EWLCJ176_2S_PnP_6	Configure 9115 AP via PNP workflow using EAP authentication	To configure 9115 AP via PNP workflow using EAP authentication	Passed	
EWLCJ176_2S_PnP_7	Configure 9105 AP via PNP workflow using EAP authentication	To configure 9105 AP via PNP workflow using EAP authentication	Passed	
EWLCJ176_2S_PnP_8	Configure 9130 AP via PNP workflow using EAP authentication	To configure 9130 AP via PNP workflow using EAP authentication	Passed	

EWLCJ176_2S_PnP_9	Configure 9105 as EWC & onboard an AP via PnP workflow with EAP authentication	To configure 9105 as EWC & onboard an AP via PnP workflow with EAP authentication	Passed	
EWLCJ176_2S_PnP_10	Configure 9115 as EWC & onboard an AP via PnP workflow with EAP authentication	To configure 9115 as EWC & onboard an AP via PnP workflow with EAP authentication	Passed	
EWLCJ176_2S_PnP_11	Configure 9120 as EWC & onboard an AP via PnP workflow with EAP authentication	To configure 9120 as EWC & onboard an AP via PnP workflow with EAP authentication	Passed	
EWLCJ176_2S_PnP_12	Configure 9130 as EWC & onboard an AP via PnP workflow with EAP authentication	To configure 9130 as EWC & onboard an AP via PnP workflow with EAP authentication	Passed	
EWLCJ176_2S_PnP_13	Configure EWC redundancy & onboard an AP via PnP workflow with EAP authentication	To configure EWC redundancy & onboard an AP via PnP workflow with EAP authentication	Passed	
EWLCJ176_2S_PnP_14	Configure AP via PnP workflow and claim multiple AP's at the same time	To configure AP via PnP workflow and claim multiple AP's at the same time	Passed	
EWCJ176_2S_PnP_1	Verify downloading CA certificates and AP's are updated in Fabric sites	To Verify downloading CA certificates and AP's are updated in Fabric sites	Passed	
EWCJ176_2S_PnP_2	Verify whether able to import the CA certificate with required authentications successfully in ISE	To Verify whether able to import the CA certificate with required authentications successfully in ISE	Passed	

EWCJ176_2S_PnP_3	Configure AP onboarding via PNP workflow by using EAP-TLS authentication	To configure AP via PNP workflow using EAP-TLS authentication	Passed	
EWCJ176_2S_PnP_4	Configure AP onboarding via PNP workflow by using EAP-PEAP authentication	To configure AP via PNP workflow using EAP-PEAP authentication	Passed	
EWCJ176_2S_PnP_5	Configure AP onboarding via PNP workflow by using EAP-FAST authentication	To configure AP via PNP workflow using EAP-FAST authentication	Passed	
EWCJ176_2S_PnP_6	Configure 4800 AP onboarding via PNP workflow by using EAP authentication	To configure 4800 AP via PNP workflow using EAP authentication	Passed	
EWCJ176_2S_PnP_7	Configure 9120 AP onboarding via PNP workflow by using EAP authentication	To configure 9120 AP via PNP workflow using EAP authentication	Passed	
EWCJ176_2S_PnP_8	Configure 9115 AP onboarding via PNP workflow by using EAP authentication	To configure 9115 AP via PNP workflow using EAP authentication	Passed	
EWCJ176_2S_PnP_9	Configure 9105 AP onboarding via PNP workflow by using EAP authentication	To configure 9105 AP via PNP workflow using EAP authentication	Passed	
EWCJ176_2S_PnP_10	Configure 9130 AP onboarding via PNP workflow by using EAP authentication	To configure 9130 AP via PNP workflow using EAP authentication	Passed	
EWCJ176_2S_PnP_11	Configure 9105 as EWC & onboard an AP via PnP workflow with EAP authentication	To configure 9105 as EWC & onboard an AP via PnP workflow with EAP authentication	Passed	

EWCJ176_2S_PnP_12	Configure 9115 as EWC & onboard an AP via PnP workflow with EAP authentication	To configure 9115 as EWC & onboard an AP via PnP workflow with EAP authentication	Passed	
EWCJ176_2S_PnP_13	Configure 9120 as EWC & onboard an AP via PnP workflow with EAP authentication	To configure 9120 as EWC & onboard an AP via PnP workflow with EAP authentication	Passed	
EWCJ176_2S_PnP_14	Configure 9130 as EWC & onboard an AP via PnP workflow with EAP authentication	To configure 9130 as EWC & onboard an AP via PnP workflow with EAP authentication	Passed	
EWCJ176_2S_PnP_15	Configure EWC redundancy & onboard an AP via PnP workflow with EAP authentication	To configure EWC redundancy & onboard an AP via PnP workflow with EAP authentication	Passed	
EWCJ176_2S_PnP_16	Configure AP via PnP workflow and claim multiple AP's at the same time	To configure AP via PnP workflow and claim multiple AP's at the same time	Passed	

C9105 EWC AP Support

Logical ID	Title	Description	Status	Defect ID
EWCJ176S_C9105_EWC_01	Converting 9105 AP into EWC	To convent 9105 AP to EWC	Passed	
EWCJ176S_C9105_EWC_02	Configuring 9105 AP in Day0 mode by connecting wireless client.	To verify the Day0 configuration of 9105 AP through wireless client.	Passed	
EWCJ176S_C9105_EWC_03	Performing Ping test for Client connected to Day0 SSID	Verifying Ping test for client connected to Day0 SSID	Passed	
EWCJ176S_C9105_EWC_04	Connecting windows client to 9105 AP with L2 security Open.	To verify the windows client connectivity with L2 Security Open.	Passed	
EWCJ176S_C9105_EWC_05	Connecting IOS client to 9105 AP with L2 security Static WEP.	To verify the IOS client connectivity with L2 Security WEP.	Passed	
EWCJ176S_C9105_EWC_06	Connecting MACOs client to 9105 PA with L2 Security - WPA/WPA2 + PSK	To verify the MACOs client connectivity with L2 Security WPA/WPA2 + PSK	Passed	
EWCJ176S_C9105_EWC_07	Connecting Android client to 9105 AP with L2 Security - WPA/WPA2 + dot1x	To verify the Android client connectivity with L2 security WPA/WPA2+dot1x	Passed	
EWCJ176S_C9105_EWC_08	Rebooting the 9105 AP	To check if the AP gets Rebooted or not and check if the AP joins the controller again.	Passed	
EWCJ176S_C9105_EWC_09	Connecting surface Go client to 9105 AP with WPA3 security	To verify the WPA3 support for 9120 AP	Passed	

EWCJ176S_C9105_EWC_10	Upgrading the EWC to the latest build.	To verify the upgrading of EWC to the latest build without any issues.	Passed	
EWCJ176S_C9105_EWC_11	Downgrading the EWC to the previous version.	To verify the Downgrading of EWC to the previous version without any issues.	Passed	
EWCJ176S_C9105_EWC_12	Upload/download config file from EWC	To verify the config retain on upload/download the config file.	Passed	
EWCJ176S_C9105_EWC_13	Configuring HA between EWC	To verify the HA pair setup between the EWC	Passed	
EWCJ176S_C9105_EWC_14	Update RMI configuration in 9105 AP and check the output	To update RMI configuration in 9105 AP and check the output	Passed	
EWCJ176S_C9105_EWC_15	Performing Intra-controller roaming for Android clients using 9105 AP's	To check whether intra-controller roaming is successful or not	Passed	
EWCJ176S_C9105_EWC_16	Performing Inter-controller roaming using 9105 AP's	To check whether intra-controller roaming is successful or not	Passed	
EWCJ176S_C9105_EWC_17	Checking client connection when local switching is enabled	To verify client is connecting properly or not when local switching is enabled	Passed	
EWCJ176S_C9105_EWC_18	Checking client connection when security type changed in 9105 AP	To verify client is disconnecting or not when security type is changed in 9105 AP	Passed	
EWCJ176S_C9105_EWC_19	Checking client connectivity when 9105 AP placed in AP group	To verify client connection when 9105 AP placed in AP group	Passed	

EWCJ176S_C9105_EWC_20	Monitoring the client connectivity after 9105 AP provisioning from DNAC	To check the client connectivity after AP provisioning from DNAC	Passed	
EWCJ176S_C9105_EWC_21	Rebooting the AP with primary controller given in High Availability	To reboot the AP by giving the primary controller IP using high availability and check if the AP joins the primary controller	Passed	
EWCJ176S_C9105_EWC_22	Checking the details of the AP through the CLI	To check the details of the AP using CLI and check if the details are correctly shown or not	Passed	
EWCJ176S_C9105_EWC_23	AP failover priority with critical	To check AP failover priority with critical and check if the AP gets connected to the next controller .	Passed	
EWCJ176S_C9105_EWC_24	AP failover priority with High priority	To check AP failover priority with critical and check if the AP gets connected to the next controller .	Passed	
EWCJ176S_C9105_EWC_25	Moving AP from 9800-40 EWC to 9800-80 through High availability	To check if the AP moves from 9800-40 EWC to 9800-80 EWC through high availability.	Passed	
EWCJ176S_C9105_EWC_26	Reassociation of client to the AP after reboot	To verify if the client gets reassociated to the to the AP .	Passed	

EWCJ176S_C9105_EWC_27	Configuring different Syslog facility for 9115 11ax AP in EWC and checking the same in the APs	To configure different syslog facility for 9115 AP in EWC AP join profile and validating the same in the AP	Passed	
EWCJ176S_C9105_EWC_28	Packet capture of client when the client is connected to 9115/9120 AP with 2.4 GHz	To capture the Packet of the client when the client is connected to AP with radio as 2.4GHz	Passed	
EWCJ176S_C9105_EWC_29	Verify details by connecting client to 2.4Ghz radio of 9105 AP.	To verify OFDMA details by connecting client to 2.4 Ghz radio.	Passed	
EWCJ176S_C9105_EWC_30	Verify details by connecting client to 5 Ghz radio of 9105 AP	To verify OFDMA details by connecting client to 5 Ghz radio.	Passed	
EWCJ176S_C9105_EWC_31	Verify 9105AP MU-MIMO details with client connecting to WPA2 configured WLAN	To verify 11ax MU-MIMO details of 9105 AP with client connecting to WPA2 configured WLAN	Passed	
EWCJ176S_C9105_EWC_32	Verify 9105AP MU-MIMO details with client connecting to WPA 3 configured WLAN	To verify 11ax MU-MIMO details of 9105 AP with client connecting to WPA 3 configured WLAN	Passed	
EWCJ176S_C9105_EWC_33	Upgrading a incorrect EWC image to the 9105 AP and check if the EWC image is upgrading	To check if EWC image is upgrading with the wrong EWC image or not	Passed	
EWCJ176S_C9105_EWC_34	Verifying EWC is able to add in PI	To verify EWC is able to add in PI or not	Passed	
EWCJ176S_C9105_EWC_35	Changing AP mode from PI	To verify AP mode is able to change from PI or not	Passed	

EWCJ176S_C9105_EWC_36	Deploying template from PI	To verify template is deploying successfully or not	Passed	
EWCJ176S_C9105_EWC_37	Undeploying template from PI	To verify template is undeploying from PI or not	Passed	
EWCJ176_2S_C9105_1	Association of 9105 AP with different eWLC model	To associate 9105 AP to eWLC with latest image and check if the AP gets associated or not	Passed	
EWCJ176_2S_C9105_2	Associating 9105 AP with different country code as with eWLC	To associate 9105 AP with different country code and check if the AP does not get joined to eWLC	Passed	
EWCJ176_2S_C9105_3	Configuring AP with duplicate IP	To configure AP with a duplicate IP address and check if the AP shows error message and AP does not join the eWLC	Passed	
EWCJ176_2S_C9105_4	Rebooting the 9105 AP	To check if the AP gets Rebooted or not and check if the AP joins the controller again.	Passed	
EWCJ176_2S_C9105_5	Rebooting the AP with primary controller given in High Availability	To reboot the AP by giving the primary controller IP using high availability and check if the AP joins the primary controller	Passed	
EWCJ176_2S_C9105_6	Checking the details of the AP through the CLI	To check the details of the AP using CLI and check if the details are correctly shown or not	Passed	

EWCJ176_2S_C9105_7	Connecting a Window client to the 9105 AP	To connect a window client to the AP and check if the client gets connected to the AP without any errors.	Failed	CSCvz07838
EWCJ176_2S_C9105_8	Connecting a Android client to the 9105 AP	To connect a Android client to the AP and check if the client gets connected to the AP without any errors.	Passed	
EWCJ176_2S_C9105_9	Connecting a IOS client to the 9105 AP	To connect a IOS client to the AP and check if the client gets connected to the AP without any errors.	Passed	
EWCJ176_2S_C9105_10	Connecting a MAC client to the 9105 AP	To connect a MAC client to the AP and check if the client gets connected to the AP without any errors.	Passed	
EWCJ176_2S_C9105_11	AP failover priority with critical	To check AP failover priority with critical and check if the AP gets connected to the next controller .	Passed	
EWCJ176_2S_C9105_12	AP failover priority with High priority	To check AP failover priority with critical and check if the AP gets connected to the next controller .	Passed	
EWCJ176_2S_C9105_13	Moving AP from 9800-40 eWLC to 9800-80 through High availability	To check if the AP moves from 9800-40 eWLC to 9800-80 eWLC through high availability.	Passed	

EWCJ176_2S_C9105_14	Reassociation of client to the AP after reboot	To verify if the client gets reassociated to the to the AP .	Passed	
EWCJ176_2S_C9105_15	Checking if the client do not connect to the AP after rebooting and joining the primary controller	To check if the client gets connected to the AP after rebooting the AP and AP joining the primary controller .where there is no same WLAN	Passed	
EWCJ176_2S_C9105_16	Performing Intra controller roaming of Android client	To check whether intra controller roaming of Android clients works properly or not	Passed	
EWCJ176_2S_C9105_17	Performing Intra controller roaming of IOS client	To check whether intra controller roaming of IOS clients works properly or not in eWLC	Passed	
EWCJ176_2S_C9105_18	Performing Intra controller roaming of Mac OS client	To check whether intra controller roaming of MacOS clients works properly or not	Passed	
EWCJ176_2S_C9105_19	Performing Inter controller roaming of Windows OS client	To check whether inter controller roaming of windows clients works properly or not	Passed	
EWCJ176_2S_C9105_20	Performing Inter controller roaming of Android client	To check whether inter controller roaming of Android clients works properly or not	Passed	
EWCJ176_2S_C9105_21	Performing Inter controller roaming of IOS client	To check whether inter controller roaming of IOS clients works properly or not	Passed	

EWCJ176_2S_C9105_22	Performing Inter controller roaming of Mac OS client	To check whether inter controller roaming of Mac OS clients works properly or not	Passed	
EWCJ176_2S_C9105_23	Change AP mode from local to Flex connect in 9105 AP.	To change the mode of AP from local mode to Flex connect mode and check if the AP does not reboot.	Passed	
EWCJ176_2S_C9105_24	Changing the AP from Flex connect to Local mode and check if the AP reboot	To check if the AP reboots when AP mode is changed from flex connect to Local mode .	Passed	
EWCJ176_2S_C9105_25	Adding two 9105 AP in the AP group and connecting a client to the AP with specific WLAN	To add two 9105 AP in AP group and map a WLAN to group and connect a client to the WLAN and check the client connectivity	Passed	
EWCJ176_2S_C9105_26	Configuring different Syslog facility for 9115 11ax AP in eWLC and checking the same in the APs	To configure different syslog facility for 9115 AP in eWLC AP join profile and validating the same in the AP	Passed	
EWCJ176_2S_C9105_27	Packet capture of client when the client is connected to 9115/9120 AP with 2.4 GHz	To capture the Packet of the client when the client is connected to AP with radio as 2.4GHz	Passed	
EWCJ176_2S_C9105_28	Verify details by connecting client to 2.4Ghz radio of 9105 AP.	To verify OFDMA details by connecting client to 2.4 Ghz radio.	Passed	
EWCJ176_2S_C9105_29	Verify details by connecting client to 5 Ghz radio of 9105 AP	To verify OFDMA details by connecting client to 5 Ghz radio.	Passed	

EWCJ176_2S_C9105_30	Verify 9105AP MU-MIMO details with client connecting to WPA2 configured WLAN	To verify 11ax MU-MIMO details of 9105 AP with client connecting to WPA2 configured WLAN	Passed	
EWCJ176_2S_C9105_31	Verify 9105AP MU-MIMO details with client connecting to WPA 3 configured WLAN	To verify 11ax MU-MIMO details of 9105 AP with client connecting to WPA 3 configured WLAN	Passed	

Regression Features - Test Summary

Multi LAG and Load Balancing based on VLAN and SSO

Logical ID	Title	Description	Status	Defect ID
EWLCJ176S_Reg_01	To Verify the Multi LAG and Load balancing on 9800-40 Controller.	To Verify the Multi LAG and Load balancing on 9800-40 Controller.	Passed	
EWLCJ176S_Reg_02	To Verify the Multi LAG and Load balancing on 9800-80 Controller.	To Verify the Multi LAG and Load balancing on 9800-80 Controller.	Passed	CSCvy09143
EWLCJ176S_Reg_03	To Verify the Multi LAG and Load balancing on 9800-L Controller.	To Verify the Multi LAG and Load balancing on 9800-L Controller.	Passed	
EWLCJ176S_Reg_04	To Verify the Multi LAG and Load balancing on 9800-40 Controller after Switch failure	To Verify the Multi LAG and Load balancing on 9800-40 Controller after Switch failure	Passed	
EWLCJ176S_Reg_05	To Verify the Multi LAG and Load balancing on 9800-80 Controller after Switch failure	To Verify the Multi LAG and Load balancing on 9800-80 Controller after Switch failure	Passed	
EWLCJ176S_Reg_06	To Verify the Multi LAG and Load balancing on 9800-L Controller after Switch failure	To Verify the Multi LAG and Load balancing on 9800-L Controller after Switch failure	Passed	
EWLCJ176_2S_Reg_133	To Verify the Multi LAG and Load balancing on 9800-40 Controller.	To Verify the Multi LAG and Load balancing on 9800-40 Controller.	Passed	
EWLCJ176_2S_Reg_134	To Verify the Multi LAG and Load balancing on 9800-80 Controller.	To Verify the Multi LAG and Load balancing on 9800-80 Controller.	Passed	
EWLCJ176_2S_Reg_135	To Verify the Multi LAG and Load balancing on 9800-L Controller.	To Verify the Multi LAG and Load balancing on 9800-L Controller.	Passed	

EWLCJ176_2S_Reg_136	To Verify the Multi LAG and Load balancing on 9800-40 Controller after Switch failure	To Verify the Multi LAG and Load balancing on 9800-40 Controller after Switch failure	Passed	
EWLCJ176_2S_Reg_137	To Verify the Multi LAG and Load balancing on 9800-80 Controller after Switch failure	To Verify the Multi LAG and Load balancing on 9800-80 Controller after Switch failure	Passed	
EWLCJ176_2S_Reg_138	To Verify the Multi LAG and Load balancing on 9800-L Controller after Switch failure	To Verify the Multi LAG and Load balancing on 9800-L Controller after Switch failure	Passed	

AdvAP_QBSS_MCAST

Logical ID	Title	Description	Status	Defect ID
EWLCJ176S_Reg_07	Verify the QBSS load information in Beacon and Probes fames by configuring WMM as allowed with qbss load for policy profile.	To check whether QBSS load showing in Beacon and Probe frames or not by configuring WMM as allowed with qbss load for policy profile.	Passed	
EWLCJ176S_Reg_08	Verify the QBSS load information in Beacon and Probes fames by configuring WMM as Required with qbss load for policy profile.	To check whether QBSS load showing in Beacon and Probe frames or not by configuring WMM as required with qbss load for policy profile	Passed	
EWLCJ176S_Reg_09	Verify the QBSS load information in Beacon and Probes fames by configuring WMM as Required with no qbss load for policy profile.	To check whether QBSS load showing in Beacon and Probe frames or not by configuring WMM as allowed with no qbss load for policy profile.	Passed	
EWLCJ176S_Reg_10	Verify the QBSS load information in Beacon and Probes fames by configuring WMM as Required with qbss load for local_auth policy profile.	To check whether QBSS load showing in Beacon and Probe frames or not by configuring WMM as required with qbss load for Local_auth policy profile	Passed	
EWLCJ176S_Reg_11	Verify the QBSS load information in Beacon and Probes fames by upload/download the configuration file from controller	To check whether QBSS load showing in Beacon and Probe frames or not by upload/download the configuration file from controller	Passed	

EWLCJ176S_Reg_12	Verify the QBSS load information in Beacon and Probes fames by configuring WMM as Required with qbss load for policy profile and Flex mode AP.	To check whether QBSS load showing in Beacon and Probe frames or not by configuring WMM as required with qbss load for policy profile and Flex mode AP	Passed	
EWLCJ176S_Reg_13	Verify the QBSS load information in Beacon and Probes fames by configuring WMM as Required with qbss load for policy profile and Bridge mode AP.	To check whether QBSS load showing in Beacon and Probe frames or not by configuring WMM as required with qbss load for policy profile and Bridge mode AP	Passed	
EWLCJ176S_Reg_14	Verify the AP name in Beacon and Probes fames by configuring Aironet IE.	To check whether AP name in Beacon and Probes fames by configuring Aironet IE.	Passed	
EWLCJ176S_Reg_15	Verify the AP name in Beacon and Probes fames by configuring Aironet IE with modified AP name.	To check whether AP name in Beacon and Probes fames by configuring Aironet IE with Modified AP name.	Passed	
EWLCJ176S_Reg_16	Verify the AP name in Beacon and Probes fames by configuring Aironet IE and upload/download the configuration file from controller.	To check whether AP name in Beacon and Probes fames by configuring Aironet IE and upload/download the configuration file from controller.	Passed	
EWLCJ176S_Reg_17	Verify the AP name in Beacon and Probes fames by configuring Aironet IE with more than 15 characters of AP name.	To check whether AP name in Beacon and Probes fames by configuring Aironet IE with more than 15 characters of AP name.	Passed	

EWLCJ176S_Reg_18	Verify the AP name in Beacon and Probes fames by configuring Aironet IE and re-join the AP's to eWLC-2 from eWLC-1.	To check whether AP name in Beacon and Probes fames by configuring Aironet IE and re-join the AP's to eWLC-2 from eWLC-1.	Passed	
EWLCJ176S_Reg_19	Verify the Multicast filter and MC2UC traffic to local-switching client	To verify the Multicast filter and local-switching client subscribed to video streaming receives MC2UC traffic	Passed	
EWLCJ176S_Reg_20	Verify the Multicast filter and MC2UC traffic to Central-switching client	To verify the Multicast filter and central-switching client subscribed to video streaming receives MC2UC traffic	Passed	
EWLCJ176S_Reg_21	Verify the Multicast filter and Flex AP reboot in connected mode when Flex LS client receiving MC2UC traffic	To verify whether client reassociates and receives MC2UC traffic when flex AP is rebooted in connected mode with multicast filter.	Passed	
EWLCJ176S_Reg_22	Verify the Multicast filter and MC2UC traffic to Central-switching client after Download/upload the configuration file to controller	To verify the Multicast filter client subscribed to video streaming receives MC2UC traffic after download/upload the configuration file from controller	Passed	
EWLCJ176_2S_Reg_139	Verify the QBSS load information in Beacon and Probes fames by configuring WMM as allowed with qbss load for policy profile.	To check whether QBSS load showing in Beacon and Probe frames or not by configuring WMM as allowed with qbss load for policy profile.	Passed	

EWLCJ176_2S_Reg_140	Verify the QBSS load information in Beacon and Probes fames by configuring WMM as Required with qbss load for policy profile.	To check whether QBSS load showing in Beacon and Probe frames or not by configuring WMM as required with qbss load for policy profile	Passed	
EWLCJ176_2S_Reg_141	Verify the QBSS load information in Beacon and Probes fames by configuring WMM as Required with no qbss load for policy profile.	To check whether QBSS load showing in Beacon and Probe frames or not by configuring WMM as allowed with no qbss load for policy profile.	Passed	
EWLCJ176_2S_Reg_142	Verify the QBSS load information in Beacon and Probes fames by configuring WMM as Required with qbss load for local_auth policy profile.	To check whether QBSS load showing in Beacon and Probe frames or not by configuring WMM as required with qbss load for Local_auth policy profile	Passed	
EWLCJ176_2S_Reg_143	Verify the QBSS load information in Beacon and Probes fames by upload/download the configuration file from controller	To check whether QBSS load showing in Beacon and Probe frames or not by upload/download the configuration file from controller	Passed	
EWLCJ176_2S_Reg_144	Verify the QBSS load information in Beacon and Probes fames by configuring WMM as Required with qbss load for policy profile and Flexmode AP.	To check whether QBSS load showing in Beacon and Probe frames or not by configuring WMM as required with qbss load for policy profile and Flexmode AP	Passed	

EWLCJ176_2S_Reg_145	Verify the QBSS load information in Beacon and Probes fames by configuring WMM as Required with qbss load for policy profile and Bridge mode AP.	To check whether QBSS load showing in Beacon and Probe frames or not by configuring WMM as required with qbss load for policy profile and Bridge mode AP	Passed	
EWLCJ176_2S_Reg_146	Verify the AP name in Beacon and Probes fames by configuring Aironet IE.	To check whether AP name in Beacon and Probes fames by configuring Aironet IE.	Passed	
EWLCJ176_2S_Reg_147	Verify the AP name in Beacon and Probes fames by configuring Aironet IE with modified AP name.	To check whether AP name in Beacon and Probes fames by configuring Aironet IE with Modified AP name.	Passed	
EWLCJ176_2S_Reg_148	Verify the AP name in Beacon and Probes fames by configuring Aironet IE and upload/download the configuration file from controller.	To check whether AP name in Beacon and Probes fames by configuring Aironet IE and upload/download the configuration file from controller.	Passed	
EWLCJ176_2S_Reg_149	Verify the AP name in Beacon and Probes fames by configuring Aironet IE with more than 15 characters of AP name.	To check whether AP name in Beacon and Probes fames by configuring Aironet IE with more than 15 characters of AP name.	Passed	
EWLCJ176_2S_Reg_150	Verify the AP name in Beacon and Probes fames by configuring Aironet IE and rejoin the AP's to eWLC-2 from eWLC-1.	To check whether AP name in Beacon and Probes fames by configuring Aironet IE and rejoin the AP's to eWLC-2 from eWLC-1.	Passed	

EWLCJ176_2S_Reg_151	Verify the Multicast filter and MC2UC traffic to local-switching client	To verify the Multicast filter and local-switching client subscribed to video streaming receives MC2UC traffic	Passed	
EWLCJ176_2S_Reg_152	Verify the Multicast filter and MC2UC traffic to Central-switching client	To verify the Multicast filter and central-switching client subscribed to video streaming receives MC2UC traffic	Passed	
EWLCJ176_2S_Reg_153	Verify the Multicast filter and Flex AP reboot in connected mode when Flex LS client receiving MC2UC traffic	To verify whether client reassociates and receives MC2UC traffic when flex AP is rebooted in connected mode with multicast filter.	Passed	
EWLCJ176_2S_Reg_154	Verify the Multicast filter and MC2UC traffic to Central-switching client after Download/upload the configuration file to controller	To verify the Multicast filter client subscribed to video streaming receives MC2UC traffic after download/upload the configuration file from controller	Passed	

OKC

Logical ID	Title	Description	Status	Defect ID
EWLCJ176S_Reg_23	Configure and verify the OKC to the WLAN configuration.	To check whether OKC configured to WLAN or not.	Passed	
EWLCJ176S_Reg_24	Configure and verify the OKC to WPA3-SAE WLAN with Inter roaming.	To check whether roaming happening or not after configuring the OKC to WPA3-SAE WLAN.	Passed	
EWLCJ176S_Reg_25	Configure and verify the OKC to WPA3-SAE WLAN with Intra roaming.	To check whether intra roaming happening or not after configuring the OKC to WPA3-SAE WLAN.	Passed	
EWLCJ176S_Reg_26	Configure and verify the OKC to WPA2-PSK WLAN with Inter roaming.	To check whether roaming happening or not after configuring the OKC to WPA2-PSK WLAN.	Passed	
EWLCJ176S_Reg_27	Configure and verify the OKC to WPA2-PSK WLAN with Intra roaming.	To check whether intra roaming happening or not after configuring the OKC to WPA2-PSK WLAN.	Passed	
EWLCJ176S_Reg_28	Configure and verify the OKC to OPEN security WLAN with Inter roaming.	To check whether roaming happening or not after configuring the OKC to OPEN security WLAN.	Passed	

EWLCJ176S_Reg_29	Configure and verify the OKC to OPEN security WLAN with Intra roaming.	To check whether intra roaming happening or not after configuring the OKC to OPEN security WLAN.	Passed	
EWLCJ176S_Reg_30	Configure and verify the OKC to WPA2-802.1x WLAN with Inter roaming.	To check whether roaming happening or not after configuring the OKC to WPA2-802.1x WLAN.	Passed	
EWLCJ176S_Reg_31	Configure and verify the OKC to WPA2-802.1x WLAN with Intra roaming.	To check whether intra roaming happening or not after configuring the OKC to WPA2-802.1x WLAN.	Passed	
EWLCJ176S_Reg_32	Configure and verify the OKC to WPA3-802.1x WLAN with Inter roaming.	To check whether roaming happening or not after configuring the OKC to WPA3-802.1x WLAN.	Passed	
EWLCJ176S_Reg_33	Configure and verify the OKC to WPA3-802.1x WLAN with Intra roaming.	To check whether intra roaming happening or not after configuring the OKC to WPA3-802.1x WLAN.	Passed	
EWLCJ176S_Reg_34	Configure and verify the OKC to WPA2-Ft-PSK WLAN with Inter roaming.	To check whether roaming happening or not after configuring the OKC to WPA2-Ft-PSK WLAN.	Passed	
EWLCJ176S_Reg_35	Configure and verify the OKC to WPA2-Ft-PSKWLAN with Intra roaming.	To check whether intra roaming happening or not after configuring the OKC to WPA2-Ft-PSK WLAN.	Passed	

EWLCJ176S_Reg_36	Configure and verify the OKC to WPA2-Ft-802.1x WLAN with Inter roaming.	To check whether roaming happening or not after configuring the OKC to WPA2-Ft-802.1x WLAN.	Passed	
EWLCJ176S_Reg_37	Configure and verify the OKC to WPA2-Ft-802.1x WLAN with Intra roaming.	To check whether intra roaming happening or not after configuring the OKC to WPA2-Ft-802.1x WLAN.	Passed	
EWLCJ176S_Reg_38	Configure and verify the OKC to WPA2+WPA3 mixed mode WLAN with Inter roaming.	To check whether roaming happening or not after configuring the OKC to WPA2+WPA3 mixed mode WLAN.	Passed	
EWLCJ176S_Reg_39	Configure and verify the OKC to WPA2+WPA3 mixed mode WLAN with Intra roaming.	To check whether intra roaming happening or not after configuring the OKC to WPA2+WPA3 mixed mode WLAN.	Passed	
EWLCJ176_2S_Reg_155	Configure and verify the OKC to the WLAN configuration.	To check whether OKC configured to WLAN or not.	Passed	
EWLCJ176_2S_Reg_156	Configure and verify the OKC to WPA3-SAE WLAN with Inter roaming.	To check whether roaming happening or not after configuring the OKC to WPA3-SAE WLAN.	Passed	
EWLCJ176_2S_Reg_157	Configure and verify the OKC to WPA3-SAE WLAN with Intra roaming.	To check whether intra roaming happening or not after configuring the OKC to WPA3-SAE WLAN.	Passed	

EWLCJ176_2S_Reg_158	Configure and verify the OKC to WPA2-PSK WLAN with Inter roaming.	To check whether roaming happening or not after configuring the OKC to WPA2-PSK WLAN.	Passed	
EWLCJ176_2S_Reg_159	Configure and verify the OKC to WPA2-PSK WLAN with Intra roaming.	To check whether intra roaming happening or not after configuring the OKC to WPA2-PSK WLAN.	Passed	
EWLCJ176_2S_Reg_160	Configure and verify the OKC to OPEN security WLAN with Inter roaming.	To check whether roaming happening or not after configuring the OKC to OPEN security WLAN.	Passed	
EWLCJ176_2S_Reg_161	Configure and verify the OKC to OPEN security WLAN with Intra roaming.	To check whether intra roaming happening or not after configuring the OKC to OPEN security WLAN.	Passed	
EWLCJ176_2S_Reg_162	Configure and verify the OKC to WPA2-802.1x WLAN with Inter roaming.	To check whether roaming happening or not after configuring the OKC to WPA2-802.1x WLAN.	Passed	
EWLCJ176_2S_Reg_163	Configure and verify the OKC to WPA2-802.1x WLAN with Intra roaming.	To check whether intra roaming happening or not after configuring the OKC to WPA2-802.1x WLAN.	Passed	
EWLCJ176_2S_Reg_164	Configure and verify the OKC to WPA3-802.1x WLAN with Inter roaming.	To check whether roaming happening or not after configuring the OKC to WPA3-802.1x WLAN.	Passed	

EWLCJ176_2S_Reg_165	Configure and verify the OKC to WPA3-802.1x WLAN with Intra roaming.	To check whether intra roaming happening or not after configuring the OKC to WPA3-802.1x WLAN.	Passed	
EWLCJ176_2S_Reg_166	Configure and verify the OKC to WPA2-Ft-PSK WLAN with Inter roaming.	To check whether roaming happening or not after configuring the OKC to WPA2-Ft-PSK WLAN.	Passed	
EWLCJ176_2S_Reg_167	Configure and verify the OKC to WPA2-Ft-PSKWLAN with Intra roaming.	To check whether intra roaming happening or not after configuring the OKC to WPA2-Ft-PSK WLAN.	Passed	
EWLCJ176_2S_Reg_168	Configure and verify the OKC to WPA2-Ft-802.1x WLAN with Inter roaming.	To check whether roaming happening or not after configuring the OKC to WPA2-Ft-802.1x WLAN.	Passed	
EWLCJ176_2S_Reg_169	Configure and verify the OKC to WPA2-Ft-802.1x WLAN with Intra roaming.	To check whether intra roaming happening or not after configuring the OKC to WPA2-Ft-802.1x WLAN.	Passed	
EWLCJ176_2S_Reg_170	Configure and verify the OKC to WPA2+WPA3 mixed mode WLAN with Inter roaming.	To check whether roaming happening or not after configuring the OKC to WPA2+WPA3 mixed mode WLAN.	Passed	

EWLCJ176_2S_Reg_171	Configure and verify the OKC to WPA2+WPA3 mixed mode WLAN with Intra roaming.	To check whether intra roaming happening or not after configuring the OKC to WPA2+WPA3 mixed mode WLAN.	Passed	

TWT support on 9130 AP

Logical ID	Title	Description	Status	Defect ID
EWLCJ176S_Reg_40	Configuring TWT in 9130 Ap	To check Whether 9130 Ap get TWT parameter details properly	Passed	
EWLCJ176S_Reg_41	Configuring TWT in 9120 Ap	To check Whether 9120 Ap get TWT parameter details properly	Passed	
EWLCJ176S_Reg_42	Associate 5G Hz client to 9130 Ap with TWT configuration.	To verify the 5GHz client associate the 9130 Ap with TWT configuration or not	Passed	
EWLCJ176S_Reg_43	Associate 2.4 GHz client to 9115/9120/9130 Ap with TWT configuration.	To verify the 2.4 GHz client associate the 9115/9120/9130 Ap with TWT configuration or not	Passed	
EWLCJ176S_Reg_44	Configuring TWT in 11ax Ap with flex connect mode	To verify the 11ax ap get TWT parameter in flex connect mode	Passed	
EWLCJ176S_Reg_45	Configuring TWT in 11ax Ap with Local mode	To verify the 11ax ap get TWT parameter in Local mode	Passed	
EWLCJ176S_Reg_46	Associate the sleeping client with 11ax Ap	To Verify sleeping client associate with 11ax Ap properly or not	Passed	
EWLCJ176S_Reg_47	Clear the TWT configuration Check the Client behaviour	To verify the client behaviour after clear the TWT configuration	Passed	

WPA3-support

Logical ID	Title	Description	Status	Defect ID
EWLCJ176S_Reg_48	Verifying the WPA3 support with SAE Auth key.	To verify the WPA3 support with SAE security Configuration.	Passed	
EWLCJ176S_Reg_49	Verifying the WPA3 support with SAE security key by connecting the windows client.	To verify the Client packets by connecting the windows client to WPA3 and SAE supported SSID	Passed	CSCvx28625
EWLCJ176S_Reg_50	Verifying the WPA3 support with SAE security key by connecting the Android client.	To verify the Client packets by connecting the Android client to WPA3 and SAE supported SSID	Passed	
EWLCJ176S_Reg_51	Verifying the WPA3 support with SAE security key by connecting the Mac os client.	To verify the Client packets by connecting the Mac os client to WPA3 and SAE supported SSID	Passed	CSCvx72977
EWLCJ176S_Reg_52	Verifying the WPA3 support with SAE and PSK security key.	To verify the Client packets by connecting the client to WPA3 and SAE and PSK supported SSID	Passed	
EWLCJ176S_Reg_53	Verifying the WPA3 support with SAE and 802.1x security key.	To verify the WPA3 Configuration with SAE and 802.1x supported SSID	Passed	
EWLCJ176S_Reg_54	Validating the WPA3 support with SAE and Layer 3 Splash page web redirect	To verify the WPA3 support with SAE and Layer3 Splash page web redirect	Passed	
EWLCJ176S_Reg_55	Validating the WPA3 support with SAE and Layer 3 On Mac filter failure.	To verify the WPA3 support with SAE and Layer3 On Mac filter failure	Passed	

EWLCJ176S_Reg_56	verifying the WPA3 support with SAE and PMF PSK Auth key.	To verify the WPA3 support with SAE and PMF PSK Auth key.	Passed	
EWLCJ176S_Reg_57	verifying the WPA3 support with SAE and PSK Auth key and Layer3 Splash page web redirect.	To verify the WPA3 support with SAE and PSK Auth key and Layer3 Splash page web redirect.	Passed	CSCvx84590
EWLCJ176S_Reg_58	Verifying the WPA3 support with 802.1x security.	To verify the WPA3 support with 802.1x security for the different clients.	Passed	
EWLCJ176S_Reg_59	Verifying the WPA3 support with 802.1x and CCKM security.	To verify the WPA3 support with 802.1x and CCKM security for the different clients.	Passed	
EWLCJ176S_Reg_60	Verifying the WPA3 support with Ft+802.1x security.	To verify the WPA3 support with +Ft_802.1x security for the different clients.	Passed	
EWLCJ176S_Reg_61	Verifying the WPA3 support with Intra client roaming by using 9115AP	To verify the Intra client roaming by using WPA3 support with 9115AP	Passed	
EWLCJ176S_Reg_62	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	
EWLCJ176S_Reg_63	Verifying the WPA3 support with Roaming between Controllers with Different Radio types	To verify whether Client is Moving between Controllers with Different Radio type or not with WPA3 WLAN.	Failed	CSCvx73022
EWLCJ176S_Reg_64	Verifying the WPA3 support Roaming between Controllers with same Radio types	To verify whether Client is Moving between Controllers with same Radio type or not with WPA3 WLAN.	Passed	

EWLCJ176S_Reg_65	Verifying the WPA3 support with SAE Auth key in local auth and local switching.	To verify the WPA3 support with SAE security in local auth and local switching.	Passed	

Mesh(Flex + Mesh) support on all 11ac Wave 2 Indoor APs

Logical ID	Title	Description	Status	Defect ID
EWLCJ176S_Reg_66	Verifying the Mesh configuration.	To check whether the Mesh configurations are configuring correct or not.	Passed	
EWLCJ176S_Reg_67	Check the Joining of 3800AP in to eWLC with Mesh /Bridge Mode	To check the Mesh/Bridge support of 3800 AP after joining in to eWLC	Passed	CSCvx91066
EWLCJ176S_Reg_68	Check the Joining of 3800AP in to eWLC with Flex Bridge Mode	To check the Flex Bridge Mode support of 3800 AP in to eWLC	Passed	
EWLCJ176S_Reg_69	Check the Joining of 4800AP in to eWLC with Mesh/Bridge Mode	To check the Mesh/Bridge support of 4800 AP after joining in to eWLC	Passed	
EWLCJ176S_Reg_70	Check the Joining of 4800AP in to eWLC with Flex Bridge Mode	To check the Flex Bridge Mode support of 4800 AP in to eWLC	Passed	
EWLCJ176S_Reg_71	Verify the Windows clients connection for bridge mode AP's with WEP security	To check whether the windows client is connected or not to bridge mode AP's	Passed	CSCvx89610
EWLCJ176S_Reg_72	Verify the Android clients connection for bridge mode AP's with WEP security	To check whether the Android client is connected or not to bridge mode AP's	Passed	
EWLCJ176S_Reg_73	Verify the IOS clients connection for bridge mode AP's with WEP security	To check whether the IOS client is connected or not to bridge mode AP's	Passed	

EWLCJ176S_Reg_74	Verify the Windows clients connection for Flex bridge mode AP's with WEP security	To check whether the windows client is connected or not to Flex bridge mode AP's	Passed	
EWLCJ176S_Reg_75	Verify the Android clients connection for Flex bridge mode AP's with WEP security	To check whether the Android client is connected or not to Flex bridge mode AP's	Passed	
EWLCJ176S_Reg_76	Verify the IOS clients connection for Flex bridge mode AP's with WEP security	To check whether the IOS client is connected or not to Flex bridge mode AP's	Passed	
EWLCJ176S_Reg_77	Verify the Windows clients connection for bridge mode AP's with WPA2-PSk security	To check whether the windows client is connected or not to bridge mode AP's with WPA2-PSK security	Passed	
EWLCJ176S_Reg_78	Verify the Android clients connection for bridge mode AP's with WPA2-PSK security	To check whether the Android client is connected or not to bridge mode AP's with WPA2-PSK security	Passed	
EWLCJ176S_Reg_79	Verify the IOS clients connection for bridge mode AP's with WPA2-PSK security	To check whether the IOS client is connected or not to bridge mode AP's with WPA2-PSK security	Passed	
EWLCJ176S_Reg_80	Verify the Windows clients connection for Flex bridge mode AP's with WPA2-PSK security	To check whether the windows client is connected or not to Flex bridge mode AP's with WPA2-PSK security	Passed	
EWLCJ176S_Reg_81	Verify the Android clients connection for Flex bridge mode AP's with WPA2-PSK security	To check whether the Android client is connected or not to Flex bridge mode AP's with WPA2-PSK security	Passed	CSCvy09686

EWLCJ176S_Reg_82	Verify the IOS clients connection for Flex bridge mode AP's with WPA2-PSK security	To check whether the IOS client is connected or not to Flex bridge mode AP's with WPA2-PSK security	Passed	
EWLCJ176S_Reg_83	Verify the Windows clients connection for bridge mode AP's with WPA3-SAE security	To check whether the windows client is connected or not to bridge mode AP's with WPA3-SAE security	Passed	
EWLCJ176S_Reg_84	Verify the Android clients connection for bridge mode AP's with WPA3-SAE security	To check whether the Android client is connected or not to bridge mode AP's with WPA3-SAE security	Passed	
EWLCJ176S_Reg_85	Verify the IOS clients connection for bridge mode AP's with WPA3-SAE security	To check whether the IOS client is connected or not to bridge mode AP's with WPA3-SAE security	Passed	
EWLCJ176S_Reg_86	Verify the Windows clients connection for Flex bridge mode AP's with WPA3-SAE security	To check whether the windows client is connected or not to Flex bridge mode AP's with WPA3-SAE security	Passed	
EWLCJ176S_Reg_87	Verify the Android clients connection for Flex bridge mode AP's with WPA3-SAE security	To check whether the Android client is connected or not to Flex bridge mode AP's with WPA3-SAEsecurity	Passed	
EWLCJ176S_Reg_88	Verify the IOS clients connection for Flex bridge mode AP's with WPA3-SAE security	To check whether the IOS client is connected or not to Flex bridge mode AP's with WPA3-SAE security	Passed	

EWLCJ176S_Reg_89	Check and verify the AP mode changes by changing From bridge mode to local	To check whether AP mode changing or not from bridge to local	Passed	
EWLCJ176S_Reg_90	Check and verify the AP mode changes by changing From Flex bridge mode to Flex connect.	To check whether AP mode changing or not from Flex bridge to Flex connect.	Passed	
EWLCJ176S_Reg_91	Check and verify the intra roaming with bridge mode AP	To check whether intra roaming happening or not with bridge mode Ap's	Passed	
EWLCJ176S_Reg_92	Check and verify the intra roaming with Flex bridge mode AP	To check whether intra roaming happening or not with Flex bridge mode Ap's	Passed	
EWLCJ176_2S_Reg_172	Verifying the Mesh configuration.	To check whether the Mesh configurations are configuring correct or not.	Passed	CSCvy27162
EWLCJ176_2S_Reg_173	Check the Joining of 3800AP in to eWLC with Mesh /Bridge Mode	To check the Mesh/Bridge support of 3800 AP after joining in to eWLC	Passed	
EWLCJ176_2S_Reg_174	Check the Joining of 3800AP in to eWLC with Flex+Bridge Mode	To check the Flex+Bridge Mode support of 3800 AP in to eWLC	Passed	
EWLCJ176_2S_Reg_175	Check the Joining of 4800AP in to eWLC with Mesh/Bridge Mode	To check the Mesh/Bridge support of 4800 AP after joining in to eWLC	Passed	
EWLCJ176_2S_Reg_176	Check the Joining of 4800AP in to eWLC with Flex+Bridge Mode	To check the Flex+Bridge Mode support of 4800 AP in to eWLC	Passed	

EWLCJ176_2S_Reg_177	Verify the Windows clients connection for bridge mode AP's with WEP security	To check whether the windows client is connected or not to bridge mode AP's	Passed	
EWLCJ176_2S_Reg_178	Verify the Android clients connection for bridge mode AP's with WEP security	To check whether the Android client is connected or not to bridge mode AP's	Passed	
EWLCJ176_2S_Reg_179	Verify the IOS clients connection for bridge mode AP's with WEP security	To check whether the IOS client is connected or not to bridge mode AP's	Passed	
EWLCJ176_2S_Reg_180	Verify the Windows clients connection for Flex+bridge mode AP's with WEP security	To check whether the windows client is connected or not to Flex+bridge mode AP's	Passed	
EWLCJ176_2S_Reg_181	Verify the Android clients connection for Flex+bridge mode AP's with WEP security	To check whether the Android client is connected or not to Flex+bridge mode AP's	Passed	
EWLCJ176_2S_Reg_182	Verify the IOS clients connection for Flex+bridge mode AP's with WEP security	To check whether the IOS client is connected or not to Flex+bridge mode AP's	Passed	
EWLCJ176_2S_Reg_183	Verify the Windows clients connection for bridge mode AP's with WPA2-PSk security	To check whether the windows client is connected or not to bridge mode AP's with WPA2-PSK security	Passed	
EWLCJ176_2S_Reg_184	Verify the Android clients connection for bridge mode AP's with WPA2-PSK security	To check whether the Android client is connected or not to bridge mode AP's with WPA2-PSK security	Passed	

EWLCJ176_2S_Reg_185	Verify the IOS clients connection for bridge mode AP's with WPA2-PSK security	To check whether the IOS client is connected or not to bridge mode AP's with WPA2-PSK security	Passed	
EWLCJ176_2S_Reg_186	Verify the Windows clients connection for Flex+bridge mode AP's with WPA2-PSK security	To check whether the windows client is connected or not to Flex+bridge mode AP's with WPA2-PSK security	Passed	
EWLCJ176_2S_Reg_187	Verify the Android clients connection for Flex+bridge mode AP's with WPA2-PSK security	To check whether the Android client is connected or not to Flex+bridge mode AP's with WPA2-PSK security	Passed	
EWLCJ176_2S_Reg_188	Verify the IOS clients connection for Flex+bridge mode AP's with WPA2-PSK security	To check whether the IOS client is connected or not to Flex+bridge mode AP's with WPA2-PSK security	Passed	
EWLCJ176_2S_Reg_189	Verify the Windows clients connection for bridge mode AP's with WPA3-SAE security	To check whether the windows client is connected or not to bridge mode AP's with WPA3-SAE security	Passed	
EWLCJ176_2S_Reg_190	Verify the Android clients connection for bridge mode AP's with WPA3-SAE security	To check whether the Android client is connected or not to bridge mode AP's with WPA3-SAE security	Passed	
EWLCJ176_2S_Reg_191	Verify the IOS clients connection for bridge mode AP's with WPA3-SAE security	To check whether the IOS client is connected or not to bridge mode AP's with WPA3-SAE security	Passed	

EWLCJ176_2S_Reg_192	Verify the Windows clients connection for Flex+bridge mode AP's with WPA3-SAE security	To check whether the windows client is connected or not to Flex+bridge mode AP's with WPA3-SAE security	Passed	
EWLCJ176_2S_Reg_193	Verify the Android clients connection for Flex+bridge mode AP's with WPA3-SAE security	To check whether the Android client is connected or not to Flex+bridge mode AP's with WPA3-SAEsecurity	Passed	
EWLCJ176_2S_Reg_194	Verify the IOS clients connection for Flex+bridge mode AP's with WPA3-SAE security	To check whether the IOS client is connected or not to Flex+bridge mode AP's with WPA3-SAE security	Passed	
EWLCJ176_2S_Reg_195	Check and verify the AP mode changes by changing From bridge mode to local	To check whether AP mode changing or not from bridge to local	Passed	
EWLCJ176_2S_Reg_196	Check and verify the AP mode changes by changing From Flex+bridge mode to Flex connect.	To check whether AP mode changing or not from Flex+bridge to Flex connect.	Passed	
EWLCJ176_2S_Reg_197	Check and verify the intra roaming with bridge mode AP	To check whether intra roaming happening or not with bridge mode Ap's	Passed	
EWLCJ176_2S_Reg_198	Check and verify the intra roaming with Flex+bridge mode AP	To check whether intra roaming happening or not with Flex+bridge mode Ap's	Passed	

mDNS Support for Wired Guest Access and Ap support

Logical ID	Title	Description	Status	Defect ID
EWLCJ176S_Reg_93	Create the Guest Lan with mDNS Mode Bridging Gateway and Verify with Apple TV	Verify able to create the Guest Lan with mDNS Mode Bridging with Apple TV	Passed	
EWLCJ176S_Reg_94	Create the Guest Lan with mDNS Mode Bridging.	Verify able to create the Guest Lan with mDNS Mode Bridging.	Passed	
EWLCJ176S_Reg_95	Edit the Guest Lan with mDNS Mode Bridging.	Verify able to edit the Guest Lan with mDNS Mode Bridging.	Passed	
EWLCJ176S_Reg_96	Delete the Guest Lan with mDNS Mode Bridging.	Verify able to Delete the Guest Lan with mDNS Mode Bridging.	Passed	
EWLCJ176S_Reg_97	Create the Guest Lan with mDNS Mode Bridging with Guest LAN Map Configuration.	Verify able to create with the Guest Lan with mDNS Mode Bridging.	Passed	
EWLCJ176S_Reg_98	Delete the Guest Lan with mDNS Mode Bridging with Guest LAN Map Configuration.	Verify able to Delete with the Guest Lan with mDNS Mode Bridging.	Passed	
EWLCJ176S_Reg_99	Create the Guest Lan with mDNS Mode Gateway: .	Verify able to Create the Guest Lan with mDNS Mode Bridging Gateway: .	Passed	
EWLCJ176S_Reg_100	Create the Guest Lan with mDNS Mode Bridging Drop.	verify able to Create the Guest Lan with mDNS Mode Drop.	Passed	
EWLCJ176_2S_Reg_199	Create the Guest Lan with mDNS Mode Bridging Gateway and Verify with Apple TV	Verify able to create the Guest Lan with mDNS Mode Bridging with Apple TV	Passed	CSCvy36350

EWLCJ176_2S_Reg_200	Create the Guest Lan with mDNS Mode Bridging.	Verify able to create the Guest Lan with mDNS Mode Bridging.	Passed	
EWLCJ176_2S_Reg_201	Edit the Guest Lan with mDNS Mode Bridging.	Verify able to edit the Guest Lan with mDNS Mode Bridging.	Passed	
EWLCJ176_2S_Reg_202	Delete the Guest Lan with mDNS Mode Bridging.	Verify able to Delete the Guest Lan with mDNS Mode Bridging.	Passed	
EWLCJ176_2S_Reg_203	Create the Guest Lan with mDNS Mode Bridging with Guest LAN Map Configuration.	Verify able to create with the Guest Lan with mDNS Mode Bridging.	Passed	
EWLCJ176_2S_Reg_204	Delete the Guest Lan with mDNS Mode Bridging with Guest LAN Map Configuration.	Verify able to Delete with the Guest Lan with mDNS Mode Bridging.	Passed	
EWLCJ176_2S_Reg_205	Create the Guest Lan with mDNS Mode Gateway: .	Verify able to Create the Guest Lan with mDNS Mode Bridging Gateway: .	Passed	
EWLCJ176_2S_Reg_206	Create the Guest Lan with mDNS Mode Bridging Drop.	verify able to Create the Guest Lan with mDNS Mode Drop.	Passed	

PSK + Mulit Auth Support for Guest

Logical ID	Title	Description	Status	Defect ID
EWLCJ176S_Reg_101	Creating Wlan with WPA2 Security with MPSK	Verify Wlan Creating with WPA2 Security with MPSK	Passed	
EWLCJ176S_Reg_102	Edit WPA2 Security PSK Keys on MPSK	Verify Wlan Edit with WPA2 Security with MPSK	Passed	
EWLCJ176S_Reg_103	Delete WPA2 Security PSK Keys on MPSK	Verify Wlan Delete with WPA2 Security with MPSK	Passed	
EWLCJ176S_Reg_104	Creating Wlan with WPA2 Security with MPSK - Format with Hexa:	Verify Creating Wlan with WPA2 Security with MPSK - Format with Hexa:	Passed	
EWLCJ176S_Reg_105	Creating Wlan with WPA2 Security with MPSK - Password Type : AES :	Verify the Security Type with Advance Security	Passed	
EWLCJ176S_Reg_106	Verify WPA2 Security with MPSK Applied in Wlan's with Window's Clients with all the 5 Key Combinations	Verify WPA2 Security with MPSK Applied in Wlan's with Window's Clients with all the 5 Key Combinations	Passed	
EWLCJ176S_Reg_107	Connect the MAC Clients	Verify Connect the MAC Clients with all the 5 Key Combinations	Passed	
EWLCJ176S_Reg_108	Connect the Android Clients	Verify Connect the Android Clients with all the 5 Key Combinations:	Passed	
EWLCJ176S_Reg_109	Connect the Apple Mobile Clients with all the 5 Key Combinations:	Verify Connect the Apple Clients with all the 5 Key Combinations:	Passed	

EWLCJ176S_Reg_110	Connect the Windows Clients with all the 5 Key Combinations:	Verify Connect the Windows Clients with all the 5 Key Combinations:	Passed	
EWLCJ176S_Reg_111	MPSK with Ap Model 9115	Verify the Configurations with Ap Different Ap Model 9115	Passed	
EWLCJ176S_Reg_112	Connect Ap Model 9120	Verify the Configurations with Ap Different Ap Model 9120:	Passed	
EWLCJ176S_Reg_113	Connect Ap Model 4800	Verify the Configurations with Ap Different Ap Model 4800:	Passed	
EWLCJ176S_Reg_114	Connect Ap Model 3800	Verify the Configurations with Ap Different Ap Model 3800	Passed	
EWLCJ176S_Reg_115	Connect Ap Model 3700	Verify the Configurations with Ap Different Ap Model 3700	Passed	
EWLCJ176S_Reg_116	Connect Ap Model 1532	Verify the Configurations with Ap Different Ap Model 1532:	Passed	
EWCJ176S_Reg_40	Creating Wlan with WPA2 Security with MPSK	Verify Wlan Creating with WPA2 Security with MPSK	Passed	
EWCJ176S_Reg_41	Edit WPA2 Security PSK Keys on MPSK	Verify Wlan Edit with WPA2 Security with MPSK	Passed	
EWCJ176S_Reg_42	Delete WPA2 Security PSK Keys on MPSK	Verify Wlan Delete with WPA2 Security with MPSK	Passed	
EWCJ176S_Reg_43	Creating Wlan with WPA2 Security with MPSK - Format with Hexa:	Verify Creating Wlan with WPA2 Security with MPSK - Format with Hexa:	Passed	

EWCJ176S_Reg_44	Creating Wlan with WPA2 Security with MPSK - Password Type : AES :	Verify the Security Type with Advance Security	Passed	
EWCJ176S_Reg_45	Verify WPA2 Security with MPSK Applied in Wlan's with Window's Clients with all the 5 Key Combinations	Verify WPA2 Security with MPSK Applied in Wlan's with Window's Clients with all the 5 Key Combinations	Passed	CSCvx26327
EWCJ176S_Reg_46	Connect the MAC Clients	Verify Connect the MAC Clients with all the 5 Key Combinations	Passed	
EWCJ176S_Reg_47	Connect the Android Clients	Verify Connect the Android Clients with all the 5 Key Combinations:	Passed	
EWCJ176S_Reg_48	Connect the Apple Mobile Clients with all the 5 Key Combinations:	Verify Connect the Apple Clients with all the 5 Key Combinations:	Passed	
EWCJ176S_Reg_49	Connect the Windows Clients with all the 5 Key Combinations:	Verify Connect the Windows Clients with all the 5 Key Combinations:	Passed	
EWCJ176S_Reg_50	MPSK with Ap Model 9115	Verify the Configurations with Ap Different Ap Model 9115	Passed	
EWCJ176S_Reg_51	Connect Ap Model 9120	Verify the Configurations with Ap Different Ap Model 9120:	Passed	
EWCJ176S_Reg_52	Connect Ap Model 4800	Verify the Configurations with Ap Different Ap Model 4800:	Passed	
EWCJ176S_Reg_53	Connect Ap Model 3800	Verify the Configurations with Ap Different Ap Model 3800	Passed	

EWCJ176S_Reg_54	Connect Ap Model 3700	Verify the Configurations with Ap Different Ap Model 3700	Passed	
EWCJ176S_Reg_55	Connect Ap Model 1532	Verify the Configurations with Ap Different Ap Model 1532:	Passed	
EWLCJ176_2S_Reg_207	Creating Wlan with WPA2 Security with MPSK	Verify Wlan Creating with WPA2 Security with MPSK	Passed	
EWLCJ176_2S_Reg_208	Edit WPA2 Security PSK Keys on MPSK	Verify Wlan Edit with WPA2 Security with MPSK	Passed	
EWLCJ176_2S_Reg_209	Delete WPA2 Security PSK Keys on MPSK	Verify Wlan Delete with WPA2 Security with MPSK	Passed	
EWLCJ176_2S_Reg_210	Creating Wlan with WPA2 Security with MPSK - Format with Hexa:	Verify Creating Wlan with WPA2 Security with MPSK - Format with Hexa:	Passed	
EWLCJ176_2S_Reg_211	Creating Wlan with WPA2 Security with MPSK - Password Type : AES :	Verify the Security Type with Advance Security	Passed	
EWLCJ176_2S_Reg_212	Verify WPA2 Security with MPSK Applied in Wlan's with Window's Clients with all the 5 Key Combinations	Verify WPA2 Security with MPSK Applied in Wlan's with Window's Clients with all the 5 Key Combinations	Passed	
EWLCJ176_2S_Reg_213	Connect the MAC Clients	Verify Connect the MAC Clients with all the 5 Key Combinations	Passed	
EWLCJ176_2S_Reg_214	Connect the Android Clients	Verify Connect the Android Clients with all the 5 Key Combinations:	Passed	

EWLCJ176_2S_Reg_215	Connect the Apple Mobile Clients with all the 5 Key Combinations:	Verify Connect the Apple Clients with all the 5 Key Combinations:	Passed	
EWLCJ176_2S_Reg_216	Connect the Windows Clients with all the 5 Key Combinations:	Verify Connect the Windows Clients with all the 5 Key Combinations:	Passed	
EWLCJ176_2S_Reg_217	MPSK with Ap Model 9115	Verify the Configurations with Ap Different Ap Model 9115	Passed	
EWLCJ176_2S_Reg_218	Connect Ap Model 9120	Verify the Configurations with Ap Different Ap Model 9120:	Passed	
EWLCJ176_2S_Reg_219	Connect Ap Model 4800	Verify the Configurations with Ap Different Ap Model 4800:	Passed	
EWLCJ176_2S_Reg_220	Connect Ap Model 3800	Verify the Configurations with Ap Different Ap Model 3800	Passed	
EWLCJ176_2S_Reg_221	Connect Ap Model 3700	Verify the Configurations with Ap Different Ap Model 3700	Passed	
EWLCJ176_2S_Reg_222	Connect Ap Model 1532	Verify the Configurations with Ap Different Ap Model 1532:	Passed	
EWCJ176_2S_Reg_60	Creating Wlan with WPA2 Security with MPSK	Verify Wlan Creating with WPA2 Security with MPSK	Passed	
EWCJ176_2S_Reg_61	Edit WPA2 Security PSK Keys on MPSK	Verify Wlan Edit with WPA2 Security with MPSK	Passed	
EWCJ176_2S_Reg_62	Delete WPA2 Security PSK Keys on MPSK	Verify Wlan Delete with WPA2 Security with MPSK	Passed	

EWCJ176_2S_Reg_63	Creating Wlan with WPA2 Security with MPSK - Format with Hexa:	Verify Creating Wlan with WPA2 Security with MPSK - Format with Hexa:	Passed	CSCvy34614
EWCJ176_2S_Reg_64	Creating Wlan with WPA2 Security with MPSK - Password Type : AES :	Verify the Security Type with Advance Security	Passed	
EWCJ176_2S_Reg_65	Verify WPA2 Security with MPSK Applied in Wlan's with Window's Clients with all the 5 Key Combinations	Verify WPA2 Security with MPSK Applied in Wlan's with Window's Clients with all the 5 Key Combinations	Passed	
EWCJ176_2S_Reg_66	Connect the MAC Clients	Verify Connect the MAC Clients with all the 5 Key Combinations	Passed	
EWCJ176_2S_Reg_67	Connect the Android Clients	Verify Connect the Android Clients with all the 5 Key Combinations:	Passed	
EWCJ176_2S_Reg_68	Connect the Apple Mobile Clients with all the 5 Key Combinations:	Verify Connect the Apple Clients with all the 5 Key Combinations:	Passed	
EWCJ176_2S_Reg_69	Connect the Windows Clients with all the 5 Key Combinations:	Verify Connect the Windows Clients with all the 5 Key Combinations:	Passed	
EWCJ176_2S_Reg_70	MPSK with Ap Model 9115	Verify the Configurations with Ap Different Ap Model 9115	Passed	
EWCJ176_2S_Reg_71	Connect Ap Model 9120	Verify the Configurations with Ap Different Ap Model 9120:	Passed	
EWCJ176_2S_Reg_72	Connect Ap Model 4800	Verify the Configurations with Ap Different Ap Model 4800:	Passed	

EWCJ176_2S_Reg_73	Connect Ap Model 3800	Verify the Configurations with Ap Different Ap Model 3800	Passed	
EWCJ176_2S_Reg_74	Connect Ap Model 3700	Verify the Configurations with Ap Different Ap Model 3700	Passed	
EWCJ176_2S_Reg_75	Connect Ap Model 1532	Verify the Configurations with Ap Different Ap Model 1532:	Passed	

iPSK Peer to Peer Blocking

Logical ID	Title	Description	Status	Defect ID
EWLCJ176S_Reg_117	Verifying the iPSK tag generation for the Connected Window JOS Client in eWLC UI/CLI	To verify whether iPSK tag generated or not When Window JOS connected to iPSK enabled WLAN Profile	Passed	
EWLCJ176S_Reg_118	Verifying the iPSK tag generation for the Connected MAC OS Client in eWLC UI/CLI	To verify whether iPSK tag generated or not When MAC OS connected to iPSK enabled WLAN Profile	Passed	
EWLCJ176S_Reg_119	Verifying the iPSK tag generation for the Connected iOS Client in eWLC UI/CLI	To verify whether iPSK tag generated or not When iOS connected to iPSK enabled WLAN Profile	Passed	
EWLCJ176S_Reg_120	Verifying the iPSK tag generation for the Connected Android Client in eWLC UI/CLI	To verify whether iPSK tag generated or not When Android connected to iPSK enabled WLAN Profile	Passed	
EWLCJ176S_Reg_121	Verifying peer to peer communication of Windows JOS clients while sharing same iPSK tag	To verify whether windows JOS clients are able to ping each other or not when they share the same iPSK tag	Passed	
EWLCJ176S_Reg_122	Verifying peer to peer communication of MAC clients while sharing same iPSK tag	To verify whether MAC OS clients are able to ping each other or not when they share the same iPSK tag	Passed	
EWLCJ176S_Reg_123	Verifying peer to peer communication of iOS clients while sharing same iPSK tag	To verify whether iOS clients are able to ping each other or not when they share the same iPSK tag	Passed	

EWLCJ176S_Reg_124	Verifying peer to peer communication of Android clients while sharing same iPSK tag	To verify whether windows Android OS clients are able to ping each other or not when they share the same iPSK tag	Passed	
EWLCJ176S_Reg_125	Verifying peer to peer communication of Windows JOS clients while sharing different iPSK tag	To verify whether windows JOS clients are able to ping each other or not when they share the different iPSK tag	Passed	
EWLCJ176S_Reg_126	Verifying peer to peer communication of MAC clients while sharing different iPSK tag	To verify whether MAC OS clients are able to ping each other or not when they share the different iPSK tag	Passed	
EWLCJ176S_Reg_127	Verifying peer to peer communication of iOS clients while sharing different iPSK tag	To verify whether iOS clients are able to ping each other or not when they share the different iPSK tag	Passed	
EWLCJ176S_Reg_128	Verifying peer to peer communication of Android clients while sharing different iPSK tag	To verify whether windows Android OS clients are able to ping each other or not when they share the different iPSK tag	Passed	
EWLCJ176S_Reg_129	Verifying peer to peer communication of different OS clients when clients share same iPSK Tag	To verify whether the different platform OS clients can ping each other or not when they share the same iPSK tag	Passed	
EWLCJ176S_Reg_130	Verifying peer to peer communication of different OS clients when clients share different iPSK Tag	To verify whether the different platform OS clients can ping each other or not when they share the same iPSK tag	Passed	

EWLCJ176S_Reg_131	Verifying peer to peer action of connected clients with same iPSK tag in case of central switching mode	To verify whether the different platform OS clients can ping each other or not when they share the same iPSK tag with central Switching	Passed	
EWLCJ176S_Reg_132	Verifying peer to peer action of connected clients with same iPSK tag in case of local switching	To verify whether the different platform OS clients can ping each other or not when they share the same iPSK tag with local switching	Passed	
EWLCJ176S_Reg_133	Verifying peer to peer action of connected clients with different iPSK tag in case of central switching mode	To verify whether the different platform OS clients can ping each other or not when they share the different iPSK tag with central Switching	Passed	
EWLCJ176S_Reg_134	Verifying peer to peer action of connected clients with different iPSK tag in case of local switching	To verify whether the different platform OS clients can ping each other or not when they share the different iPSK tag with local switching	Passed	
EWLCJ176S_Reg_135	Verifying connected clients with the particular iPSK tag in CLI	To verify whether all the clients sharing iPSK tag are shown or not in eWLC CLI	Passed	
EWLCJ176S_Reg_136	Verifying the wlan configuration with iPSK tag Configuration through eWLC Web	To verify whether wlan profile can be created or not with the iPSK configuration through the eWLC Web	Passed	

EWLCJ176S_Reg_137	Verifying the wlan generation with iPSK tag Configuration through eWLC CLI	To verify whether wlan profile can be created or not with the iPSK configuration through the eWLC CLI	Passed	
EWLCJ176S_Reg_138	Verifying iPSK tag for the for different OS clients with Flex Bridge Mode	To verify whether iPSK tag is generated or not for the connected clients	Passed	
EWLCJ176S_Reg_139	Verifying clients connectivity with iPSK tag while radius fallback is enabled	To verify whether clients iPSK is being generated from secondary AAA server or not	Passed	
EWLCJ176S_Reg_140	Verifying generation of iPSK tag with FT-PSK for different OS clients	To verify whether iPSK generated or not when WLAN is enabled with FT-PSK	Passed	
EWLCJ176S_Reg_141	Verifying connectivity among the clients when clients are connected to different WLAN	To verify whether the different platform OS clients can ping each other or not based on the iPSK tag	Passed	
EWLCJ176S_Reg_142	Verifying iPSK WLAN configuration after importing and exporting the same configuration file	To verify whether the wlan configuration retains same or not after exporting the same configuration file	Passed	
EWLCJ176S_Reg_143	Verifying peer to peer action of connected clients with same iPSK tag in case of central switching mode	To verify whether the same platform OS clients can ping each other or not when they share the same iPSK tag with central Switching	Passed	

EWLCJ176S_Reg_144	Verifying peer to peer action of connected clients with same iPSK tag in case of local switching	To verify whether the same platform OS clients can ping each other or not when they share the same iPSK tag with local switching	Passed	
EWLCJ176S_Reg_145	Verifying peer to peer action of connected clients with different iPSK tag in case of central switching mode	To verify whether the same platform OS clients can ping each other or not when they share the different iPSK tag with central Switching	Passed	
EWLCJ176S_Reg_146	Verifying peer to peer action of connected clients with different iPSK tag in case of local switching	To verify whether the same platform OS clients can ping each other or not when they share the different iPSK tag with local switching	Passed	
EWLCJ176S_Reg_147	Verifying iPSK tag for the for Same OS clients with Flex Bridge Mode	To verify whether iPSK tag is generated or not for the connected clients	Passed	
EWLCJ176S_Reg_148	Verifying generation of iPSK tag with FT-PSK for same OS clients.	To verify whether iPSK generated or not when WLAN is enabled with FT-PSK for same OS Clients.	Passed	
EWLCJ176S_Reg_149	Verifying peer to peer action of same OS clients with different iPSK tag in case of local switching with FT-PSK.	To verify whether the same platform OS clients can ping each other or not when they share the different iPSK tag in case of local switching with FT-PSK.	Passed	

EWLCJ176S_Reg_150	Verifying peer to peer action of different OS clients with different iPSK tag in case of local switching with FT-PSK	To verify whether the different platform OS clients can ping each other or not when they share the different iPSK tag in case of local switching with FT-PSK for the	Passed	
EWLCJ176S_Reg_151	Verifying the iPSK tag generation for the Connected AnyConnect Client in eWLC UI/CLI	To verify whether iPSK tag generated or not When AnyConnect client connected to iPSK enabled WLAN Profile	Passed	
EWLCJ176S_Reg_152	Verifying the iPSK tag generation for the same password with different groups.	To verify whether iPSK tag generated or not for the same password with different groups	Passed	
EWLCJ176S_Reg_153	Verifying the generation of ipsk tag with WPA-TKIP-PSk for same/different os clients.	To verify whether iPSK generated or not when WLAN is enabled with WPA-TkIP-PSK	Passed	
EWLCJ176S_Reg_154	Verifying the peer to peer communication of different clients connected to different SSIDs in same network group in case of Central Switching.	To Verify the peer to peer communication of different clients connected to different SSIDs in same network group in case of central switching.	Passed	
EWLCJ176S_Reg_155	Verifying the peer to peer communication of different clients connected to different SSIDs in Different network groups in case of central switching.	To Verify the peer to peer communication of different clients connected to different SSIDs in different network group in case of central switching.	Passed	

EWLCJ176S_Reg_156	Verifying the peer to peer communication of different clients connected to different SSIDs in same network group in case of Local Switching.	To Verify the peer to peer communication of different clients connected to different SSIDs in same network group in case of local switching.	Passed	
EWLCJ176S_Reg_157	Verifying the peer to peer communication of different clients connected to different SSIDs in Different network group in case of local switching.	To Verify the peer to peer communication of different clients connected to different SSIDs in different network group in case of local switching.	Passed	
EWLCJ176S_Reg_158	Verifying iPSK tag and peer to peer communication for the for Same OS clients with Flex Bridge Mode in case of local switching with same group	To verify whether iPSK tag and peer to peer communication for Same OS clients with Flex Bridge Mode in case of local switching with same group	Passed	
EWLCJ176S_Reg_159	Verifying iPSK tag and peer to peer communication for the for different OS clients with Flex Bridge Mode in case of local switching with same group	To verify whether iPSK tag and peer to peer communication for different OS clients with Flex Bridge Mode in case of local switching with same group	Passed	
EWLCJ176S_Reg_160	Verifying iPSK tag and peer to peer communication for the for Same OS clients with Flex Bridge Mode in case of local switching with different group	To verify whether iPSK tag and peer to peer communication for Same OS clients with Flex Bridge Mode in case of local switching with different group	Passed	

EWLCJ176S_Reg_161	Verifying iPSK tag and peer to peer communication for the for different OS clients with Flex Bridge Mode in case of local switching with different group	To verify whether iPSK tag and peer to peer communication for different OS clients with Flex Bridge Mode in case of local switching with different group	Passed	
EWLCJ176S_Reg_162	Verifying clients roaming with same iPSK tag	To verify whether the client is roaming from one Ap to another Ap.	Passed	
EWLCJ176S_Reg_163	Verifying clients roaming with different iPSK tag	To verify whether the client is roaming from one Ap to another Ap.	Passed	
EWCJ176S_Reg_67	Verifying the iPSK tag generation for the Connected Window JOS Client in EWC UI/CLI	To verify whether iPSK tag generated or not When Window JOS connected to iPSK enabled WLAN Profile	Passed	
EWCJ176S_Reg_68	Verifying the iPSK tag generation for the Connected MAC OS Client in EWC UI/CLI	To verify whether iPSK tag generated or not When MAC OS connected to iPSK enabled WLAN Profile	Passed	
EWCJ176S_Reg_69	Verifying the iPSK tag generation for the Connected iOS Client in EWC UI/CLI	To verify whether iPSK tag generated or not When iOS connected to iPSK enabled WLAN Profile	Passed	
EWCJ176S_Reg_70	Verifying the iPSK tag generation for the Connected Android Client in EWC UI/CLI	To verify whether iPSK tag generated or not When Android connected to iPSK enabled WLAN Profile	Passed	

EWCJ176S_Reg_71	Verifying peer to peer communication of Windows JOS clients while sharing same iPSK tag	To verify whether windows JOS clients are able to ping each other or not when they share the same iPSK tag	Passed	
EWCJ176S_Reg_72	Verifying peer to peer communication of MAC clients while sharing same iPSK tag	To verify whether MAC OS clients are able to ping each other or not when they share the same iPSK tag	Passed	
EWCJ176S_Reg_73	Verifying peer to peer communication of iOS clients while sharing same iPSK tag	To verify whether iOS clients are able to ping each other or not when they share the same iPSK tag	Passed	
EWCJ176S_Reg_74	Verifying peer to peer communication of Android clients while sharing same iPSK tag	To verify whether windows Android OS clients are able to ping each other or not when they share the same iPSK tag	Passed	
EWCJ176S_Reg_75	Verifying peer to peer communication of Windows JOS clients while sharing different iPSK tag	To verify whether windows JOS clients are able to ping each other or not when they share the different iPSK tag	Passed	
EWCJ176S_Reg_76	Verifying peer to peer communication of MAC clients while sharing different iPSK tag	To verify whether MAC OS clients are able to ping each other or not when they share the different iPSK tag	Passed	
EWCJ176S_Reg_77	Verifying peer to peer communication of iOS clients while sharing different iPSK tag	To verify whether iOS clients are able to ping each other or not when they share the different iPSK tag	Passed	

EWCJ176S_Reg_78	Verifying peer to peer communication of Android clients while sharing different iPSK tag	To verify whether windows Android OS clients are able to ping each other or not when they share the different iPSK tag	Passed	
EWCJ176S_Reg_79	Verifying peer to peer communication of different OS clients when clients share same iPSK Tag	To verify whether the different platform OS clients can ping each other or not when they share the same iPSK tag	Passed	
EWCJ176S_Reg_80	Verifying peer to peer communication of different OS clients when clients share different iPSK Tag	To verify whether the different platform OS clients can ping each other or not when they share the same iPSK tag	Passed	
EWCJ176S_Reg_81	Verifying peer to peer action of connected clients with same iPSK tag in case of central switching mode	To verify whether the different platform OS clients can ping each other or not when they share the same iPSK tag with central Switching	Passed	
EWCJ176S_Reg_82	Verifying peer to peer action of connected clients with same iPSK tag in case of local switching	To verify whether the different platform OS clients can ping each other or not when they share the same iPSK tag with local switching	Passed	
EWCJ176S_Reg_83	Verifying peer to peer action of connected clients with different iPSK tag in case of central switching mode	To verify whether the different platform OS clients can ping each other or not when they share the different iPSK tag with central Switching	Passed	

EWCJ176S_Reg_84	Verifying peer to peer action of connected clients with different iPSK tag in case of local switching	To verify whether the different platform OS clients can ping each other or not when they share the different iPSK tag with local switching	Passed	
EWCJ176S_Reg_85	Verifying connected clients with the particular iPSK tag in CLI	To verify whether all the clients sharing iPSK tag are shown or not in EWC CLI	Passed	
EWCJ176S_Reg_86	Verifying the wlan configuration with iPSK tag Configuration through EWC Web	To verify whether wlan profile can be created or not with the iPSK configuration through the EWC Web	Passed	
EWCJ176S_Reg_87	Verifying the wlan generation with iPSK tag Configuration through EWC CLI	To verify whether wlan profile can be created or not with the iPSK configuration through the EWC CLI	Passed	
EWCJ176S_Reg_88	Verifying iPSK tag for the for different OS clients with Flex+Bridge Mode	To verify whether iPSK tag is generated or not for the connected clients	Passed	
EWCJ176S_Reg_89	Verifying clients connectivity with iPSK tag while radius fallback is enabled	To verify whether clients iPSK is being generated from secondary AAA server or not	Passed	
EWCJ176S_Reg_90	Verifying generation of iPSK tag with FT-PSK for different OS clients	To verify whether iPSK generated or not when WLAN is enabled with FT-PSK	Passed	

EWCJ176S_Reg_91	Verifying connectivity among the clients when clients are connected to different WLAN	To verify whether the different platform OS clients can ping each other or not based on the iPSK tag	Passed	
EWCJ176S_Reg_92	Verifying iPSK WLAN configuration after importing and exporting the same configuration file	To verify whether the wlan configuration retains same or not after exporting the same configuration file	Passed	
EWCJ176S_Reg_93	Verifying peer to peer action of connected clients with same iPSK tag in case of central switching mode	To verify whether the same platform OS clients can ping each other or not when they share the same iPSK tag with central Switching	Passed	
EWCJ176S_Reg_94	Verifying peer to peer action of connected clients with same iPSK tag in case of local switching	To verify whether the same platform OS clients can ping each other or not when they share the same iPSK tag with local switching	Passed	
EWCJ176S_Reg_95	Verifying peer to peer action of connected clients with different iPSK tag in case of central switching mode	To verify whether the same platform OS clients can ping each other or not when they share the different iPSK tag with central Switching	Passed	
EWCJ176S_Reg_96	Verifying peer to peer action of connected clients with different iPSK tag in case of local switching	To verify whether the same platform OS clients can ping each other or not when they share the different iPSK tag with local switching	Passed	
EWCJ176S_Reg_97	Verifying iPSK tag for the for Same OS clients with Flex+Bridge Mode	To verify whether iPSK tag is generated or not for the connected clients	Passed	

EWCJ176S_Reg_98	Verifying generation of iPSK tag with FT-PSK for same OS clients.	To verify whether iPSK generated or not when WLAN is enabled with FT-PSK for same OS Clients.	Passed	
EWCJ176S_Reg_99	Verifying peer to peer action of same OS clients with different iPSK tag in case of local switching with FT-PSK.	To verify whether the same platform OS clients can ping each other or not when they share the different iPSK tag in case of local switching with FT-PSK.	Passed	
EWCJ176S_Reg_100	Verifying peer to peer action of different OS clients with different iPSK tag in case of local switching with FT-PSK	To verify whether the different platform OS clients can ping each other or not when they share the different iPSK tag in case of local switching with FT-PSK for the	Passed	
EWCJ176S_Reg_101	Verifying the iPSK tag generation for the Connected AnyConnect Client in EWC UI/CLI	To verify whether iPSK tag generated or not When AnyConnect client connected to iPSK enabled WLAN Profile	Passed	
EWCJ176S_Reg_102	Verifying the iPSK tag generation for the same password with different groups.	To verify whether iPSK tag generated or not for the same password with different groups	Passed	
EWCJ176S_Reg_103	Verifying the generation of ipsk tag with WPA-TKIP-PSk for same/different os clients.	To verify whether iPSK generated or not when WLAN is enabled with WPA-TkIP-PSK	Passed	

EWCJ176S_Reg_104	Verifying the peer to peer communication of different clients connected to different SSIDs in same network group in case of Central Switching.	To Verify the peer to peer communication of different clients connected to different SSIDs in same network group in case of central switching.	Passed	
EWCJ176S_Reg_105	Verifying the peer to peer communication of different clients connected to different SSIDs in Different network groups in case of central switching.	To Verify the peer to peer communication of different clients connected to different SSIDs in different network group in case of central switching.	Passed	
EWCJ176S_Reg_106	Verifying the peer to peer communication of different clients connected to different SSIDs in same network group in case of Local Switching.	To Verify the peer to peer communication of different clients connected to different SSIDs in same network group in case of local switching.	Passed	
EWCJ176S_Reg_107	Verifying the peer to peer communication of different clients connected to different SSIDs in Different network group in case of local switching.	To Verify the peer to peer communication of different clients connected to different SSIDs in different network group in case of local switching.	Passed	
EWCJ176S_Reg_108	Verifying iPSK tag and peer to peer communication for the for Same OS clients with Flex+Bridge Mode in case of local switching with same group	To verify whether iPSK tag and peer to peer communication for Same OS clients with Flex+Bridge Mode in case of local switching with same group	Passed	

EWCJ176S_Reg_109	Verifying iPSK tag and peer to peer communication for the for different OS clients with Flex+Bridge Mode in case of local switching with same group	To verify whether iPSK tag and peer to peer communication for different OS clients with Flex+Bridge Mode in case of local switching with same group	Passed	
EWCJ176S_Reg_110	Verifying iPSK tag and peer to peer communication for the for Same OS clients with Flex+Bridge Mode in case of local switching with different group	To verify whether iPSK tag and peer to peer communication for Same OS clients with Flex+Bridge Mode in case of local switching with different group	Passed	
EWCJ176S_Reg_111	Verifying iPSK tag and peer to peer communication for the for different OS clients with Flex+Bridge Mode in case of local switching with different group	To verify whether iPSK tag and peer to peer communication for different OS clients with Flex+Bridge Mode in case of local switching with different group	Passed	
EWCJ176S_Reg_112	Verifying clients roaming with same iPSK tag	To verify whether the client is roaming from one Ap to another Ap.	Passed	
EWCJ176S_Reg_113	Verifying clients roaming with different iPSK tag	To verify whether the client is roaming from one Ap to another Ap.	Passed	
EWLCJ176_2S_Reg_223	Verifying the iPSK tag generation for the Connected Window JOS Client in eWLC UI/CLI	To verify whether iPSK tag generated or not When Window JOS connected to iPSK enabled WLAN Profile	Passed	
EWLCJ176_2S_Reg_224	Verifying the iPSK tag generation for the Connected MAC OS Client in eWLC UI/CLI	To verify whether iPSK tag generated or not When MAC OS connected to iPSK enabled WLAN Profile	Passed	

EWLCJ176_2S_Reg_225	Verifying the iPSK tag generation for the Connected iOS Client in eWLC UI/CLI	To verify whether iPSK tag generated or not When iOS connected to iPSK enabled WLAN Profile	Passed	
EWLCJ176_2S_Reg_226	Verifying the iPSK tag generation for the Connected Android Client in eWLC UI/CLI	To verify whether iPSK tag generated or not When Android connected to iPSK enabled WLAN Profile	Passed	
EWLCJ176_2S_Reg_227	Verifying peer to peer communication of Windows JOS clients while sharing same iPSK tag	To verify whether windows JOS clients are able to ping each other or not when they share the same iPSK tag	Passed	
EWLCJ176_2S_Reg_228	Verifying peer to peer communication of MAC clients while sharing same iPSK tag	To verify whether MAC OS clients are able to ping each other or not when they share the same iPSK tag	Passed	
EWLCJ176_2S_Reg_229	Verifying peer to peer communication of iOS clients while sharing same iPSK tag	To verify whether iOS clients are able to ping each other or not when they share the same iPSK tag	Passed	
EWLCJ176_2S_Reg_230	Verifying peer to peer communication of Android clients while sharing same iPSK tag	To verify whether windows Android OS clients are able to ping each other or not when they share the same iPSK tag	Passed	
EWLCJ176_2S_Reg_231	Verifying peer to peer communication of Windows JOS clients while sharing different iPSK tag	To verify whether windows JOS clients are able to ping each other or not when they share the different iPSK tag	Passed	

EWLCJ176_2S_Reg_232	Verifying peer to peer communication of MAC clients while sharing different iPSK tag	To verify whether MAC OS clients are able to ping each other or not when they share the different iPSK tag	Passed	
EWLCJ176_2S_Reg_233	Verifying peer to peer communication of iOS clients while sharing different iPSK tag	To verify whether iOS clients are able to ping each other or not when they share the different iPSK tag	Passed	
EWLCJ176_2S_Reg_234	Verifying peer to peer communication of Android clients while sharing different iPSK tag	To verify whether windows Android OS clients are able to ping each other or not when they share the different iPSK tag	Passed	
EWLCJ176_2S_Reg_235	Verifying peer to peer communication of different OS clients when clients share same iPSK Tag	To verify whether the different platform OS clients can ping each other or not when they share the same iPSK tag	Passed	
EWLCJ176_2S_Reg_236	Verifying peer to peer communication of different OS clients when clients share different iPSK Tag	To verify whether the different platform OS clients can ping each other or not when they share the same iPSK tag	Passed	
EWLCJ176_2S_Reg_237	Verifying peer to peer action of connected clients with same iPSK tag in case of central switching mode	To verify whether the different platform OS clients can ping each other or not when they share the same iPSK tag with central Switching	Passed	

EWLCJ176_2S_Reg_238	Verifying peer to peer action of connected clients with same iPSK tag in case of local switching	To verify whether the different platform OS clients can ping each other or not when they share the same iPSK tag with local switching	Passed	
EWLCJ176_2S_Reg_239	Verifying peer to peer action of connected clients with different iPSK tag in case of central switching mode	To verify whether the different platform OS clients can ping each other or not when they share the different iPSK tag with central Switching	Passed	
EWLCJ176_2S_Reg_240	Verifying peer to peer action of connected clients with different iPSK tag in case of local switching	To verify whether the different platform OS clients can ping each other or not when they share the different iPSK tag with local switching	Passed	
EWLCJ176_2S_Reg_241	Verifying connected clients with the particular iPSK tag in CLI	To verify whether all the clients sharing iPSK tag are shown or not in eWLC CLI	Passed	
EWLCJ176_2S_Reg_242	Verifying the wlan configuration with iPSK tag Configuration through eWLC Web	To verify whether wlan profile can be created or not with the iPSK configuration through the eWLC Web	Passed	
EWLCJ176_2S_Reg_243	Verifying the wlan generation with iPSK tag Configuration through eWLC CLI	To verify whether wlan profile can be created or not with the iPSK configuration through the eWLC CLI	Passed	
EWLCJ176_2S_Reg_244	Verifying iPSK tag for the for different OS clients with Flex+Bridge Mode	To verify whether iPSK tag is generated or not for the connected clients	Passed	

EWLCJ176_2S_Reg_245	Verifying clients connectivity with iPSK tag while radius fallback is enabled	To verify whether clients iPSK is being generated from secondary AAA server or not	Passed	
EWLCJ176_2S_Reg_246	Verifying generation of iPSK tag with FT-PSK for different OS clients	To verify whether iPSK generated or not when WLAN is enabled with FT-PSK	Passed	
EWLCJ176_2S_Reg_247	Verifying connectivity among the clients when clients are connected to different WLAN	To verify whether the different platform OS clients can ping each other or not based on the iPSK tag	Passed	
EWLCJ176_2S_Reg_248	Verifying iPSK WLAN configuration after importing and exporting the same configuration file	To verify whether the wlan configuration retains same or not after exporting the same configuration file	Passed	
EWLCJ176_2S_Reg_249	Verifying peer to peer action of connected clients with same iPSK tag in case of central switching mode	To verify whether the same platform OS clients can ping each other or not when they share the same iPSK tag with central Switching	Passed	
EWLCJ176_2S_Reg_250	Verifying peer to peer action of connected clients with same iPSK tag in case of local switching	To verify whether the same platform OS clients can ping each other or not when they share the same iPSK tag with local switching	Passed	
EWLCJ176_2S_Reg_251	Verifying peer to peer action of connected clients with different iPSK tag in case of central switching mode	To verify whether the same platform OS clients can ping each other or not when they share the different iPSK tag with central Switching	Passed	

EWLCJ176_2S_Reg_252	Verifying peer to peer action of connected clients with different iPSK tag in case of local switching	To verify whether the same platform OS clients can ping each other or not when they share the different iPSK tag with local switching	Passed	
EWLCJ176_2S_Reg_253	Verifying iPSK tag for the for Same OS clients with Flex+Bridge Mode	To verify whether iPSK tag is generated or not for the connected clients	Passed	
EWLCJ176_2S_Reg_254	Verifying generation of iPSK tag with FT-PSK for same OS clients.	To verify whether iPSK generated or not when WLAN is enabled with FT-PSK for same OS Clients.	Passed	
EWLCJ176_2S_Reg_255	Verifying peer to peer action of same OS clients with different iPSK tag in case of local switching with FT-PSK.	To verify whether the same platform OS clients can ping each other or not when they share the different iPSK tag in case of local switching with FT-PSK.	Passed	
EWLCJ176_2S_Reg_256	Verifying peer to peer action of different OS clients with different iPSK tag in case of local switching with FT-PSK	To verify whether the different platform OS clients can ping each other or not when they share the different iPSK tag in case of local switching with FT-PSK for the	Passed	
EWLCJ176_2S_Reg_257	Verifying the iPSK tag generation for the Connected AnyConnect Client in eWLC UI/CLI	To verify whether iPSK tag generated or not When AnyConnect client connected to iPSK enabled WLAN Profile	Passed	
EWLCJ176_2S_Reg_258	Verifying the iPSK tag generation for the same password with different groups.	To verify whether iPSK tag generated or not for the same password with different groups	Passed	

EWLCJ176_2S_Reg_259	Verifying the generation of ipsk tag with WPA-TKIP-PSk for same/different os clients.	To verify whether iPSK generated or not when WLAN is enabled with WPA-TkIP-PSK	Passed	
EWLCJ176_2S_Reg_260	Verifying the peer to peer communication of different clients connected to different SSIDs in same network group in case of Central Switching.	To Verify the peer to peer communication of different clients connected to different SSIDs in same network group in case of central switching.	Passed	
EWLCJ176_2S_Reg_261	Verifying the peer to peer communication of different clients connected to different SSIDs in Different network groups in case of central switching.	To Verify the peer to peer communication of different clients connected to different SSIDs in different network group in case of central switching.	Passed	
EWLCJ176_2S_Reg_262	Verifying the peer to peer communication of different clients connected to different SSIDs in same network group in case of Local Switching.	To Verify the peer to peer communication of different clients connected to different SSIDs in same network group in case of local switching.	Passed	
EWLCJ176_2S_Reg_263	Verifying the peer to peer communication of different clients connected to different SSIDs in Different network group in case of local switching.	To Verify the peer to peer communication of different clients connected to different SSIDs in different network group in case of local switching.	Passed	

EWLCJ176_2S_Reg_264	Verifying iPSK tag and peer to peer communication for the for Same OS clients with Flex+Bridge Mode in case of local switching with same group	To verify whether iPSK tag and peer to peer communication for Same OS clients with Flex+Bridge Mode in case of local switching with same group	Passed	
EWLCJ176_2S_Reg_265	Verifying iPSK tag and peer to peer communication for the for different OS clients with Flex+Bridge Mode in case of local switching with same group	To verify whether iPSK tag and peer to peer communication for different OS clients with Flex+Bridge Mode in case of local switching with same group	Passed	
EWLCJ176_2S_Reg_266	Verifying iPSK tag and peer to peer communication for the for Same OS clients with Flex+Bridge Mode in case of local switching with different group	To verify whether iPSK tag and peer to peer communication for Same OS clients with Flex+Bridge Mode in case of local switching with different group	Passed	
EWLCJ176_2S_Reg_267	Verifying iPSK tag and peer to peer communication for the for different OS clients with Flex+Bridge Mode in case of local switching with different group	To verify whether iPSK tag and peer to peer communication for different OS clients with Flex+Bridge Mode in case of local switching with different group	Passed	
EWLCJ176_2S_Reg_268	Verifying clients roaming with same iPSK tag	To verify whether the client is roaming from one Ap to another Ap.	Passed	
EWLCJ176_2S_Reg_269	Verifying clients roaming with different iPSK tag	To verify whether the client is roaming from one Ap to another Ap.	Passed	

EWCJ176_2S_Reg_87	Verifying the iPSK tag generation for the Connected Window JOS Client in EWC UI/CLI	To verify whether iPSK tag generated or not When Window JOS connected to iPSK enabled WLAN Profile	Passed	
EWCJ176_2S_Reg_88	Verifying the iPSK tag generation for the Connected MAC OS Client in EWC UI/CLI	To verify whether iPSK tag generated or not When MAC OS connected to iPSK enabled WLAN Profile	Failed	CSCvy34218
EWCJ176_2S_Reg_89	Verifying the iPSK tag generation for the Connected iOS Client in EWC UI/CLI	To verify whether iPSK tag generated or not When iOS connected to iPSK enabled WLAN Profile	Passed	
EWCJ176_2S_Reg_90	Verifying the iPSK tag generation for the Connected Android Client in EWC UI/CLI	To verify whether iPSK tag generated or not When Android connected to iPSK enabled WLAN Profile	Passed	
EWCJ176_2S_Reg_91	Verifying peer to peer communication of Windows JOS clients while sharing same iPSK tag	To verify whether windows JOS clients are able to ping each other or not when they share the same iPSK tag	Passed	
EWCJ176_2S_Reg_92	Verifying peer to peer communication of MAC clients while sharing same iPSK tag	To verify whether MAC OS clients are able to ping each other or not when they share the same iPSK tag	Passed	
EWCJ176_2S_Reg_93	Verifying peer to peer communication of iOS clients while sharing same iPSK tag	To verify whether iOS clients are able to ping each other or not when they share the same iPSK tag	Passed	

EWCJ176_2S_Reg_94	Verifying peer to peer communication of Android clients while sharing same iPSK tag	To verify whether windows Android OS clients are able to ping each other or not when they share the same iPSK tag	Passed	
EWCJ176_2S_Reg_95	Verifying peer to peer communication of Windows JOS clients while sharing different iPSK tag	To verify whether windows JOS clients are able to ping each other or not when they share the different iPSK tag	Passed	
EWCJ176_2S_Reg_96	Verifying peer to peer communication of MAC clients while sharing different iPSK tag	To verify whether MAC OS clients are able to ping each other or not when they share the different iPSK tag	Passed	
EWCJ176_2S_Reg_97	Verifying peer to peer communication of iOS clients while sharing different iPSK tag	To verify whether iOS clients are able to ping each other or not when they share the different iPSK tag	Passed	
EWCJ176_2S_Reg_98	Verifying peer to peer communication of Android clients while sharing different iPSK tag	To verify whether windows Android OS clients are able to ping each other or not when they share the different iPSK tag	Passed	
EWCJ176_2S_Reg_99	Verifying peer to peer communication of different OS clients when clients share same iPSK Tag	To verify whether the different platform OS clients can ping each other or not when they share the same iPSK tag	Passed	
EWCJ176_2S_Reg_100	Verifying peer to peer communication of different OS clients when clients share different iPSK Tag	To verify whether the different platform OS clients can ping each other or not when they share the same iPSK tag	Passed	

EWCJ176_2S_Reg_101	Verifying peer to peer action of connected clients with same iPSK tag in case of central switching mode	To verify whether the different platform OS clients can ping each other or not when they share the same iPSK tag with central Switching	Passed	
EWCJ176_2S_Reg_102	Verifying peer to peer action of connected clients with same iPSK tag in case of local switching	To verify whether the different platform OS clients can ping each other or not when they share the same iPSK tag with local switching	Passed	
EWCJ176_2S_Reg_103	Verifying peer to peer action of connected clients with different iPSK tag in case of central switching mode	To verify whether the different platform OS clients can ping each other or not when they share the different iPSK tag with central Switching	Passed	
EWCJ176_2S_Reg_104	Verifying peer to peer action of connected clients with different iPSK tag in case of local switching	To verify whether the different platform OS clients can ping each other or not when they share the different iPSK tag with local switching	Passed	
EWCJ176_2S_Reg_105	Verifying connected clients with the particular iPSK tag in CLI	To verify whether all the clients sharing iPSK tag are shown or not in EWC CLI	Passed	
EWCJ176_2S_Reg_106	Verifying the wlan configuration with iPSK tag Configuration through EWC Web	To verify whether wlan profile can be created or not with the iPSK configuration through the EWC Web	Passed	

EWCJ176_2S_Reg_107	Verifying the wlan generation with iPSK tag Configuration through EWC CLI	To verify whether wlan profile can be created or not with the iPSK configuration through the EWC CLI	Passed	
EWCJ176_2S_Reg_108	Verifying iPSK tag for the for different OS clients with Flex+Bridge Mode	To verify whether iPSK tag is generated or not for the connected clients	Passed	
EWCJ176_2S_Reg_109	Verifying clients connectivity with iPSK tag while radius fallback is enabled	To verify whether clients iPSK is being generated from secondary AAA server or not	Passed	
EWCJ176_2S_Reg_110	Verifying generation of iPSK tag with FT-PSK for different OS clients	To verify whether iPSK generated or not when WLAN is enabled with FT-PSK	Passed	
EWCJ176_2S_Reg_111	Verifying connectivity among the clients when clients are connected to different WLAN	To verify whether the different platform OS clients can ping each other or not based on the iPSK tag	Passed	
EWCJ176_2S_Reg_112	Verifying iPSK WLAN configuration after importing and exporting the same configuration file	To verify whether the wlan configuration retains same or not after exporting the same configuration file	Passed	
EWCJ176_2S_Reg_113	Verifying peer to peer action of connected clients with same iPSK tag in case of central switching mode	To verify whether the same platform OS clients can ping each other or not when they share the same iPSK tag with central Switching	Passed	

EWCJ176_2S_Reg_114	Verifying peer to peer action of connected clients with same iPSK tag in case of local switching	To verify whether the same platform OS clients can ping each other or not when they share the same iPSK tag with local switching	Passed	
EWCJ176_2S_Reg_115	Verifying peer to peer action of connected clients with different iPSK tag in case of central switching mode	To verify whether the same platform OS clients can ping each other or not when they share the different iPSK tag with central Switching	Passed	
EWCJ176_2S_Reg_116	Verifying peer to peer action of connected clients with different iPSK tag in case of local switching	To verify whether the same platform OS clients can ping each other or not when they share the different iPSK tag with local switching	Passed	
EWCJ176_2S_Reg_117	Verifying iPSK tag for the for Same OS clients with Flex+Bridge Mode	To verify whether iPSK tag is generated or not for the connected clients	Passed	
EWCJ176_2S_Reg_118	Verifying generation of iPSK tag with FT-PSK for same OS clients.	To verify whether iPSK generated or not when WLAN is enabled with FT-PSK for same OS Clients.	Passed	
EWCJ176_2S_Reg_119	Verifying peer to peer action of same OS clients with different iPSK tag in case of local switching with FT-PSK.	To verify whether the same platform OS clients can ping each other or not when they share the different iPSK tag in case of local switching with FT-PSK.	Passed	

EWCJ176_2S_Reg_120	Verifying peer to peer action of different OS clients with different iPSK tag in case of local switching with FT-PSK	To verify whether the different platform OS clients can ping each other or not when they share the different iPSK tag in case of local switching with FT-PSK for the	Passed	
EWCJ176_2S_Reg_121	Verifying the iPSK tag generation for the Connected AnyConnect Client in EWC UI/CLI	To verify whether iPSK tag generated or not When AnyConnect client connected to iPSK enabled WLAN Profile	Passed	
EWCJ176_2S_Reg_122	Verifying the iPSK tag generation for the same password with different groups.	To verify whether iPSK tag generated or not for the same password with different groups	Passed	
EWCJ176_2S_Reg_123	Verifying the generation of ipsk tag with WPA-TKIP-PSk for same/different os clients.	To verify whether iPSK generated or not when WLAN is enabled with WPA-TkIP-PSK	Passed	
EWCJ176_2S_Reg_124	Verifying the peer to peer communication of different clients connected to different SSIDs in same network group in case of Central Switching.	To Verify the peer to peer communication of different clients connected to different SSIDs in same network group in case of central switching.	Passed	
EWCJ176_2S_Reg_125	Verifying the peer to peer communication of different clients connected to different SSIDs in Different network groups in case of central switching.	To Verify the peer to peer communication of different clients connected to different SSIDs in different network group in case of central switching.	Passed	

EWCJ176_2S_Reg_126	Verifying the peer to peer communication of different clients connected to different SSIDs in same network group in case of Local Switching.	To Verify the peer to peer communication of different clients connected to different SSIDs in same network group in case of local switching.	Passed	
EWCJ176_2S_Reg_127	Verifying the peer to peer communication of different clients connected to different SSIDs in Different network group in case of local switching.	To Verify the peer to peer communication of different clients connected to different SSIDs in different network group in case of local switching.	Passed	
EWCJ176_2S_Reg_128	Verifying iPSK tag and peer to peer communication for the for Same OS clients with Flex+Bridge Mode in case of local switching with same group	To verify whether iPSK tag and peer to peer communication for Same OS clients with Flex+Bridge Mode in case of local switching with same group	Passed	
EWCJ176_2S_Reg_129	Verifying iPSK tag and peer to peer communication for the for different OS clients with Flex+Bridge Mode in case of local switching with same group	To verify whether iPSK tag and peer to peer communication for different OS clients with Flex+Bridge Mode in case of local switching with same group	Passed	
EWCJ176_2S_Reg_130	Verifying iPSK tag and peer to peer communication for the for Same OS clients with Flex+Bridge Mode in case of local switching with different group	To verify whether iPSK tag and peer to peer communication for Same OS clients with Flex+Bridge Mode in case of local switching with different group	Passed	

EWCJ176_2S_Reg_131	Verifying iPSK tag and peer to peer communication for the for different OS clients with Flex+Bridge Mode in case of local switching with different group	To verify whether iPSK tag and peer to peer communication for different OS clients with Flex+Bridge Mode in case of local switching with different group	Passed	
EWCJ176_2S_Reg_132	Verifying clients roaming with same iPSK tag	To verify whether the client is roaming from one Ap to another Ap.	Passed	
EWCJ176_2S_Reg_133	Verifying clients roaming with different iPSK tag	To verify whether the client is roaming from one Ap to another Ap.	Passed	

Inter Release Controller Mobility

Logical ID	Title	Description	Status	Defect ID
EWLCJ176S_Reg_164	Setting UP the secure mobility tunnel between 9800 Controller & 5520 WLC	To check whether both Control & Data path gets UP or not between 9800 Controller & 5520 Controller	Passed	
EWLCJ176S_Reg_165	Checking the mobility groups configuration after upload/download the config file in 5520 WLC via TFTP	To check whether mobility groups configurations gets retained or not after upload/download the config file via TFTP in 5520 WLC	Passed	
EWLCJ176S_Reg_166	Checking the mobility groups configuration after backup/restore the config file in 9800 Controller via TFTP	To check whether mobility groups configurations gets retained or not after backup/restore the config file via TFTP in Cat 9800 Controller	Passed	
EWLCJ176S_Reg_167	Configuring the Anchor controller option in a WLAN in 5520 WLC UI	To check whether Anchor option can be configured or not in a WLAN for WLC's	Passed	
EWLCJ176S_Reg_168	Configuring the Anchor controller option in 9800 WLC UI	To check whether Anchor option can be configured or not in a 9800 Controller.	Passed	
EWLCJ176S_Reg_169	Performing Inter Controller roaming of Windows client between 9800 Controller and 5520 WLC	To check whether Inter Controller roaming works properly or not for Windows clients between 5520 WLC and 9800 Controller with secure mobility tunnel config	Passed	

EWLCJ176S_Reg_170	Performing Inter Controller roaming of Android client between 9800 Controller and 5520 WLC	To check whether Inter Controller roaming works properly or not for Android clients between 5520 WLC and 9800 Controller with secure mobility tunnel config	Passed	
EWLCJ176S_Reg_171	Checking Inter Controller roaming of Mac Os client between 9800 Controller and 5520 WLC	To check whether Inter Controller roaming works properly or not for Mac os clients between 5520 WLC and 9800 Controller with secure mobility tunnel config	Passed	
EWLCJ176S_Reg_172	Verifying Inter Controller roaming of different OS clients between 9800 Controller and 5520 WLC with WPA2+dot1x (PEAP)	To check whether Inter Controller roaming works properly or not for clients between 5520 WLC and 9800 Controller with security type WPA2+dot1x (PEAP)	Passed	
EWLCJ176S_Reg_173	Checking the Anchor controller functionality during the roaming of Windows Client with L2 security-WEP	To check whether Anchor controller functionality works properly or not in Cat 9800 Controller during the roaming of Windows Client	Passed	
EWLCJ176S_Reg_174	Checking the Anchor controller functionality during the roaming of Android Client with L2 security-WEP	To check whether Anchor controller functionality works properly or not in Cat 9800 Controller during the roaming of Android Client	Passed	

EWLCJ176S_Reg_175	Checking the Anchor controller functionality during the roaming of IOS Client with L2 security-WEP	To check whether Anchor controller functionality works properly or not in Cat 9800 Controller during the roaming of IOS Client	Passed	
EWLCJ176S_Reg_176	Checking the Mobility groups configuration in Active/Standby HA WLC	To check whether mobility group configurations gets synced or not in Standby WLC during HA	Passed	
EWLCJ176S_Reg_177	Checking the Mobility groups configuration in Active/Standby HA WLC	To check whether mobility group configurations gets synced or not in Standby WLC during HA	Passed	
EWLCJ176S_Reg_178	Checking the Anchor controller functionality during the roaming of Windows Client with L2 security-WPA3-SAE	To check whether Anchor controller functionality works properly or not in Cat 9800 Controller during the roaming of Windows Client with WPA3-SAE security	Passed	
EWLCJ176S_Reg_179	Checking the Anchor controller functionality during the roaming of Android Client with L2 security-WPA3-SAE	To check whether Anchor controller functionality works properly or not in Cat 9800 Controller during the roaming of Android Client with WPA3-SAE security	Passed	
EWLCJ176S_Reg_180	Checking the Anchor controller functionality during the roaming of IOS Client with L2 security-WPA3-SAE	To check whether Anchor controller functionality works properly or not in Cat 9800 Controller during the roaming of IOS Client with WPA3-SAE security	Passed	

EWLCJ176S_Reg_181	Checking Inter Controller roaming of Windows client between 9800 Controller and 3504 WLC	To check whether Anchor controller functionality works properly or not in Cat 9800 Controller during the roaming of Windows Client with WPA3-SAE security	Passed	
EWLCJ176S_Reg_182	Checking Inter Controller roaming of Android client between 9800 Controller and 3504 WLC	To check whether Anchor controller functionality works properly or not in Cat 9800 Controller during the roaming of Android Client with WPA3-SAE security	Passed	
EWLCJ176S_Reg_183	Checking Inter Controller roaming of IOS client between 9800 Controller and 3504 WLC	To check whether Anchor controller functionality works properly or not in Cat 9800 Controller during the roaming of IOS Client with WPA3-SAE security	Passed	
EWLCJ176S_Reg_184	Checking Inter Controller roaming of Windows client between 9800 Controller and 8540 WLC	To check whether Anchor controller functionality works properly or not in Cat 9800 Controller during the roaming of Windows Client with WPA3-SAE security	Passed	
EWLCJ176S_Reg_185	Checking Inter Controller roaming of Android client between 9800 Controller and 8540 WLC	To check whether Anchor controller functionality works properly or not in Cat 9800 Controller during the roaming of Android Client with WPA3-SAE security	Passed	

EWLCJ176S_Reg_186	Checking Inter Controller roaming of IOS client between 9800 Controller and 8540 WLC	To check whether Anchor controller functionality works properly or not in Cat 9800 Controller during the roaming of IOS Client with WPA3-SAE security	Passed	

ISSU Enhancement(Zero downtime for Wireless N/W)

Logical ID	Title	Description	Status	Defect ID
EWLCJ176S_Reg_187	Performing Upgradation using ISSU	To check whether the upgradation is performed or not via ftp	Failed	CSCvy01415
EWLCJ176S_Reg_188	Performing Rollback for controller using ISSU.	To check whether the rollback happening for Controller image or not.	Passed	
EWLCJ176S_Reg_189	Disabling the Rollback timer during upgrading controller using ISSU.	To check that the rollback doesn't happen for Controller image or not.	Passed	
EWLCJ176S_Reg_190	Aborting the upgradation of Controller using ISSU.	To check whether the upgradation for Controller image is aborted or not.	Passed	
EWLCJ176S_Reg_191	Performing Upgradation for controller using ISSU via tftp server.	To check whether the Controller Upgradation via tftp is happening or not.	Passed	
EWLCJ176S_Reg_192	Performing Upgradation for Controller using ISSU via sftp server.	To check whether the Controller Upgradation via sftp is happening or not.	Passed	
EWLCJ176S_Reg_193	Performing Upgradation for controller using ISSU via http server.	To check whether the Controller Upgradation via http is happening or not.	Passed	
EWLCJ176S_Reg_194	Checking the client connectivity	To check whether the client continuously connecting during the upgrade of AP	Passed	

TACACS

Logical ID	Title	Description	Status	Defect ID
EWLCJ176S_Reg_195	Allowing the user for complete access to eWLC network via TACACS	To check whether user can able to read-write access the complete eWLC network or not via TACACS	Passed	
EWLCJ176S_Reg_196	Providing the user for lobby admin access to the eWLC via TACACS	To check whether user can able to have lobby admin access or not to eWLC via TACACS	Passed	
EWLCJ176S_Reg_197	Providing the user for monitoring access to the eWLC via TACACS	To check whether user can able to have monitoring access (which is read-only) or not to eWLC via TACACS	Passed	
EWLCJ176S_Reg_198	Trying to login eWLC via TACACS with invalid credentials	To check whether user can able to login or not in eWLC via TACACS with invalid credentials	Passed	
EWLCJ176S_Reg_199	Providing the user for selected access to the eWLC via TACACS	To check whether user can able to have access with the selected checkbox's like "WLAN" and "Controller" checkboxes.	Passed	
EWLCJ176S_Reg_200	Providing the user for selected access to the eWLC via TACACS	To check whether user can able to have access with the selected checkbox's like "Wireless" and "Security" checkboxes.	Passed	

EWLCJ176S_Reg_201	Providing the user for selected access to the eWLC via TACACS	To check whether user can able to have access with the selected checkbox's like "Command" and "Management" checkboxes.	Passed	
EWLCJ176S_Reg_202	Providing the user for selected access to the eWLC via TACACS	To check whether user can able to have access with the selected checkbox's like "WLAN, Controller,Wireless, Security,Commands Line Interfaces and "Management" checkboxes.	Passed	
EWLCJ176S_Reg_203	Trying to login eWLC network via TACACS with Invalid credentials.	To verify whether user can able to login or not in eWLC via TACACS with invalid credentials	Passed	
EWCJ176S_Reg_153	Allowing the user for complete access to ME EWLC network via TACACS	To check whether user can able to read-write access the complete ME EWLC network or not via TACACS	Passed	
EWCJ176S_Reg_154	Providing the user for lobby admin access to the ME EWLC via TACACS	To check whether user can able to have lobby admin access or not to ME EWLC via TACACS	Passed	
EWCJ176S_Reg_155	Providing the user for monitoring access to the ME EWLC via TACACS	To check whether user can able to have monitoring access (which is read-only) or not to ME EWLC via TACACS	Passed	
EWCJ176S_Reg_156	Trying to login ME EWLC via TACACS with invalid credentials	To check whether user can able to login or not in ME EWLC via TACACS with invalid credentials	Passed	

EWCJ176S_Reg_157	Providing the user for selected access to the ME EWLC via TACACS	To check whether user can able to have access with the selected checkbox's like "WLAN" and "Controller" checkboxes.	Passed	
EWCJ176S_Reg_158	Providing the user for selected access to the ME EWLC via TACACS	To check whether user can able to have access with the selected checkbox's like "Wireless" and "Security" checkboxes.	Passed	
EWCJ176S_Reg_159	Providing the user for selected access to the ME EWLC via TACACS	To check whether user can able to have access with the selected checkbox's like "Command" and "Management" checkboxes.	Passed	
EWCJ176S_Reg_160	Providing the user for selected access to the ME EWLC via TACACS	To check whether user can able to have access with the selected checkbox's like "WLAN, Controller, Wireless, Security,Commands Line Interfaces and "Management" checkboxes.	Passed	
EWCJ176S_Reg_161	Trying to login ME EWLC network via TACACS with Invalid credentials.	To verify whether user can able to login or not in ME EWLC via TACACS with invalid credentials	Passed	
EWCJ176_2S_Reg_171	Allowing the user for complete access to ME EWLC network via TACACS	To check whether user can able to read-write access the complete ME EWLC network or not via TACACS	Passed	

EWCJ176_2S_Reg_172	Providing the user for lobby admin access to the ME EWLC via TACACS	To check whether user can able to have lobby admin access or not to ME EWLC via TACACS	Passed	
EWCJ176_2S_Reg_173	Providing the user for monitoring access to the ME EWLC via TACACS	To check whether user can able to have monitoring access (which is read-only) or not to ME EWLC via TACACS	Passed	
EWCJ176_2S_Reg_174	Trying to login ME EWLC via TACACS with invalid credentials	To check whether user can able to login or not in ME EWLC via TACACS with invalid credentials	Passed	
EWCJ176_2S_Reg_175	Providing the user for selected access to the ME EWLC via TACACS	To check whether user can able to have access with the selected checkbox's like "WLAN" and "Controller" checkboxes.	Passed	
EWCJ176_2S_Reg_176	Providing the user for selected access to the ME EWLC via TACACS	To check whether user can able to have access with the selected checkbox's like "Wireless" and "Security" checkboxes.	Passed	
EWCJ176_2S_Reg_177	Providing the user for selected access to the ME EWLC via TACACS	To check whether user can able to have access with the selected checkbox's like "Command" and "Management" checkboxes.	Passed	
EWCJ176_2S_Reg_178	Providing the user for selected access to the ME EWLC via TACACS	To check whether user can able to have access with the selected checkbox's like "WLAN", "Wireless", "Command" Line Interfaces and "Management" checkboxes.	Passed	

EWCJ176_2S_Reg_179	Trying to login ME EWLC network via TACACS with Invalid credentials.	To verify whether user can able to login or not in ME EWLC via TACACS with invalid credentials	Passed	

Syslog's

Logical ID	Title	Description	Status	Defect ID
EWLCJ176S_Reg_204	Adding syslog server in eWLC and checking the syslog messages in syslog server	To check whether syslog's are generating in syslog server after adding in Ewlc	Passed	
EWLCJ176S_Reg_205	Configuring multiple syslog servers in eWLC and checking the syslog messages in syslog server	To verify whether syslog's are generating in syslog server after adding multiple servers in Ewlc	Passed	
EWLCJ176S_Reg_206	Downloading the syslog's after generated in Ewlc	To check whether able to download the syslog's from Ewlc	Passed	
EWLCJ176S_Reg_207	Clearing the logs in controller after generated successfully	To verify whether user able to clear the all generated logs in Ewlc	Passed	
EWLCJ176S_Reg_208	Checking the alert messages after configured syslog server level as "alert"	To check the alert syslog's in syslog server after configured severity level as alert	Passed	
EWLCJ176S_Reg_209	Configuring syslog servers in eWLC with log level setting as critical	To verify the critical logs in syslog server after configuration in device	Passed	
EWLCJ176S_Reg_210	Checking the information messages after configured syslog server level as "information"	To check the information syslog's in syslog server after configured severity level as information	Passed	
EWLCJ176S_Reg_211	Checking the debugging messages after configured syslog server level as "debugging"	To check the debugging syslog's in syslog server after configured severity level as debugging	Passed	

CWA (Central Web Authentication)

Logical ID	Title	Description	Status	Defect ID
EWLCJ176S_Reg_212	Creating a CWA along with ACL Configuration in eWLc UI	To check Whether CWA along with ACL Configuration in eWLC UI created or not	Passed	
EWLCJ176S_Reg_213	Associating a Japanese Windows Client to a SSID which is mapped with ISE	To verify whether Japanese Windows Client which is mapped to ISE is redirected successfully or not	Passed	
EWLCJ176S_Reg_214	Associating a iOS Client to a SSID which is mapped with ISE	To verify whether iOS Client which is mapped to ISE is redirected successfully or not	Passed	
EWLCJ176S_Reg_215	Associating a Android Client to a SSID which is mapped with ISE	To verify whether Android Client which is mapped to ISE is redirected successfully or not	Passed	
EWLCJ176S_Reg_216	Associating a MAC OS Client to a SSID which is mapped with ISE	To verify whether MAC Client which is mapped to ISE is redirected successfully or not	Passed	
EWLCJ176S_Reg_217	Associating a different Clients to SSID which is mapped with ISE and redirecting to Guest portal page with invalid credentials	To verify whether client connected to ssid redirecting to Guest portal page with invalid credentials	Passed	
EWLCJ176S_Reg_218	Associating a different Clients to a SSID which is mapped with ISE by creating AVC profile	To verify whether different Clients is redirected successfully and checking that particular application is dropped or not	Passed	

EWLCJ176S_Reg_219	Associating a different Clients to a SSID which is mapped with ISE by denying the action in ACL	To verify whether Clients gets denied when it is connected to SSID which is mapped with ISE	Passed	
EWLCJ176S_Reg_220	Associating a different Clients to a SSID which is mapped with ISE by permitting the action in ACL using TCP protocol	To verify whether Clients gets connected to SSID which is mapped with ISE by permitting the action in ACL using TCP protocol	Passed	
EWLCJ176S_Reg_221	Associating a different Clients to a SSID which is mapped with ISE by permitting the action in ACL using UDP protocol	To verify whether Clients gets connected to SSID which is mapped with ISE by permitting the action in ACL using UDP protocol	Passed	
EWLCJ176S_Reg_222	Associating a different Clients to a SSID which is mapped with ISE by permitting the action in ACL using ICMP protocol	To verify whether Clients gets connected to SSID which is mapped with ISE by permitting the action in ACL using ICMP protocol	Passed	
EWLCJ176S_Reg_223	Checking the expired Radius Guest User for proper error message	To verify whether the expired Guest user gets proper Error messages when he logging in	Passed	
EWLCJ176S_Reg_224	Validate whether eWLC is switch between configured Radius servers	To verify whether AAA authentication is occurring when one radius server goes down	Passed	
EWLCJ176S_Reg_225	Reboot the Controller after CWA enabling	To verify whether Configurations are showing same or different after controller reboot	Passed	

EWLCJ176S_Reg_226	Creating a CWA along with ACL Configuration through CLI	To verify whether ACL rule is created or not through CLI	Passed	
EWLCJ176S_Reg_227	Checking the configuration of CWA when the user is in Read-only	To verify whether configuration display error message or not when the user is in Read-only	Passed	
EWLCJ176S_Reg_228	Exporting/Importing configuration of CWA	To verify whether export and import is done successfully	Passed	

CMX Support

Logical ID	Title	Description	Status	Defect ID
EWLCJ176S_Reg_229	Adding Cisco eWLCto CMX	To add a Cisco eWLCto CMX and check if the eWLCgets added to the CMX with the eWLCstatus showing	Passed	
EWLCJ176S_Reg_230	Importing maps from prime infrastructure	To import maps from prime infrastructure and check if the maps gets imported to the cmx .	Passed	
EWLCJ176S_Reg_231	Importing the maps with Access points from PI to CMX	To import the maps from prime infra to CMX with Access points and check if the access point details are shown correctly including Clients connected .	Passed	
EWLCJ176S_Reg_232	Connecting the Client to the access point on the floor and check if the details of the Client.	To connect a Client to the access point on the floor and check if the details of the Clients are shown correctly or not.	Passed	
EWLCJ176S_Reg_233	Connecting many Clients from different place and check the location of the Clients	To connect many Client from different place to the access points and check if the location of the Client are shown in CMX	Passed	
EWLCJ176S_Reg_234	Using MAC address the Client devices are searched	To check whether Client device can be searched by specifying its MAC address or not	Passed	

EWLCJ176S_Reg_235	Using IP address the Client devices are searched	To check whether Client device can be searched by specifying its IP address or not	Passed	
EWLCJ176S_Reg_236	Using SSID the Client devices are searched	To verify whether Client device can be searched by specifying the SSID or not	Passed	
EWLCJ176S_Reg_237	Number of Clients visiting the building and floor in hourly and daily basis	Verifying the number of Clients visiting the building or floor on hourly and daily basis	Passed	
EWLCJ176S_Reg_238	Number of Client visits to the building and the floor	To check the number of new Clients and repeated Clients to the building or floor .	Passed	

MC2UC (Video streaming)

Logical ID	Title	Description	Status	Defect ID
EWLCJ176S_Reg_239	MC2UC traffic to local-switching client	To verify that the local-switching client subscribed to video streaming receives MC2UC traffic	Passed	
EWLCJ176S_Reg_240	MC2UC traffic to local-switching client when MC2UC is disabled	To verify the local switching client receiving MC traffic when MC2UC is disabled at the WLAN	Passed	
EWLCJ176S_Reg_241	MC2UC traffic to local-switching client when Media stream is removed at AP	To verify the local switching client receiving MC traffic when Media Stream is disabled at AP	Passed	
EWLCJ176S_Reg_242	Multiple LS clients in same vlan, same wlan, receiving MC2UC traffic	To verify whether the multiple local-switching clients receives MC2UC traffic when subscribed to video stream	Passed	
EWLCJ176S_Reg_243	Client disassociates when receiving MC2UC traffic	To verify whether AP stops sending traffic when client disassociates	Passed	
EWLCJ176S_Reg_244	LS client receiving MC2UC traffic roam between radios at the AP	To verify the local-switching client receiving MC2UC traffic roaming between radios of the AP	Passed	
EWLCJ176S_Reg_245	Flex LS client receiving MC2UC traffic when AP move from connected > SA > connected with same config	To verify whether the LS client receives continuous MC2UC traffic when AP moves from connected > SA > connected with same config	Passed	

EWLCJ176S_Reg_246	Flex LS client receiving MC2UC traffic when AP move from connected > SA > connected with different config	To verify whether the LS client receives continuous MC2UC traffic when AP moves from connected > SA > connected with different config	Passed	
EWLCJ176S_Reg_247	Flex AP reboot in connected mode when Flex LS client receiving MC2UC traffic	To verify whether client reassociates and receives MC2UC traffic when flex AP is rebooted in connected mode.	Passed	
EWLCJ176S_Reg_248	Videstream config sync for LS WLAN in HA setup	To verify whether the video streaming config for LS WLAN has been synced between the Active and Standby in HA setup	Passed	
EWLCJ176S_Reg_249	LS client with MC2UC enabled receiving traffic after switchover in HA pair	To verify whether LS client with MC2UC enabled receives unicast traffic after switchover	Passed	

UL/DL OFDMA Support for 9130

Logical ID	Title	Description	Status	Defect ID
EWLCJ176S_Reg_250	Configuring 11ax Access Points, Channel width, OFDMA & radio parameters for 5Ghz band.	To configure 11ax Access Points, Channel width, OFDMA & radio parameters for 5Ghz band.	Passed	
EWLCJ176S_Reg_251	Configuring 11ax Access Points, Channel width, OFDMA & radio parameters for 2.4Ghz band.	To configure 11ax Access Points, Channel width, OFDMA & radio parameters for 2.4Ghz band.	Passed	

Out of band access to standby WLC in a SSO pair

Logical ID	Title	Description	Status	Defect ID
EWLCJ176S_Reg_252	Configure HA SSO RMI & validate Standby Environmental Comments	To validate Standby Environmental Comments	Passed	
EWLCJ176S_Reg_253	Configure HA SSO RMI & validate Standby process Comments	To validate Standby process Comments	Passed	
EWLCJ176S_Reg_254	Configure HA SSO RMI & validate Standby debugging Comments	To validate Standby debugging Comments	Passed	
EWLCJ176S_Reg_255	Configure HA SSO RMI & validate Standby memory Comments	To validate Standby memory Comments	Passed	
EWLCJ176S_Reg_256	Configure HA SSO RMI & validate Standby File System Comments	To validate Standby File System Comments	Passed	
EWLCJ176S_Reg_257	Configure HA SSO RMI & validate HA RMI parameters.	To Configure HA SSO RMI	Passed	
EWLCJ176S_Reg_258	Verify HA setup details from Standby console	To verify HA setup details in Standby console	Passed	
EWLCJ176S_Reg_259	Check interfaces state from standby console	To check interfaces state from standby console	Passed	
EWLCJ176S_Reg_260	Check environment details from standby console	To monitor environment details from standby console	Passed	
EWLCJ176S_Reg_261	Check process usage details in standby console	To check process usage details in standby console	Passed	

RLAN Support for Fabric and across all modes in IOS-XE

Logical ID	Title	Description	Status	Defect ID
EWLCJ176S_Reg_262	Configuring RLAN in eWLC via UI	To Configure RLAN in eWLC through UI and check if the RLAN is created or not	Passed	
EWLCJ176S_Reg_263	Checking the client connectivity to RLAN configured with Open security and macfiltering	To verify whether client is connecting to RLAN with open security and macfiltering	Passed	
EWLCJ176S_Reg_264	Enabling the 802.1x security and MAC filtering to RLAN	To create a RLAN with 802.1x security and MAC filtering connecting a windows client to the RLAN and check if the client gets connected to the RLAN port in the AP or not	Passed	
EWLCJ176S_Reg_265	Configuring RLAN with open security and connect two wired clients (windows,MAC)	To verify whether two wired clients gets connected with open security	Passed	
EWLCJ176S_Reg_266	Configuring RLAN with open+macfilter security and connect 2 wired clients (windows,MAC)	To verify whether two wired clients gets connected with open+macfilter security	Passed	
EWLCJ176S_Reg_267	Connecting the client to the RLAN configuring with 802.1x security and host mode as single Host	To verify whether a windows client connecting to the RLAN with 802.1x security and host mode as single Host	Passed	
EWLCJ176S_Reg_268	Configuring RLAN with 802.1x security and host mode as multi host and connect the client	To verify whether a client connecting to RLAN with 802.1x security and host mode as multi host	Passed	

EWLCJ176S_Reg_269	Configuring RLAN with 802.1x security and host mode as multi domain and connect the client	To verify whether a client connecting to RLAN with 802.1x security and host mode as multi domain	Passed	
EWLCJ176S_Reg_270	Checking the client connectivity to a RLAN with 802.1x security and mapping a AVC profile	To create a RLAN with 802.1x security and applying AVC profile, connecting a windows client to the RLAN and check if the AVC profile gets applied to the client connecting to it or not.	Passed	
EWLCJ176S_Reg_271	Checking the client connectivity with 802.1x security and host mode as single Host and violation mode as Replace	To verify whether client connecting to a RLAN with 802.1x security and host mode as single host along with violation mode as Replace	Passed	
EWLCJ176S_Reg_272	Checking the client connectivity with 802.1x security and host mode as single Host and violation mode as Shutdown	To verify whether client connecting to a RLAN with 802.1x security and host mode as single host along with violation mode as Shutdown	Passed	
EWLCJ176S_Reg_273	Checking the client connectivity with 802.1x security and host mode as single Host and violation mode as protect	To verify whether client connecting to a RLAN with 802.1x security and host mode as single host along with violation mode as Protect	Passed	
EWLCJ176S_Reg_274	Rebooting the eWLC after connecting the client to RLAN	Checking whether RLAN configurations showing same or different after rebooting	Passed	

EWLCJ176S_Reg_275	Downgrading the eWLC after configuring RLAN and connect the client	Checking whether RLAN configurations showing same or different after downgrading and also verifying client connectivity	Passed	
EWLCJ176S_Reg_276	Upgrade the eWLC after configuring RLAN and connect the client	Checking whether RLAN configurations showing same or different after upgrading theeWLC and also verifying client connectivity	Passed	
EWLCJ176S_Reg_277	Uploading and downloading the config file and checking the RLAN configuration	To verify whether RLAN configurations showing same or different after uploading and downloading file to eWLC and also verifying client connectivity	Passed	
EWLCJ176_2S_Reg_270	Configuring RLAN in eWLC via UI	To Configure RLAN in eWLC through UI and check if the RLAN is created or not	Passed	
EWLCJ176_2S_Reg_271	Checking the client connectivity to RLAN configured with Open security and MA filtering	To verify whether client is connecting to RLAN with open security and MA filtering	Passed	
EWLCJ176_2S_Reg_272	Enabling the 802.1x security and MAC filtering to RLAN	To create a RLAN with 802.1x security and MAC filtering connecting a windows client to the RLAN and check if the client gets connected to the RLAN port in the AP or not	Passed	

EWLCJ176_2S_Reg_273	Configuring RLAN with open security and connect two wired clients (windows,MAC)	To verify whether two wired clients gets connected with open security	Passed	
EWLCJ176_2S_Reg_274	Configuring RLAN with open+macfilter security and connect 2 wired clients (windows,MAC)	To verify whether two wired clients gets connected with open+macfilter security	Passed	
EWLCJ176_2S_Reg_275	Connecting the client to the RLAN configuring with 802.1x security and host mode as single Host	To verify whether a windows client connecting to the RLAN with 802.1x security and host mode as single Host	Passed	
EWLCJ176_2S_Reg_276	Configuring RLAN with 802.1x security and host mode as multi host and connect the client	To verify whether a client connecting to RLAN with 802.1x security and host mode as multi host	Passed	
EWLCJ176_2S_Reg_277	Configuring RLAN with 802.1x security and host mode as multi domain and connect the client	To verify whether a client connecting to RLAN with 802.1x security and host mode as multi domain	Passed	
EWLCJ176_2S_Reg_278	Checking the client connectivity to a RLAN with 802.1x security and mapping a AVC profile	To create a RLAN with 802.1x security and applying AVC profile, connecting a windows client to the RLAN and check if the AVC profile gets applied to the client connecting to it or not.	Passed	
EWLCJ176_2S_Reg_279	Checking the client connectivity with 802.1x security and host mode as single Host and violation mode as Replace	To verify whether client connecting to a RLAN with 802.1x security and host mode as single host along with violation mode as Replace	Passed	

EWLCJ176_2S_Reg_280	Checking the client connectivity with 802.1x security and host mode as single Host and violation mode as Shutdown	To verify whether client connecting to a RLAN with 802.1x security and host mode as single host along with violation mode as Shutdown	Passed	
EWLCJ176_2S_Reg_281	Checking the client connectivity with 802.1x security and host mode as single Host and violation mode as protect	To verify whether client connecting to a RLAN with 802.1x security and host mode as single host along with violation mode as Protect	Passed	
EWLCJ176_2S_Reg_282	Rebooting the eWLC after connecting the client to RLAN	Checking whether RLAN configurations showing same or different after rebooting	Passed	
EWLCJ176_2S_Reg_283	Downgrading the eWLC after configuring RLAN and connect the client	Checking whether RLAN configurations showing same or different after downgradingeWLC and also verifying client connectivity	Passed	
EWLCJ176_2S_Reg_284	Upgrade the eWLC after configuring RLAN and connect the client	Checking whether RLAN configurations showing same or different after upgrading the WLC and also verifying client connectivity	Passed	
EWLCJ176_2S_Reg_285	Uploading and downloading the config file and checking the RLAN configuration	To verify whether RLAN configurations showing same or different after uploading and downloading file to eWLC and also verifying client connectivity	Passed	

COS AP Packet Tracer Phase 2

Logical ID	Title	Description	Status	Defect ID
EWLCJ176S_Reg_278	Enabling client trace dump in 3800 COS AP	To check if the client trace dump is enabled on the 3800 AP and check the behaviour of the AP	Passed	
EWLCJ176S_Reg_279	Enabling client trace dump in 2800 COS AP	To check if the client trace dump is enabled on the 2800 AP and check the behaviour of the AP	Passed	
EWLCJ176S_Reg_280	Enabling client trace dump in 4800 COS AP	To check if the client trace dump is enabled on the 4800 AP and check the behaviour of the AP	Passed	
EWLCJ176S_Reg_281	Capturing client trace dump for the client connected with Open security with 2800 AP	To capture the client trace dump using 2800 AP for the client connected with OPEN security	Passed	
EWLCJ176S_Reg_282	Capturing client trace dump for the client connected with WPA 2 security with 2800 AP	To capture the client trace dump using 2800 AP for the client connected with WPA 2 security	Passed	
EWLCJ176S_Reg_283	Capturing client trace dump for the client connected with WPA 3 security with 2800 AP	To capture the client trace dump using 2800 AP for the client connected with WPA 3 security	Passed	
EWLCJ176S_Reg_284	Capturing client trace dump for the client connected with Open security with 3800 AP	To capture the client trace dump using 3800 AP for the client connected with OPEN security	Passed	

EWLCJ176S_Reg_285	Capturing client trace dump for the client connected with WPA 2 security with 3800 AP	To capture the client trace dump using 3800 AP for the client connected with WPA 2 security	Passed	
EWLCJ176S_Reg_286	Capturing client trace dump for the client connected with WPA 3 security with 3800 AP	To capture the client trace dump using 3800 AP for the client connected with WPA 3 security	Passed	
EWLCJ176S_Reg_287	Capturing client trace dump for the client connected with Open security with 4800 AP	To capture the client trace dump using 4800 AP for the client connected with OPEN security	Passed	
EWLCJ176S_Reg_288	Capturing client trace dump for the client connected with WPA 2 security with 4800 AP	To capture the client trace dump using 4800 AP for the client connected with WPA 2 security	Passed	
EWLCJ176S_Reg_289	Capturing client trace dump for the client connected with WPA 3 security with 4800 AP	To capture the client trace dump using 4800 AP for the client connected with WPA 3 security	Passed	
EWLCJ176S_Reg_290	Analysing the client trace for windows client connected to COS AP	To analyse the client trace dump for the windows client connected to COS AP	Passed	
EWLCJ176S_Reg_291	Analysing the client trace for Android client connected to COS AP	To analyse the client trace dump for the Android client connected to COS AP	Passed	
EWLCJ176S_Reg_292	Analysing the client trace for IOS client connected to COS AP	To analyse the client trace dump for the IOS client connected to COS AP	Passed	

EWLCJ176S_Reg_293	Analysing the client trace for MAC os client connected to COS AP	To analyse the client trace dump for the MAC os client connected to COS AP	Passed	
EWLCJ176S_Reg_294	Connecting 4 clients to the COS AP and analysing the client trace dump in AP	To analyse the client trace dump for the MAC os client connected to COS AP	Passed	
EWLCJ176S_Reg_295	Check if the client trace dump is triggered when the AP operating in 2.4 GHz	To check if the client trace dump is generated when the AP is operating in 2.4GHz and client connected to it	Passed	
EWLCJ176S_Reg_296	Check if the client trace dump is triggered when the AP operating in 5 GHz	To check if the client trace dump is generated when the AP is operating in 5 GHz and client connected to it	Passed	

DL 11ax Mu-MIMO for (VC/SS)APs

Logical ID	Title	Description	Status	Defect ID
EWLCJ176S_Reg_297	Configuring 11ax Access Points, Channel width, 11ax MU-MIMO & radio parameters for 5Ghz band.	To configure 11ax Access Points, Channel width, 11ax MU-MIMO & radio parameters for 5Ghz band.	Passed	
EWLCJ176S_Reg_298	Configuring 11ax Access Points, Channel width, 11ax MU-MIMO & radio parameters for 2.4Ghz band.	To configure 11ax Access Points, Channel width, 11ax MU-MIMO & radio parameters for 2.4Ghz band.	Passed	
EWLCJ176S_Reg_299	Verifying details with 11ax Android client connected.	To verify 11ax MU-MIMO details with 11ax Android client connected.	Passed	
EWLCJ176S_Reg_300	Verifying details with 11ax iPhone client connected.	To verify 11ax MU-MIMO details with 11ax iPhone client connected.	Passed	
EWLCJ176S_Reg_301	Verifying details with non 11ax Windows client connected.	To verify 11ax MU-MIMO details with non 11ax Windows client connected.	Passed	
EWLCJ176S_Reg_302	Verifying details with non 11ax Mac client connected.	To verify 11ax MU-MIMO details with non 11ax Mac client connected.	Passed	
EWLCJ176S_Reg_303	Verify details by connecting client to 2.4Ghz radio.	To verify 11ax MU-MIMO details by connecting client to 2.4Ghz radio.	Passed	
EWLCJ176S_Reg_304	Verify MU-MIMO using different models of AP - 9115, 9120, 9130.	To verify MU-MIMO using different models of AP - 9115, 9120, 9130.	Passed	

EWLCJ176S_Reg_305	Check 11ax MU-MIMO support for AP configured in Local mode.	To check 11ax MU-MIMO support for AP configured in Local mode.	Passed	
EWLCJ176S_Reg_306	Check 11ax MU-MIMO support for AP configured in Flex-connect mode.	To check 11ax MU-MIMO support for AP configured in Flex-connect mode.	Passed	
EWLCJ176S_Reg_307	Check 11ax MU-MIMO support for AP configured in Bridge mode.	To check 11ax MU-MIMO support for AP configured in Bridge mode.	Passed	
EWLCJ176S_Reg_308	Check 11ax MU-MIMO support for AP configured in Flex Mesh mode.	To check 11ax MU-MIMO support for AP configured in Flex Mesh mode.	Passed	
EWLCJ176S_Reg_309	Verify 11ax MU-MIMO details with client connecting to WPA2 - PSK configured WLAN	To verify 11ax MU-MIMO details with client connecting to WPA2 - PSK configured WLAN	Passed	
EWLCJ176S_Reg_310	Verify 11ax MU-MIMO details with client connecting to WPA3 - Dot1x configured WLAN	To verify 11ax MU-MIMO details with client connecting to WPA3 - Dot1x configured WLAN	Passed	
EWLCJ176S_Reg_311	Connect upto 8 clients and monitor DL/UL 11ax MU-MIMO statistics	To connect upto 8 clients and monitor DL/UL 11ax MU-MIMO statistics	Passed	
EWLCJ176S_Reg_312	Modify spatial stream config to 1 stream and monitor 11ax MU-MIMO statistics.	To modify spatial stream config to 1 stream and monitor 11ax MU-MIMO statistics.	Passed	
EWLCJ176S_Reg_313	Modify spatial stream config to 2 streams and monitor 11ax MU-MIMO statistics.	To modify spatial stream config to 2 streams and monitor 11ax MU-MIMO statistics.	Passed	

EWLCJ176S_Reg_314	Modify spatial stream config to 3 streams and monitor 11ax MU-MIMO statistics.	To modify spatial stream config to 3 streams and monitor 11ax MU-MIMO statistics.	Passed	
EWLCJ176S_Reg_315	Modify spatial stream config to 4 streams and monitor 11ax MU-MIMO statistics.	To modify spatial stream config to 4 streams and monitor 11ax MU-MIMO statistics.	Passed	
EWLCJ176S_Reg_316	Enable video stream and monitor DL/UL 11ax MU-MIMO statistics	To enable video stream and monitor DL/UL 11ax MU-MIMO statistics	Passed	
EWLCJ176S_Reg_317	Modify MCS data rates & monitor 11ax MU-MIMO stats with 11ax Android client connected.	To modify MCS data rates & monitor 11ax MU-MIMO stats with 11ax Android client connected.	Passed	
EWLCJ176S_Reg_318	Check 11ax MU-MIMO stats with roaming client scenario	Check 11ax MU-MIMO stats with roaming client scenario	Passed	
EWLCJ176_2S_Reg_286	Configuring 11ax Access Points, Channel width, 11ax MU-MIMO & radio parameters for 5Ghz band.	To configure 11ax Access Points, Channel width, 11ax MU-MIMO & radio parameters for 5Ghz band.	Passed	
EWLCJ176_2S_Reg_287	Configuring 11ax Access Points, Channel width, 11ax MU-MIMO & radio parameters for 2.4Ghz band.	To configure 11ax Access Points, Channel width, 11ax MU-MIMO & radio parameters for 2.4Ghz band.	Passed	
EWLCJ176_2S_Reg_288	Verifying details with 11ax Android client connected.	To verify 11ax MU-MIMO details with 11ax Android client connected.	Passed	
EWLCJ176_2S_Reg_289	Verifying details with 11ax iPhone client connected.	To verify 11ax MU-MIMO details with 11ax iPhone client connected.	Passed	

EWLCJ176_2S_Reg_290	Verifying details with non 11ax Windows client connected.	To verify 11ax MU-MIMO details with non 11ax Windows client connected.	Passed	
EWLCJ176_2S_Reg_291	Verifying details with non 11ax Mac client connected.	To verify 11ax MU-MIMO details with non 11ax Mac client connected.	Passed	
EWLCJ176_2S_Reg_292	Verify details by connecting client to 2.4Ghz radio.	To verify 11ax MU-MIMO details by connecting client to 2.4Ghz radio.	Passed	
EWLCJ176_2S_Reg_293	Verify MU-MIMO using different models of AP - 9115, 9120, 9130.	To verify MU-MIMO using different models of AP - 9115, 9120, 9130.	Passed	
EWLCJ176_2S_Reg_294	Check 11ax MU-MIMO support for AP configured in Local mode.	To check 11ax MU-MIMO support for AP configured in Local mode.	Passed	
EWLCJ176_2S_Reg_295	Check 11ax MU-MIMO support for AP configured in Flex-connect mode.	To check 11ax MU-MIMO support for AP configured in Flex-connect mode.	Passed	
EWLCJ176_2S_Reg_296	Check 11ax MU-MIMO support for AP configured in Bridge mode.	To check 11ax MU-MIMO support for AP configured in Bridge mode.	Passed	
EWLCJ176_2S_Reg_297	Check 11ax MU-MIMO support for AP configured in Flex+Mesh mode.	To check 11ax MU-MIMO support for AP configured in Flex+Mesh mode.	Passed	
EWLCJ176_2S_Reg_298	Verify 11ax MU-MIMO details with client connecting to WPA2 - PSK configured WLAN	To verify 11ax MU-MIMO details with client connecting to WPA2 - PSK configured WLAN	Passed	

EWLCJ176_2S_Reg_299	Verify 11ax MU-MIMO details with client connecting to WPA3 - Dot1x configured WLAN	To verify 11ax MU-MIMO details with client connecting to WPA3 - Dot1x configured WLAN	Passed	
EWLCJ176_2S_Reg_300	Connect upto 8 clients and monitor DL/UL 11ax MU-MIMO statistics	To connect upto 8 clients and monitor DL/UL 11ax MU-MIMO statistics	Passed	
EWLCJ176_2S_Reg_301	Modify spatial stream config to 1 stream and monitor 11ax MU-MIMO statistics.	To modify spatial stream config to 1 stream and monitor 11ax MU-MIMO statistics.	Passed	
EWLCJ176_2S_Reg_302	Modify spatial stream config to 2 streams and monitor 11ax MU-MIMO statistics.	To modify spatial stream config to 2 streams and monitor 11ax MU-MIMO statistics.	Passed	
EWLCJ176_2S_Reg_303	Modify spatial stream config to 3 streams and monitor 11ax MU-MIMO statistics.	To modify spatial stream config to 3 streams and monitor 11ax MU-MIMO statistics.	Passed	
EWLCJ176_2S_Reg_304	Modify spatial stream config to 4 streams and monitor 11ax MU-MIMO statistics.	To modify spatial stream config to 4 streams and monitor 11ax MU-MIMO statistics.	Passed	
EWLCJ176_2S_Reg_305	Enable video stream and monitor DL/UL 11ax MU-MIMO statistics	To enable video stream and monitor DL/UL 11ax MU-MIMO statistics	Passed	
EWLCJ176_2S_Reg_306	Modify MCS data rates & monitor 11ax MU-MIMO stats with 11ax Android client connected.	To modify MCS data rates & monitor 11ax MU-MIMO stats with 11ax Android client connected.	Passed	
EWLCJ176_2S_Reg_307	Check 11ax MU-MIMO stats with roaming client scenario	Check 11ax MU-MIMO stats with roaming client scenario	Passed	

Web UI for Golden monitor for Packet drops

Logical ID	Title	Description	Status	Defect ID
EWLCJ176S_Reg_320	Verify that display of Datapath utilization information for 9800-CL .	To Verify that display of Datapath utilization information for Virtual EWLC in UI is same as CLI.	Passed	
EWLCJ176S_Reg_321	Verify that display of Datapath utilization information for 9800-80	To Verify that display of Datapath utilization information for 9800-80 is same as CLI	Passed	
EWLCJ176S_Reg_322	Verify that display of Datapath utilization information for 9800-L	To Verify that display of Datapath utilization information for 9800-L is same as CLI	Passed	
EWLCJ176S_Reg_323	Verify that display of Datapath utilization information for 9800-40	To Verify that display of Datapath utilization information for Gladius is same as CLI	Passed	
EWLCJ176S_Reg_324	Verify that display of CPU allocation dashlet is not available for appliance based controllers	To Verify that display of CPU allocation dashlet is not available for appliance based controllers same as CLI	Passed	
EWLCJ176S_Reg_325	Verify that display of right unit for tx and rx of packets per port for all controller types	To Verify that display of right unit for tx and rx of packets per port for all controller types same as CLI	Passed	

EWLCJ176S_Reg_326	Verify that display of CPU vs Time graph is shown properly in Appliance based ewlc	To Verify that display of CPU vs Time graph is shown properly as per CLI in Appliance based ewlc	Passed	
EWLCJ176S_Reg_327	Verify that display of CPU allocation during export/import of config files for ewlc 9800-CL	To Verify that display of CPU allocation during export/import of config files for ewlc 9800-CL	Passed	
EWLCJ176S_Reg_328	Verify that display of CPU utilization during backup/restore of config files for appliance based ewlc	To Verify that display of CPU utilization during backup/restore of config files for appliance based ewlc	Passed	
EWLCJ176S_Reg_329	Verify that display of CPU allocation after performing upgrade/downgrade of ewlc 9800-CL	To Verify that display of CPU allocation after performing upgrade/downgrade of ewlc 9800-CL	Passed	
EWLCJ176S_Reg_330	Verify that display of CPU allocation after performing AP upgrade/downgrade for ewlc 9800-CL	To Verify that display of CPU allocation after performing AP upgrade/downgrade for ewlc 9800-CL	Passed	
EWLCJ176S_Reg_331	Verify that display of CPU allocation after Performing Rolling AP upgrade from PI or DNAC then check the CPU Allocation	To Verify that display of CPU allocation after Performing Rolling AP upgrade from PI or DNAC then check the CPU Allocation	Passed	
EWLCJ176S_Reg_332	Verify that display of CPU Utilization after Enabling all the debug commands together	To Verify that display of CPU Utilization after Enabling all the debug commands together	Passed	

EWLCJ176S_Reg_333	Verify that display of Datapath utilization information for eWLC after connecting more than one clients in different AP's .	To Verify that display of Datapath utilization information for eWLC after connecting more than one clients in different AP's .	Passed	
EWLCJ176S_Reg_319	Verify that display of CPU allocation dashlet is available only for 9800-CL	To Verify that display of CPU allocation dashlet is available only for virtual platform and same as CLI output	Passed	

Dynamic Protocol Pack Upgrade - WLC and AP

Logical ID	Title	Description	Status	Defect ID
EWLCJ176S_Reg_352	Checking the Dynamic Protocol Pack Upgrade tab in AVC page is opening or not	To check if the Dynamic Protocol Pack Upgrade tab in AVC page is opening or not and check if the page is loaded properly	Passed	
EWLCJ176S_Reg_353	Checking the Dynamic Protocol Pack Upgrade tab in AVC page is opening or not with dark mode enabled	To check if the Dynamic Protocol Pack Upgrade tab in AVC page is opening or not with dark mode enabled and check if the page is loaded properly	Passed	
EWLCJ176S_Reg_354	Check the active protocol pack in the controller using the CLI command	To check the active protocol pack in the controller using the CLI command and verify the same using UI	Passed	
EWLCJ176S_Reg_355	Adding the protocol pack for eWLC 9800-40	To upgrade the protocol pack for eWLC for 9800-40	Passed	
EWLCJ176S_Reg_356	Adding the protocol pack for eWLC 9800-80	To upgrade the protocol pack for eWLC for 9800-80	Passed	
EWLCJ176S_Reg_357	Adding the protocol pack for eWLC 9800-L	To upgrade the protocol pack for eWLC for 9800-L	Passed	
EWLCJ176S_Reg_358	Adding the protocol pack for eWLC 9800-CL	To upgrade the protocol pack for eWLC for 9800-CL	Passed	
EWLCJ176S_Reg_359	Deleting the protocol pack upgraded to eWLC 9800-40 to check	To delete the upgraded protocol pack from eWLC 9800-40 and check if the pack is deleted .	Passed	

EWLCJ176S_Reg_360	Deleting the protocol pack upgraded to eWLC 9800-80 to check	To delete the upgraded protocol pack from eWLC 9800-80 and check if the pack is deleted .	Passed	
EWLCJ176S_Reg_361	Deleting the protocol pack upgraded to eWLC 9800-L to check	To delete the upgraded protocol pack from eWLC 9800-CL and check if the pack is deleted .	Passed	
EWLCJ176S_Reg_362	Deleting the protocol pack upgraded to eWLC 9800-CL to check	To delete the upgraded protocol pack from eWLC 9800-CL and check if the pack is deleted .	Passed	
EWLCJ176S_Reg_363	Check if the upgrade of protocol pack happens in eWLC 9800-40 when the memory of boot flash is very less	To check if the upgrade of the protocol pack happens if the space is less in the boot flash of the eWLC 9800-40 device	Passed	
EWLCJ176S_Reg_364	Check if the upgrade of protocol pack happens in eWLC 9800-40 when the memory of boot flash is very less	To check if the upgrade of the protocol pack happens if the space is less in the boot flash of the eWLC 9800-40 device	Passed	
EWLCJ176S_Reg_365	Check if the upgrade of protocol pack happens in eWLC 9800-40 when the memory of boot flash is very less	To check if the upgrade of the protocol pack happens if the space is less in the boot flash of the eWLC 9800-40 device	Passed	
EWLCJ176S_Reg_366	Check if the upgrade of protocol pack happens in eWLC 9800-40 when the memory of boot flash is very less	To check if the upgrade of the protocol pack happens if the space is less in the boot flash of the eWLC 9800-40 device	Passed	

EWLCJ176S_Reg_367	Upgrading the protocol pack and also upgrading the eWLC 9800-40 to watch the protocol pack	To upgrade the protocol pack and eWLC 9800-40 and check if the protocol pack if same before and after upgrading	Passed	
EWLCJ176S_Reg_368	Downgrading the eWLC 9800-40 after upgrading the protocol pack	To downgrade the eWLC 9800-40 after upgrading the protocol pack and check the version of the protocol pack after downgrade	Passed	
EWLCJ176S_Reg_369	Upgrading the protocol pack and also upgrading the eWLC 9800-80 to watch the protocol pack	To upgrade the protocol pack and eWLC 9800-80 and check if the protocol pack if same before and after upgrading	Passed	
EWLCJ176S_Reg_370	Downgrading the eWLC 9800-80 after upgrading the protocol pack	To downgrade the eWLC 9800-80 after upgrading the protocol pack and check the version of the protocol pack after downgrade	Passed	
EWLCJ176S_Reg_371	Upgrading the protocol pack and also upgrading the eWLC 9800-CL to watch the protocol pack	To upgrade the protocol pack and eWLC 9800-CL and check if the protocol pack if same before and after upgrading	Passed	
EWLCJ176S_Reg_372	Downgrading the eWLC 9800-CL after upgrading the protocol pack	To downgrade the eWLC 9800-CL after upgrading the protocol pack and check the version of the protocol pack after downgrade	Passed	
EWLCJ176S_Reg_373	Upgrading the protocol pack and also upgrading the eWLC 9800-L to watch the protocol pack	To upgrade the protocol pack and eWLC 9800-L and check if the protocol pack if same before and after upgrading	Passed	

EWLCJ176S_Reg_374	Downgrading the eWLC 9800-L after upgrading the protocol pack	To downgrade the eWLC 9800-L after upgrading the protocol pack and check the version of the protocol pack after downgrade	Passed	

Umbrella Enhancements

Logical ID	Title	Description	Status	Defect ID
EWLCJ176S_Reg_441	Verifying ewlc registered with Umbrella Dashboard	To verify ewlc registered with Umbrella Dashboard	Passed	CSCvx41349
EWLCJ176S_Reg_442	Verifying syslog's/error messages related to splitdns after changing AP from Local mode to Flex mode	To verify syslog's/error messages related to splitdns when AP is in Flex mode	Passed	
EWLCJ176S_Reg_443	Configure Umbrella Parameter Map through CLI and verify details in GUI	To configure Umbrella Parameter Map through CLI and verifying the same in GUI	Passed	
EWLCJ176S_Reg_444	Enabling or disabling DNScrypt in GUI and CLI and verify the details	To verify DNScrypt enabling or disabling through GUI and CLI	Passed	
EWLCJ176S_Reg_445	Configure whitelist with patterns, set up AP in flex and connect end devices (like Windows, Android etc) to Umbrella enabled WLAN profile	To configure whitelist with patterns, set up AP in flex and to connect any client to Umbrella enabled WLAN profile	Passed	CSCvx44999
EWLCJ176S_Reg_446	Configure whitelist with patterns, set up AP in flex and connect end devices to Umbrella enabled WLAN profile and verify packets sent to clients and verify there are no errors/syslog's	To configure whitelist with patterns, set up AP in flex and to connect any client to Umbrella enabled WLAN profile and verify packets sent to clients and verify there are no errors/syslog's	Passed	CSCvx43702

EWLCJ176S_Reg_447	Configure custom parameter maps, set up ap in flex, configure whitelist with patterns, check multi-profile splitdns works or not and check no error/syslog messages	To configure custom parameter maps, set up ap in flex, configure whitelist with patterns, check multi-profile splitdns works or not and verify no syslog's/no error messages	Passed	
EWLCJ176S_Reg_448	Verify show commands on controller: Configure controller in flex mode, multiple maps, multiple whitelists, IPv4 server list, IPv6 server list, join clients. Check output is correct. Same check on AP.	To verify show commands on controller: Configure controller in flex mode, multiple maps, multiple whitelists, IPv4 server list, IPv6 server list, join clients. Check output is correct. Same check on AP.	Passed	
EWLCJ176S_Reg_449	Verify client connected or not when global parameter enabled in Local Mode	To verify whether client connected or not when global parameter enabled in Local Mode	Passed	
EWLCJ176S_Reg_450	Verify multiple clients connected or not when global parameter and multiple whitelists configured in Local mode	To verify whether multiple clients connected or not when global parameter and multiple whitelists configured in Local mode	Passed	
EWLCJ176S_Reg_451	Verify multiple clients connected or not when custom global parameter and multiple whitelists configured in Local mode	To verify whether multiple clients connected or not when custom global parameter and multiple whitelists configured in Local mode	Passed	

EWLCJ176S_Reg_452	Verify show commands on controller: Configure controller in local mode, multiple maps, multiple whitelists, IPv4 server list, IPv6 server list, join clients. Check output is correct. Same check on AP.	To verify show commands on controller: Configure controller in local mode, multiple maps, multiple whitelists, IPv4 server list, IPv6 server list, join clients. Check output is correct. Same check on AP.	Passed	
EWLCJ176S_Reg_453	Configure regex param-map with various patterns. Check that the whitelist cannot be associated to an Umbrella profile if it contains unsupported patterns for wireless (config validation)	To configure regex param-map with various patterns. Check that the whitelist cannot be associated to an Umbrella profile if it contains unsupported patterns for wireless (config validation)	Passed	
EWLCJ176S_Reg_454	Reload: Configure multiple pmps and multiple local domains, reload the controller and verify configured data exists or not	Reload: To configure multiple pmps and multiple local domains, reload the controller and to verify configured data exists or not	Passed	
EWLCJ176S_Reg_455	Reload: Configure multiple pmps and multiple local domains, reload the controller with 17.5 build and verify configured data exists or not in 17.4 build	Reload: To configure multiple pmps and multiple local domains, reload the controller with 17.5 build and to verify configured data exists or not in 17.4 build	Passed	
EWLCJ176S_Reg_456	Reload: configure resolver ipv4 address, reload the controller, verify there are no errors	Reload: To configure resolver ipv4 address, reload the controller, to verify there are no errors	Passed	

HA SSO RMI

Logical ID	Title	Description	Status	Defect ID
EWLCJ176S_Reg_375	Configure HA setup using RP option.	To configure HA setup using RP option.	Passed	
EWLCJ176S_Reg_376	Validate the HA setup parameters.	To validate the HA setup parameters.	Passed	
EWLCJ176S_Reg_377	Unpairing HA setup using no RP-Method	To unpair the HA setup using no RP-Method	Passed	
EWLCJ176S_Reg_378	Configure HA SSO RMI	To Configure HA SSO RMI	Passed	
EWLCJ176S_Reg_379	Validate the HA RMI parameters.	To validate the HA RMI parameters.	Passed	
EWLCJ176S_Reg_380	Update RMI configuration in eWLC UI and check the output	To update RMI configuration in eWLC UI and check the output	Passed	
EWLCJ176S_Reg_381	Enable gateway failover, verify output details and monitor devices for switchover.	To enable gateway failover, verify output details & monitor devices for switchover.	Passed	
EWLCJ176S_Reg_382	Force-switchover to verify HA SSO RMI behaviour.	To verify HA SSO RMI behaviour on force-switchover.	Passed	
EWLCJ176S_Reg_383	Enabling the RP method with RMI enabled already.	To enable the RP method with RMI option enabled already.	Passed	
EWLCJ176S_Reg_384	ISSU upgrade with HA SSO RMI	To perform ISSU upgrade in HA SSO RMI setup and monitor behaviour	Passed	
EWLCJ176S_Reg_385	Check ISSU downgrade with HA SSO RMI	To perform ISSU upgrade in HA SSO RMI setup and monitor behaviour	Passed	
EWLCJ176S_Reg_386	Client retention during ISSU upgrade/downgrade	To verify client retention after ISSU upgrade/downgrade.	Passed	

EWLCJ176S_Reg_387	Force multiple switchover after upgrade to check if RMI link is up or not	To force multiple switchover after upgrade to check if RMI link is up or not	Passed	
EWLCJ176S_Reg_388	Force multiple switchover and verify AP & client association	To force multiple switchover and verify AP & client association	Passed	
EWLCJ176S_Reg_389	Validate licensing information after ISSU upgrade/downgrade	To validate licensing information after ISSU upgrade/downgrade	Passed	
EWLCJ176S_Reg_390	Validate licensing information after multiple switchover and reload	To validate licensing information after multiple switchover and reload	Passed	
EWLCJ176S_Reg_391	Clear RMI based configuration from UI	To clear RMI based configuration from UI	Passed	
EWLCJ176S_Reg_392	Clear RMI based configuration from CLI	To clear RMI based configuration from CLI	Passed	
EWLCJ176S_Reg_393	Configure HA SSO RMI after RP-clear & validate HA RMI parameters.	To configure HA SSO RMI after RP-clear & validate HA RMI parameters.	Passed	
EWLCJ176S_Reg_394	Verify HA setup details from Standby console	To verify HA setup details in Standby console	Passed	
EWLCJ176S_Reg_395	Check interfaces state from standby console	To check interfaces state from standby console	Passed	
EWLCJ176S_Reg_396	Check environment details from standby console	To monitor environment details from standby console	Passed	
EWLCJ176S_Reg_397	Check process usage details in standby console	To check process usage details in standby console	Passed	

EWLCJ176S_Reg_398	Monitor running process in Standby unit from Active unit console	To monitor running process in Standby unit from Active unit console	Passed	
EWLCJ176S_Reg_399	SSH to standby console directly and check connectivity	To SSH to standby console directly and check connectivity	Passed	
EWLCJ176_2S_Reg_308	Configure HA setup using RP option.	To configure HA setup using RP option.	Passed	
EWLCJ176_2S_Reg_309	Validate the HA setup parameters.	To validate the HA setup parameters.	Passed	
EWLCJ176_2S_Reg_310	Unpairing HA setup using no RP-Method	To unpair the HA setup using no RP-Method	Passed	
EWLCJ176_2S_Reg_311	Configure HA SSO RMI	To Configure HA SSO RMI	Passed	
EWLCJ176_2S_Reg_312	Validate the HA RMI parameters.	To validate the HA RMI parameters.	Passed	
EWLCJ176_2S_Reg_313	Update RMI configuration in eWLC UI and check the output	To update RMI configuration in eWLC UI and check the output	Passed	
EWLCJ176_2S_Reg_314	Enable gateway failover, verify output details and monitor devices for switchover.	To enable gateway failover, verify output details & monitor devices for switchover.	Passed	
EWLCJ176_2S_Reg_315	Force-switchover to verify HA SSO RMI behaviour.	To verify HA SSO RMI behaviour on force-switchover.	Passed	
EWLCJ176_2S_Reg_316	Enabling the RP method with RMI enabled already.	To enable the RP method with RMI option enabled already.	Passed	
EWLCJ176_2S_Reg_317	ISSU upgrade with HA SSO RMI	To perform ISSU upgrade in HA SSO RMI setup and monitor behaviour	Passed	
EWLCJ176_2S_Reg_318	Check ISSU downgrade with HA SSO RMI	To perform ISSU upgrade in HA SSO RMI setup and monitor behaviour	Passed	

EWLCJ176_2S_Reg_319	Client retention during ISSU upgrade/downgrade	To verify client retention after ISSU upgrade/downgrade.	Passed	
EWLCJ176_2S_Reg_320	Force multiple switchover after upgrade to check if RMI link is up or not	To force multiple switchover after upgrade to check if RMI link is up or not	Passed	
EWLCJ176_2S_Reg_321	Force multiple switchover and verify AP & client association	To force multiple switchover and verify AP & client association	Passed	
EWLCJ176_2S_Reg_322	Validate licensing information after ISSU upgrade/downgrade	To validate licensing information after ISSU upgrade/downgrade	Passed	
EWLCJ176_2S_Reg_323	Validate licensing information after multiple switchover and reload	To validate licensing information after multiple switchover and reload	Passed	
EWLCJ176_2S_Reg_324	Clear RMI based configuration from UI	To clear RMI based configuration from UI	Passed	
EWLCJ176_2S_Reg_325	Clear RMI based configuration from CLI	To clear RMI based configuration from CLI	Passed	
EWLCJ176_2S_Reg_326	Configure HA SSO RMI after RP-clear & validate HA RMI parameters.	To configure HA SSO RMI after RP-clear & validate HA RMI parameters.	Passed	
EWLCJ176_2S_Reg_327	Verify HA setup details from Standby console	To verify HA setup details in Standby console	Passed	
EWLCJ176_2S_Reg_328	Check interfaces state from standby console	To check interfaces state from standby console	Passed	
EWLCJ176_2S_Reg_329	Check environment details from standby console	To monitor environment details from standby console	Passed	

EWLCJ176_2S_Reg_330	Check process usage details in standby console	To check process usage details in standby console	Passed	
EWLCJ176_2S_Reg_331	Monitor running process in Standby unit from Active unit console	To monitor running process in Standby unit from Active unit console	Passed	
EWLCJ176_2S_Reg_332	SSH to standby console directly and check connectivity	To SSH to standby console directly and check connectivity	Passed	

Smart Licencing

Logical ID	Title	Description	Status	Defect ID
EWLCJ176S_Reg_400	Smart Account Creation, registration and activation.	To verify smart Account Creation, registration and activation.	Passed	
EWLCJ176S_Reg_401	Enable Smart Licensing and Register Device	To enable Smart Licensing and Register Device	Passed	
EWLCJ176S_Reg_402	Smart License Reservation	To perform Smart License Reservation and verify details	Passed	
EWLCJ176S_Reg_403	Deleting SLR Licenses	To verify by deleting SLR Licenses	Passed	
EWLCJ176S_Reg_404	Smart Licensing HA Support	To verify Smart Licensing for HA Support	Passed	
EWLCJ176S_Reg_405	Change a SLR on a C9800 SSO HA pair	To change a SLR on a C9800 SSO HA pair	Passed	
EWLCJ176S_Reg_406	Removing SLR from a C9800 SSO HA pair	To verify by removing SLR from a C9800 SSO HA pair	Passed	
EWLCJ176S_Reg_407	Validate license info in HA SSO RMI pair	To validate license info in HA SSO RMI pair	Passed	
EWLCJ176S_Reg_408	Validate license info on Standby unit directly	To validate license info on standby unit directly	Passed	
EWLCJ176S_Reg_409	Validate license info after ISSU upgrade	To validate license info after ISSU upgrade	Passed	
EWLCJ176S_Reg_410	Validate license info after multiple switchover	To validate license info after multiple switchover	Passed	
EWLCJ176S_Reg_411	Validate license info on multiple reload	To validate license info on multiple reboot	Passed	

EWCJ176S_Reg_333	Smart Account Creation, registration and activation.	To verify smart Account Creation, registration and activation.	Passed	
EWCJ176S_Reg_334	Generate token from CSSM	To Generate token from CSSM	Passed	
EWCJ176S_Reg_335	Product instance direct-connect using trust token	To verify Product instance direct-connect using trust token	Passed	
EWCJ176S_Reg_336	verify device status in CSSM	To verify device status in CSSM	Passed	
EWCJ176S_Reg_337	verify Smart Licensing Support in eWC HA	To verify Smart Licensing Support in eWC HA	Passed	
EWCJ176S_Reg_338	verify device details and license count changes in CSSM	To verify device details and license count changes in CSSM	Passed	
EWCJ176S_Reg_339	Add More AP's to device and Install trust token validate count on CSSM	To Add More AP's to device after Installing trust token to validate license count on CSSM	Passed	
EWCJ176S_Reg_340	Validate license info after switchover in AP	To validate license info after switchover in AP	Passed	
EWCJ176S_Reg_341	Validate license info on multiple reload	To validate license info on multiple reboot	Passed	
EWCJ176S_Reg_342	Install CSLU and add device and check status	Install CSLU and add device and check status	Passed	
EWCJ176S_Reg_343	Verify product details in CSSM after successfully shared product details from CSLU	Verify product details in CSSM after successfully shared product details from CSLU	Passed	
EWLCJ176_2S_Reg_333	Smart Account Creation, registration and activation.	To verify smart Account Creation, registration and activation.	Passed	

EWLCJ176_2S_Reg_334	Enable Smart Licensing and Register Device	To enable Smart Licensing and Register Device	Passed	
EWLCJ176_2S_Reg_335	Smart License Reservation	To perform Smart License Reservation and verify details	Passed	
EWLCJ176_2S_Reg_336	Deleting SLR Licenses	To verify by deleting SLR Licenses	Passed	
EWLCJ176_2S_Reg_337	Smart Licensing HA Support	To verify Smart Licensing for HA Support	Passed	
EWLCJ176_2S_Reg_338	Change a SLR on a C9800 SSO HA pair	To change a SLR on a C9800 SSO HA pair	Passed	
EWLCJ176_2S_Reg_339	Removing SLR from a C9800 SSO HA pair	To verify by removing SLR from a C9800 SSO HA pair	Passed	
EWLCJ176_2S_Reg_340	Validate license info in HA SSO RMI pair	To validate license info in HA SSO RMI pair	Passed	
EWLCJ176_2S_Reg_341	Validate license info on Standby unit directly	To validate license info on standby unit directly	Passed	
EWLCJ176_2S_Reg_342	Validate license info after ISSU upgrade	To validate license info after ISSU upgrade	Passed	
EWLCJ176_2S_Reg_343	Validate license info after multiple switchover	To validate license info after multiple switchover	Passed	
EWLCJ176_2S_Reg_344	Validate license info on multiple reload	To validate license info on multiple reboot	Passed	
EWCJ176_2S_Reg_311	Smart Account Creation, registration and activation.	To verify smart Account Creation, registration and activation.	Passed	
EWCJ176_2S_Reg_312	Generate token from CSSM	To Generate token from CSSM	Passed	
EWCJ176_2S_Reg_313	Product instance direct-connect using trust token	To verify Product instance direct-connect using trust token	Passed	

EWCJ176_2S_Reg_314	verify device status in CSSM	To verify device status in CSSM	Passed	
EWCJ176_2S_Reg_315	verify Smart Licensing Support in eWC HA	To verify Smart Licensing Support in eWC HA	Passed	
EWCJ176_2S_Reg_316	verify device details and license count changes in CSSM	To verify device details and license count changes in CSSM	Passed	
EWCJ176_2S_Reg_317	Add More AP's to device and Install trust token validate count on CSSM	To Add More AP's to device after Installing trust token to validate license count on CSSM	Passed	
EWCJ176_2S_Reg_318	Validate license info after switchover in AP	To validate license info after switchover in AP	Passed	
EWCJ176_2S_Reg_319	Validate license info on multiple reload	To validate license info on multiple reboot	Passed	
EWCJ176_2S_Reg_320	Install CSLU and add device and check status	Install CSLU and add device and check status	Passed	
EWCJ176_2S_Reg_321	Verify product details in CSSM after successfully shared product details from CSLU	Verify product details in CSSM after successfully shared product details from CSLU	Passed	

11ax Advanced traffic based scheduler for scheduling SU, OFDMA and MU traffic on 9105/9115/9120

Logical ID	Title	Description	Status	Defect ID
EWLCJ176S_Reg_412	Configuring 11ax Access Points, Channel width, OFDMA & radio parameters for 5Ghz band.	To configure 11ax Access Points, Channel width, OFDMA & radio parameters for 5Ghz band.	Passed	
EWLCJ176S_Reg_413	Configuring 11ax Access Points, Channel width, OFDMA & radio parameters for 2.4Ghz band.	To configure 11ax Access Points, Channel width, OFDMA & radio parameters for 2.4Ghz band.	Failed	CSCvx65348
EWLCJ176S_Reg_414	Monitor traffic with 11ax Android client connected.	To verify OFDMA details with 11ax Android client connected.	Passed	
EWLCJ176S_Reg_415	Monitor traffic with 11ax iPhone client connected.	To verify OFDMA details with 11ax iPhone client connected.	Passed	
EWLCJ176S_Reg_416	Monitor traffic with non 11ax Windows client connected.	To verify OFDMA details with non 11ax Windows client connected.	Passed	
EWLCJ176S_Reg_417	Monitor traffic with non 11ax Mac client connected.	To verify OFDMA details with non 11ax Mac client connected.	Passed	
EWLCJ176S_Reg_418	Monitor traffic by connecting client to 2.4Ghz radio.	To verify OFDMA details by connecting client to 2.4Ghz radio.	Passed	
EWLCJ176S_Reg_419	Verify OFDMA details with client connecting to WPA2 - PSK configured WLAN	To verify OFDMA details with client connecting to WPA2 - PSK configured WLAN	Passed	

EWLCJ176S_Reg_420	Verify OFDMA details with client connecting to WPA3 - Dot1x configured WLAN	To verify OFDMA details with client connecting to WPA3 - Dot1x configured WLAN	Passed	
EWLCJ176S_Reg_421	Connect upto 8 clients and monitor DL/UL OFDMA statistics	To connect upto 8 clients and monitor DL/UL OFDMA statistics	Passed	
EWLCJ176S_Reg_422	Modify spatial stream config to 1 stream and monitor OFDMA statistics.	To modify spatial stream config to 1 stream and monitor OFDMA statistics.	Passed	
EWLCJ176S_Reg_423	Modify spatial stream config to 2 streams and monitor OFDMA statistics.	To modify spatial stream config to 2 streams and monitor OFDMA statistics.	Passed	
EWLCJ176S_Reg_424	Modify spatial stream config to 3 streams and monitor OFDMA statistics.	To modify spatial stream config to 3 streams and monitor OFDMA statistics.	Passed	
EWLCJ176S_Reg_425	Modify spatial stream config to 4 streams and monitor OFDMA statistics.	To modify spatial stream config to 4 streams and monitor OFDMA statistics.	Passed	
EWLCJ176S_Reg_426	Enable video stream and monitor DL/UL OFDMA statistics	To enable video stream and monitor DL/UL OFDMA statistics	Passed	
EWLCJ176S_Reg_427	Modify MCS data rates & monitor OFDMA stats with 11ax Android client connected.	To modify MCS data rates & monitor OFDMA stats with 11ax Android client connected.	Passed	
EWLCJ176S_Reg_428	Configuring 11ax Access Points, Channel width, 11ax MU & radio parameters for 5Ghz band.	To configure 11ax Access Points, Channel width, 11ax MU & radio parameters for 5Ghz band.	Passed	

EWLCJ176S_Reg_429	Configuring 11ax Access Points, Channel width, 11ax MU & radio parameters for 2.4Ghz band.	To configure 11ax Access Points, Channel width, 11ax MU & radio parameters for 2.4Ghz band.	Passed	
EWLCJ176S_Reg_430	Monitor traffic with 11ax Android client connected.	To verify 11ax MU details with 11ax Android client connected.	Passed	
EWLCJ176S_Reg_431	Monitor traffic with 11ax iPhone client connected.	To verify 11ax MU details with 11ax iPhone client connected.	Passed	
EWLCJ176S_Reg_432	Monitor traffic with non 11ax Windows client connected.	To verify 11ax MU details with non 11ax Windows client connected.	Passed	
EWLCJ176S_Reg_433	Monitor traffic with non 11ax Mac client connected.	To verify 11ax MU details with non 11ax Mac client connected.	Passed	
EWLCJ176S_Reg_434	Monitor traffic by connecting client to 2.4Ghz radio.	To verify 11ax MU details by connecting client to 2.4Ghz radio.	Passed	
EWLCJ176S_Reg_435	Verify 11ax MU details with client connecting to WPA2 - PSK configured WLAN	To verify 11ax MU details with client connecting to WPA2 - PSK configured WLAN	Passed	
EWLCJ176S_Reg_436	Verify 11ax MU details with client connecting to WPA3 - Dot1x configured WLAN	To verify 11ax MU details with client connecting to WPA3 - Dot1x configured WLAN	Passed	
EWLCJ176S_Reg_437	Connect upto 8 clients and monitor DL/UL 11ax MU statistics	To connect upto 8 clients and monitor DL/UL 11ax MU statistics	Passed	
EWLCJ176S_Reg_438	Check 11ax MU stats with roaming client scenario	Check 11ax MU stats with roaming client scenario	Passed	

EWLCJ176S_Reg_439	Monitor 11ax traffic over mixed mode with both OFDMA and SU, MU traffic	To monitor 11ax traffic over mixed mode with both OFDMA and SU, MU traffic	Passed	
EWLCJ176S_Reg_440	Monitor 11ax traffic over mixed mode with both OFDMA and SU, MU traffic for AP models - 9105, 9115, 9120	To monitor 11ax traffic over mixed mode with both OFDMA and SU, MU traffic - 9105, 9115, 9120	Passed	
EWCJ176S_Reg_354	Configuring 11ax Access Points, Channel width, OFDMA & radio parameters for 5Ghz band.	To configure 11ax Access Points, Channel width, OFDMA & radio parameters for 5Ghz band.	Passed	
EWCJ176S_Reg_355	Configuring 11ax Access Points, Channel width, OFDMA & radio parameters for 2.4Ghz band.	To configure 11ax Access Points, Channel width, OFDMA & radio parameters for 2.4Ghz band.	Passed	
EWCJ176S_Reg_356	Monitor traffic with 11ax Android client connected.	To verify OFDMA details with 11ax Android client connected.	Passed	
EWCJ176S_Reg_357	Monitor traffic with 11ax iPhone client connected.	To verify OFDMA details with 11ax iPhone client connected.	Passed	
EWCJ176S_Reg_358	Monitor traffic with non 11ax Windows client connected.	To verify OFDMA details with non 11ax Windows client connected.	Passed	
EWCJ176S_Reg_359	Monitor traffic with non 11ax Mac client connected.	To verify OFDMA details with non 11ax Mac client connected.	Passed	
EWCJ176S_Reg_360	Monitor traffic by connecting client to 2.4Ghz radio.	To verify OFDMA details by connecting client to 2.4Ghz radio.	Passed	

EWCJ176S_Reg_361	Verify OFDMA details with client connecting to WPA2 - PSK configured WLAN	To verify OFDMA details with client connecting to WPA2 - PSK configured WLAN	Passed	
EWCJ176S_Reg_362	Verify OFDMA details with client connecting to WPA3 - Dot1x configured WLAN	To verify OFDMA details with client connecting to WPA3 - Dot1x configured WLAN	Passed	
EWCJ176S_Reg_363	Connect up to 8 clients and monitor DL/UL OFDMA statistics	To connect up to 8 clients and monitor DL/UL OFDMA statistics	Passed	
EWCJ176S_Reg_364	Modify spatial stream config to 1 stream and monitor OFDMA statistics.	To modify spatial stream config to 1 stream and monitor OFDMA statistics.	Passed	
EWCJ176S_Reg_365	Modify spatial stream config to 2 streams and monitor OFDMA statistics.	To modify spatial stream config to 2 streams and monitor OFDMA statistics.	Passed	
EWCJ176S_Reg_366	Modify spatial stream config to 3 streams and monitor OFDMA statistics.	To modify spatial stream config to 3 streams and monitor OFDMA statistics.	Passed	
EWCJ176S_Reg_367	Modify spatial stream config to 4 streams and monitor OFDMA statistics.	To modify spatial stream config to 4 streams and monitor OFDMA statistics.	Passed	
EWCJ176S_Reg_368	Enable video stream and monitor DL/UL OFDMA statistics	To enable video stream and monitor DL/UL OFDMA statistics	Passed	
EWCJ176S_Reg_369	Modify MCS data rates & monitor OFDMA stats with 11ax Android client connected.	To modify MCS data rates & monitor OFDMA stats with 11ax Android client connected.	Passed	
EWCJ176S_Reg_370	Configuring 11ax Access Points, Channel width, 11ax MU & radio parameters for 5Ghz band.	To configure 11ax Access Points, Channel width, 11ax MU & radio parameters for 5Ghz band.	Passed	

EWCJ176S_Reg_371	Configuring 11ax Access Points, Channel width, 11ax MU & radio parameters for 2.4Ghz band.	To configure 11ax Access Points, Channel width, 11ax MU & radio parameters for 2.4Ghz band.	Passed	
EWCJ176S_Reg_372	Monitor traffic with 11ax Android client connected.	To verify 11ax MU details with 11ax Android client connected.	Passed	
EWCJ176S_Reg_373	Monitor traffic with 11ax iPhone client connected.	To verify 11ax MU details with 11ax iPhone client connected.	Passed	
EWCJ176S_Reg_374	Monitor traffic with non 11ax Windows client connected.	To verify 11ax MU details with non 11ax Windows client connected.	Passed	
EWCJ176S_Reg_375	Monitor traffic with non 11ax Mac client connected.	To verify 11ax MU details with non 11ax Mac client connected.	Passed	
EWCJ176S_Reg_376	Monitor traffic by connecting client to 2.4Ghz radio.	To verify 11ax MU details by connecting client to 2.4Ghz radio.	Passed	
EWCJ176S_Reg_377	Verify 11ax MU details with client connecting to WPA2 - PSK configured WLAN	To verify 11ax MU details with client connecting to WPA2 - PSK configured WLAN	Passed	
EWCJ176S_Reg_378	Verify 11ax MU details with client connecting to WPA3 - Dot1x configured WLAN	To verify 11ax MU details with client connecting to WPA3 - Dot1x configured WLAN	Passed	
EWCJ176S_Reg_379	Connect up to 8 clients and monitor DL/UL 11ax MU statistics	To connect up to 8 clients and monitor DL/UL 11ax MU statistics	Passed	
EWCJ176S_Reg_380	Check 11ax MU stats with roaming client scenario	Check 11ax MU stats with roaming client scenario	Passed	

EWCJ176S_Reg_381	Monitor 11ax traffic over mixed mode with both OFDMA and SU, MU traffic	To monitor 11ax traffic over mixed mode with both OFDMA and SU, MU traffic	Passed	
EWCJ176S_Reg_382	Monitor 11ax traffic over mixed mode with both OFDMA and SU, MU traffic for AP models - 9105, 9115, 9120	To monitor 11ax traffic over mixed mode with both OFDMA and SU, MU traffic - 9105, 9115, 9120	Passed	
EWLCJ176_2S_Reg_363	Configuring 11ax Access Points, Channel width, OFDMA & radio parameters for 5Ghz band.	To configure 11ax Access Points, Channel width, OFDMA & radio parameters for 5Ghz band.	Passed	
EWLCJ176_2S_Reg_364	Configuring 11ax Access Points, Channel width, OFDMA & radio parameters for 2.4Ghz band.	To configure 11ax Access Points, Channel width, OFDMA & radio parameters for 2.4Ghz band.	Passed	
EWLCJ176_2S_Reg_365	Monitor traffic with 11ax Android client connected.	To verify OFDMA details with 11ax Android client connected.	Passed	
EWLCJ176_2S_Reg_366	Monitor traffic with 11ax iPhone client connected.	To verify OFDMA details with 11ax iPhone client connected.	Passed	
EWLCJ176_2S_Reg_367	Monitor traffic with non 11ax Windows client connected.	To verify OFDMA details with non 11ax Windows client connected.	Passed	
EWLCJ176_2S_Reg_368	Monitor traffic with non 11ax Mac client connected.	To verify OFDMA details with non 11ax Mac client connected.	Passed	
EWLCJ176_2S_Reg_369	Monitor traffic by connecting client to 2.4Ghz radio.	To verify OFDMA details by connecting client to 2.4Ghz radio.	Passed	

EWLCJ176_2S_Reg_370	Verify OFDMA details with client connecting to WPA2 - PSK configured WLAN	To verify OFDMA details with client connecting to WPA2 - PSK configured WLAN	Passed	
EWLCJ176_2S_Reg_371	Verify OFDMA details with client connecting to WPA3 - Dot1x configured WLAN	To verify OFDMA details with client connecting to WPA3 - Dot1x configured WLAN	Passed	
EWLCJ176_2S_Reg_372	Connect upto 8 clients and monitor DL/UL OFDMA statistics	To connect upto 8 clients and monitor DL/UL OFDMA statistics	Passed	
EWLCJ176_2S_Reg_373	Modify spatial stream config to 1 stream and monitor OFDMA statistics.	To modify spatial stream config to 1 stream and monitor OFDMA statistics.	Passed	
EWLCJ176_2S_Reg_374	Modify spatial stream config to 2 streams and monitor OFDMA statistics.	To modify spatial stream config to 2 streams and monitor OFDMA statistics.	Passed	
EWLCJ176_2S_Reg_375	Modify spatial stream config to 3 streams and monitor OFDMA statistics.	To modify spatial stream config to 3 streams and monitor OFDMA statistics.	Passed	
EWLCJ176_2S_Reg_376	Modify spatial stream config to 4 streams and monitor OFDMA statistics.	To modify spatial stream config to 4 streams and monitor OFDMA statistics.	Passed	
EWLCJ176_2S_Reg_377	Enable video stream and monitor DL/UL OFDMA statistics	To enable video stream and monitor DL/UL OFDMA statistics	Passed	
EWLCJ176_2S_Reg_378	Modify MCS data rates & monitor OFDMA stats with 11ax Android client connected.	To modify MCS data rates & monitor OFDMA stats with 11ax Android client connected.	Passed	
EWLCJ176_2S_Reg_379	Configuring 11ax Access Points, Channel width, 11ax MU & radio parameters for 5Ghz band.	To configure 11ax Access Points, Channel width, 11ax MU & radio parameters for 5Ghz band.	Passed	

EWLCJ176_2S_Reg_380	Configuring 11ax Access Points, Channel width, 11ax MU & radio parameters for 2.4Ghz band.	To configure 11ax Access Points, Channel width, 11ax MU & radio parameters for 2.4Ghz band.	Passed	
EWLCJ176_2S_Reg_381	Monitor traffic with 11ax Android client connected.	To verify 11ax MU details with 11ax Android client connected.	Passed	
EWLCJ176_2S_Reg_382	Monitor traffic with 11ax iPhone client connected.	To verify 11ax MU details with 11ax iPhone client connected.	Passed	
EWLCJ176_2S_Reg_383	Monitor traffic with non 11ax Windows client connected.	To verify 11ax MU details with non 11ax Windows client connected.	Passed	
EWLCJ176_2S_Reg_384	Monitor traffic with non 11ax Mac client connected.	To verify 11ax MU details with non 11ax Mac client connected.	Passed	
EWLCJ176_2S_Reg_385	Monitor traffic by connecting client to 2.4Ghz radio.	To verify 11ax MU details by connecting client to 2.4Ghz radio.	Passed	
EWLCJ176_2S_Reg_386	Verify 11ax MU details with client connecting to WPA2 - PSK configured WLAN	To verify 11ax MU details with client connecting to WPA2 - PSK configured WLAN	Passed	
EWLCJ176_2S_Reg_387	Verify 11ax MU details with client connecting to WPA3 - Dot1x configured WLAN	To verify 11ax MU details with client connecting to WPA3 - Dot1x configured WLAN	Passed	
EWLCJ176_2S_Reg_388	Connect upto 8 clients and monitor DL/UL 11ax MU statistics	To connect upto 8 clients and monitor DL/UL 11ax MU statistics	Passed	
EWLCJ176_2S_Reg_389	Check 11ax MU stats with roaming client scenario	Check 11ax MU stats with roaming client scenario	Passed	

EWLCJ176_2S_Reg_390	Monitor 11ax traffic over mixed mode with both OFDMA and SU, MU traffic	To monitor 11ax traffic over mixed mode with both OFDMA and SU, MU traffic	Passed	
EWLCJ176_2S_Reg_391	Monitor 11ax traffic over mixed mode with both OFDMA and SU, MU traffic for AP models - 9105, 9115, 9120	To monitor 11ax traffic over mixed mode with both OFDMA and SU, MU traffic - 9105, 9115, 9120	Passed	
EWCJ176_2S_Reg_322	Configuring 11ax Access Points, Channel width, OFDMA & radio parameters for 5Ghz band.	To configure 11ax Access Points, Channel width, OFDMA & radio parameters for 5Ghz band.	Passed	
EWCJ176_2S_Reg_323	Configuring 11ax Access Points, Channel width, OFDMA & radio parameters for 2.4Ghz band.	To configure 11ax Access Points, Channel width, OFDMA & radio parameters for 2.4Ghz band.	Passed	
EWCJ176_2S_Reg_324	Monitor traffic with 11ax Android client connected.	To verify OFDMA details with 11ax Android client connected.	Passed	
EWCJ176_2S_Reg_325	Monitor traffic with 11ax iPhone client connected.	To verify OFDMA details with 11ax iPhone client connected.	Passed	
EWCJ176_2S_Reg_326	Monitor traffic with non 11ax Windows client connected.	To verify OFDMA details with non 11ax Windows client connected.	Passed	
EWCJ176_2S_Reg_327	Monitor traffic with non 11ax Mac client connected.	To verify OFDMA details with non 11ax Mac client connected.	Passed	
EWCJ176_2S_Reg_328	Monitor traffic by connecting client to 2.4Ghz radio.	To verify OFDMA details by connecting client to 2.4Ghz radio.	Passed	

EWCJ176_2S_Reg_329	Verify OFDMA details with client connecting to WPA2 - PSK configured WLAN	To verify OFDMA details with client connecting to WPA2 - PSK configured WLAN	Passed	
EWCJ176_2S_Reg_330	Verify OFDMA details with client connecting to WPA3 - Dot1x configured WLAN	To verify OFDMA details with client connecting to WPA3 - Dot1x configured WLAN	Passed	
EWCJ176_2S_Reg_331	Connect upto 8 clients and monitor DL/UL OFDMA statistics	To connect upto 8 clients and monitor DL/UL OFDMA statistics	Passed	
EWCJ176_2S_Reg_332	Modify spatial stream config to 1 stream and monitor OFDMA statistics.	To modify spatial stream config to 1 stream and monitor OFDMA statistics.	Passed	
EWCJ176_2S_Reg_333	Modify spatial stream config to 2 streams and monitor OFDMA statistics.	To modify spatial stream config to 2 streams and monitor OFDMA statistics.	Passed	
EWCJ176_2S_Reg_334	Modify spatial stream config to 3 streams and monitor OFDMA statistics.	To modify spatial stream config to 3 streams and monitor OFDMA statistics.	Passed	
EWCJ176_2S_Reg_335	Modify spatial stream config to 4 streams and monitor OFDMA statistics.	To modify spatial stream config to 4 streams and monitor OFDMA statistics.	Passed	
EWCJ176_2S_Reg_336	Enable video stream and monitor DL/UL OFDMA statistics	To enable video stream and monitor DL/UL OFDMA statistics	Passed	
EWCJ176_2S_Reg_337	Modify MCS data rates & monitor OFDMA stats with 11ax Android client connected.	To modify MCS data rates & monitor OFDMA stats with 11ax Android client connected.	Passed	
EWCJ176_2S_Reg_338	Configuring 11ax Access Points, Channel width, 11ax MU & radio parameters for 5Ghz band.	To configure 11ax Access Points, Channel width, 11ax MU & radio parameters for 5Ghz band.	Passed	

EWCJ176_2S_Reg_339	Configuring 11ax Access Points, Channel width, 11ax MU & radio parameters for 2.4Ghz band.	To configure 11ax Access Points, Channel width, 11ax MU & radio parameters for 2.4Ghz band.	Passed	
EWCJ176_2S_Reg_340	Monitor traffic with 11ax Android client connected.	To verify 11ax MU details with 11ax Android client connected.	Passed	
EWCJ176_2S_Reg_341	Monitor traffic with 11ax iPhone client connected.	To verify 11ax MU details with 11ax iPhone client connected.	Passed	
EWCJ176_2S_Reg_342	Monitor traffic with non 11ax Windows client connected.	To verify 11ax MU details with non 11ax Windows client connected.	Passed	
EWCJ176_2S_Reg_343	Monitor traffic with non 11ax Mac client connected.	To verify 11ax MU details with non 11ax Mac client connected.	Passed	
EWCJ176_2S_Reg_344	Monitor traffic by connecting client to 2.4Ghz radio.	To verify 11ax MU details by connecting client to 2.4Ghz radio.	Passed	
EWCJ176_2S_Reg_345	Verify 11ax MU details with client connecting to WPA2 - PSK configured WLAN	To verify 11ax MU details with client connecting to WPA2 - PSK configured WLAN	Passed	
EWCJ176_2S_Reg_346	Verify 11ax MU details with client connecting to WPA3 - Dot1x configured WLAN	To verify 11ax MU details with client connecting to WPA3 - Dot1x configured WLAN	Passed	
EWCJ176_2S_Reg_347	Connect upto 8 clients and monitor DL/UL 11ax MU statistics	To connect upto 8 clients and monitor DL/UL 11ax MU statistics	Passed	
EWCJ176_2S_Reg_348	Check 11ax MU stats with roaming client scenario	Check 11ax MU stats with roaming client scenario	Passed	

EWCJ176_2S_Reg_349	Monitor 11ax traffic over mixed mode with both OFDMA and SU, MU traffic	To monitor 11ax traffic over mixed mode with both OFDMA and SU, MU traffic	Passed	
EWCJ176_2S_Reg_350	Monitor 11ax traffic over mixed mode with both OFDMA and SU, MU traffic for AP models - 9105, 9115, 9120	To monitor 11ax traffic over mixed mode with both OFDMA and SU, MU traffic - 9105, 9115, 9120	Passed	

11ax OFDMA Support (8Users UL, 16Users DL) on 9105/9115/9120

Logical ID	Title	Description	Status	Defect ID
EWLCJ176S_Reg_546	Configuring 11ax Access Points, Channel width, OFDMA & radio parameters for 5Ghz band.	To configure 11ax Access Points, Channel width, OFDMA & radio parameters for 5Ghz band.	Passed	CSCvy05131
EWLCJ176S_Reg_547	Configuring 11ax Access Points, Channel width, OFDMA & radio parameters for 2.4Ghz band.	To configure 11ax Access Points, Channel width, OFDMA & radio parameters for 2.4Ghz band.	Passed	CSCvy12668
EWLCJ176S_Reg_548	Verifying details with 11ax Android client connected.	To verify OFDMA details with 11ax Android client connected.	Passed	
EWLCJ176S_Reg_549	Verifying details with 11ax iPhone client connected.	To verify OFDMA details with 11ax iPhone client connected.	Passed	
EWLCJ176S_Reg_550	Verifying the details with non 11ax Windows client connected.	To verify OFDMA details with non 11ax Windows client connected.	Passed	
EWLCJ176S_Reg_551	Verifying the details with non 11ax Mac client connected.	To verify OFDMA details with non 11ax Mac client connected.	Passed	
EWLCJ176S_Reg_552	Verify details by connecting client to 2.4Ghz radio.	To verify OFDMA details by connecting client to 2.4Ghz radio.	Passed	
EWLCJ176S_Reg_553	Check OFDMA support for AP configured in Local mode.	To check OFDMA support for AP configured in Local mode.	Passed	
EWLCJ176S_Reg_554	Check OFDMA support for AP configured in Flex-connect mode.	To check OFDMA support for AP configured in Flex-connect mode.	Passed	

EWLCJ176S_Reg_555	Check OFDMA support for AP configured in Bridge mode.	To check OFDMA support for AP configured in Bridge mode.	Passed	
EWLCJ176S_Reg_556	Verify OFDMA details with client connecting to WPA2 - PSK configured WLAN	To verify OFDMA details with client connecting to WPA2 - PSK configured WLAN	Passed	
EWLCJ176S_Reg_557	Verify OFDMA details with client connecting to WPA3 - Dot1x configured WLAN	To verify OFDMA details with client connecting to WPA3 - Dot1x configured WLAN	Passed	
EWLCJ176S_Reg_558	Connect upto 8 clients and monitor DL/UL OFDMA statistics	To connect upto 8 clients and monitor DL/UL OFDMA statistics	Passed	
EWLCJ176S_Reg_559	Connect upto 16 clients and monitor DL/UL OFDMA statistics	To connect upto 16 clients and monitor DL/UL OFDMA statistics	Passed	
EWLCJ176S_Reg_560	Modify spatial stream config to 1 stream and monitor OFDMA statistics.	To modify spatial stream config to 1 stream and monitor OFDMA statistics.	Passed	
EWLCJ176S_Reg_561	Modify spatial stream config to 2 streams and monitor OFDMA statistics.	To modify spatial stream config to 2 streams and monitor OFDMA statistics.	Passed	
EWLCJ176S_Reg_562	Modify spatial stream config to 3 streams and monitor OFDMA statistics.	To modify spatial stream config to 3 streams and monitor OFDMA statistics.	Passed	
EWLCJ176S_Reg_563	Modify spatial stream config to 4 streams and monitor OFDMA statistics.	To modify spatial stream config to 4 streams and monitor OFDMA statistics.	Passed	
EWLCJ176S_Reg_564	Enable video stream and monitor DL/UL OFDMA statistics	To enable video stream and monitor DL/UL OFDMA statistics	Passed	

EWLCJ176S_Reg_565	Modify MCS data rates & monitor OFDMA stats with 11ax Android client connected.	To modify MCS data rates & monitor OFDMA stats with 11ax Android client connected.	Passed	
EWLCJ176S_Reg_566	Check OFDMA stats with roaming client scenario in different eWLC with different 11 ax Aps	To check OFDMA stats with roaming client scenario	Passed	
EWCJ176S_Reg_383	Configuring 11ax Access Points, Channel width, OFDMA & radio parameters for 5Ghz band.	To configure 11ax Access Points, Channel width, OFDMA & radio parameters for 5Ghz band.	Passed	
EWCJ176S_Reg_384	Configuring 11ax Access Points, Channel width, OFDMA & radio parameters for 2.4Ghz band.	To configure 11ax Access Points, Channel width, OFDMA & radio parameters for 2.4Ghz band.	Passed	
EWCJ176S_Reg_385	Verifying details with 11ax Android client connected.	To verify OFDMA details with 11ax Android client connected.	Passed	
EWCJ176S_Reg_386	Verifying details with 11ax iPhone client connected.	To verify OFDMA details with 11ax iPhone client connected.	Passed	
EWCJ176S_Reg_387	Verifying the details with non 11ax Windows client connected.	To verify OFDMA details with non 11ax Windows client connected.	Passed	
EWCJ176S_Reg_388	Verifying the details with non 11ax Mac client connected.	To verify OFDMA details with non 11ax Mac client connected.	Passed	
EWCJ176S_Reg_389	Verify details by connecting client to 2.4Ghz radio.	To verify OFDMA details by connecting client to 2.4Ghz radio.	Passed	

EWCJ176S_Reg_390	Check OFDMA support for AP configured in Local mode.	To check OFDMA support for AP configured in Local mode.	Passed	
EWCJ176S_Reg_391	Check OFDMA support for AP configured in Flex-connect mode.	To check OFDMA support for AP configured in Flex-connect mode.	Passed	
EWCJ176S_Reg_392	Check OFDMA support for AP configured in Bridge mode.	To check OFDMA support for AP configured in Bridge mode.	Passed	
EWCJ176S_Reg_393	Verify OFDMA details with client connecting to WPA2 - PSK configured WLAN	To verify OFDMA details with client connecting to WPA2 - PSK configured WLAN	Passed	
EWCJ176S_Reg_394	Verify OFDMA details with client connecting to WPA3 - Dot1x configured WLAN	To verify OFDMA details with client connecting to WPA3 - Dot1x configured WLAN	Passed	
EWCJ176S_Reg_395	Connect up to 8 clients and monitor DL/UL OFDMA statistics	To connect up to 8 clients and monitor DL/UL OFDMA statistics	Passed	
EWCJ176S_Reg_396	Connect up to 16 clients and monitor DL/UL OFDMA statistics	To connect up to 16 clients and monitor DL/UL OFDMA statistics	Passed	
EWCJ176S_Reg_397	Modify spatial stream config to 1 stream and monitor OFDMA statistics.	To modify spatial stream config to 1 stream and monitor OFDMA statistics.	Passed	
EWCJ176S_Reg_398	Modify spatial stream config to 2 streams and monitor OFDMA statistics.	To modify spatial stream config to 2 streams and monitor OFDMA statistics.	Passed	
EWCJ176S_Reg_399	Modify spatial stream config to 3 streams and monitor OFDMA statistics.	To modify spatial stream config to 3 streams and monitor OFDMA statistics.	Passed	
EWCJ176S_Reg_400	Modify spatial stream config to 4 streams and monitor OFDMA statistics.	To modify spatial stream config to 4 streams and monitor OFDMA statistics.	Passed	

EWCJ176S_Reg_401	Modify MCS data rates & monitor OFDMA stats with 11ax Android client connected.	To modify MCS data rates & monitor OFDMA stats with 11ax Android client connected.	Passed	
EWCJ176S_Reg_402	Check OFDMA stats with roaming client scenario in different eWC with different 11 ax Aps	To check OFDMA stats with roaming client scenario	Passed	
EWLCJ176_2S_Reg_453	Configuring 11ax Access Points, Channel width, OFDMA & radio parameters for 5Ghz band.	To configure 11ax Access Points, Channel width, OFDMA & radio parameters for 5Ghz band.	Passed	
EWLCJ176_2S_Reg_454	Configuring 11ax Access Points, Channel width, OFDMA & radio parameters for 2.4Ghz band.	To configure 11ax Access Points, Channel width, OFDMA & radio parameters for 2.4Ghz band.	Passed	
EWLCJ176_2S_Reg_455	Verifying details with 11ax Android client connected.	To verify OFDMA details with 11ax Android client connected.	Passed	
EWLCJ176_2S_Reg_456	Verifying details with 11ax iPhone client connected.	To verify OFDMA details with 11ax iPhone client connected.	Passed	
EWLCJ176_2S_Reg_457	Verifying the details with non 11ax Windows client connected.	To verify OFDMA details with non 11ax Windows client connected.	Passed	
EWLCJ176_2S_Reg_458	Verifying the details with non 11ax Mac client connected.	To verify OFDMA details with non 11ax Mac client connected.	Passed	
EWLCJ176_2S_Reg_459	Verify details by connecting client to 2.4Ghz radio.	To verify OFDMA details by connecting client to 2.4Ghz radio.	Passed	

EWLCJ176_2S_Reg_460	Check OFDMA support for AP configured in Local mode.	To check OFDMA support for AP configured in Local mode.	Passed	
EWLCJ176_2S_Reg_461	Check OFDMA support for AP configured in Flex-connect mode.	To check OFDMA support for AP configured in Flex-connect mode.	Passed	
EWLCJ176_2S_Reg_462	Check OFDMA support for AP configured in Bridge mode.	To check OFDMA support for AP configured in Bridge mode.	Passed	
EWLCJ176_2S_Reg_463	Verify OFDMA details with client connecting to WPA2 - PSK configured WLAN	To verify OFDMA details with client connecting to WPA2 - PSK configured WLAN	Passed	
EWLCJ176_2S_Reg_464	Verify OFDMA details with client connecting to WPA3 - Dot1x configured WLAN	To verify OFDMA details with client connecting to WPA3 - Dot1x configured WLAN	Passed	
EWLCJ176_2S_Reg_465	Connect upto 8 clients and monitor DL/UL OFDMA statistics	To connect upto 8 clients and monitor DL/UL OFDMA statistics	Passed	
EWLCJ176_2S_Reg_466	Connect upto 16 clients and monitor DL/UL OFDMA statistics	To connect upto 16 clients and monitor DL/UL OFDMA statistics	Passed	
EWLCJ176_2S_Reg_467	Modify spatial stream config to 1 stream and monitor OFDMA statistics.	To modify spatial stream config to 1 stream and monitor OFDMA statistics.	Passed	
EWLCJ176_2S_Reg_468	Modify spatial stream config to 2 streams and monitor OFDMA statistics.	To modify spatial stream config to 2 streams and monitor OFDMA statistics.	Passed	
EWLCJ176_2S_Reg_469	Modify spatial stream config to 3 streams and monitor OFDMA statistics.	To modify spatial stream config to 3 streams and monitor OFDMA statistics.	Passed	
EWLCJ176_2S_Reg_470	Modify spatial stream config to 4 streams and monitor OFDMA statistics.	To modify spatial stream config to 4 streams and monitor OFDMA statistics.	Passed	

EWLCJ176_2S_Reg_471	Enable video stream and monitor DL/UL OFDMA statistics	To enable video stream and monitor DL/UL OFDMA statistics	Passed	
EWLCJ176_2S_Reg_472	Modify MCS data rates & monitor OFDMA stats with 11ax Android client connected.	To modify MCS data rates & monitor OFDMA stats with 11ax Android client connected.	Passed	
EWLCJ176_2S_Reg_473	Check OFDMA stats with roaming client scenario in different eWLC with different 11 ax Aps	To check OFDMA stats with roaming client scenario	Passed	
EWCJ176_2S_Reg_351	Configuring 11ax Access Points, Channel width, OFDMA & radio parameters for 5Ghz band.	To configure 11ax Access Points, Channel width, OFDMA & radio parameters for 5Ghz band.	Passed	
EWCJ176_2S_Reg_352	Configuring 11ax Access Points, Channel width, OFDMA & radio parameters for 2.4Ghz band.	To configure 11ax Access Points, Channel width, OFDMA & radio parameters for 2.4Ghz band.	Passed	
EWCJ176_2S_Reg_353	Verifying details with 11ax Android client connected.	To verify OFDMA details with 11ax Android client connected.	Passed	
EWCJ176_2S_Reg_354	Verifying details with 11ax iPhone client connected.	To verify OFDMA details with 11ax iPhone client connected.	Passed	
EWCJ176_2S_Reg_355	Verifying the details with non 11ax Windows client connected.	To verify OFDMA details with non 11ax Windows client connected.	Passed	
EWCJ176_2S_Reg_356	Verifying the details with non 11ax Mac client connected.	To verify OFDMA details with non 11ax Mac client connected.	Passed	

EWCJ176_2S_Reg_357	Verify details by connecting client to 2.4Ghz radio.	To verify OFDMA details by connecting client to 2.4Ghz radio.	Passed	
EWCJ176_2S_Reg_358	Check OFDMA support for AP configured in Local mode.	To check OFDMA support for AP configured in Local mode.	Passed	
EWCJ176_2S_Reg_359	Check OFDMA support for AP configured in Flex-connect mode.	To check OFDMA support for AP configured in Flex-connect mode.	Passed	
EWCJ176_2S_Reg_360	Check OFDMA support for AP configured in Bridge mode.	To check OFDMA support for AP configured in Bridge mode.	Passed	
EWCJ176_2S_Reg_361	Verify OFDMA details with client connecting to WPA2 - PSK configured WLAN	To verify OFDMA details with client connecting to WPA2 - PSK configured WLAN	Passed	
EWCJ176_2S_Reg_362	Verify OFDMA details with client connecting to WPA3 - Dot1x configured WLAN	To verify OFDMA details with client connecting to WPA3 - Dot1x configured WLAN	Passed	
EWCJ176_2S_Reg_363	Connect upto 8 clients and monitor DL/UL OFDMA statistics	To connect upto 8 clients and monitor DL/UL OFDMA statistics	Passed	
EWCJ176_2S_Reg_364	Connect upto 16 clients and monitor DL/UL OFDMA statistics	To connect upto 16 clients and monitor DL/UL OFDMA statistics	Passed	
EWCJ176_2S_Reg_365	Modify spatial stream config to 1 stream and monitor OFDMA statistics.	To modify spatial stream config to 1 stream and monitor OFDMA statistics.	Passed	
EWCJ176_2S_Reg_366	Modify spatial stream config to 2 streams and monitor OFDMA statistics.	To modify spatial stream config to 2 streams and monitor OFDMA statistics.	Passed	
EWCJ176_2S_Reg_367	Modify spatial stream config to 3 streams and monitor OFDMA statistics.	To modify spatial stream config to 3 streams and monitor OFDMA statistics.	Passed	

EWCJ176_2S_Reg_368	Modify spatial stream config to 4 streams and monitor OFDMA statistics.	To modify spatial stream config to 4 streams and monitor OFDMA statistics.	Passed	
EWCJ176_2S_Reg_369	Modify MCS data rates & monitor OFDMA stats with 11ax Android client connected.	To modify MCS data rates & monitor OFDMA stats with 11ax Android client connected.	Passed	
EWCJ176_2S_Reg_370	Check OFDMA stats with roaming client scenario in different eWC with different 11 ax Aps	To check OFDMA stats with roaming client scenario	Passed	

Easy PSK:WLAN Client Onboarding w/o registration

Logical ID	Title	Description	Status	Defect ID
EWLCJ176S_Reg_474	Verify you can configure a wlan with easy psk feature on it when aaa override is set on the associated policy profile. Verify no syslog is thrown.	To Verify whether you can configure a wlan with easy psk feature on it when aaa override is set on the associated policy profile. Verify no syslog is thrown.	Passed	
EWLCJ176S_Reg_475	Verify that if you configure a wlan with easy psk feature and its associated policy profile does not have the aaa override set, a syslog is thrown.	To Verify that whether you configure a wlan with easy psk feature and its associated policy profile does not have the aaa override set, a syslog is thrown.	Passed	
EWLCJ176S_Reg_476	Verify that it is not possible to configure Easy PSK if one of the following option is set on the same wlan: mPSK PSK key WPA3 CCKM dot1x	To Verify that it is not possible to configure Easy PSK if one of the following option is set on the same wlan: mPSK PSK key WPA3 CCKM dot1x	Passed	CSCvx42701
EWLCJ176S_Reg_477	Verify that it is not possible to configure any of the following option on a wlan where Easy PSK is enabled mPSK PSK key WPA3 CCKM dot1x	To Verify that it is not possible to configure any of the following option on a wlan where Easy PSK is enabled mPSK PSK key WPA3 CCKM dot1x	Passed	
EWLCJ176S_Reg_478	Verify that when configuring the feature on a wlan that is pushed on an AP configured in flex mode, a syslog is thrown.	To Verify that when configuring the feature on a wlan that is pushed on an AP configured in flex mode, a syslog is thrown.	Failed	CSCvx88789

EWLCJ176S_Reg_479	Verify that the feature can't be configured on a EWC device	To Verify that the feature can't be configured on a EWC device	Passed	
EWLCJ176S_Reg_480	Verify that if the feature is configured together with local authentication, a syslog is thrown.	To Verify that if the feature is configured together with local authentication, a syslog is thrown.	Passed	
EWLCJ176S_Reg_481	Verify that if the feature is configured together with local switching, a syslog is thrown.	To Verify that if the feature is configured together with local switching, a syslog is thrown.	Passed	
EWLCJ176S_Reg_482	With a valid configuration, save the configuration and perform a reboot. Verify that the configuration is kept and valid, and no syslog is thrown.	To verify with a valid configuration, save the configuration and perform a reboot. Verify that the configuration is kept and valid, and no syslog is thrown.	Passed	
EWLCJ176S_Reg_483	Remove the Easy PSK feature from the configured wlan in the previous test through yang. Verify that the same config can be observed in the CLI.	To Remove the Easy PSK feature from the configured wlan in the previous test through yang. Verify that the same config can be observed in the CLI.	Passed	
EWLCJ176S_Reg_484	Configure a new wlan with easy PSK through SNMP. Verify that the configuration is effective through CLI. Remove the easy PSK from the wlan and verify in the CLI that the same config is no longer applied.	To Configure a new wlan with easy PSK through SNMP. Verify that the configuration is effective through CLI. Remove the easy PSK from the wlan and verify in the CLI that the same config is no longer applied.	Passed	

EWLCJ176S_Reg_485	Configure a wlan with easy PSK through CLI. Verify that the configuration is effective through SNMP.	To Configure a wlan with easy PSK through CLI. Verify that the configuration is effective through SNMP.	Passed	
EWLCJ176S_Reg_486	Configure a wlan with Easy PSK feature through the CLI. Verify that you can get the same configuration through yang.	To Configure a wlan with Easy PSK feature through the CLI. Verify that you can get the same configuration through yang.	Passed	
EWLCJ176S_Reg_487	Configure a WLAN with easy PSK, the Radius with two valid PSKs. Connect one client with the first PSK. Verify the exchange between the controller and the Radius with a capture (verify new AAA attributes are filled correctly). Verify that the client can ping the gateway	To Configure a WLAN with easy PSK, the Radius with two valid PSKs. Connect one client with the first PSK. Verify the exchange between the controller and the Radius with a capture (verify new AAA attributes are filled correctly). Verify that the client can ping the gateway	Passed	
EWLCJ176S_Reg_488	Following the previous test, disconnect the client and connect it again using the second PSK. Verify again the Radius exchange and the client can reach Run state and can ping the gateway.	Following the previous test, disconnect the client and connect it again using the second PSK. Verify again the Radius exchange and the client can reach Run state and can ping the gateway.	Passed	

EWLCJ176S_Reg_489	Configure 16 wlans with easy PSK enabled. Connect one client to each WLAN. Verify each client reaches Run state and can ping the gateway.	To Configure 16 wlans with easy PSK enabled. Connect one client to each WLAN. Verify each client reaches Run state and can ping the gateway.	Passed	CSCvx70145
EWLCJ176S_Reg_490	Configure an easy psk wlan using a aaa server that is not reachable. Verify that the client can't reach Run state and is deleted.	To Configure an easy psk wlan using a aaa server that is not reachable. Verify that the client can't reach Run state and is deleted.	Passed	
EWLCJ176S_Reg_491	Configure a wlan with easy psk and webauth on map failure. Make sure that the webauth on map failure is not applied in case the client is connecting with a non supported passphrase.	To Configure a wlan with easy psk and webauth on map failure. Make sure that the webauth on map failure is not applied in case the client is connecting with a non supported passphrase.	Passed	
EWLCJ176_2S_Reg_409	Verify you can configure a wlan with easy psk feature on it when aaa override is set on the associated policy profile. Verify no syslog is thrown.	To Verify whether you can configure a wlan with easy psk feature on it when aaa override is set on the associated policy profile. Verify no syslog is thrown.	Passed	
EWLCJ176_2S_Reg_410	Verify that if you configure a wlan with easy psk feature and its associated policy profile does not have the aaa override set, a syslog is thrown.	To Verify that whether you configure a wlan with easy psk feature and its associated policy profile does not have the aaa override set, a syslog is thrown.	Passed	

EWLCJ176_2S_Reg_411	Verify that it is not possible to configure Easy PSK if one of the following option is set on the same wlan: mPSK PSK key WPA3 CCKM dot1x	To Verify that it is not possible to configure Easy PSK if one of the following option is set on the same wlan: mPSK PSK key WPA3 CCKM dot1x	Passed	
EWLCJ176_2S_Reg_412	Verify that it is not possible to configure any of the following option on a wlan where Easy PSK is enabled mPSK PSK key WPA3 CCKM dot1x	To Verify that it is not possible to configure any of the following option on a wlan where Easy PSK is enabled mPSK PSK key WPA3 CCKM dot1x	Passed	
EWLCJ176_2S_Reg_413	Verify that when configuring the feature on a wlan that is pushed on an AP configured in flex mode, a syslog is thrown.	To Verify that when configuring the feature on a wlan that is pushed on an AP configured in flex mode, a syslog is thrown.	Passed	
EWLCJ176_2S_Reg_414	Verify that the feature can't be configured on a EWC device	To Verify that the feature can't be configured on a EWC device	Passed	
EWLCJ176_2S_Reg_415	Verify that if the feature is configured together with local authentication, a syslog is thrown.	To Verify that if the feature is configured together with local authentication, a syslog is thrown.	Passed	
EWLCJ176_2S_Reg_416	Verify that if the feature is configured together with local switching, a syslog is thrown.	To Verify that if the feature is configured together with local switching, a syslog is thrown.	Passed	

EWLCJ176_2S_Reg_417	With a valid configuration, save the configuration and perform a reboot. Verify that the configuration is kept and valid, and no syslog is thrown.	To verify with a valid configuration, save the configuration and perform a reboot. Verify that the configuration is kept and valid, and no syslog is thrown.	Passed	
EWLCJ176_2S_Reg_418	Remove the Easy PSK feature from the configured wlan in the previous test through yang. Verify that the same config can be observed in the CLI.	To Remove the Easy PSK feature from the configured wlan in the previous test through yang. Verify that the same config can be observed in the CLI.	Passed	
EWLCJ176_2S_Reg_419	Configure a new wlan with easy PSK through SNMP. Verify that the configuration is effective through CLI. Remove the easy PSK from the wlan and verify in the CLI that the same config is no longer applied.	To Configure a new wlan with easy PSK through SNMP. Verify that the configuration is effective through CLI. Remove the easy PSK from the wlan and verify in the CLI that the same config is no longer applied.	Passed	
EWLCJ176_2S_Reg_420	Configure a wlan with easy PSK through CLI. Verify that the configuration is effective through SNMP.	To Configure a wlan with easy PSK through CLI. Verify that the configuration is effective through SNMP.	Passed	
EWLCJ176_2S_Reg_421	Configure a wlan with Easy PSK feature through the CLI. Verify that you can get the same configuration through yang.	To Configure a wlan with Easy PSK feature through the CLI. Verify that you can get the same configuration through yang.	Passed	

EWLCJ176_2S_Reg_422	Configure a WLAN with easy PSK, the Radius with two valid PSKs. Connect one client with the first PSK. Verify the exchange between the controller and the Radius with a capture (verify new AAA attributes are filled correctly). Verify that the client can ping the gateway	To Configure a WLAN with easy PSK, the Radius with two valid PSKs. Connect one client with the first PSK. Verify the exchange between the controller and the Radius with a capture (verify new AAA attributes are filled correctly). Verify that the client can ping the gateway	Passed	
EWLCJ176_2S_Reg_423	Following the previous test, disconnect the client and connect it again using the second PSK. Verify again the Radius exchange and the client can reach Run state and can ping the gateway.	Following the previous test, disconnect the client and connect it again using the second PSK. Verify again the Radius exchange and the client can reach Run state and can ping the gateway.	Passed	
EWLCJ176_2S_Reg_424	Configure 16 wlans with easy PSK enabled. Connect one client to each WLAN. Verify each client reaches Run state and can ping the gateway.	To Configure 16 wlans with easy PSK enabled. Connect one client to each WLAN. Verify each client reaches Run state and can ping the gateway.	Passed	
EWLCJ176_2S_Reg_425	Configure an easy psk wlan using a aaa server that is not reachable. Verify that the client can't reach Run state and is deleted.	To Configure an easy psk wlan using a aaa server that is not reachable. Verify that the client can't reach Run state and is deleted.	Passed	

EWLCJ176_2S_Reg_426	Configure a wlan with easy psk and webauth on mac failure. Make sure that the webauth on mac failure is not applied in case the client is connecting with a non supported passphrase.	To Configure a wlan with easy psk and webauth on mab failure. Make sure that the webauth on mab failure is not applied in case the client is connecting with a non supported passphrase.	Passed	

Application Experience Support on IOS-XE Wireless Platforms for Flex and Fabric

Logical ID	Title	Description	Status	Defect ID
EWLCJ176S_Reg_492	Creating a policy profile in eWLC 9800-40 and check if the profile is shown in Application visibility page	To create a policy profile in 9800-40 eWLC and check if the policy profile is shown in the application visibility page or not	Passed	
EWLCJ176S_Reg_493	Creating a policy profile in eWLC 9800-80 and check if the profile is shown in Application visibility page	To create a policy profile in 9800-80 eWLC and check if the policy profile is shown in the application visibility page or not	Passed	
EWLCJ176S_Reg_494	Creating a policy profile in eWLC 9800-CL and check if the profile is shown in Application visibility page	To create a policy profile in 9800-CL eWLC and check if the policy profile is shown in the application visibility page or not	Passed	
EWLCJ176S_Reg_495	Mapping the created policy profile under Application visibility in eWLC 9800-40 and check the behaviour	To map the created policy profile under Application visibility in eWLC 9800-40 and check the behaviour .	Passed	
EWLCJ176S_Reg_496	Mapping the created policy profile under Application visibility in eWLC 9800-80 and check the behaviour	To map the created policy profile under Application visibility in eWLC 9800-80 and check the behaviour .	Passed	

EWLCJ176S_Reg_497	Mapping the created policy profile under Application visibility in eWLC 9800-CL and check the behaviour	To map the created policy profile under Application visibility in eWLC 9800-CL and check the behaviour .	Passed	
EWLCJ176S_Reg_498	Enabling External Collector address for the policy profile mapped in Application visibility and checking the behaviour	To enabling External Collector address for the policy profile mapped in Application visibility and checking the behaviour	Passed	
EWLCJ176S_Reg_499	Checking if the local Collector in the Application visibility works for the eWLC which works in Standalone mode	To check if the local collector for the application visibility works or not for the eWLC which works on standalone mode	Passed	
EWLCJ176S_Reg_500	Checking if the local Collector in the Application visibility works for the eWLC which works in Active mode	To check if the local collector for the application visibility works or not for the eWLC which works on Active mode	Passed	
EWLCJ176S_Reg_501	Checking if the local Collector in the Application visibility works for the eWLC which is in HA mode	To check if the local collector for the application visibility works or not for the eWLC which is in HA mode	Passed	
EWLCJ176_2S_Reg_427	Creating a policy profile in eWLC 9800-40 and check if the profile is shown in Application visibility page	To create a policy profile in 9800-40 eWLC and check if the policy profile is shown in the application visibility page or not	Passed	

EWLCJ176_2S_Reg_428	Creating a policy profile in eWLC 9800-80 and check if the profile is shown in Application visibility page	To create a policy profile in 9800-80 eWLC and check if the policy profile is shown in the application visibility page or not	Passed	
EWLCJ176_2S_Reg_429	Creating a policy profile in eWLC 9800-CL and check if the profile is shown in Application visibility page	To create a policy profile in 9800-CL eWLC and check if the policy profile is shown in the application visibility page or not	Passed	
EWLCJ176_2S_Reg_430	Mapping the created policy profile under Application visibility in eWLC 9800-40 and check the behaviour	To map the created policy profile under Application visibility in eWLC 9800-40 and check the behaviour .	Passed	
EWLCJ176_2S_Reg_431	Mapping the created policy profile under Application visibility in eWLC 9800-80 and check the behaviour	To map the created policy profile under Application visibility in eWLC 9800-80 and check the behaviour .	Passed	
EWLCJ176_2S_Reg_432	Mapping the created policy profile under Application visibility in eWLC 9800-CL and check the behaviour	To map the created policy profile under Application visibility in eWLC 9800-CL and check the behaviour .	Passed	
EWLCJ176_2S_Reg_433	Enabling External Collector address for the policy profile mapped in Application visibility and checking the behaviour	To enabling External Collector address for the policy profile mapped in Application visibility and checking the behaviour	Passed	

EWLCJ176_2S_Reg_434	Checking if the local Collector in the Application visibility works for the eWLC which works in Standalone mode	To check if the local collector for the application visibility works or not for the eWLC which works on standalone mode	Passed	
EWLCJ176_2S_Reg_435	Checking if the local Collector in the Application visibility works for the eWLC which works in Active mode	To check if the local collector for the application visibility works or not for the eWLC which works on Active mode	Passed	
EWLCJ176_2S_Reg_436	Checking if the local Collector in the Application visibility works for the eWLC which is in HA mode	To check if the local collector for the application visibility works or not for the eWLC which is in HA mode	Passed	

Extend Packet Tracer into eWLC processes

Logical ID	Title	Description	Status	Defect ID
EWLCJ176S_Reg_502	Enabling Packet trace and conditional debug in eWLC 9800-40	To check if the packet trace and conditional debug is enabled on 9800-40 or not	Passed	
EWLCJ176S_Reg_503	Enabling Packet trace and conditional debug in eWLC 9800-80	To check if the packet trace and conditional debug is enabled on 9800-80 or not	Passed	
EWLCJ176S_Reg_504	Enabling Packet trace and conditional debug in eWLC 9800-CL	To check if the packet trace and conditional debug is enabled on 9800-CL or not	Passed	
EWLCJ176S_Reg_505	Enabling Packet trace and conditional debug in eWLC 9800 with HA setup	To check if the packet trace and conditional debug is enabled or not	Passed	
EWLCJ176S_Reg_506	Verifying if the packet trace for 9800-40 are captured and the details shown correctly	To check if the packet trace is enabled and the configured command output are shown for the eWLC 9800-40 or not	Passed	
EWLCJ176S_Reg_507	Verifying if the packet trace for 9800-80 are captured and the details shown correctly	To check if the packet trace is enabled and the configured command output are shown for the eWLC 9800-80 or not	Passed	

EWLCJ176S_Reg_508	Verifying if the packet trace for 9800-CL are captured and the details shown correctly	To check if the packet trace is enabled and the configured command output are shown for the eWLC 9800-CL or not	Passed	
EWLCJ176S_Reg_509	Verifying if the packet trace for 9800 HA are captured and the details shown correctly	To check if the packet trace is enabled and the configured command output are shown for the eWLC 9800 HA or not	Passed	
EWLCJ176S_Reg_510	Upgrading the eWLC after configuring the Packet trace and conditional debug command and check	To check if the configured packet trace and conditional debug are same even after the upgrade of the eWLC	Passed	
EWLCJ176S_Reg_511	Downgrading the eWLC after configuring the Packet trace and conditional debug command and check	To check if the configured packet trace and conditional debug are same even after the downgrade of the eWLC	Passed	

Image Upgrade Data Models for Controller

Logical ID	Title	Description	Status	Defect ID
EWLCJ176S_Reg_512	Verify whether AP image gets predownloaded or not	Netconf programmable support for ap image predownload	Passed	
EWLCJ176S_Reg_513	Verify whether AP image predownload completed or not	Netconf programmable support for ap image predownload with SSO Switchover	Passed	
EWLCJ176S_Reg_514	Verify whether AP image predownload abort or not	Netconf programmable support for ap image predownload abort	Passed	
EWLCJ176S_Reg_515	Verify AP image predownload statistics	Netconf programmable support for ap image predownload statistics	Passed	
EWLCJ176S_Reg_516	Verify whether rollback, rollback id details correct or not	Netconf programmable support for show install rollback, rollback id	Passed	
EWLCJ176S_Reg_517	Verify rollback profile information correct or not	Netconf programmable support for show install profile, profile <profile name>	Passed	
EWLCJ176S_Reg_518	Verify AP image and AP image file summary correct or not	Netconf programmable support for show ap image, show ap image file summary	Passed	

EWLCJ176S_Reg_519	Verify whether AP upgrade image details showing correctly or not	Netconf programmable support for show ap upgrade, show ap upgrade summary, show ap upgrade name <report-name>	Passed	
EWLCJ176S_Reg_520	Verify whether async notification from Netconf server generating or not when ap predownload is initiated	Predownload async notification - INSTALL_AP_IMAGE_PRE_DWNLD_INITIATED	Passed	
EWLCJ176S_Reg_521	Verify whether async notification from Netconf server generating or not when ap predownload is InProgress	Predownload async notification - INSTALL_AP_IMAGE_ PRE_DWNLD_IN_PROGRESS	Passed	
EWCJ176S_Reg_344	Verify whether AP image gets predownloaded or not	Netconf programmable support for ap image predownload	Passed	
EWCJ176S_Reg_345	Verify whether AP image predownload completed or not	Netconf programmable support for ap image predownload with SSO Switchover	Passed	
EWCJ176S_Reg_346	Verify whether AP image predownload abort or not	Netconf programmable support for ap image predownload abort	Passed	
EWCJ176S_Reg_347	Verify AP image predownload statistics	Netconf programmable support for ap image predownload statistics	Passed	

EWCJ176S_Reg_348	Verify whether rollback, rollback id details correct or not	Netconf programmable support for show install rollback, rollback id	Passed	
EWCJ176S_Reg_349	Verify rollback profile information correct or not	Netconf programmable support for show install profile, profile <profile name>	Passed	
EWCJ176S_Reg_350	Verify AP image and AP image file summary correct or not	Netconf programmable support for show ap image, show ap image file summary	Passed	
EWCJ176S_Reg_351	Verify whether AP upgrade image details showing correctly or not	Netconf programmable support for show ap upgrade, show ap upgrade summary, show ap upgrade name <report-name>	Passed	
EWCJ176S_Reg_352	Verify whether async notification from Netconf server generating or not when ap predownload is initiated	Predownload async notification - INSTALL_AP_ IMAGE_ PRE_DWNLD_ INITIATED	Passed	
EWCJ176S_Reg_353	Verify whether async notification from Netconf server generating or not when ap predownload is InProgress	Predownload async notification - INSTALL_AP_ IMAGE_PRE_DWNLD_ IN_PROGRESS	Passed	

Client Debug Bundle

Logical ID	Title	Description	Status	Defect ID
EWLCJ176S_Reg_522	Verify the tech wireless command	To Verify the tech wireless command	Passed	
EWLCJ176S_Reg_523	Verify the debugs error , events, info , payload , client details , keep alive in 9115	To Verify the debugs error , events, info , payload , client details , keep alive in 9115	Passed	
EWLCJ176S_Reg_524	Verify the debugs error , events, info , payload , client details , keep alive in 9117	To Verify the debugs error , events, info , payload , client details , keep alive in 9117	Passed	
EWLCJ176S_Reg_525	Verify the debugs error , events, info , payload , client details , keep alive in 9120	To Verify the debugs error , events, info , payload , client details , keep alive in 9120	Passed	
EWLCJ176S_Reg_526	Verify the debugs error , events, info , payload , client details , keep alive in 9130	To Verify the debugs error , events, info , payload , client details , keep alive in 9130	Passed	
EWLCJ176S_Reg_527	Verify mobility stats on Controller with different MAC clients	To Verify mobility stats on Controller with different MAC clients	Passed	
EWLCJ176S_Reg_528	Verify mobility stats on Controller with different Android clients	To Verify mobility stats on Controller with different Android clients	Passed	
EWLCJ176S_Reg_529	Verify mobility stats on Controller with different Windows clients	To Verify mobility stats on Controller with different Windows clients	Passed	
EWCJ176S_Reg_268	Verify the tech wireless command	To Verify the tech wireless command	Passed	

EWCJ176S_Reg_269	Verify the debugs error , events, info , payload , client details , keep alive in 9115	To Verify the debugs error , events, info , payload , client details , keep alive in 9115	Passed	
EWCJ176S_Reg_270	Verify the debugs error , events, info , payload , client details , keep alive in 9117	To Verify the debugs error , events, info , payload , client details , keep alive in 9117	Passed	
EWCJ176S_Reg_271	Verify the debugs error , events, info , payload , client details , keep alive in 9120	To Verify the debugs error , events, info , payload , client details , keep alive in 9120	Passed	
EWCJ176S_Reg_272	Verify the debugs error , events, info , payload , client details , keep alive in 9130	To Verify the debugs error , events, info , payload , client details , keep alive in 9130	Passed	
EWCJ176S_Reg_273	Verify mobility stats on Controller with different MAC clients	To Verify mobility stats on Controller with different MAC clients	Passed	
EWCJ176S_Reg_274	Verify mobility stats on Controller with different Android clients	To Verify mobility stats on Controller with different Android clients	Passed	
EWCJ176S_Reg_275	Verify mobility stats on Controller with different Windows clients	To Verify mobility stats on Controller with different Windows clients	Passed	

ICAP Support for C9130 for 8 users

Logical ID	Title	Description	Status	Defect ID
EWLCJ176S_Reg_530	Packet capture of client when the client is connected to 9130 AP with 2.4 GHz	To capture the Packet of the client when the client is connected to AP with radio as 2.4 GHz in EWLC	Passed	
EWLCJ176S_Reg_531	Packet capture of client when the client is connected to 9130 AP with 5 GHz	To capture the Packet of the client when the client is connected to AP with radio as 5 GHz in EWLC	Passed	
EWLCJ176S_Reg_532	Packet capture for Android client using Intelligent Capture option in Apgroup	To verify the packet capture for Android client using Intelligent capture in APgroup	Passed	
EWLCJ176S_Reg_533	Packet capture for Windows JOS client using Intelligent Capture option in APgroup	To verify the packet capture for Windows client using Intelligent capture in APgroup	Passed	
EWLCJ176S_Reg_534	Packet capture for IOS client using Intelligent Capture option in APgroup	To verify the packet capture for IOS client using Intelligent capture in APgroup	Passed	
EWLCJ176S_Reg_535	Packet capture for Mac OS client using Intelligent Capture option in APgroup	To verify the packet capture for MAC OS client using Intelligent capture in APgroup	Passed	
EWLCJ176S_Reg_536	Capturing of Packet of the client when the client is connected with open security	To capture packet when the client is connected to the iOS AP with security as OPEN in EWLC	Passed	

EWLCJ176S_Reg_537	Capturing of Packet of the client when the client is connected with WPA 2 PSK security	To capture packet when the client is connected to the iOS AP with security as WPA 2 PSK in EWLC	Passed	
EWLCJ176S_Reg_538	Capturing of Packet of the client when the client is connected with WPA 2 Enterprise security	To capture packet when the client is connected to the iOS AP with security as WPA 2 Enterprise in EWLC	Passed	
EWLCJ176S_Reg_539	Capturing of Packet of the client when the client is connected with captive portal-web consent	To capture packet when the client is connected to the AP with security as Captive portal-web consent	Passed	
EWLCJ176S_Reg_540	Packet capture for AnyConnect client using Intelligent Capture option in APgroup page	To verify the packet capture for AnyConnect client using Intelligent capture in APgroup page	Passed	
EWLCJ176S_Reg_541	Packet capture for Windows JOS client using Intelligent Capture option in AP page	To verify the packet capture for Windows JOS client using Intelligent capture in AP page	Passed	
EWLCJ176S_Reg_542	Packet capture for Android client using Intelligent Capture option in AP page	To verify the packet capture for Android client using Intelligent capture in AP page	Passed	
EWLCJ176S_Reg_543	Packet capture for iOS client using Intelligent Capture option in AP page	To verify the packet capture for iOS client using Intelligent capture in AP page	Passed	
EWLCJ176S_Reg_544	Packet capture for MacOS client using Intelligent Capture option in AP page	To verify the packet capture for MacOS client using Intelligent capture in AP page	Passed	

EWLCJ176S_Reg_545	Packet capture for AnyConnect client using Intelligent Capture option in AP page	To verify the packet capture for AnyConnect client using Intelligent capture in AP page	Passed	
EWCJ176S_Reg_202	Packet capture of client when the client is connected to 9130 AP with 2.4 GHz	To capture the Packet of the client when the client is connected to AP with radio as 2.4 GHz in EWC	Passed	
EWCJ176S_Reg_203	Packet capture of client when the client is connected to 9130 AP with 5 GHz	To capture the Packet of the client when the client is connected to AP with radio as 5 GHz in EWC	Passed	
EWCJ176S_Reg_204	Packet capture for Android client using Intelligent Capture option in Apgroup	To verify the packet capture for Android client using Intelligent capture in APgroup	Passed	
EWCJ176S_Reg_205	Packet capture for Windows JOS client using Intelligent Capture option in APgroup	To verify the packet capture for Windows client using Intelligent capture in APgroup	Passed	
EWCJ176S_Reg_206	Packet capture for IOS client using Intelligent Capture option in APgroup	To verify the packet capture for IOS client using Intelligent capture in APgroup	Passed	
EWCJ176S_Reg_207	Packet capture for Mac OS client using Intelligent Capture option in APgroup	To verify the packet capture for MAC OS client using Intelligent capture in APgroup	Passed	
EWCJ176S_Reg_208	Capturing of Packet of the client when the client is connected with open security	To capture packet when the client is connected to the iOS AP with security as OPEN in EWC	Passed	

EWCJ176S_Reg_209	Capturing of Packet of the client when the client is connected with WPA 2 PSK security	To capture packet when the client is connected to the iOS AP with security as WPA 2 PSK in EWC	Passed	
EWCJ176S_Reg_210	Capturing of Packet of the client when the client is connected with WPA 2 Enterprise security	To capture packet when the client is connected to the iOS AP with security as WPA 2 Enterprise in EWC	Passed	
EWCJ176S_Reg_211	Capturing of Packet of the client when the client is connected with captive portal-web consent	To capture packet when the client is connected to the AP with security as Captive portal-web consent	Passed	
EWCJ176S_Reg_212	Packet capture for AnyConnect client using Intelligent Capture option in APgroup page	To verify the packet capture for AnyConnect client using Intelligent capture in APgroup page	Passed	
EWCJ176S_Reg_213	Packet capture for Windows JOS client using Intelligent Capture option in AP page	To verify the packet capture for Windows JOS client using Intelligent capture in AP page	Passed	
EWCJ176S_Reg_214	Packet capture for Android client using Intelligent Capture option in AP page	To verify the packet capture for Android client using Intelligent capture in AP page	Passed	
EWCJ176S_Reg_215	Packet capture for iOS client using Intelligent Capture option in AP page	To verify the packet capture for iOS client using Intelligent capture in AP page	Passed	
EWCJ176S_Reg_216	Packet capture for MacOS client using Intelligent Capture option in AP page	To verify the packet capture for MacOS client using Intelligent capture in AP page	Passed	

EWCJ176S_Reg_217	Packet capture for AnyConnect client using Intelligent Capture option in AP page	To verify the packet capture for AnyConnect client using Intelligent capture in AP page	Passed	
EWLCJ176_2S_Reg_437	Packet capture of client when the client is connected to 9130 AP with 2.4 GHz	To capture the Packet of the client when the client is connected to AP with radio as 2.4 GHz in EWLC	Passed	
EWLCJ176_2S_Reg_438	Packet capture of client when the client is connected to 9130 AP with 5 GHz	To capture the Packet of the client when the client is connected to AP with radio as 5 GHz in EWLC	Passed	
EWLCJ176_2S_Reg_439	Packet capture for Android client using Intelligent Capture option in Apgroup	To verify the packet capture for Android client using Intelligent capture in APgroup	Passed	
EWLCJ176_2S_Reg_440	Packet capture for Windows JOS client using Intelligent Capture option in APgroup	To verify the packet capture for Windows client using Intelligent capture in APgroup	Passed	
EWLCJ176_2S_Reg_441	Packet capture for IOS client using Intelligent Capture option in APgroup	To verify the packet capture for IOS client using Intelligent capture in APgroup	Passed	
EWLCJ176_2S_Reg_442	Packet capture for Mac OS client using Intelligent Capture option in APgroup	To verify the packet capture for MAC OS client using Intelligent capture in APgroup	Passed	
EWLCJ176_2S_Reg_443	Capturing of Packet of the client when the client is connected with open security	To capture packet when the client is connected to the iOS AP with security as OPEN in EWLC	Passed	

EWLCJ176_2S_Reg_444	Capturing of Packet of the client when the client is connected with WPA 2 PSK security	To capture packet when the client is connected to the iOS AP with security as WPA 2 PSK in EWLC	Passed	
EWLCJ176_2S_Reg_445	Capturing of Packet of the client when the client is connected with WPA 2 Enterprise security	To capture packet when the client is connected to the iOS AP with security as WPA 2 Enterprise in EWLC	Passed	
EWLCJ176_2S_Reg_446	Capturing of Packet of the client when the client is connected with captive portal-web consent	To capture packet when the client is connected to the AP with security as Captive portal-web consent	Passed	
EWLCJ176_2S_Reg_447	Packet capture for AnyConnect client using Intelligent Capture option in APgroup page	To verify the packet capture for AnyConnect client using Intelligent capture in APgroup page	Passed	
EWLCJ176_2S_Reg_448	Packet capture for Windows JOS client using Intelligent Capture option in AP page	To verify the packet capture for Windows JOS client using Intelligent capture in AP page	Passed	
EWLCJ176_2S_Reg_449	Packet capture for Android client using Intelligent Capture option in AP page	To verify the packet capture for Android client using Intelligent capture in AP page	Passed	
EWLCJ176_2S_Reg_450	Packet capture for iOS client using Intelligent Capture option in AP page	To verify the packet capture for iOS client using Intelligent capture in AP page	Passed	
EWLCJ176_2S_Reg_451	Packet capture for MacOS client using Intelligent Capture option in AP page	To verify the packet capture for MacOS client using Intelligent capture in AP page	Passed	

EWLCJ176_2S_Reg_452	Packet capture for AnyConnect client using Intelligent Capture option in AP page	To verify the packet capture for AnyConnect client using Intelligent capture in AP page	Passed	
EWCJ176_2S_Reg_235	Packet capture of client when the client is connected to 9130 AP with 2.4 GHz	To capture the Packet of the client when the client is connected to AP with radio as 2.4 GHz in EWC	Passed	
EWCJ176_2S_Reg_236	Packet capture of client when the client is connected to 9130 AP with 5 GHz	To capture the Packet of the client when the client is connected to AP with radio as 5 GHz in EWC	Passed	
EWCJ176_2S_Reg_237	Packet capture for Android client using Intelligent Capture option in Apgroup	To verify the packet capture for Android client using Intelligent capture in APgroup	Passed	
EWCJ176_2S_Reg_238	Packet capture for Windows JOS client using Intelligent Capture option in APgroup	To verify the packet capture for Windows client using Intelligent capture in APgroup	Passed	
EWCJ176_2S_Reg_239	Packet capture for IOS client using Intelligent Capture option in APgroup	To verify the packet capture for IOS client using Intelligent capture in APgroup	Passed	
EWCJ176_2S_Reg_240	Packet capture for Mac OS client using Intelligent Capture option in APgroup	To verify the packet capture for MAC OS client using Intelligent capture in APgroup	Passed	
EWCJ176_2S_Reg_241	Capturing of Packet of the client when the client is connected with open security	To capture packet when the client is connected to the iOS AP with security as OPEN in EWC	Passed	

EWCJ176_2S_Reg_242	Capturing of Packet of the client when the client is connected with WPA 2 PSK security	To capture packet when the client is connected to the iOS AP with security as WPA 2 PSK in EWC	Passed	
EWCJ176_2S_Reg_243	Capturing of Packet of the client when the client is connected with WPA 2 Enterprise security	To capture packet when the client is connected to the iOS AP with security as WPA 2 Enterprise in EWC	Passed	
EWCJ176_2S_Reg_244	Capturing of Packet of the client when the client is connected with captive portal-web consent	To capture packet when the client is connected to the AP with security as Captive portal-web consent	Passed	
EWCJ176_2S_Reg_245	Packet capture for AnyConnect client using Intelligent Capture option in APgroup page	To verify the packet capture for AnyConnect client using Intelligent capture in APgroup page	Passed	
EWCJ176_2S_Reg_246	Packet capture for Windows JOS client using Intelligent Capture option in AP page	To verify the packet capture for Windows JOS client using Intelligent capture in AP page	Passed	
EWCJ176_2S_Reg_247	Packet capture for Android client using Intelligent Capture option in AP page	To verify the packet capture for Android client using Intelligent capture in AP page	Passed	
EWCJ176_2S_Reg_248	Packet capture for iOS client using Intelligent Capture option in AP page	To verify the packet capture for iOS client using Intelligent capture in AP page	Passed	
EWCJ176_2S_Reg_249	Packet capture for MacOS client using Intelligent Capture option in AP page	To verify the packet capture for MacOS client using Intelligent capture in AP page	Passed	

EWCJ176_2S_Reg_250	Packet capture for AnyConnect client using Intelligent Capture option in AP page	To verify the packet capture for AnyConnect client using Intelligent capture in AP page	Passed	

Called Station ID with AP Ethernet MAC

Logical ID	Title	Description	Status	Defect ID
EWLCJ176S_Reg_567	Configure radius-server wireless attribute call station id for authentication and accounting with “policy-tag-name”	To Configure radius-server wireless attribute call station id for authentication and accounting with “policy-tag-name”	Passed	
EWLCJ176S_Reg_568	Configure radius-server wireless attribute call station id for authentication and accounting with “flex-profile-name	To Configure radius-server wireless attribute call station id for authentication and accounting with “flex-profile-name	Passed	
EWLCJ176S_Reg_569	Configure radius-server wireless attribute call station id for authentication and accounting with “ ap- ethmac- ssid -flexprofilename”	To Configure radius-server wireless attribute call station id for authentication and accounting with “ ap- ethmac- ssid -flexprofilename”	Passed	
EWLCJ176S_Reg_570	Configure radius-server wireless attribute call station id for authentication and accounting with “ ap-macaddress -ssid -flexprofilename	To Configure radius-server wireless attribute call station id for authentication and accounting with “ ap-macaddress -ssid -flexprofilename	Passed	
EWLCJ176S_Reg_571	Configure radius-server wireless attribute call station id for authentication and accounting with “ ap - ethmac -ssid -policytagname”	To Configure radius-server wireless attribute call station id for authentication and accounting with “ ap -ethmac- ssid -policytagname”	Passed	

EWLCJ176S_Reg_572	Configure radius-server wireless attribute call station id for authentication and accounting with “ ap-macaddress -ssid -policytagname”	To Configure radius-server wireless attribute call station id for authentication and accounting with “ ap -macaddress -ssid -policytagname”	Passed	
EWLCJ176S_Reg_573	Configure radius-server wireless attribute call station id for authentication and accounting with “ ap -ethmac- ssid -sitetagname”	To Configure radius-server wireless attribute call station id for authentication and accounting with “ap -ethmac- ssid -sitetagname”	Passed	
EWLCJ176S_Reg_574	Configure radius-server wireless attribute call station id for authentication and accounting with “ ap -macaddress- ssid- sitetagname”	To Configure radius-server wireless attribute call station id for authentication and accounting with “ ap -macaddress -ssid - sitetagname”	Passed	
EWLCJ176S_Reg_575	configure different servers for authentication and accounting	To configure different servers for authentication and accounting	Passed	
EWLCJ176S_Reg_576	configuring both AAA and local authentication	To configuring both AAA and local authentication	Passed	
EWLCJ176S_Reg_577	downgrade and upgrade impact	To verify config impact after downgrade and upgrade	Passed	
EWLCJ176S_Reg_578	HA active to stanby config impact	To verify config impact HA active to stanby	Passed	
EWLCJ176S_Reg_579	active to stanby to active config impact	To verify config impact when active to stanby to active	Passed	

EWLCJ176S_Reg_580	Change mac address format in attribute and check config impact "radius-server attribute 31 mac format ? "	To Change mac address format in attribute and check config	Passed	
EWLCJ176S_Reg_581	with mac filtering configured in AAA	To Configure mac filtering and verify client connectivity	Passed	
EWLCJ176S_Reg_582	Change station id case and verify config impact "radius-server attribute wireless authentication callstationIdCase upper/lower"	To Change station id case and verify config impact	Passed	
EWCJ176S_Reg_403	Configure radius-server wireless attribute call station id for authentication and accounting with “policy-tag-name”	To Configure radius-server wireless attribute call station id for authentication and accounting with “policy-tag-name”	Passed	
EWCJ176S_Reg_404	Configure radius-server wireless attribute call station id for authentication and accounting with “flex-profile-name	To Configure radius-server wireless attribute call station id for authentication and accounting with “flex-profile-name	Passed	
EWCJ176S_Reg_405	Configure radius-server wireless attribute call station id for authentication and accounting with “ ap-ethmac- ssid -flexprofilename”	To Configure radius-server wireless attribute call station id for authentication and accounting with “ ap-ethmac- ssid -flexprofilename”	Passed	

EWCJ176S_Reg_406	Configure radius-server wireless attribute call station id for authentication and accounting with " ap -macaddress-ssid -flexprofilename	To Configure radius-server wireless attribute call station id for authentication and accounting with " ap -macaddress-ssid-flexprofilename	Passed	
EWCJ176S_Reg_407	Configure radius-server wireless attribute call station id for authentication and accounting with " ap-ethmac- ssid -policytagname"	To Configure radius-server wireless attribute call station id for authentication and accounting with " ap -ethmac- ssid -policytagname"	Passed	
EWCJ176S_Reg_408	Configure radius-server wireless attribute call station id for authentication and accounting with " ap-macaddress -ssid -policytagname"	To Configure radius-server wireless attribute call station id for authentication and accounting with " ap-macaddress -ssid -policytagname"	Passed	
EWCJ176S_Reg_409	Configure radius-server wireless attribute call station id for authentication and accounting with " ap-ethmac- ssid -sitetagname"	To Configure radius-server wireless attribute call station id for authentication and accounting with " ap-ethmac- ssid -sitetagname"	Passed	
EWCJ176S_Reg_410	Configure radius-server wireless attribute call station id for authentication and accounting with " ap -macaddress -ssid -sitetagname"	To Configure radius-server wireless attribute call station id for authentication and accounting with " ap -macaddress -ssid -sitetagname"	Passed	
EWCJ176S_Reg_411	configure different servers for authentication and accounting	To configure different servers for authentication and accounting	Passed	
EWCJ176S_Reg_412	configuring both AAA and local authentication	To configuring both AAA and local authentication	Passed	

EWCJ176S_Reg_413	downgrade and upgrade impact	To verify config impact after downgrade and upgrade	Passed	CSCvx46901
EWCJ176S_Reg_414	HA active to stanby config impact	To verify config impact HA active to stanby	Passed	
EWCJ176S_Reg_415	active to stanby to active config impact	To verify config impact when active to stanby to active	Passed	
EWCJ176S_Reg_416	Change mac address format in attribute and check config impact "radius-server attribute 31 mac format ? "	To Change mac address format in attribute and check config	Passed	
EWCJ176S_Reg_417	with mac filtering configured in AAA	To Configure mac filtering and verify client connectivity	Passed	
EWCJ176S_Reg_418	Change station id case and verify config impact "radius-server attribute wireless authentication callstationIdCase upper/lower"	To Change station id case and verify config impact	Passed	
EWLCJ176_2S_Reg_474	Configure radius-server wireless attribute call station id for authentication and accounting with “policy-tag-name”	To Configure radius-server wireless attribute call station id for authentication and accounting with “policy-tag-name”	Passed	
EWLCJ176_2S_Reg_475	Configure radius-server wireless attribute call station id for authentication and accounting with “flex-profile-name	To Configure radius-server wireless attribute call station id for authentication and accounting with “flex-profile-name	Passed	

EWLCJ176_2S_Reg_476	Configure radius-server wireless attribute call station id for authentication and accounting with “ap-ethmac- ssid-flex profile name”	To Configure radius-server wireless attribute call station id for authentication and accounting with “ap-ethmac-ssid-flex profile name”	Passed	
EWLCJ176_2S_Reg_477	Configure radius-server wireless attribute call station id for authentication and accounting with “ap-mac address-ssid-flex profile name	To Configure radius-server wireless attribute call station id for authentication and accounting with “ap--ssid- flex profile name	Passed	
EWLCJ176_2S_Reg_478	Configure radius-server wireless attribute call station id for authentication and accounting with “ap-ethmac-ssid-policy tag name”	To Configure radius-server wireless attribute call station id for authentication and accounting with “ap-ethmac- ssid-policy tag name”	Passed	
EWLCJ176_2S_Reg_479	Configure radius-server wireless attribute call station id for authentication and accounting with “ap--ssid- policy tag name”	To Configure radius-server wireless attribute call station id for authentication and accounting with “ap--ssid- policy tag name”	Passed	
EWLCJ176_2S_Reg_480	Configure radius-server wireless attribute call station id for authentication and accounting with “ap-ethmac- ssid-site tag name”	To Configure radius-server wireless attribute call station id for authentication and accounting with “ap-ethmac-ssid-site tag name”	Passed	

EWLCJ176_2S_Reg_481	Configure radius-server wireless attribute call station id for authentication and accounting with “ap--ssid-site tag name”	To Configure radius-server wireless attribute call station id for authentication and accounting with “ap--ssid-site tag name”	Passed	
EWLCJ176_2S_Reg_482	configure different servers for authentication and accounting	To configure different servers for authentication and accounting	Passed	
EWLCJ176_2S_Reg_483	configuring both AAA and local authentication	To configuring both AAA and local authentication	Passed	
EWLCJ176_2S_Reg_484	downgrade and upgrade impact	To verify config impact after downgrade and upgrade	Passed	
EWLCJ176_2S_Reg_485	HA active to standby config impact	To verify config impact HA active to standby	Passed	
EWLCJ176_2S_Reg_486	active to standby to active config impact	To verify config impact when active to standby to active	Passed	
EWLCJ176_2S_Reg_487	Change mac address format in attribute and check config impact "radius-server attribute 31 mac format ? "	To Change mac address format in attribute and check config	Passed	
EWLCJ176_2S_Reg_488	with mac filtering configured in AAA	To Configure mac filtering and verify client connectivity	Passed	
EWLCJ176_2S_Reg_489	Change station id case and verify config impact "radius-server attribute wireless authentication callstationIdCase upper/lower"	To Change station id case and verify config impact	Passed	

EWCJ176_2S_Reg_371	Configure radius-server wireless attribute call station id for authentication and accounting with “policy-tag-name”	To Configure radius-server wireless attribute call station id for authentication and accounting with “policy-tag-name”	Passed	CSCvy34145
EWCJ176_2S_Reg_372	Configure radius-server wireless attribute call station id for authentication and accounting with “flex-profile-name	To Configure radius-server wireless attribute call station id for authentication and accounting with “flex-profile-name	Passed	
EWCJ176_2S_Reg_373	Configure radius-server wireless attribute call station id for authentication and accounting with “ap-ethmac-ssid-flex profile name”	To Configure radius-server wireless attribute call station id for authentication and accounting with “ap-ethmac-ssid-flex profile name”	Passed	
EWCJ176_2S_Reg_374	Configure radius-server wireless attribute call station id for authentication and accounting with “ap-mac address-ssid-flex profile name	To Configure radius-server wireless attribute call station id for authentication and accounting with “ap-mac address-ssid-flex profile name	Passed	
EWCJ176_2S_Reg_375	Configure radius-server wireless attribute call station id for authentication and accounting with “ap-ethmac-ssid-policy tag name”	To Configure radius-server wireless attribute call station id for authentication and accounting with “ap-ethmac-ssid-policy tag name”	Passed	

EWCJ176_2S_Reg_376	Configure radius-server wireless attribute call station id for authentication and accounting with “ap-macaddress-ssid-policy tag name”	To Configure radius-server wireless attribute call station id for authentication and accounting with “ap-macaddress-ssid-policy tag name”	Passed	
EWCJ176_2S_Reg_377	Configure radius-server wireless attribute call station id for authentication and accounting with “ap-ethmac-ssid-site tag name”	To Configure radius-server wireless attribute call station id for authentication and accounting with “ap-ethmac-ssid-site tag name”	Passed	
EWCJ176_2S_Reg_378	Configure radius-server wireless attribute call station id for authentication and accounting with “ap-mac address-ssid-site tag name”	To Configure radius-server wireless attribute call station id for authentication and accounting with “ap-macaddress-ssid-site tag name”	Passed	
EWCJ176_2S_Reg_379	configure different servers for authentication and accounting	To configure different servers for authentication and accounting	Passed	
EWCJ176_2S_Reg_380	configuring both AAA and local authentication	To configuring both AAA and local authentication	Passed	
EWCJ176_2S_Reg_381	downgrade and upgrade impact	To verify config impact after downgrade and upgrade	Passed	
EWCJ176_2S_Reg_382	HA active to standby config impact	To verify config impact HA active to standby	Passed	
EWCJ176_2S_Reg_383	active to standby to active config impact	To verify config impact when active to standby to active	Passed	

EWCJ176_2S_Reg_384	Change mac address format in attribute and check config impact "radius-server attribute 31 mac format ? "	To Change mac address format in attribute and check config	Passed	
EWCJ176_2S_Reg_385	with mac filtering configured in AAA	To Configure mac filtering and verify client connectivity	Failed	CSCvy96687
EWCJ176_2S_Reg_386	Change station id case and verify config impact "radius-server attribute wireless authentication call station Id Case upper/ lower"	To Change station id case and verify config impact	Passed	

Capability to enable/disable 11ax features per SSID

Logical ID	Title	Description	Status	Defect ID
EWLCJ176S_Reg_601	Check the 11 ax enabling or not via GUI	To verify whether the 11 ax parameters enable or not via GUI	Passed	
EWLCJ176S_Reg_602	Check the 11 ax disabling or not via GUI	To verify whether the 11 ax parameters disable or not via GUI	Passed	
EWLCJ176S_Reg_603	Check the 11 ax enabling or not via CLI	To verify whether the 11 ax parameters enable or not via CLI	Passed	
EWLCJ176S_Reg_604	Check the 11 ax disabling or not via CLI	To verify whether the 11 ax parameters disable or not via CLI	Passed	
EWLCJ176S_Reg_605	Disabling 11 ax radio and checking the client connectivity	To check the client connectivity after disabling 11 ax	Passed	
EWLCJ176S_Reg_606	Checking the 11 ax parameters after AP reboot	To verify the 11 ax for after AP reboot	Passed	
EWLCJ176S_Reg_607	Checking the 11 ax parameters after AP radio change	To check whether the 11 ax parameters showing or not after changing the AP radio	Passed	
EWLCJ176S_Reg_608	Verifying 11 ax parameters for different AP models	To Verify the 11 ax parameters for different AP models	Passed	
EWLCJ176S_Reg_609	Validating the 11ax parameters after disjoin the AP	To validate the 11 ax parameters for after Ap disjoin	Passed	
EWLCJ176S_Reg_610	Verifying the 11 ax parameters after deleting the client	To verify the 11 ax parameters for deleted client	Passed	

EWLCJ176S_Reg_611	monitoring the 11 ax parameters after AP provisioning from DNAC	To check the 11 ax parameters after AP provisioning from DNAC	Passed	
EWLCJ176S_Reg_612	Verifying the 11 ax parameters by deleting the SSID	To Verify the 11 ax parameters after Deleting SSID	Passed	
EWLCJ176S_Reg_613	Verifying the 11 ax parameters for intra roaming client	To Verify the 11 ax parameters after client roaming between AP's	Passed	
EWLCJ176S_Reg_614	Checking the 11 ax parameters for inter roaming client	To Verify the 11 ax parameters status after client roaming between controllers	Passed	
EWLCJ176S_Reg_615	Verifying the 11 ax status by changing the security type	To check the11 ax parameters after changing the security type	Passed	
EWLCJ176S_Reg_616	Validating the 11ax status for Virtual EWLC	To validate the 11 ax parameters for vEWLC	Passed	
EWLCJ176_2S_Reg_490	Check the 11 ax enabling or not via GUI	To verify whether the 11 ax parameters enable or not via GUI	Passed	
EWLCJ176_2S_Reg_491	Check the 11 ax disabling or not via GUI	To verify whether the 11 ax parameters disable or not via GUI	Passed	
EWLCJ176_2S_Reg_492	Check the 11 ax enabling or not via CLI	To verify whether the 11 ax parameters enable or not via CLI	Passed	
EWLCJ176_2S_Reg_493	Check the 11 ax disabling or not via CLI	To verify whether the 11 ax parameters disable or not via CLI	Passed	
EWLCJ176_2S_Reg_494	Disabling 11 ax radio and checking the client connectivity	To check the client connectivity after disabling 11 ax	Passed	
EWLCJ176_2S_Reg_495	Checking the 11 ax parameters after AP reboot	To verify the 11 ax for after AP reboot	Passed	

EWLCJ176_2S_Reg_496	Checking the 11 ax parameters after AP radio change	To check whether the 11 ax parameters showing or not after changing the AP radio	Passed	
EWLCJ176_2S_Reg_497	Verifying 11 ax parameters for different AP models	To Verify the 11 ax parameters for different AP models	Passed	
EWLCJ176_2S_Reg_498	Validating the 11ax parameters after disjoin the AP	To validate the 11 ax parameters for after Ap disjoin	Passed	
EWLCJ176_2S_Reg_499	Verifying the 11 ax parameters after deleting the client	To verify the 11 ax parameters for deleted client	Passed	
EWLCJ176_2S_Reg_500	monitoring the 11 ax parameters after AP provisioning from DNAC	To check the 11 ax parameters after AP provisioning from DNAC	Passed	
EWLCJ176_2S_Reg_501	Verifying the 11 ax parameters by deleting the SSID	To Verify the 11 ax parameters after Deleting SSID	Passed	
EWLCJ176_2S_Reg_502	Verifying the 11 ax parameters for intra roaming client	To Verify the 11 ax parameters after client roaming between AP's	Passed	
EWLCJ176_2S_Reg_503	Checking the 11 ax parameters for inter roaming client	To Verify the 11 ax parameters status after client roaming between controllers	Passed	
EWLCJ176_2S_Reg_504	Verifying the 11 ax status by changing the security type	To check the11 ax parameters after changing the security type	Passed	
EWLCJ176_2S_Reg_505	Validating the 11ax status for Virtual EWLC	To validate the 11 ax parameters for vEWLC	Passed	

ISSU Data Model Support

Logical ID	Title	Description	Status	Defect ID
EWLCJ176S_Reg_657	Configure HA setup using RP/RMI option.	To configure HA setup using RP/RMI option.	Passed	
EWLCJ176S_Reg_658	ISSU upgrade with HA SSO RMI	To perform ISSU upgrade in HA SSO RMI setup and monitor behaviour	Passed	
EWLCJ176S_Reg_659	Check ISSU downgrade with HA SSO RMI	To perform ISSU upgrade in HA SSO RMI setup and monitor behaviour	Passed	
EWLCJ176S_Reg_660	Client retention during ISSU upgrade/downgrade	To verify client retention after ISSU upgrade/downgrade.	Passed	
EWLCJ176S_Reg_661	Performing Rollback for controller using ISSU.	To check whether the rollback happening for Controller image or not.	Passed	
EWLCJ176S_Reg_662	Disabling the Rollback timer during upgrading controller using ISSU.	To check that the rollback doesn't happen for Controller image or not.	Passed	
EWLCJ176S_Reg_663	Aborting the upgradation of Controller using ISSU.	To check whether the upgradation for Controller image is aborted or not.	Passed	
EWLCJ176S_Reg_664	Performing Upgradation for controller using ISSU via tftp server.	To check whether the Controller Upgradation via tftp is happening or not.	Passed	
EWLCJ176S_Reg_665	Performing Upgradation for Controller using ISSU via sftp server.	To check whether the Controller Upgradation via sftp is happening or not.	Passed	

EWLCJ176S_Reg_666	Performing Upgradation for controller using ISSU via http server.	To check whether the Controller Upgradation via http is happening or not.	Failed	CSCvx41202
EWLCJ176S_Reg_667	Checking the client connectivity	To check whether the client continuously connecting during the upgrade of AP	Passed	
EWLCJ176S_Reg_668	Profile addition during ISSU	To add profile during ISSU operation	Passed	
EWLCJ176S_Reg_669	Verify AP upgrade related during ISSU	To verify AP upgrade related during ISSU	Passed	
EWLCJ176S_Reg_670	Verify that config-sync related commands are not supported	To verify that config-sync related commands are not supported	Passed	
EWLCJ176S_Reg_671	ISSU support on yang enabled scenario	To check ISSU support on yang enabled scenario	Passed	
EWLCJ176S_Reg_672	APDP/APSP support on yang model enabled	To check APDP/APSP support on yang enabled scenario	Passed	
EWLCJ176S_Reg_673	SMU support on yang model	To check SMU support on yang enabled scenario	Passed	
EWLCJ176S_Reg_674	Validation of Auto upgrade scenario	To validate auto upgrade scenario	Passed	
EWLCJ176S_Reg_675	Rolling AP upgrade/AP predownload support on yang model	To check rolling AP upgrade/AP predownload support on yang model	Passed	
EWLCJ176_2S_Reg_506	Configure HA setup using RP/RMI option.	To configure HA setup using RP/RMI option.	Passed	
EWLCJ176_2S_Reg_507	ISSU upgrade with HA SSO RMI	To perform ISSU upgrade in HA SSO RMI setup and monitor behaviour	Passed	

EWLCJ176_2S_Reg_508	Check ISSU downgrade with HA SSO RMI	To perform ISSU upgrade in HA SSO RMI setup and monitor behaviour	Passed	
EWLCJ176_2S_Reg_509	Client retention during ISSU upgrade/downgrade	To verify client retention after ISSU upgrade/downgrade.	Passed	
EWLCJ176_2S_Reg_510	Performing Rollback for controller using ISSU.	To check whether the rollback happening for Controller image or not.	Passed	
EWLCJ176_2S_Reg_511	Disabling the Rollback timer during upgrading controller using ISSU.	To check that the rollback doesn't happen for Controller image or not.	Passed	
EWLCJ176_2S_Reg_512	Aborting the upgradation of Controller using ISSU.	To check whether the upgradation for Controller image is aborted or not.	Passed	
EWLCJ176_2S_Reg_513	Performing Upgradation for controller using ISSU via tftp server.	To check whether the Controller Upgradation via tftp is happening or not.	Passed	
EWLCJ176_2S_Reg_514	Performing Upgradation for Controller using ISSU via sftp server.	To check whether the Controller Upgradation via sftp is happening or not.	Passed	
EWLCJ176_2S_Reg_515	Performing Upgradation for controller using ISSU via http server.	To check whether the Controller Upgradation via http is happening or not.	Passed	
EWLCJ176_2S_Reg_516	Checking the client connectivity	To check whether the client continuously connecting during the upgrade of AP	Passed	
EWLCJ176_2S_Reg_517	Profile addition during ISSU	To add profile during ISSU operation	Passed	
EWLCJ176_2S_Reg_518	Verify AP upgrade related during ISSU	To verify AP upgrade related during ISSU	Passed	

EWLCJ176_2S_Reg_519	Verify that config-sync related commands are not supported	To verify that config-sync related commands are not supported	Passed	
EWLCJ176_2S_Reg_520	ISSU support on yang enabled scenario	To check ISSU support on yang enabled scenario	Passed	
EWLCJ176_2S_Reg_521	APDP/APSP support on yang model enabled	To check APDP/APSP support on yang enabled scenario	Passed	
EWLCJ176_2S_Reg_522	SMU support on yang model	To check SMU support on yang enabled scenario	Passed	
EWLCJ176_2S_Reg_523	Validation of Auto upgrade scenario	To validate auto upgrade scenario	Passed	
EWLCJ176_2S_Reg_524	Rolling AP upgrade/AP predownloaded support on yang model	To check rolling AP upgrade/AP predownloaded support on yang model	Passed	

RRM assurance for granular reasons for power and channel change

Logical ID	Title	Description	Status	Defect ID
EWLCJ176S_Reg_583	Configuring Access Points, Channel width radio parameters for 5Ghz band.	To configure Access Points, Channel width radio parameters for 5Ghz band.	Passed	
EWLCJ176S_Reg_584	Configuring Access Points, Channel width radio parameters for 2.4Ghz band.	To configure Access Points, Channel width radio parameters for 2.4Ghz band.	Passed	
EWLCJ176S_Reg_585	Configure channel parameters for 5ghz band and monitor in DNAC	To configure channel parameters for 5ghz band and monitor in DNAC	Passed	
EWLCJ176S_Reg_586	Configure channel parameters for 5ghz band slot 2 and monitor in DNAC	To configure channel parameters for 5ghz band slot 2 and monitor in DNAC	Passed	
EWLCJ176S_Reg_587	Configure channel parameters for 24ghz band and monitor in DNAC	To configure channel parameters for 24ghz band and monitor in DNAC	Passed	
EWLCJ176S_Reg_588	Configure channel parameters for dual band and monitor in DNAC	To configure channel parameters for dual band and monitor in DNAC	Passed	
EWLCJ176S_Reg_589	Channel updating and monitor assurance in DNAC	To perform channel updating and monitor assurance in DNAC	Passed	
EWLCJ176S_Reg_590	Configure tx power for 5ghz band and monitor in DNAC	To configure tx power for 5ghz band and monitor in DNAC	Passed	
EWLCJ176S_Reg_591	Configure tx power for 24ghz band and monitor in DNAC	To configure tx power for 24ghz band and monitor in DNAC	Passed	

EWLCJ176S_Reg_592	Configure tx power for dual band and monitor in DNAC	To configure tx power for dual band and monitor in DNAC	Passed	
EWLCJ176S_Reg_593	Configure tx power for 5ghz rrm band and monitor in DNAC	To configure tx power for 5ghz rrm band and monitor in DNAC	Passed	
EWLCJ176S_Reg_594	Configure tx power for 24ghz rrm band and monitor in DNAC	To configure tx power for 24ghz rrm band and monitor in DNAC	Passed	
EWLCJ176S_Reg_595	Validate assurance via RRM using Android client	To validate assurance via RRM using Android client	Passed	
EWLCJ176S_Reg_596	Validate assurance via RRM using Surface client	To validate assurance via RRM using Surface client	Passed	
EWLCJ176S_Reg_597	Validate assurance via RRM using mac client	To validate assurance via RRM using mac client	Passed	
EWLCJ176S_Reg_598	Validate assurance via RRM using different models of AP	To validate assurance via RRM using different models of AP	Passed	
EWLCJ176S_Reg_599	Validate assurance via RRM using EWC-AP	To validate assurance via RRM using EWC-AP	Passed	
EWLCJ176S_Reg_600	Validate assurance via RRM using HA pair	To validate assurance via RRM using HA pair	Passed	
EWCJ176S_Reg_419	Configuring Access Points, Channel width radio parameters for 5Ghz band.	To configure Access Points, Channel width radio parameters for 5Ghz band.	Passed	
EWCJ176S_Reg_420	Configuring Access Points, Channel width radio parameters for 2.4Ghz band.	To configure Access Points, Channel width radio parameters for 2.4Ghz band.	Passed	CSCvx86095
EWCJ176S_Reg_421	Configure channel parameters for 5ghz band and monitor in DNAC	To configure channel parameters for 5ghz band and monitor in DNAC	Passed	

EWCJ176S_Reg_422	Configure channel parameters for 5ghz band slot 2 and monitor in DNAC	To configure channel parameters for 5ghz band slot 2 and monitor in DNAC	Passed	
EWCJ176S_Reg_423	Configure channel parameters for 24ghz band and monitor in DNAC	To configure channel parameters for 24ghz band and monitor in DNAC	Passed	CSCvx52243
EWCJ176S_Reg_424	Configure channel parameters for dual band and monitor in DNAC	To configure channel parameters for dual band and monitor in DNAC	Passed	
EWCJ176S_Reg_425	Channel updating and monitor assurance in DNAC	To perform channel updating and monitor assurance in DNAC	Passed	
EWCJ176S_Reg_426	Configure tx power for 5ghz band and monitor in DNAC	To configure tx power for 5ghz band and monitor in DNAC	Passed	
EWCJ176S_Reg_427	Configure tx power for 24ghz band and monitor in DNAC	To configure tx power for 24ghz band and monitor in DNAC	Passed	
EWCJ176S_Reg_428	Configure tx power for dual band and monitor in DNAC	To configure tx power for dual band and monitor in DNAC	Passed	
EWCJ176S_Reg_429	Configure tx power for 5ghz rrm band and monitor in DNAC	To configure tx power for 5ghz rrm band and monitor in DNAC	Passed	
EWCJ176S_Reg_430	Configure tx power for 24ghz rrm band and monitor in DNAC	To configure tx power for 24ghz rrm band and monitor in DNAC	Passed	
EWCJ176S_Reg_431	Validate assurance via RRM using Android client	To validate assurance via RRM using Android client	Passed	
EWCJ176S_Reg_432	Validate assurance via RRM using Surface client	To validate assurance via RRM using Surface client	Passed	

EWCJ176S_Reg_433	Validate assurance via RRM using mac client	To validate assurance via RRM using mac client	Passed	
EWCJ176S_Reg_434	Validate assurance via RRM using different models of AP	To validate assurance via RRM using different models of AP	Passed	
EWCJ176S_Reg_435	Validate assurance via RRM using EWC-AP	To validate assurance via RRM using EWC-AP	Passed	
EWCJ176S_Reg_436	Validate assurance via RRM using HA pair	To validate assurance via RRM using HA pair	Passed	
EWCJ176_2S_Reg_203	Configuring Access Points, Channel width radio parameters for 5Ghz band.	To configure Access Points, Channel width radio parameters for 5Ghz band.	Passed	
EWCJ176_2S_Reg_204	Configuring Access Points, Channel width radio parameters for 2.4Ghz band.	To configure Access Points, Channel width radio parameters for 2.4Ghz band.	Passed	
EWCJ176_2S_Reg_205	Configure channel parameters for 5ghz band and monitor in DNAC	To configure channel parameters for 5ghz band and monitor in DNAC	Passed	
EWCJ176_2S_Reg_206	Configure channel parameters for 5ghz band slot 2 and monitor in DNAC	To configure channel parameters for 5ghz band slot 2 and monitor in DNAC	Passed	
EWCJ176_2S_Reg_207	Configure channel parameters for 24ghz band and monitor in DNAC	To configure channel parameters for 24ghz band and monitor in DNAC	Passed	
EWCJ176_2S_Reg_208	Configure channel parameters for dual band and monitor in DNAC	To configure channel parameters for dual band and monitor in DNAC	Passed	
EWCJ176_2S_Reg_209	Channel updation and monitor assurance in DNAC	To perform channel updation and monitor assurance in DNAC	Passed	

EWCJ176_2S_Reg_210	Configure tx power for 5ghz band and monitor in DNAC	To configure tx power for 5ghz band and monitor in DNAC	Passed	
EWCJ176_2S_Reg_211	Configure tx power for 24ghz band and monitor in DNAC	To configure tx power for 24ghz band and monitor in DNAC	Passed	
EWCJ176_2S_Reg_212	Configure tx power for dual band and monitor in DNAC	To configure tx power for dual band and monitor in DNAC	Passed	
EWCJ176_2S_Reg_213	Configure tx power for 5ghz rrm band and monitor in DNAC	To configure tx power for 5ghz rrm band and monitor in DNAC	Passed	
EWCJ176_2S_Reg_214	Configure tx power for 24ghz rrm band and monitor in DNAC	To configure tx power for 24ghz rrm band and monitor in DNAC	Passed	
EWCJ176_2S_Reg_215	Validate assurance via RRM using Android client	To validate assurance via RRM using Android client	Passed	
EWCJ176_2S_Reg_216	Validate assurance via RRM using Surface client	To validate assurance via RRM using Surface client	Passed	
EWCJ176_2S_Reg_217	Validate assurance via RRM using mac client	To validate assurance via RRM using mac client	Passed	
EWCJ176_2S_Reg_218	Validate assurance via RRM using different models of AP	To validate assurance via RRM using different models of AP	Passed	
EWCJ176_2S_Reg_219	Validate assurance via RRM using EWC-AP	To validate assurance via RRM using EWC-AP	Passed	
EWCJ176_2S_Reg_220	Validate assurance via RRM using HA pair	To validate assurance via RRM using HA pair	Passed	

APSP/APDP support in WebUI for EWLC-ME

Logical ID	Title	Description	Status	Defect ID
EWCJ176S_Reg_01	Adding the APSP configuration in EWC for AP image upgrade.	To check whether the APSP configuration is added successfully and AP is upgraded or not.	Passed	
EWCJ176S_Reg_02	Adding the APDP configuration in EWC for AP image upgrade.	To check whether the APDP configuration is added successfully and AP is upgraded or not.	Passed	
EWCJ176S_Reg_03	Adding the APSP/APDP configuration in EWC for AP image upgrade using SFTP type.	To check whether the APSP/APDP configuration is added successfully and AP is upgraded or not.	Passed	
EWCJ176S_Reg_04	Adding the APSP/APDP configuration in EWC for AP image upgrade using FTP type.	To check whether the APSP/APDP configuration is added successfully and AP is upgraded or not.	Passed	
EWCJ176S_Reg_05	Adding the APSP/APDP configuration in EWC for AP image upgrade using Device type.	To check whether the APSP/APDP configuration is added successfully and AP is upgraded or not.	Passed	
EWCJ176S_Reg_06	Verifying whether APSP/APDP is accepting a invalid file path.	To check whether APSP/APDP is accepting invalid file path or not	Passed	
EWCJ176S_Reg_07	Verifying whether APSP/APDP is accepting a invalid ip address.	To check whether APSP/APDP is accepting invalid Ip address or not	Passed	
EWCJ176S_Reg_08	Verifying whether APSP/APDP is accepting a invalid credentials.	To check whether APSP/APDP is accepting invalid credentials or not	Passed	

EWCJ176S_Reg_09	Verifying whether APSP/APDP is accepting a invalid credentials.	To check whether APSP/APDP is accepting invalid credentials or not	Passed	
EWCJ176S_Reg_10	Connecting client after upgrading AP image using APSP/APDP.	To check whether connecting clients after the ap image upgradation using APSP/APDP	Passed	
EWCJ176_2S_Reg_21	Adding the APSP configuration in EWC for AP image upgrade.	To check whether the APSP configuration is added successfully and AP is upgraded or not.	Passed	
EWCJ176_2S_Reg_22	Adding the APDP configuration in EWC for AP image upgrade.	To check whether the APDP configuration is added successfully and AP is upgraded or not.	Passed	
EWCJ176_2S_Reg_23	Adding the APSP/APDP configuration in EWC for AP image upgrade using SFTP type.	To check whether the APSP/APDP configuration is added successfully and AP is upgraded or not.	Passed	
EWCJ176_2S_Reg_24	Adding the APSP/APDP configuration in EWC for AP image upgrade using FTP type.	To check whether the APSP/APDP configuration is added successfully and AP is upgraded or not.	Passed	
EWCJ176_2S_Reg_25	Adding the APSP/APDP configuration in EWC for AP image upgrade using Device type.	To check whether the APSP/APDP configuration is added successfully and AP is upgraded or not.	Passed	
EWCJ176_2S_Reg_26	Verifying whether APSP/APDP is accepting a invalid file path.	To check whether APSP/APDP is accepting invalid file path or not	Passed	
EWCJ176_2S_Reg_27	Verifying whether APSP/APDP is accepting a invalid ip address.	To check whether APSP/APDP is accepting invalid Ip address or not	Passed	

EWCJ176_2S_Reg_28	Verifying whether APSP/APDP is accepting a invalid credentials.	To check whether APSP/APDP is accepting invalid credentials or not	Passed	
EWCJ176_2S_Reg_29	Verifying whether APSP/APDP is accepting a invalid credentials.	To check whether APSP/APDP is accepting invalid credentials or not	Passed	
EWCJ176_2S_Reg_30	Connecting client after upgrading AP image using APSP/APDP.	To check whether connecting clients after the ap image upgradation using APSP/APDP	Passed	

Standby Monitoring Enhancements

Logical ID	Title	Description	Status	Defect ID
EWLCJ176S_Reg_642	Configure HA SSO RMI & validate HA RMI parameters.	To Configure HA SSO RMI	Passed	
EWLCJ176S_Reg_643	Verify HA setup details from Standby console	To verify HA setup details in Standby console	Passed	
EWLCJ176S_Reg_644	Check interfaces state from standby console	To check interfaces state from standby console	Passed	
EWLCJ176S_Reg_645	Check environment details from standby console	To monitor environment details from standby console	Passed	
EWLCJ176S_Reg_646	Check process usage details in standby console	To check process usage details in standby console	Passed	
EWLCJ176S_Reg_647	Monitor running process in Standby unit from Active unit console	To monitor running process in Standby unit from Active unit console	Passed	
EWLCJ176S_Reg_648	SSH to standby console directly and check connectivity	To SSH to standby console directly and check connectivity	Passed	
EWLCJ176S_Reg_649	SSH to standby console via AAA authentication	To SSH to standby console via AAA authentication	Passed	
EWLCJ176S_Reg_650	SSH to standby console via Tacacs authentication	To SSH to standby console via Tacacs authentication	Passed	
EWLCJ176S_Reg_651	Monitor health of the system	To monitor health of the system	Passed	
EWLCJ176S_Reg_652	Preventing write access in standby console	To prevent write access in standby console	Passed	
EWLCJ176S_Reg_653	Validating inventory information on standby	To validate inventory information on standby	Passed	

EWLCJ176S_Reg_654	Check logging information of standby chassis	To check logging information of standby chassis	Passed	
EWLCJ176S_Reg_655	Monitor failure fan state via SNMP	To monitor failure fan state via SNMP	Passed	
EWLCJ176S_Reg_656	Validation of Auto upgrade scenario	To validate auto upgrade scenario from standby chassis	Passed	

Fabric In A Box (webUI for Embedded Wireless on 9k Switches)

Logical ID	Title	Description	Status	Defect ID
EWCJ176_2S_Reg_31	To Deploy Fabric configuration from webUI on 9300	To Verify Fabric UI on 9300	Passed	
EWCJ176_2S_Reg_32	To Deploy Fabric configuration from webUI on 9300 and Windows Client	To Verify Fabric UI on 9300 with Window Client	Passed	
EWCJ176_2S_Reg_33	To Deploy Fabric configuration from webUI on 9300 and Android Client	To Verify Fabric UI on 9300 with Android Client	Passed	
EWCJ176_2S_Reg_34	To Deploy Fabric configuration from webUI on 9300 and MAC Client	To Verify Fabric UI on 9300 with MAC Client	Passed	
EWCJ176_2S_Reg_35	To Deploy Fabric configuration from webUI on 9300 and Apple Mobile Client	To Verify Fabric UI on 9300 with Apple Mobile Client	Passed	
EWCJ176_2S_Reg_36	To Deploy Fabric configuration from webUI on 9400	To Verify Fabric UI on 9400	Passed	
EWCJ176_2S_Reg_37	To Deploy Fabric configuration from webUI on 9400 and Windows Client	To Verify Fabric UI on 9400 with Window Client	Passed	
EWCJ176_2S_Reg_38	To Deploy Fabric configuration from webUI on 9400 and Android Client	To Verify Fabric UI on 9400 with Android Client	Passed	
EWCJ176_2S_Reg_39	To Deploy Fabric configuration from webUI on 9400 and MAC Client	To Verify Fabric UI on 9400 with MAC Client	Passed	
EWCJ176_2S_Reg_40	To Deploy Fabric configuration from webUI on 9400 and Apple Mobile Client	To Verify Fabric UI on 9400 with Apple Mobile Client	Passed	

EWCJ176_2S_Reg_41	To Deploy Fabric configuration from webUI on 9500	To Verify Fabric UI on 9500	Passed	
EWCJ176_2S_Reg_42	To Deploy Fabric configuration from webUI on 9500 and Windows Client	To Verify Fabric UI on 9500 with Window Client	Passed	
EWCJ176_2S_Reg_43	To Deploy Fabric configuration from webUI on 9500 and Android Client	To Verify Fabric UI on 9500 with Android Client	Passed	
EWCJ176_2S_Reg_44	To Deploy Fabric configuration from webUI on 9500 and MAC Client	To Verify Fabric UI on 9500 with MAC Client	Passed	
EWCJ176_2S_Reg_45	To Deploy Fabric configuration from webUI on 9500 and Apple Mobile Client	To Verify Fabric UI on 9500 with Apple Mobile Client	Passed	

BSS Coloring on AX APs

Logical ID	Title	Description	Status	Defect ID
EWCJ176S_Reg_114	Configuring Automatic BSS colouring for 2.4 ghz AP radios	To Check whether automatic BSS colouring is applied or not in 2.4 ghz ap radio	Passed	
EWCJ176S_Reg_115	Configuring automatic BSS colour for 5ghz radio	To Check whether automatic BSS colouring is applied or not in 5 ghz ap radio	Passed	
EWCJ176S_Reg_116	Configuring auto BSS colour appearing 2.4 to 5 Ghz radio or vice versa	To verify whether different BSS colouring is occur while Changing the AP radios 2.4 to 5 viseversa	Passed	
EWCJ176S_Reg_117	Configuring Manual BSS colour configuration for 2.4/5 ghz radio	To Check whether Manual BSS colouring is applied or not in 2.4 ghz ap radio	Passed	
EWCJ176S_Reg_118	Verifying the static BSS colour assignment for the 5 ghz radio in Flex-connect mode	To Check whether Static BSS colouring is applied or not in 5 ghz ap radio	Passed	
EWCJ176S_Reg_119	Checking the manual BSS colouring while changing the AP radio from 2.4 ghz to 5 ghz	To verify whether different BSS colouring is occur while Changing the AP radios	Passed	
EWCJ176S_Reg_120	Checking the BSS colour details are retained after AP and Controller reload	To Check whether the BSS colour retained after AP & Controller reload	Passed	
EWCJ176S_Reg_121	Verifying BSS colouring with Intra client roaming by using 9115AP	To verify whether BSS colouring with client roaming between AP's or not	Passed	

EWCJ176S_Reg_122	Verifying BSS colouring with inter roaming client using different radio	To check whether BSS colouring is appearing or not , when different radio clients are roaming between controllers	Passed	
EWCJ176S_Reg_123	Verifying BSS colouring with inter roaming client using same radio	To check whether BSS colouring is appearing or not , when same radio clients are roaming between controllers	Passed	
EWCJ176S_Reg_124	Capturing the Windows client connectivity & BSS colouring using Wireshark	To check the window client connectivity & BSS colouring using Wireshark	Passed	
EWCJ176S_Reg_125	Capturing the Android client connectivity & BSS colouring using Wireshark	To check the Android client connectivity & BSS colouring using Wireshark	Passed	
EWCJ176S_Reg_126	Capturing the Mac OS client connectivity & BSS colouring using Wireshark	To check the Mac OS client connectivity & BSS colouring using Wireshark	Passed	
EWCJ176S_Reg_127	Changing 9115 AP mode from local to Flex connect & check the BSS colouring Configuration	To change the mode of AP from local mode to Flexconnect mode and check the BSS colouring configuration in 9115 Ap	Passed	
EWCJ176S_Reg_128	Changing 9115 AP mode from flex to local & check the BSS colouring Configuration	To change the mode of AP from flex mode to local mode and check the BSS colouring configuration in 9115 Ap	Failed	CSCvx98966

EoGRE Support for ME

Logical ID	Title	Description	Status	Defect ID
EWCJ176S_Reg_56	Creating EoGRE Tunnel Gateway.	To check whether the tunnel gateway is created or not.	Passed	
EWCJ176S_Reg_57	Creating EoGRE Tunnel Domain	To check whether the tunnel Domain is created or not.	Passed	
EWCJ176S_Reg_58	Configuring the Global Parameter for the EoGRE.	To check whether the global parameters are configured or not.	Passed	
EWCJ176S_Reg_59	Configuring the tunnel Profile.	To check whether the tunnel profile is created or not.	Passed	
EWCJ176S_Reg_60	Associate the WLAN to the Wireless policy profile.	To check whether the wlan is associated with the policy profile.	Passed	
EWCJ176S_Reg_61	Adding a policy tag and site tag to AP	To check whether the policy and site tag is added to an AP.	Passed	
EWCJ176S_Reg_62	Checking the client connectivity.	To check whether the client is connected or not	Passed	
EWCJ176S_Reg_63	Getting the EoGRE tunnel from PI	To check whether the tunnel is exported from PI or not	Passed	
EWCJ176S_Reg_64	Connect the iOS clients and check the connectivity.	To check whether the iOS clients get connected successfully.	Passed	
EWCJ176S_Reg_65	Connect the mac os clients and check the connectivity.	To check whether the mac os clients get connected successfully.	Passed	
EWCJ176S_Reg_66	Checking the traffic in the tunnel.	To check whether the traffic in the tunnel is managed or not.	Passed	

EWCJ176_2S_Reg_76	Creating EoGRE Tunnel Gateway.	To check whether the tunnel gateway is created or not.	Passed	
EWCJ176_2S_Reg_77	Creating EoGRE Tunnel Domain	To check whether the tunnel Domain is created or not.	Passed	
EWCJ176_2S_Reg_78	Configuring the Global Parameter for the EoGRE.	To check whether the global parameters are configured or not.	Passed	
EWCJ176_2S_Reg_79	Configuring the tunnel Profile.	To check whether the tunnel profile is created or not.	Passed	
EWCJ176_2S_Reg_80	Associate the WLAN to the Wireless policy profile.	To check whether the wlan is associated with the policy profile.	Passed	
EWCJ176_2S_Reg_81	Adding a policy tag and site tag to AP	To check whether the policy and site tag is added to an AP.	Passed	
EWCJ176_2S_Reg_82	Checking the client connectivity.	To check whether the client is connected or not	Passed	
EWCJ176_2S_Reg_83	Getting the EoGRE tunnel from PI	To check whether the tunnel is exported from PI or not	Passed	
EWCJ176_2S_Reg_84	Connect the ios clients and check the connectivity.	To check whether the ios clients get connected successfully.	Passed	
EWCJ176_2S_Reg_85	Connect the mac os clients and check the connectivity.	To check whether the mac os clients get connected successfully.	Passed	
EWCJ176_2S_Reg_86	Checking the traffic in the tunnel.	To check whether the traffic in the tunnel is managed or not.	Passed	

CMX Parity for eWLC ME

Logical ID	Title	Description	Status	Defect ID
EWCJ176S_Reg_129	Adding eWC-ME to CMX & CMX to DNAC	To Check Whether the eWLC-ME gets added to CMX & CMX added to DNAC successfully or not	Passed	
EWCJ176S_Reg_130	Connecting the IOS Client to the access point on the floor and check the details of the Client.	To connect a IOS Client to the access point on the floor and check if the details of the IOS Clients are shown correctly or not.	Passed	
EWCJ176S_Reg_131	Connecting the MacOS Client to the access point on the floor and check the details of the Client.	To connect a MacOS Client to the access point on the floor and check if the details of the MacOS Clients are shown correctly or not.	Passed	
EWCJ176S_Reg_132	Connecting the Android Client to the access point on the floor and check the details of the Client.	To connect a Android Client to the access point on the floor and check if the details of the IOS Clients are shown correctly or not.	Passed	
EWCJ176S_Reg_133	Connecting many Clients from different place and check the location of the Clients	To connect many Client from different place to the access points and check if the location of the Client are shown in CMX	Passed	
EWCJ176S_Reg_134	Connecting a 2.4 ghz Client to the access point which is placed in floor and checking the client details	To connect a 2.4 ghz Client to the access point on the floor and check if the details of the Clients are shown correctly or not.	Passed	

EWCJ176S_Reg_135	Connecting a 5 ghz Client to the access point which is placed in floor and checking the client details	To connect a 5 ghz Client to the access point on the floor and check if the details of the Clients are shown correctly or not.	Passed	
EWCJ176S_Reg_136	Connecting a Dual band Client to the access point which is placed in floor and checking the client details	To connect a Dual band Client to the access point on the floor and check if the details of the Clients are shown correctly or not.	Passed	
EWCJ176S_Reg_137	Verify the Disconnected client details in CMX	To check whether the client is disconnected or not in CMX	Passed	
EWCJ176S_Reg_138	Verifying the Intra client roaming in CMX	To verify whether the client is roaming between AP's or not	Passed	
EWCJ176S_Reg_139	Verifying the Inter client roaming in CMX	To verify whether the clients are roaming between controllers	Passed	
EWCJ176S_Reg_140	Verifying the Wired client details in CMX	To Check whether the Wired client details are showing or not in CMX	Passed	
EWCJ176S_Reg_141	Verifying the guest LAN client details in CMX	To Check whether the Guest LAN client details are showing or not in CMX	Passed	
EWCJ176S_Reg_142	Verifying MIMO client details using Wireshark	To check Whether all the clients getting same BW & data rate or not	Passed	

EWC Day0 Elimination

Logical ID	Title	Description	Status	Defect ID
EWCJ176S_Reg_143	Provisioning the eWLC_ME in day0 via PnP profile	Verify that user is able to Provisioned the eWLC_ME in day0 via PnP profile or not	Passed	
EWCJ176S_Reg_144	Manually adding single device Pnp details and Provisioning the 9115AX eWLC_ME in day0	Verify that user is able to Provisioned the eWLC_ME in day0 after adding Pnp Details manually	Passed	
EWCJ176S_Reg_145	Adding the device details in PnP with importing the .csv file in Bulk devices option	Verify that user is able to Provisioned the 1815eWLC_ME in day0 after adding Pnp Details with importing .csv file	Passed	
EWCJ176S_Reg_146	Checking the image version after Provisioning Ewlc_ME with PnP	Verifying the image version after Provisioning Ewlc_ME with PnP	Passed	
EWCJ176S_Reg_147	Checking the AP details after Provisioning Ewlc_ME with PnP	Verifying the AP details after Provisioning Ewlc_ME with PnP	Passed	
EWCJ176S_Reg_148	Checking WLANs broadcasting or not after provisioning	To verify whether WLANs are broadcasting or not after provisioning	Passed	
EWCJ176S_Reg_149	Connecting client to created WLAN and checking the client details	Verifying the client details after connecting WLAN	Passed	
EWCJ176S_Reg_150	Configuring wrong DNAC IP address in switch and trying for the provisioning	To verify whether user is able to Provisioned the eWLC_ME with providing wrong DNAC IP in Switch	Passed	

EWCJ176S_Reg_151	Configuring wrong details for PnP while claiming the device	To verify whether user is able to Provisioned the eWLC_ME with providing wrong PnP configuration in DNAC	Passed	
EWCJ176S_Reg_152	Checking the eWLC_ME after configuring factory reset with save config	Verifying whether user able to bring device to day0 or not with save config as yes	Passed	
EWCJ176_2S_Reg_161	Provisioning the eWLC_ME in day0 via PnP profile	Verify that user is able to Provisioned the eWLC_ME in day0 via PnP profile or not	Passed	
EWCJ176_2S_Reg_162	Manually adding single device Pnp details and Provisioning the 9115AX eWLC_ME in day0	Verify that user is able to Provisioned the eWLC_ME in day0 after adding Pnp Details manually	Passed	
EWCJ176_2S_Reg_163	Adding the device details in PnP with importing the .csv file in Bulk devices option	Verify that user is able to Provisioned the 1815eWLC_ME in day0 after adding Pnp Details with importing .csv file	Passed	
EWCJ176_2S_Reg_164	Checking the image version after Provisioning Ewlc_ME with PnP	Verifying the image version after Provisioning Ewlc_ME with PnP	Passed	
EWCJ176_2S_Reg_165	Checking the AP details after Provisioning Ewlc_ME with PnP	Verifying the AP details after Provisioning Ewlc_ME with PnP	Passed	
EWCJ176_2S_Reg_166	Checking WLANs broadcasting or not after provisioning	To verify whether WLANs are broadcasting or not after provisioning	Passed	
EWCJ176_2S_Reg_167	Connecting client to created WLAN and checking the client details	Verifying the client details after connecting WLAN	Passed	

EWCJ176_2S_Reg_168	Configuring wrong DNAC IP address in switch and trying for the provisioning	To verify whether user is able to Provisioned the eWLC_ME with providing wrong DNAC IP in Switch	Passed	
EWCJ176_2S_Reg_169	Configuring wrong details for PnP while claiming the device	To verify whether user is able to Provisioned the eWLC_ME with providing wrong PnP configuration in DNAC	Passed	
EWCJ176_2S_Reg_170	Checking the eWLC_ME after configuring factory reset with save config	Verifying whether user able to bring device to day0 or not with save config as yes	Passed	

Internal DHCP Server

Logical ID	Title	Description	Status	Defect ID
EWCJ176S_Reg_170	Mapping a Internal DHCP pool to WLAN and verifying Windows Client IP Address and vlan id	To verify whether a window client get Ip address and vlan id from a specified DHCP pool or not	Passed	
EWCJ176S_Reg_171	Mapping a Internal DHCP pool to WLAN and verifying Android Client IP Address and vlan id	To verify whether a Android client get Ip address and vlan id from a specified DHCP pool or not	Passed	
EWCJ176S_Reg_172	Mapping a Internal DHCP pool to WLAN and verifying MAC Client IP Address and vlan id	To verify whether a MAC Os client get Ip address and vlan id from a specified DHCP pool or not	Passed	
EWCJ176S_Reg_173	Mapping a Internal DHCP pool to WLAN and verifying iOS Client IP Address and vlan id	To verify whether a iOS client get Ip address and vlan id from a specified DHCP pool or not	Passed	
EWCJ176S_Reg_174	Checking lease period for connected Client through a DHCP pool	To verify whether DHCP release a particular IP address or not after a certain lease period for client	Passed	

200 Country Code

Logical ID	Title	Description	Status	Defect ID
EWCJ176S_Reg_236	Verifying by Configuring the country code in EWC GUI.	To Check whether the country code is Configured Properly or not in GUI	Passed	
EWCJ176S_Reg_237	Verifying the country code by connecting Mac OS clients.	To Check whether Mac OS clients are connected successfully after a change in the country code.	Passed	
EWCJ176S_Reg_238	Verifying by Configuring the Country code and upgrading the controller.	To Check whether the country code is Configured Properly after the upgradation process.	Passed	
EWCJ176S_Reg_239	Verifying by Configuring the Country code and downgrading the controller.	To Check whether the country code is Configured Properly after the downgradation process.	Passed	
EWCJ176S_Reg_240	Verifying the Configuration of the country code during day 0 Configuration.	To Check whether the country code is configured during day 0 Configuration.	Passed	
EWCJ176S_Reg_241	Verifying the country code by connecting Android clients.	To Check whether android clients are connected successfully after a change in the country code.	Passed	
EWCJ176S_Reg_242	Verifying whether the country code is configured without disabling the radio's	To verify whether the country code is configured without disabling the radio's	Passed	
EWCJ176S_Reg_243	Verifying the country code by connecting Windows clients.	To Check whether Windows clients are connected successfully after a change in the country code.	Passed	

802-1x support with EAP-TLS and EAP-PEAP

Logical ID	Title	Description	Status	Defect ID
EWCJ176S_Reg_175	Enabling dot1x auth for AP and ioining AP to WLC	To check whether AP joins WLC or not after dot1x authentication from Switch/ISE	Passed	
EWCJ176S_Reg_176	Associating Windows clients to AP joined via Dot1x authentication	To check whether Windows clients associated successfully or not once AP joined via dot1x authentication from Switch/ISE	Passed	
EWCJ176S_Reg_177	Joining COS AP to WLC through Dot1x+PEAP authentication	To check whether COS AP joins WLC or not after dot1x authentication from Switch/ISE via EAP method PEAP	Passed	
EWCJ176S_Reg_178	Joining iOS AP to WLC through Dot1x+EAP TLS authentication	To check whether iOS AP joins WLC or not after dot1x authentication from Switch/ISE via EAP method TLS	Passed	
EWCJ176S_Reg_179	Trying to join AP's through Dot1x authentication with LSC provisioning	To check whether AP's joins WLC or not through LSC provisioning & dot1x authentication	Passed	
EWCJ176S_Reg_180	Providing invalid credentials for AP authentication and checking the status of AP in console	To check whether AP throws error message or not when invalid credentials provided during dot1x authentication	Passed	
EWCJ176S_Reg_181	Disabling dot1x support in Switch and trying to associate AP via Dot1x authentication to WLC	To check whether AP joins WLC or not even dot1x is disabled in switch	Passed	

EWCJ176S_Reg_182	Enabling dot1x auth for AP in 3850 Switch	Configuring the 3850 Switch for Dot1x authentication by mapping the identity profiles to a port.	Passed	
EWCJ176S_Reg_183	Checking the configuration of 802.1x authentication parameters after export/import the config file	To check whether 802.1x auth parameters restores or not after export/import the config file in WLC UI via TFTP	Passed	
EWCJ176S_Reg_184	Associating Mac OS clients to AP joined via Dot1x authentication	To check whether Mac OS clients associated successfully or not once AP joined via dot1x authentication from Switch/ISE	Passed	
EWCJ176S_Reg_185	Associating Android clients to AP joined via Dot1x authentication	To check whether Android clients associated successfully or not once AP joined via dot1x authentication from Switch/ISE	Passed	
EWCJ176S_Reg_186	Associating iOS clients to AP joined via Dot1x authentication	To check whether iOS clients associated successfully or not once AP joined via dot1x authentication from Switch/ISE	Passed	
EWCJ176S_Reg_187	Trying to configure of 802.1x authentication parameters via Read-only User	To check whether Read only user can be able to configure or not the 802.1x auth parameters in WLC UI	Passed	
EWCJ176_2S_Reg_190	Enabling dot1x auth for AP and ioining AP to WLC	To check whether AP joins WLC or not after dot1x authentication from Switch/ISE	Passed	

EWCJ176_2S_Reg_191	Associating Windows clients to AP joined via Dot1x authentication	To check whether Windows clients associated successfully or not once AP joined via dot1x authentication from Switch/ISE	Passed	
EWCJ176_2S_Reg_192	Joining COS AP to WLC through Dot1x+PEAP authentication	To check whether COS AP joins WLC or not after dot1x authentication from Switch/ISE via EAP method PEAP	Passed	
EWCJ176_2S_Reg_193	Joining iOS AP to WLC through Dot1x+EAP TLS authentication	To check whether iOS AP joins WLC or not after dot1x authentication from Switch/ISE via EAP method TLS	Passed	
EWCJ176_2S_Reg_194	Trying to join AP's through Dot1x authentication with LSC provisioning	To check whether AP's joins WLC or not through LSC provisioning & dot1x authentication	Passed	
EWCJ176_2S_Reg_195	Providing invalid credentials for AP authentication and checking the status of AP in console	To check whether AP throws error message or not when invalid credentials provided during dot1x authentication	Passed	
EWCJ176_2S_Reg_196	Disabling dot1x support in Switch and trying to associate AP via Dot1x authentication to WLC	To check whether AP joins WLC or not even dot1x is disabled in switch	Passed	
EWCJ176_2S_Reg_197	Enabling dot1x auth for AP in 3850 Switch	Configuring the 3850 Switch for Dot1x authentication by mapping the identity profiles to a port.	Passed	

EWCJ176_2S_Reg_198	Checking the configuration of 802.1x authentication parameters after export/import the config file	To check whether 802.1x auth parameters restores or not after export/import the config file in WLC UI via TFTP	Passed	
EWCJ176_2S_Reg_199	Associating Mac OS clients to AP joined via Dot1x authentication	To check whether Mac OS clients associated successfully or not once AP joined via dot1x authentication from Switch/ISE	Passed	
EWCJ176_2S_Reg_200	Associating Android clients to AP joined via Dot1x authentication	To check whether Android clients associated successfully or not once AP joined via dot1x authentication from Switch/ISE	Passed	
EWCJ176_2S_Reg_201	Associating iOS clients to AP joined via Dot1x authentication	To check whether iOS clients associated successfully or not once AP joined via dot1x authentication from Switch/ISE	Passed	
EWCJ176_2S_Reg_202	Trying to configure of 802.1x authentication parameters via Read-only User	To check whether Read only user can be able to configure or not the 802.1x auth parameters in WLC UI	Passed	

Optimized Roaming

Logical ID	Title	Description	Status	Defect ID
EWCJ176S_Reg_188	Configuring optimized roaming with 2.4 GHz band and roam Android client	To verify that optimized roaming with 2.4 GHz band gets configured or not and check association of Android client	Passed	
EWCJ176S_Reg_189	Configuring optimized roaming with 2.4 GHz band ,1 MBPS Thresholds and roam Android client	To verify that optimized roaming with 2.4 GHz band,1 MBPS Thresholds gets configured or not and check association of Android client	Passed	
EWCJ176S_Reg_190	Configuring optimized roaming with 5 GHz band and roam Android client	To verify that optimized roaming with 5 GHz band and check association of Android client	Failed	CSCvx34344
EWCJ176S_Reg_191	Configuring optimized roaming with 5 GHz band , 6 MBPS Threshold and roam Android client	To verify that optimized roaming with 5 GHz band , 6 MBPS Threshold configured and check association of Android client	Passed	
EWCJ176S_Reg_192	Configuring optimized roaming with 2.4 GHz band ,5.5 MBPS Threshold and roam iOS client	To verify that optimized roaming with 2.4 GHz band ,5.5 MBPS Threshold configured successfully and check association of iOS client	Passed	

EWCJ176S_Reg_193	Configuring optimized roaming with 2.4 GHz band ,9 MBPS Threshold and roam iOS client	To verify that optimized roaming with 2.4 GHz band ,9 MBPS Threshold configured and check association of iOS client	Passed	
EWCJ176S_Reg_194	Configuring optimized roaming with 5 GHz band and roam iOS client	To verify that optimized roaming with 5 GHz band &customized interval(40 Sec) configured successfully and check association of iOS client	Passed	
EWCJ176S_Reg_195	Configuring optimized roaming with 5 GHz band , 12 MBPS Threshold and roam iOS client	To verify that optimized roaming with 5 GHz band , 12 MBPS Threshold configured successfully and check association of iOS client	Failed	CSCvx38809
EWCJ176S_Reg_196	Moving the Android client from AP after enable optimized roaming	To verify that client got disassociated when signal is poor while moving from AP	Passed	
EWCJ176S_Reg_197	Moving the iOS client from AP after disabling the optimized roaming	To verify that client wouldn't disassociated when signal is poor while moving from AP	Failed	CSCvx69538
EWCJ176S_Reg_198	Moving the Android client from AP after enable optimized roaming in ME with interference availability	To verify that client got disassociated when signal is poor while moving from 2700 AP with interference availability	Passed	
EWCJ176S_Reg_199	Connect iOS client from where SSID signal is week	To verify that iOS client connecting or not from where SSID signal is week	Passed	CSCvy05454

EWCJ176S_Reg_200	Restarting the ME eWC after optimized roaming configuration	To verify that optimization roaming configuration remain same after reboot	Passed	
EWCJ176S_Reg_201	Importing/exporting configuration file after optimized roaming configuring	To verify that optimization roaming configuration remain same after import and export configuration file	Passed	
EWCJ176_2S_Reg_221	Configuring optimized roaming with 2.4 GHz band and roam Android client	To verify that optimized roaming with 2.4 GHz band gets configured or not and check association of Android client	Passed	
EWCJ176_2S_Reg_222	Configuring optimized roaming with 2.4 GHz band ,1 MBPS Thresholds and roam Android client	To verify that optimized roaming with 2.4 GHz band,1 MBPS Thresholds gets configured or not and check association of Android client	Passed	
EWCJ176_2S_Reg_223	Configuring optimized roaming with 5 GHz band and roam Android client	To verify that optimized roaming with 5 GHz band and check association of Android client	Failed	CSCvy81617
EWCJ176_2S_Reg_224	Configuring optimized roaming with 5 GHz band , 6 MBPS Threshold and roam Android client	To verify that optimized roaming with 5 GHz band , 6 MBPS Threshold configured and check association of Android client	Passed	

EWCJ176_2S_Reg_225	Configuring optimized roaming with 2.4 GHz band ,5.5 MBPS Threshold and roam iOS client	To verify that optimized roaming with 2.4 GHz band ,5.5 MBPS Threshold configured successfully and check association of iOS client	Passed	
EWCJ176_2S_Reg_226	Configuring optimized roaming with 2.4 GHz band ,9 MBPS Threshold and roam iOS client	To verify that optimized roaming with 2.4 GHz band ,9 MBPS Threshold configured and check association of iOS client	Passed	
EWCJ176_2S_Reg_227	Configuring optimized roaming with 5 GHz band and roam iOS client	To verify that optimized roaming with 5 GHz band &customized interval(40 Sec) configured successfully and check association of iOS client	Passed	
EWCJ176_2S_Reg_228	Configuring optimized roaming with 5 GHz band , 12 MBPS Threshold and roam iOS client	To verify that optimized roaming with 5 GHz band , 12 MBPS Threshold configured successfully and check association of iOS client	Passed	
EWCJ176_2S_Reg_229	Moving the Android client from AP after enable optimized roaming	To verify that client got disassociated when signal is poor while moving from AP	Passed	
EWCJ176_2S_Reg_230	Moving the iOS client from AP after disabling the optimized roaming	To verify that client wouldn't disassociated when signal is poor while moving from AP	Passed	

EWCJ176_2S_Reg_231	Moving the Android client from AP after enable optimized roaming in ME with interference availability	To verify that client got disassociated when signal is poor while moving from 2700 AP with interference availability	Passed	
EWCJ176_2S_Reg_232	Connect iOS client from where SSID signal is week	To verify that iOS client connecting or not from where SSID signal is week	Passed	
EWCJ176_2S_Reg_233	Restarting the ME eWC after optimized roaming configuration	To verify that optimization roaming configuration remain same after reboot	Passed	
EWCJ176_2S_Reg_234	Importing/exporting configuration file after optimized roaming configuring	To verify that optimization roaming configuration remain same after import and export configuration file	Passed	

mDNS gateway support for flex/Mobility Express

Logical ID	Title	Description	Status	Defect ID
EWCJ176S_Reg_218	Checking the mDNS Ap with Flex connect group configuration.	To check whether mDNS AP with Flex connect group configurations are able to configure or not.	Passed	
EWCJ176S_Reg_219	Creating mDNS profile by adding required services	To verify whether mDNS profile is created with required services	Passed	
EWCJ176S_Reg_220	Checking mDNS gateway are applying to Apple Tv clients after enabling the mdns AP to 9115AP	To check whether the mdns gateway applying to Apple Tv clients or not after enabling the mDNS-ap to 9115AP.	Passed	
EWCJ176S_Reg_221	Checking mDNS gateway are applying to Mac OS clients after enabling the mdns AP to 9120AP	To check whether the mdns gateway applying to Mac OS and Apple Tv clients after enabling the mDNS-ap to 9120AP	Passed	
EWCJ176S_Reg_222	Checking mDNS gateway are applied to Apple TV and authentication server as radius in ME	To verify mDNS gateway are applied to Apple TV and authentication server as radius in ME.	Passed	
EWCJ176S_Reg_223	Checking mDNS gateway are applying to Mac OS and Apple Tv clients after enabling the mdns AP to 4800AP	To check whether the mdns gateway applying to Mac OS and Apple Tv clients or not after enabling the mDNS-ap to 4800AP.	Passed	

EWCJ176S_Reg_224	Verifying the mDNS gateway configurations after changing the AP mode to monitor from flex	To check whether mDNS gateway configurations after changing the AP mode to Monitor from flex	Passed	
EWCJ176S_Reg_225	Checking mDNS gateway are applying to Apple iPad and Apple Chromecast clients with Static WEP security after enabling the mdns AP to 9130/9115/ 4800/9120/ 3700AP's	To check whether the mdns gateway are applying to Apple iPad and Apple Chromecast clients with Static WEP security or not after enabling the mDNS-ap to9130/9115/ 4800/9120/ 3700AP's.	Passed	
EWCJ176S_Reg_226	Checking mDNS gateway are applied to MAC OS with wlan open security	Verifying mDNS gateway are applied to Mac OS with open ssid	Passed	
EWCJ176S_Reg_227	Checking mDNS gateway are applied to MacOS and IOS with wlan WPA2 personal security	Verifying mDNS gateway are applied to MacOS and IOS with WPA2 personal security	Passed	
EWCJ176S_Reg_228	Checking mDNS gateway are applied to MacOS and IOS with wlan WPA3-SAE security	To Check mDNS gateway are applied to MacOS and IOS with WPA3-SAE security	Passed	
EWCJ176S_Reg_229	Checking mDNS gateway are applied to Apple Devices with Fast transition enabled	To Check mDNS gateway are applied to Apple Devices with fast transition enabled	Passed	
EWCJ176S_Reg_230	Performing client communication between two clients connected two different vlan	To Check whether client communicate between two clients connected to different vlan	Passed	
EWCJ176S_Reg_231	Performing roaming operation when mDNS is applied	To Check the roaming operation when mDNS is applied	Passed	

EWCJ176S_Reg_232	Checking mDNS config after exporting config file	To check whether the mDNS config is same after exporting config file	Passed	
EWCJ176S_Reg_233	Checking mDNS gateway are applied to IOS with wlan Static WEP security	To verify whether mDNS gateway are applied to IOS with Static WEP SSID	Passed	
EWCJ176S_Reg_234	Verifying the mDNS configuration in DNAC	To Verify the mDNS gateway configuration in DNAC	Passed	
EWCJ176S_Reg_235	Verifying mDNS configuration Via EWC CLI	To verify the mDNS configuration through EWC CLI	Passed	
EWCJ176_2S_Reg_251	Checking the mDNS Ap with Flex connect group configuration.	To check whether mDNS AP with Flex connect group configurations are able to configure or not.	Passed	
EWCJ176_2S_Reg_252	Creating mDNS profile by adding required services	To verify whether mDNS profile is created with required services	Passed	
EWCJ176_2S_Reg_253	Checking mDNS gateway are applying to Apple Tv clients after enabling the mdns AP to 9115AP	To check whether the mdns gateway applying to Apple Tv clients or not after enabling the mDNS-ap to 9115AP.	Passed	
EWCJ176_2S_Reg_254	Checking mDNS gateway are applying to Mac OS clients after enabling the mdns AP to 9120AP	To check whether the mdns gateway applying to Mac OS and Apple Tv clients after enabling the mDNS-ap to 9120AP	Passed	
EWCJ176_2S_Reg_255	Checking mDNS gateway are applied to Apple TV and authentication server as radius in ME	To verify mDNS gateway are applied to AppleTV and authentication server as radius in ME.	Passed	

EWCJ176_2S_Reg_256	Checking mDNS gateway are applying to Mac OS and Apple Tv clients after enabling the mdns AP to 4800AP	To check whether the mdns gateway applying to Mac OS and Apple Tv clients or not after enabling the mDNS-ap to 4800AP.	Passed	
EWCJ176_2S_Reg_257	Verifying the mDNS gateway configurations after changing the AP mode to monitor from flex	To check whether mDNS gateway configurations after changing the AP mode to Monitor from flex	Passed	
EWCJ176_2S_Reg_258	Checking mDNS gateway are applying to Apple iPad and Apple Chromecast clients with Static WEP security after enabling the mdns AP to 9130/9115/4800/ 9120/3700AP's	To check whether the mdns gateway are applying to Apple iPad and Apple Chromecast clients with Static WEP security or not after enabling the mDNS-ap to9130/9115/ 4800/9120/3700AP's.	Passed	
EWCJ176_2S_Reg_259	Checking mDNS gateway are applied to MAC OS with wlan open security	Verifying mDNS gateway are applied to Mac OS with open ssid	Passed	
EWCJ176_2S_Reg_260	Checking mDNS gateway are applied to MacOS and IOS with wlan WPA2 personal security	Verifying mDNS gateway are applied to MacOS and IOS with WPA2 personal security	Passed	
EWCJ176_2S_Reg_261	Checking mDNS gateway are applied to MacOS and IOS with wlan WPA3-SAE security	To Check mDNS gateway are applied to MacOS and IOS with WPA3-SAE security	Passed	
EWCJ176_2S_Reg_262	Checking mDNS gateway are applied to Apple Devices with Fast transition enabled	To Check mDNS gateway are applied to Apple Devices with fast transition enabled	Passed	

EWCJ176_2S_Reg_263	Performing client communication between two clients connected two different vlan	To Check whether client communicate between two clients connected to different vlan	Passed	
EWCJ176_2S_Reg_264	Performing roaming operation when mDNS is applied	To Check the roaming operation when mDNS is applied	Passed	
EWCJ176_2S_Reg_265	Checking mDNS config after exporting config file	To check whether the mDNS config is same after exporting config file	Passed	
EWCJ176_2S_Reg_266	Checking mDNS gateway are applied to IOS with wlan Static WEP security	To verify whether mDNS gateway are applied to IOS with Static WEP SSID	Passed	
EWCJ176_2S_Reg_267	Verifying the mDNS configuration in DNAC	To Verify the mDNS gateway configuration in DNAC	Passed	
EWCJ176_2S_Reg_268	Verifying mDNS configuration Via EWC CLI	To verify the mDNS configuration through EWC CLI	Passed	

Explicit Warning for Configuration -Triggered Downtime

Logical ID	Title	Description	Status	Defect ID
EWCJ176S_Reg_244	Verifying the warning message after changing AP/RF/Site tags	To verify the warning message after changing AP/RF / site Tag	Passed	
EWCJ176S_Reg_245	Checking the warning message for after changing the AP tag in Flex mode AP	To check the warning message for changing Ap tag in flex mode AP	Passed	
EWCJ176S_Reg_246	Validating the warning message for after changing the RF tag in flex mode AP	To Validate the warning message for changing RF tag in flex mode AP	Passed	
EWCJ176S_Reg_247	Verifying the warning message for after changing the Site tag in Flex mode AP	To Verify the warning message for changing Site tag in flex mode AP	Passed	
EWCJ176S_Reg_248	Verifying the warning message for after changing the AP tag in Local mode AP	To Verify the warning message for changing Ap tag in Local mode AP	Passed	
EWCJ176S_Reg_249	Verifying the warning message for after changing the RF tag in Local mode AP	To Verify the warning message for changing RF tag in Local mode AP	Passed	
EWCJ176S_Reg_250	Verifying the warning message for after changing the Site tag in Local mode AP	To Verify the warning message for changing Site tag in local mode AP	Passed	
EWCJ176S_Reg_251	Verifying the warning message by editing the policy Tag in WLAN	To verify whether the warning message showing or not after editing Policy Tag in WLAN	Passed	

EWCJ176S_Reg_252	Checking the Warning message for editing the policy profile	To check the warning message for editing the Policy profile	Passed	
EWCJ176S_Reg_253	Checking the Warning message after AP reboot	To verify the warning message for after AP reboot	Passed	
EWCJ176S_Reg_254	Checking warning message after AP radio change	To check whether the warning message showing or not after changing the AP radio	Passed	
EWCJ176S_Reg_255	Verifying the warning message for different AP models	To Verify the warning message for different AP models	Passed	
EWCJ176S_Reg_256	Validating the warning message after disjoin the AP	To validate the warning message for after Ap disjoin	Passed	
EWCJ176S_Reg_257	Verifying the warning message after deleting the client	To verify the warning message for deleted client	Passed	
EWCJ176S_Reg_258	Verifying the warning message after 2.4/5 ghz radio down	To verify the warning message after 2.4/5 ghz radio down	Passed	
EWCJ176S_Reg_259	Verifying the warning message by changing the AP ip Address	To validate the warning message by changing the AP ip Address	Passed	
EWCJ176S_Reg_260	Validating the warning message for Virtual EWLC	To validate the warning message for vEWLC	Passed	
EWCJ176S_Reg_261	Checking the warning message after deleting the AP tag	To validate the warning message after deleting the AP tag	Passed	
EWCJ176S_Reg_262	Checking the warning message after deleting the RF tag	To validate the warning message after deleting the RF tag	Passed	
EWCJ176S_Reg_263	Checking the warning message after deleting the Site tag	To validate the warning message after deleting the Site tag	Passed	

EWCJ176S_Reg_264	monitoring the warning message after changing AP tag Via CLI	To check the warning message for changing Ap tag via CLI	Passed	
EWCJ176S_Reg_265	monitoring the warning message after changing RF tag Via CLI	To check the warning message for changing RF tag via CLI	Passed	
EWCJ176S_Reg_266	monitoring the warning message after changing site tag Via CLI	To check the warning message for changing Site tag via CLI	Passed	
EWCJ176S_Reg_267	monitoring the warning message after AP provisioning from DNAC	To check the warning message after AP provisioning from DNAC	Passed	

Active Config Visualization

Logical ID	Title	Description	Status	Defect ID
EWCJ176S_Reg_276	verify the virtual config in EWC 9115	To verify the virtual config in EWC 9115	Passed	
EWCJ176S_Reg_277	verify the virtual config in EWC 9117	To verify the virtual config in EWC 9117	Passed	
EWCJ176S_Reg_278	verify the virtual config in EWC 9120	To verify the virtual config in EWC 9120	Passed	
EWCJ176S_Reg_279	verify the virtual config in EWC 9130	To verify the virtual config in EWC 9130	Passed	

Copy of webauth tar bundle in EWC HA setup

Logical ID	Title	Description	Status	Defect ID
EWCJ176S_Reg_280	Download WebAuth Bundle with TFTP option	To Download WebAuth Bundle with TFTP option	Passed	
EWCJ176S_Reg_281	Download WebAuth Bundle with FTP option	To Download WebAuth Bundle with FTP option	Passed	
EWCJ176S_Reg_282	Download WebAuth Bundle with SFTP option	To Download WebAuth Bundle with SFTP option	Passed	
EWCJ176S_Reg_283	Download WebAuth Bundle with HTTP option	To Download WebAuth Bundle with HTTP option	Passed	
EWCJ176S_Reg_284	Verify Pop-up/Alert when space is low FTP	To Verify Pop-up/Alert when space is low FTP	Passed	
EWCJ176S_Reg_285	Verify Pop-up/Alert when space is low SFTP	To Verify Pop-up/Alert when space is low SFTP	Passed	
EWCJ176S_Reg_286	Verify Pop-up/Alert when space is low TFTP	To Verify Pop-up/Alert when space is low TFTP	Passed	
EWCJ176S_Reg_287	Verify tar file should have been copied to both boot flash and stby-bootflash in EWC 9115	To Verify tar file should have been copied to both boot flash and stby-bootflash in EWC 9115	Passed	
EWCJ176S_Reg_288	Verify tar file should have been copied to both boot flash and stby-bootflash in EWC 9117	To Verify tar file should have been copied to both boot flash and stby-bootflash in EWC 9117	Passed	
EWCJ176S_Reg_289	Verify tar file should have been copied to both boot flash and stby-bootflash in EWC 9120	To Verify tar file should have been copied to both boot flash and stby-bootflash in EWC 9120	Passed	

EWCJ176S_Reg_290	Verify tar file should have been copied to both boot flash and stby-bootflash in EWC 9130	To Verify tar file should have been copied to both boot flash and stby-bootflash in EWC 9130	Passed	

Ethernet VLAN tag on AP

Logical ID	Title	Description	Status	Defect ID
EWCJ176S_Reg_312	Providing the VLAN tag to the 9115 AP from eWC CLI.	To Verify the VLAN tag status of the 9115 AP after reboot and join back to the EWC.	Passed	
EWCJ176S_Reg_313	Unassign the VLAN tag to the 9115 AP from EWC CLI.	To Verify the VLAN tag status of the 9115 AP after reboot and join back to the EWC.	Passed	
EWCJ176S_Reg_314	Providing the VLAN tag to the 9120 AP from EWC CLI.	To Verify the VLAN tag status of the 9120 AP after reboot and join back to the EWC.	Passed	
EWCJ176S_Reg_315	Unassign the VLAN tag to the 9120 AP from EWC CLI.	To Verify the VLAN tag status of the 9120 AP after reboot and join back to the EWC.	Passed	
EWCJ176S_Reg_316	Providing the VLAN tag to the 9130 AP from EWC CLI.	To Verify the VLAN tag status of the 9130 AP after reboot and join back to the EWC.	Passed	
EWCJ176S_Reg_317	Unassign the VLAN tag to the 9130 AP from EWC CLI.	To Verify the VLAN tag status of the 9130 AP after reboot and join back to the EWC.	Passed	
EWCJ176S_Reg_318	Providing the VLAN tag to the 4800 AP from EWC CLI.	To Verify the VLAN tag status of the 4800 AP after reboot and join back to the EWC.	Passed	
EWCJ176S_Reg_319	Unassign the VLAN tag to the 4800 AP from EWC CLI.	To Verify the VLAN tag status of the 4800 AP after reboot and join back to the EWC.	Passed	

EWCJ176S_Reg_320	Check the VLAN tag is overriding or not via CLI	To verify whether the VLAN tag is overriding or not after assigning VLAN Tag to the particular Ap	Passed	
EWCJ176S_Reg_321	Check the VLAN tag is overriding or not via GUI	To verify whether the VLAN tag is overriding or not after assigning to new VLAN tag to particular Ap	Passed	
EWCJ176S_Reg_322	Checking the VLAN Tag after DCA Mode change	To check the VLAN tag after changing DCA mode	Passed	
EWCJ176S_Reg_323	Checking the VLAN Tag after changing Radio band	To check the VLAN tag after changing radio band	Passed	
EWCJ176S_Reg_324	Providing the VLAN tag to the 9115/9120/9130 AP's from EWC CLI and connect the Android Client.	To Verify the VLAN tag status of the 9115/9120/9130 AP's after reboot and join back to the EWC and Verify the Android client connectivity.	Passed	
EWCJ176S_Reg_325	Providing the VLAN tag to the 9115/9120/9130 AP's from EWC CLI and connect the Windows Client.	To Verify the VLAN tag status of the 9115/9120/9130 AP's after reboot and join back to the EWC and Verify the Windows client connectivity.	Passed	
EWCJ176S_Reg_326	Providing the VLAN tag to the 9115/9120/9130 AP's from EWC CLI and connect the IOS Client.	To Verify the VLAN tag status of the 9115/9120/9130 AP's after reboot and join back to the EWC and Verify the IOS client connectivity.	Passed	

EWCJ176S_Reg_327	Providing the VLAN tag to the 9115/9120/9130 AP's from EWC CLI and connect the AnyConnect Client.	To Verify the VLAN tag status of the 9115/9120/9130 AP's after reboot and join back to the EWC and Verify the AnyConnect client connectivity.	Passed	
EWCJ176S_Reg_328	Providing the VLAN tag to the Group of AP's from EWC CLI.	To Verify the VLAN tag status of the Group of AP's after reboot and join back to the EWC.	Passed	
EWCJ176S_Reg_329	Unassign the VLAN tag to the Group of AP's from EWC CLI.	To Verify the VLAN tag status of the Group of AP's after reboot and join back to the EWC.	Passed	
EWCJ176S_Reg_330	Providing the VLAN tag to the Catalyst AP's from EWC CLI and change the mode of the AP to Monitor from local.	To Verify the VLAN tag status of the Catalyst AP's after changing the mode of the AP to monitor from local.	Passed	
EWCJ176S_Reg_331	Providing the VLAN tag to the Catalyst AP from EWC CLI and change the mode of the AP to flex from Local.	To Verify the VLAN tag status of the Catalyst AP's after changing the mode of the AP to flex from local.	Passed	
EWCJ176S_Reg_332	Providing the VLAN tag to the 4800 AP from EWC CLI and change the mode of the AP to sniffer from Local.	To Verify the VLAN tag status of the 4800 AP after changing the mode of the AP to sniffer from local.	Passed	
EWCJ176_2S_Reg_290	Providing the VLAN tag to the 9115 AP from eWC CLI.	To Verify the VLAN tag status of the 9115 AP after reboot and join back to the EWC.	Passed	

EWCJ176_2S_Reg_291	Unassign the VLAN tag to the 9115 AP from EWC CLI.	To Verify the VLAN tag status of the 9115 AP after reboot and join back to the EWC.	Passed	
EWCJ176_2S_Reg_292	Providing the VLAN tag to the 9120 AP from EWC CLI.	To Verify the VLAN tag status of the 9120 AP after reboot and join back to the EWC.	Passed	
EWCJ176_2S_Reg_293	Unassign the VLAN tag to the 9120 AP from EWC CLI.	To Verify the VLAN tag status of the 9120 AP after reboot and join back to the EWC.	Passed	
EWCJ176_2S_Reg_294	Providing the VLAN tag to the 9130 AP from EWC CLI.	To Verify the VLAN tag status of the 9130 AP after reboot and join back to the EWC.	Passed	
EWCJ176_2S_Reg_295	Unassign the VLAN tag to the 9130 AP from EWC CLI.	To Verify the VLAN tag status of the 9130 AP after reboot and join back to the EWC.	Passed	
EWCJ176_2S_Reg_296	Providing the VLAN tag to the 4800 AP from EWC CLI.	To Verify the VLAN tag status of the 4800 AP after reboot and join back to the EWC.	Passed	
EWCJ176_2S_Reg_297	Unassign the VLAN tag to the 4800 AP from EWC CLI.	To Verify the VLAN tag status of the 4800 AP after reboot and join back to the EWC.	Passed	
EWCJ176_2S_Reg_298	Check the VLAN tag is overriding or not via CLI	To verify whether the VLAN tag is overriding or not after assigning VLAN Tag to the particular Ap	Passed	
EWCJ176_2S_Reg_299	Check the VLAN tag is overriding or not via GUI	To verify whether the VLAN tag is overriding or not after assigning to new VLAN tag to particular Ap	Passed	

EWCJ176_2S_Reg_300	Checking the VLAN Tag after DCA Mode change	To check the VLAN tag after changing DCA mode	Passed	
EWCJ176_2S_Reg_301	Checking the VLAN Tag after changing Radio band	To check the VLAN tag after changing radio band	Passed	
EWCJ176_2S_Reg_302	Providing the VLAN tag to the 9115/9120/9130 AP's from EWC CLI and connect the Android Client.	To Verify the VLAN tag status of the 9115/9120/9130 AP's after reboot and join back to the EWC and Verify the Android client connectivity.	Passed	
EWCJ176_2S_Reg_303	Providing the VLAN tag to the 9115/9120/9130 AP's from EWC CLI and connect the Windows Client.	To Verify the VLAN tag status of the 9115/9120/9130 AP's after reboot and join back to the EWC and Verify the Windows client connectivity.	Passed	
EWCJ176_2S_Reg_304	Providing the VLAN tag to the 9115/9120/9130 AP's from EWC CLI and connect the IOS Client.	To Verify the VLAN tag status of the 9115/9120/9130 AP's after reboot and join back to the EWC and Verify the IOS client connectivity.	Passed	
EWCJ176_2S_Reg_305	Providing the VLAN tag to the 9115/9120/9130 AP's from EWC CLI and connect the AnyConnect Client.	To Verify the VLAN tag status of the 9115/9120/9130 AP's after reboot and join back to the EWC and Verify the AnyConnect client connectivity.	Passed	
EWCJ176_2S_Reg_306	Providing the VLAN tag to the Group of AP's from EWC CLI.	To Verify the VLAN tag status of the Group of AP's after reboot and join back to the EWC.	Passed	

EWCJ176_2S_Reg_307	Unassign the VLAN tag to the Group of AP's from EWC CLI.	To Verify the VLAN tag status of the Group of AP's after reboot and join back to the EWC.	Passed	
EWCJ176_2S_Reg_308	Providing the VLAN tag to the Catalyst AP's from EWC CLI and change the mode of the AP to Monitor from local.	To Verify the VLAN tag status of the Catalyst AP's after changing the mode of the AP to monitor from local.	Passed	
EWCJ176_2S_Reg_309	Providing the VLAN tag to the Catalyst AP from EWC CLI and change the mode of the AP to flex from Local.	To Verify the VLAN tag status of the Catalyst AP's after changing the mode of the AP to flex from local.	Passed	
EWCJ176_2S_Reg_310	Providing the VLAN tag to the 4800 AP from EWC CLI and change the mode of the AP to sniffer from Local.	To Verify the VLAN tag status of the 4800 AP after changing the mode of the AP to sniffer from local.	Passed	

Mac filtering (for L2 security)

Logical ID	Title	Description	Status	Defect ID
EWCJ176S_Reg_162	Adding Windows 10 Client mac address in eWC and checking the connection of Clients	To add the windows Client mac address in mac filtering in eWC and checking whether Clients gets associated or not successfully in	Passed	
EWCJ176S_Reg_163	Uploading the empty CSV file in eWC UI	To check whether an blank CSV file could be uploaded in eWC UI	Passed	
EWCJ176S_Reg_164	Importing the .CSV file with modifications in eWC	To check whether .CSV file gets imported or not after importing the updated file with some changes in it	Passed	
EWCJ176S_Reg_165	Connecting the Client with wlan security mac filtering + WPA personal	To Connect the Client with wlan security mac filtering + WPA personal	Passed	
EWCJ176S_Reg_166	Connecting the Client with wlan security mac filtering + WPA enterprise	To Connect the Client with wlan security mac filtering + WPA enterprise	Passed	
EWCJ176S_Reg_167	Connecting the Client with Wlan Security Type as WPA Enterprise enabling MAC Filtering option Choosing Authentication Server as External Radius and RADIUS Compatibility as other	To Connect the Client with MAC Filtering using WPA Enterprise as security type choosing Authentication Server as External Radius and RADIUS Compatibility as other	Passed	

EWCJ176S_Reg_168	Connecting the client after client identity account expired in ISE	To Connect the Client after client identity account expired in ISE	Passed	
EWCJ176S_Reg_169	Connecting the Client and then moving it to block using MAC address	To Connect the client and then blocking it using the MAC address	Passed	

11ax BSS Coloring(OBSS PD) on 9105/9115/9120 APs

Logical ID	Title	Description	Status	Defect ID
EWLCJ176_2S_Reg_392	Enable Global OBSS PD for 5ghz band	To verify whether the OBBSS PD enable or not for 5 GHz band	Passed	
EWLCJ176_2S_Reg_393	Disable Global OBSS PD for 5ghz band	To Check whether the OBBSS PD disable or not for 5 GHz	Passed	
EWLCJ176_2S_Reg_394	Enable Global OBSS PD for 2.4 ghz band	To verify whether the OBBSS PD enable or not for 2.4 Ghz band	Passed	
EWLCJ176_2S_Reg_395	Disable Global OBSS PD for 2.4 ghz band	To Check whether the OBBSS PD disable or not for 2.4 GHz	Passed	
EWLCJ176_2S_Reg_396	Set OBSS PD value for 5 GHZ band	To verify whether the values set for 5 Ghz band or not	Passed	
EWLCJ176_2S_Reg_397	Set OBSS PD value for 2.4 GHZ band	To verify whether the values set for 2.4 ghz band or not	Passed	
EWLCJ176_2S_Reg_398	Creating RF Profile with OBSS PD enabled for 5/2.4 GHz band	To Validate whether RF Profile created with OBSS PD enable for 5/2.4 GHz band	Passed	
EWLCJ176_2S_Reg_399	Disabling OBSS PD in RF Profile	To Validate whether RF Profile is created with OBSS PD enable for 5/2.4 GHz band	Passed	
EWLCJ176_2S_Reg_400	Viewing OBSS PD supports in different AP models	To checking the OBSS PD supports in different AP models	Passed	
EWLCJ176_2S_Reg_401	Configuring BSS colour details in AP & controller CLIs	To Verify Configured colour details is reflected in AP and Controller CLIs	Passed	

EWLCJ176_2S_Reg_402	Checking the BSS colour details are retained after AP and Controller reload	To Check whether the BSS colour retained after AP & Controller reload	Passed	
EWLCJ176_2S_Reg_403	Verify enable/disable of BSS colouring on radio is reflected in management packets	To verify whether the BSS colour is reflected in Management packets or not	Passed	
EWLCJ176_2S_Reg_404	Verifying OBSS PD with inter roaming client using different radio	To check whether OBSS PD is enable or not , when different radio clients are roaming between controllers	Passed	
EWLCJ176_2S_Reg_405	Verifying OBSS PD enabled with inter roaming client using same radio	To check whether OBSS PD enable or not , when same radio clients are roaming between controllers	Passed	
EWLCJ176_2S_Reg_406	Verifying OBSS PD enabled with Intra client roaming by using 9115AP	To verify whether OBSS PD enabled with client roaming between AP's or not	Passed	
EWLCJ176_2S_Reg_407	Changing 9115 AP mode from local to Flex connect & check the BSS colouring Configuration	To change the mode of AP from local mode to Flex connect mode and check the BSS colouring configuration in 9115 Ap	Passed	
EWLCJ176_2S_Reg_408	Changing 9115 AP mode from flex to local & check the BSS colouring Configuration	To change the mode of AP from flex mode to local mode and check the BSS colouring configuration in 9115 Ap	Passed	

Mesh on EWC

Logical ID	Title	Description	Status	Defect ID
EWCJ176_2S_Reg_134	Verifying the Mesh configuration.	To check whether the Mesh configurations are configuring correct or not.	Failed	CSCvy79693
EWCJ176_2S_Reg_135	Check the Joining of 3800AP in to eWLC with Mesh /Bridge Mode	To check the Mesh/Bridge support of 3800 AP after joining in to eWLC	Passed	
EWCJ176_2S_Reg_136	Check the Joining of 3800AP in to eWLC with Flex+Bridge Mode	To check the Flex+Bridge Mode support of 3800 AP in to eWLC	Passed	
EWCJ176_2S_Reg_137	Check the Joining of 4800AP in to eWLC with Mesh/Bridge Mode	To check the Mesh/Bridge support of 4800 AP after joining in to eWLC	Passed	
EWCJ176_2S_Reg_138	Check the Joining of 4800AP in to eWLC with Flex+Bridge Mode	To check the Flex+Bridge Mode support of 4800 AP in to eWLC	Passed	
EWCJ176_2S_Reg_139	Verify the Windows clients connection for bridge mode AP's with WEP security	To check whether the windows client is connected or not to bridge mode AP's	Passed	
EWCJ176_2S_Reg_140	Verify the Android clients connection for bridge mode AP's with WEP security	To check whether the Android client is connected or not to bridge mode AP's	Passed	
EWCJ176_2S_Reg_141	Verify the IOS clients connection for bridge mode AP's with WEP security	To check whether the IOS client is connected or not to bridge mode AP's	Passed	

EWCJ176_2S_Reg_142	Verify the Windows clients connection for Flex+bridge mode AP's with WEP security	To check whether the windows client is connected or not to Flex+bridge mode AP's	Passed	
EWCJ176_2S_Reg_143	Verify the Android clients connection for Flex+bridge mode AP's with WEP security	To check whether the Android client is connected or not to Flex+bridge mode AP's	Passed	
EWCJ176_2S_Reg_144	Verify the IOS clients connection for Flex+bridge mode AP's with WEP security	To check whether the IOS client is connected or not to Flex+bridge mode AP's	Passed	
EWCJ176_2S_Reg_145	Verify the Windows clients connection for bridge mode AP's with WPA2-PSk security	To check whether the windows client is connected or not to bridge mode AP's with WPA2-PSK security	Passed	
EWCJ176_2S_Reg_146	Verify the Android clients connection for bridge mode AP's with WPA2-PSK security	To check whether the Android client is connected or not to bridge mode AP's with WPA2-PSK security	Passed	
EWCJ176_2S_Reg_147	Verify the IOS clients connection for bridge mode AP's with WPA2-PSK security	To check whether the IOS client is connected or not to bridge mode AP's with WPA2-PSK security	Passed	
EWCJ176_2S_Reg_148	Verify the Windows clients connection for Flex+bridge mode AP's with WPA2-PSK security	To check whether the windows client is connected or not to Flex+bridge mode AP's with WPA2-PSK security	Passed	
EWCJ176_2S_Reg_149	Verify the Android clients connection for Flex+bridge mode AP's with WPA2-PSK security	To check whether the Android client is connected or not to Flex+bridge mode AP's with WPA2-PSK security	Passed	

EWCJ176_2S_Reg_150	Verify the IOS clients connection for Flex+bridge mode AP's with WPA2-PSK security	To check whether the IOS client is connected or not to Flex+bridge mode AP's with WPA2-PSK security	Passed	
EWCJ176_2S_Reg_151	Verify the Windows clients connection for bridge mode AP's with WPA3-SAE security	To check whether the windows client is connected or not to bridge mode AP's with WPA3-SAE security	Passed	
EWCJ176_2S_Reg_152	Verify the Android clients connection for bridge mode AP's with WPA3-SAE security	To check whether the Android client is connected or not to bridge mode AP's with WPA3-SAE security	Passed	
EWCJ176_2S_Reg_153	Verify the IOS clients connection for bridge mode AP's with WPA3-SAE security	To check whether the IOS client is connected or not to bridge mode AP's with WPA3-SAE security	Passed	
EWCJ176_2S_Reg_154	Verify the Windows clients connection for Flex+bridge mode AP's with WPA3-SAE security	To check whether the windows client is connected or not to Flex+bridge mode AP's with WPA3-SAE security	Passed	
EWCJ176_2S_Reg_155	Verify the Android clients connection for Flex+bridge mode AP's with WPA3-SAE security	To check whether the Android client is connected or not to Flex+bridge mode AP's with WPA3-SAEsecurity	Passed	
EWCJ176_2S_Reg_156	Verify the IOS clients connection for Flex+bridge mode AP's with WPA3-SAE security	To check whether the IOS client is connected or not to Flex+bridge mode AP's with WPA3-SAE security	Passed	

EWCJ176_2S_Reg_157	Check and verify the AP mode changes by changing From bridge mode to local	To check whether AP mode changing or not from bridge to local	Passed	
EWCJ176_2S_Reg_158	Check and verify the AP mode changes by changing From Flex+bridge mode to Flexconnect.	To check whether AP mode changing or not from Flex+bridge to Flexconnect.	Passed	
EWCJ176_2S_Reg_159	Check and verify the intra roaming with bridge mode AP	To check whether intra roaming happening or not with bridge mode Ap's	Passed	
EWCJ176_2S_Reg_160	Check and verify the intra roaming with Flex+bridge mode AP	To check whether intra roaming happening or not with Flex+bridge mode Ap's	Passed	

OpenDNS

Logical ID	Title	Description	Status	Defect ID
EWCJ176_2S_Reg_180	verifying ewc registered with open DNS server	To Verify whether the ewc registered in open DNS and ewc got the device ID or not	Passed	
EWCJ176_2S_Reg_181	Verifying the created profile mapped with ewc GUI and CLI	To Verify whether the profile mapped with ewc and reflected in ewc GUI & CLI or not	Passed	
EWCJ176_2S_Reg_182	Verifying the WLAN created with open DNS configuration	To verify whether the WLAN created with open DNS configuration or not	Passed	
EWCJ176_2S_Reg_183	Verifying the open DNS configuration for the connected Windows Client in ewc UI/CLI	To Verify whether the open DNS configured or not when Windows JOS connected to Umbrella enabled WLAN Profile	Failed	CSCvy79837
EWCJ176_2S_Reg_184	Verifying the open DNS configuration for the connected MAC OS Client in ewc UI/CLI	To Verify whether the open DNS configured or not when MAC OS connected to Umbrella enabled WLAN Profile	Passed	
EWCJ176_2S_Reg_185	Verifying the open DNS configuration for the connected iOS Client in ewc UI/CLI	To Verify whether the open DNS configured or not when iOS client connected to Umbrella enabled WLAN Profile	Passed	
EWCJ176_2S_Reg_186	Verifying the open DNS configuration for the connected Android Client in ewc UI/CLI	To Verify whether the open DNS configured or not when Android client connected to Umbrella enabled WLAN Profile	Passed	

EWCJ176_2S_Reg_187	clear the data plane stats in open DNS configuration	To verify whether the data plate stats is cleared or not	Passed	
EWCJ176_2S_Reg_188	Perform the roaming between 9115 & 9120 Aps	To verify the open DNs configuration after client roaming between 9115 & 9120 Aps	Passed	
EWCJ176_2S_Reg_189	Perform the roaming between two ewc	To verify the open dns after Inter roaming	Passed	

Config Wireless

Logical Id	Title	Discription	Status	Defect ID
EWLCJ176S_config_1	6ghz Low Data Rates option needs to remove from Best Practices	6ghz Low Data Rates option needs to remove from Best Practices	Failed	CSCvy09070
EWLCJ176S_config_2	Attack Detected and Cleared messages on AIR-CAP3702I-Q-K9 AP console	Attack Detected and Cleared messages on AIR-CAP3702I-Q-K9 AP console	Failed	CSCvx32288
EWLCJ176S_config_3	Telnet support for newer AP models to be updated	Telnet support for newer AP models to be updated	Passed	CSCvx94077
EWLCJ176S_config_4	WLAN List shown empty after refresh button is hit continuously	WLAN List shown empty after refresh button is hit continuously	Failed	CSCvx64102
EWLCJ176S_config_5	Max RF Bandwidth cannot be configured due to Pop-up overlap	Max RF Bandwidth cannot be configured due to Pop-up overlap	Passed	CSCvx68495
EWLCJ176S_config_6	Add radius server Pop Up cannot be closed	Add radius server Pop Up cannot be closed	Failed	CSCvy02731
EWLCJ176S_config_7	Multi BSSID profile are duplicated on clicking refresh twice	Multi BSSID profile are duplicated on clicking refresh twice	Passed	CSCvx84448
EWCJ176S_config_1	Dark Mode background issues observed stealthwatch page	Dark Mode background issues observed stealthwatch page	Passed	CSCvy11277
EWCJ176S_config_3	Remove client allowed and blocklist feature from EWC webUI	Remove client allowed and blocklist feature from EWC webUI	Passed	CSCvx42676
EWCJ176_2S_config_1	JP locale : Unable to see month selection and week days in dark mode (background issue)	JP locale : Unable to see month selection and week days in dark mode (background issue)	Failed	CSCvy24458

SRCFD

Logical ID	Title	Description	Status	Defect ID
EWLCJ176S_SR_01	Check AAA Authentication shared key from GUI	To check AAA Authentication shared key from GUI	Passed	
EWLCJ176S_SR_02	Configure AAA Authentication shared key with more than 16 characters from GUI	To configure AAA Authentication shared key with more than 16 characters from GUI	Passed	
EWLCJ176S_SR_03	Connect client with shared key of more than 16 characters	to connect client with shared key of more than 16 characters	Passed	
EWLCJ176S_SR_04	Verify any errors while connecting 2800 AP to the controller	To verify errors while connecting 2800 AP to the controller	Passed	
EWLCJ176S_SR_05	Connect 2800 AP in flex mode to the controller	To connect 2800 AP in flex mode to the controller	Passed	
EWLCJ176S_SR_06	Verify whether your able to connect client using 2800 AP	To verify whether your able to connect client using 2800 AP	Passed	
EWLCJ176S_SR_07	Verify any crashes generated or not in 9800-80 by enabling BSS transition dual list	To verify any crashes generated or not in 9800-80by enabling BSS transition dual list	Passed	
EWLCJ176S_SR_08	Verify any crashes generated or not in 9800-40 by enabling BSS transition dual list	To verify any crashes generated or not in 9800-40by enabling BSS transition dual list	Passed	
EWLCJ176S_SR_09	Verify any crashes generated or not in HA setup by enabling BSS transition dual list	To verify any crashes generated or not in HA setup by enabling BSS transition dual list	Passed	

EWLCJ176S_SR_10	Check whether your able to generate and download Radioactive logs or not	To check whether your able to generate and download Radioactive logs or not	Passed	
EWLCJ176S_SR_11	Check whether Debug wireless command executing or not when exec prompt timestamp is configured	To check whether Debug wireless command executing or not when exec prompt timestamp is configured	Passed	
EWLCJ176S_SR_12	Check Data Plane Tracing	To check Data Plane Tracing	Passed	
EWLCJ176S_SR_13	Roam 11ax client between 9105 Aps	To check roaming happening or not for 11ax client between 9105 Aps	Passed	
EWLCJ176S_SR_14	Check commination between 11ax client and wired client	To check commination between 11ax client and wired client	Passed	
EWLCJ176S_SR_15	Verify the AP name in Beacon and Probes fames by configuring Aironet IE.	To check whether AP name in Beacon and Probes fames by configuring Aironet IE.	Passed	
EWLCJ176S_SR_16	Verify the AP name in Beacon and Probes fames by configuring Aironet IE with modified AP name.	To check whether AP name in Beacon and Probes fames by configuring Aironet IE with Modified AP name.	Passed	
EWLCJ176S_SR_17	Verify the QBSS load information in Beacon and Probes fames by configuring WMM as allowed with qbss load for policy profile.	To check whether QBSS load showing in Beacon and Probe frames or not by configuring WMM as allowed with qbss load for policy profile.	Passed	
EWLCJ176S_SR_18	Verify whether client is associating or not when 11ax ap configured TWT parameter in Local mode	To verify whether client is associating or not when 11ax ap configured TWT parameter in Local mode	Passed	

EWLCJ176S_SR_19	Verify whether sleeping client is associating or not when 11ax ap configured TWT parameter	To verify whether sleeping client is associating or not when 11ax ap configured TWT parameter	Passed	
EWLCJ176S_SR_20	Associate 2.4 GHz client to 9115/9120 Ap with TWT configuration.	To verify the 2.4 GHz client associate the 9115/9120 Ap with TWT configuration or not	Passed	
EWLCJ176S_SR_21	Associate 5G Hz client to 9115/9120 Ap with TWT configuration.	To verify the 5GHz client associate the 9115/9120 Ap with TWT configuration or not	Passed	
EWLCJ176S_SR_22	Verify whether client is associating or not when 11ax ap configured TWT parameter in Flex mode	To verify whether client is associating or not when 11ax ap configured TWT parameter in Flex mode	Passed	
EWLCJ176S_SR_23	Clear the TWT configuration Check the Client behaviour	To verify the client behaviour after clear the TWT configuration	Passed	
EWLCJ176S_SR_24	Check if the client session report generated for client connected with WPA3 security	To verify if the client session report generated for client connected with WPA3 security and validate the report generated	Passed	
EWLCJ176S_SR_25	Generating client Trend report for client connected with WPA3 security	To verify if the client Trend report generated for client connected with WPA3 security and validate the report generated	Passed	
EWLCJ176S_SR_26	Associate a 9105 AP to controller and check AP details in report	To associate a new AP to controller and check AP details in report	Passed	

EWLCJ176S_SR_27	Checking any duplex mismatch error in 9200 switch when connecting 4800 AP	Verifying any duplex mismatch error is generating in switch when connecting 4800 AP	Passed	
EWLCJ176S_SR_28	Checking any duplex mismatch error in 9200 switch when connecting 9105 AP after changing port to full duplex	Verifying any duplex mismatch error is generating in switch when connecting 9105 AP after changing port to full duplex	Passed	
EWLCJ176S_SR_29	Checking any duplex mismatch error in 9500 switch when connecting 9120 AP after changing port to full duplex	Verifying any duplex mismatch error is generating in switch when connecting 9120 AP after changing port to full duplex	Passed	
EWLCJ176S_SR_30	Checking any duplex mismatch error in 9400 switch when connecting 9120 AP after changing port to full duplex	Verifying any duplex mismatch error is generating in switch when connecting 9120 AP after changing port to full duplex	Passed	
EWLCJ176S_SR_31	Changing the inline power in switch port to which the 9105 AP connected and validating the behaviour of the client connected	To change the inline power in switch where the 9105 AP is connected and check the behaviour of the client connected to the AP	Passed	
EWLCJ176S_SR_32	Changing the inline power in switch port to which the 9115 AP connected and validating the behaviour of the client connected	To change the inline power in switch where the 9115 AP is connected and check the behaviour of the client connected to the AP	Passed	
EWLCJ176S_SR_33	Changing the Power Level Assignment and Channel Assignment when the client is connected to the AP	To check the behaviour of the client when the Power Level and Channel Assignment is changed	Passed	

EWLCJ176S_SR_34	Assigning channel number 36 to 100 for 5 GHz radio for J4 for mesh AP	To assign channel for 5 GHz radio for the -Q domain AP which is operating as mesh Ap and check if the channel is reflected in AP and eWLC	Passed	
EWLCJ176S_SR_35	Assigning channel number 100 to 140 for 5 GHz radio for J4 for mesh AP	To assign channel for 5 GHz radio for the -Q domain AP which is operating as mesh Ap and check if the channel is reflected in AP and eWLC	Passed	
EWLCJ176S_SR_36	Configuring AVC in eWLC 9800-40 and passing traffic to client for 24 hours and check for any memory leaks	To configure AVC in 9800-40 eWLC and connecting a client and passing traffic for 24 hours and check the behaviour of the client and verify if any memory leak happens	Passed	
EWLCJ176S_SR_37	Configuring AVC in eWLC 9800-80 and passing traffic to client for 24 hours and check for any memory leaks	To configure AVC in 9800-80 eWLC and connecting a client and passing traffic for 24 hours and check the behaviour of the client and verify if any memory leak happens	Passed	
EWLCJ176S_SR_38	Configuring AVC in eWLC 9800-L and passing traffic to client for 24 hours and check for any memory leaks	To configure AVC in 9800-L eWLC and connecting a client and passing traffic for 24 hours and check the behaviour of the client and verify if any memory leak happens	Passed	

EWLCJ176S_SR_39	Configuring AVC in eWLC 9800-CL and passing traffic to client for 24 hours and check for any memory leaks	To configure AVC in 9800-CL eWLC and connecting a client and passing traffic for 24 hours and check the behaviour of the client and verify if any memory leak happens	Passed	
EWLCJ176S_SR_40	Configuring AVC in eWLC and passing traffic to client for 24 to 48 hours which is connected to 9115 AP and check for any memory leaks	To configure AVC in eWLC and connecting a client and passing traffic for 24 hours which is connected to 9115 AP. check the behaviour of the client and verify if any memory leak happens	Passed	
EWLCJ176S_SR_41	Configuring AVC in eWLC and passing traffic to client for 24 to 48 hours which is connected to 9105 AP and check for any memory leaks	To configure AVC in eWLC and connecting a client and passing traffic for 24 hours which is connected to 9105 AP. check the behaviour of the client and verify if any memory leak happens	Passed	
EWLCJ176S_SR_42	Configuring AVC in eWLC and passing traffic to client for 24 to 48 hours which is connected to 4800 AP and check for any memory leaks	To configure AVC in eWLC and connecting a client and passing traffic for 24 hours which is connected to 4800 AP. check the behaviour of the client and verify if any memory leak happens	Passed	
EWLCJ176S_SR_43	Detection of the rogue using 2800 in Local mode	To detect the rogue using 2800 in local mode and verify the details of the rogue	Passed	

EWLCJ176S_SR_44	Configure Rogue Detection Security Level to low and classifying the rogue detected	To configure rogue detection security level to low to detect the rogue and verify if the rogue can be manually classified	Passed	
EWLCJ176S_SR_45	Check if the rogue detection works on the 2800 AP connected in eWLC	To check if the rogue AP and clients are detected by AP connected in eWLC	Passed	
EWLCJ176S_SR_46	Manual date and time adjustment does not survive a reload	Verify clock timings and manually set the date and time in PI	Passed	
EWLCJ176S_SR_47	Set manually time zone as required and verify time zone updated or not	To configure time zone as required and verify whether time zone updating in PI cli or not	Passed	
EWLCJ176S_SR_48	Manual time zone and clock time does not survive a reload	To configure manually clock time and time zone and Verify whether updating with the changes applied or not	Passed	
EWLCJ176S_SR_49	Verifying the mobility configuration roaming occurring when android client is connected.	To verify whether roaming occurring in the Android client or not	Passed	
EWLCJ176S_SR_50	Monitoring the mobility configuration roaming status in DNAC using Android Client	To verify whether roaming status is showing in DNAC using Android Client	Passed	

EWLCJ176S_SR_51	Verifying the mobility configuration roaming occurring when android client is connected with Different Radio types in DNAC	To verify whether roaming occurring in the Android client or not with Different Radio types in DNAC	Passed	
EWLCJ176S_SR_52	Monitor the network health updated as required or not	To verify whether the network health updated as required or not	Passed	
EWLCJ176S_SR_53	Monitor the Summary metrics updated as required or not	To verify whether Summary metrics updated as required or not	Passed	
EWLCJ176S_SR_54	Monitor the Cache and location details updated as required or not	To verify whether Cache and location details are updated as required or not	Passed	
EWLCJ176S_SR_55	Configure either SNMP RO and RW in eWLC UI	To configure either SNMP RO and RW in eWLC UI	Passed	
EWLCJ176S_SR_56	Configured SNMP RO and RW created data is updated in CMX or not	To verify whether SNMP RO and RW created data is updated in CMX or not	Passed	
EWLCJ176S_SR_57	Configured SNMP RO and RW data is deleted in CMX or not	To verify whether SNMP RO and RW created data is deleted in CMX or not	Passed	
EWLCJ176S_SR_58	Join AP to controller by disabling MIC and Reboot AP	To verify by joining AP to controller by disabling MIC and Reboot AP	Passed	
EWLCJ176S_SR_59	Join AP to controller by enabling MIC and Reboot AP	To verify by joining AP to controller or not by enabling MIC and Rebooting AP	Passed	

EWLCJ176S_SR_60	Configuring AP LSC Provision List in eWC UI	To verify whether able to Configure AP LSC Provision List in eWC UI or not	Passed	
EWLCJ176S_SR_61	Check connectivity between two clients connected to 2 ewc with ISE/AAA overridden VLAN in 5Ghz radio.	To Check connectivity between two clients connected to 2 different autonomous APs with ISE/AAA overridden VLAN in 5Ghz radio.	Passed	
EWLCJ176S_SR_62	Check connectivity between two clients connected to 2 different ewc without ISE/AAA overridden VLAN in 5Ghz radio.	To Check connectivity between two clients connected to 2 different autonomous APs without ISE/AAA overridden VLAN in 5Ghz radio.	Passed	
EWLCJ176S_SR_63	Check connectivity between two clients connected to 2 different ewc-ap with ISE/AAA overridden VLAN in 2.4Ghz radio.	To Check connectivity between two clients connected to 2 different autonomous APs with ISE/AAA overridden VLAN in 2.4Ghz radio.	Passed	
EWLCJ176S_SR_64	Check connectivity between two clients connected to 2 different autonomous APs without ISE/AAA overridden VLAN in 2.4Ghz radio.	To Check connectivity between two clients connected to 2 different autonomous APs without ISE/AAA overridden VLAN in 2.4Ghz radio.	Passed	
EWLCJ176S_SR_65	connectivity between Clients connected to same SSID using different ewc Aps(9120 and 9105) in 2.4Ghz	To verify connectivity between Clients connected to same SSID using different autonomous Cisco 2702 Aps in 2.4Ghz	Passed	

EWLCJ176S_SR_66	connectivity between Clients connected to same SSID using different ewc-ap(9120 and 9105) in 5Ghz	To verify connectivity between Clients connected to same SSID using different autonomous Cisco 2702 Aps in 5Ghz	Passed	
EWLCJ176S_SR_67	connectivity between Clients connected to same SSID using different ewc Aps(9120 and 9130) in 2.4Ghz	To verify connectivity between Clients connected to same SSID using different autonomous Cisco 3702 Aps in 2.4Ghz	Passed	
EWLCJ176S_SR_68	connectivity between Clients connected to same SSID using different ewc Aps(9120 and 9130) in 5Ghz	To verify connectivity between Clients connected to same SSID using different autonomous Cisco 3702 Aps in 5Ghz	Passed	
EWLCJ176S_SR_69	connectivity between Clients connected to same SSID using different AP(9105 and 9130) in 2.4Ghz	To verify connectivity between Clients connected to same SSID using different autonomous Cisco 3702 Ap and 2702 AP in 2.4Ghz	Passed	
EWLCJ176S_SR_70	connectivity between Clients connected to same SSID using different ewc (9105 and 9130) in 5Ghz	To verify connectivity between Clients connected to same SSID using different autonomous Cisco 3702 Ap and 2702 AP in 5Ghz	Passed	
EWLCJ176S_SR_71	Connect client to 4800 AP and verify connectivity in 2.4ghz/5ghz radio	To verify Connect client to 4800 AP and verify connectivity in 2.4ghz/5ghz radio	Passed	
EWLCJ176S_SR_72	Connect client to 3800 AP and verify connectivity in 2.4ghz/5ghz radio	To verify Connect client to 3800 AP and verify connectivity in 2.4ghz/5ghz radio	Passed	

EWLCJ176S_SR_73	Connect client to 2800 AP and verify connectivity in 2.4ghz/5ghz radio	To verify Connect client to 2800 AP and verify connectivity in 2.4ghz/5ghz radio	Passed	
EWLCJ176S_SR_74	Connect client to 4800 AP and verify connectivity in 2.4ghz/5ghz radio	To verify Connect client to 4800 AP and verify connectivity in 2.4ghz/5ghz radio	Passed	
EWLCJ176S_SR_75	Connect client to 3800 AP and verify connectivity in 2.4ghz/5ghz radio	To verify Connect client to 3800 AP and verify connectivity in 2.4ghz/5ghz radio	Passed	
EWLCJ176S_SR_76	Connect client to 2800 AP and verify connectivity in 2.4ghz/5ghz radio	To verify Connect client to 2800 AP and verify connectivity in 2.4ghz/5ghz radio	Passed	
EWLCJ176S_SR_77	Configure DHCP for specific client mac address	To Configure DHCP for specific client mac address	Passed	
EWLCJ176S_SR_78	Check AP port status after reboot	To Check AP port status after reboot	Passed	
EWLCJ176S_SR_79	Check AP port status after software upgrade/downgrade	To Check AP port status after software upgrade/downgrade	Passed	
EWLCJ176S_SR_80	Associate client to 5 GHz radio policy with slot 0	To verify probe request/response details shown in slot 0 or not	Passed	
EWLCJ176S_SR_81	Associate client to 5 GHz radio policy with slot 1	To verify probe request/response details shown in slot 1 or not	Passed	
EWLCJ176S_SR_82	Associate client to 5 GHz radio policy with slot 2	To verify probe request/response details shown in slot 2 or not	Passed	
EWLCJ176S_SR_83	Observe crash while Inter roaming	To Monitor crash happen or not during Inter roaming	Passed	

EWLCJ176S_SR_84	Observe crash while Intra roaming	To Monitor crash happen or not during Inter roaming	Passed	
EWLCJ176S_SR_85	Observe crash while IRCM roaming	To Monitor crash happen or not during Inter roaming	Passed	
EWLCJ176S_SR_86	Configure catalyst AP as autonomous ap with flex connect mode	To Validate the client connectivity	Passed	
EWLCJ176S_SR_87	Perform Intra roaming and verify the client connectivity	To Validate the client connectivity	Passed	
EWLCJ176S_SR_88	Configure catalyst AP as autonomous ap with Local mode	To Validate the client connectivity	Passed	
EWLCJ176S_SR_89	Perform Intra roaming and verify the client connectivity	To Validate the client connectivity	Passed	
EWLCJ176S_SR_90	Onboard the client with open SSID	To Monitor the client onboarding	Passed	
EWLCJ176S_SR_91	Onboard the client with WPA2 SSID	To Monitor the client onboarding	Passed	
EWLCJ176S_SR_92	Onboard the client with WPA3 SSID	To Monitor the client onboarding	Passed	
EWLCJ176S_SR_93	Monitor the logs client association	To Monitor the logs for client Assoc	Passed	
EWLCJ176S_SR_94	Monitor the logs client deletion	To Monitor the logs for client delete	Passed	
EWLCJ176S_SR_95	Monitor the logs client re-association	To Monitor the logs for client re-Assoc	Passed	
EWLCJ176S_SR_96	Export the device list without credentials	To Export the device details and validate the details	Passed	
EWLCJ176S_SR_97	Export the device list with credentials	To Export the device details and validate the details	Passed	

EWLCJ176S_SR_98	Export the device list with wrong credentials	To Export the device details and validate the details	Passed	
EWLCJ176S_SR_99	Check smart licensing in 9800 setup.	To check smart licensing in HA setup.	Passed	
EWLCJ176S_SR_100	Check smart licensing in HA setup.	To check smart licensing in HA setup.	Passed	
EWLCJ176S_SR_101	Check license info after multiple reload in HA setup.	To check license info after multiple reload in HA setup.	Passed	
EWLCJ176S_SR_102	Check license info after multiple switchover in HA setup.	To check license info after multiple switchover in HA setup.	Passed	
EWLCJ176S_SR_103	Check license info after upgrading to latest build in HA setup.	To check license info after upgrading to latest build in HA setup.	Passed	
EWLCJ176S_SR_104	Check license info after downgrading to older build in HA setup.	To check license info after downgrading to older build in HA setup.	Passed	
EWLCJ176S_SR_105	Check license info after upgrading to latest build.	To check license info after upgrading to latest build.	Passed	
EWLCJ176S_SR_106	Check license info after upgrading to latest build in HA setup.	To check license info after upgrading to latest build in HA setup.	Passed	
EWLCJ176S_SR_107	Check license info after upgrading to latest build in EWC setup.	To check license info after upgrading to latest build in EWC setup.	Passed	
EWLCJ176S_SR_108	Check CA certificate after reboot for different models of controller	To check CA certificate after reboot	Passed	
EWLCJ176S_SR_109	Check CA certificate after reboot for HA setup	To check CA certificate after reboot	Passed	

EWLCJ176S_SR_110	Check CA certificate after device upgrade	To check CA certificate after reboot	Passed	
EWLCJ176S_SR_111	Configure HA SSO RMI setup with gateway failover and perform reload	To configure HA SSO RMI setup with gateway failover and perform reload	Passed	
EWLCJ176S_SR_112	Configure HA SSO RMI setup with gateway failover and perform upgrade	To configure HA SSO RMI setup with gateway failover and perform upgrade	Passed	
EWLCJ176S_SR_113	Configure HA SSO RMI gateway failover & monitor the behaviour on gateway connection failure	To configure HA SSO RMI gateway failover & monitor the behaviour on gateway connection failure	Passed	
EWLCJ176S_SR_114	Configure HA SSO with RMI IP and verify if its not synced with Standby	To configure HA SSO with RMI IP and verify if its not synced with Standby	Passed	
EWLCJ176S_SR_115	Configure separate IP address for both Active/Standby EWC chassis	To configure separate IP address for both Active/Standby EWC chassis	Passed	
EWLCJ176S_SR_116	Verify the NETCONF with out crash	To verify the NETCONF with out crash	Passed	
EWLCJ176S_SR_117	Configure separate IP address for both Active/Standby EWC chassis	To verify the client connects with 2.4 GHz enabled	Passed	
EWLCJ176S_SR_118	Configure separate IP address for both Active/Standby EWC chassis	To Verify the Ap When we install new AP and it goes into image download state	Passed	
EWLCJ176S_SR_119	Configure separate IP address for both Active/Standby EWC chassis	To verify both radios slot 0 and 1	Passed	

EWLCJ176S_SR_120	Modify Band steering RSSI Value as minimum & check the client connectivity	To modify the band steering rssi value as minimum & check the client connectivity	Passed	
EWLCJ176S_SR_121	Modify Band steering RSSI Value as default & check the client connectivity	To modify the band steering rssi value as default & check the client connectivity	Passed	
EWLCJ176S_SR_122	Checking the Android client connectivity for 2.4/5 Ghz radio	To verify the client connection status based in 2.4 and 5 G radio.	Passed	
EWLCJ176S_SR_123	Checking the windows client connectivity for 2.4/5 Ghz radio	To verify the client connection status based in 2.4 and 5 G radio.	Passed	
EWLCJ176S_SR_124	Checking the Surface Go client connectivity for 2.4/5 Ghz radio	To verify the client connection status based in 2.4 and 5 G radio.	Passed	
EWLCJ176S_SR_125	Checking the payload values after changing AP Radio(2.4/5 Ghz)	To check the payload values after changing the AP radio(2.4/5 Ghz)	Passed	
EWLCJ176S_SR_126	Bootup Catalyst AP and capture logs	To bootup and verify any unwanted messages are displayed in logs	Passed	
EWLCJ176S_SR_127	Bootup COS AP and capture logs	To bootup and verify any unwanted messages are displayed in logs	Passed	
EWLCJ176S_SR_128	Validate DE authenticate logs while continuous roaming	To verify the DE authentication logs received or not while performing continues roaming	Passed	
EWLCJ176S_SR_129	Validate DE authenticate logs in HA	To verify the DE authentication logs received or not while Primary goes down in HA pair	Passed	

EWLCJ176S_SR_130	Validate the DE authenticate logs in IRCM	To verify the DE authentication logs received or not while performing IRCM	Passed	
EWLCJ176S_SR_131	Verify the bridge mode option shown in 9120 AP	To verify the bridge mode option shown or not in catalyst Ap	Passed	
EWLCJ176S_SR_132	Verify the bridge mode option shown in 9130 AP	To verify the bridge mode option shown or not in catalyst Ap	Passed	
EWLCJ176S_SR_133	Verify the bridge mode option shown in 9115 AP	To verify the bridge mode option shown or not in catalyst Ap	Passed	
EWLCJ176S_SR_134	Verify the bridge mode option shown in 9105 AP	To verify the bridge mode option shown or not in catalyst Ap	Passed	
EWLCJ176S_SR_135	HA setup using RP option in 9800-40 or 9800-80 Ewlc	To Configure HA setup using RP option	Passed	
EWLCJ176S_SR_136	Check if it showing any errors in CLI of HA setup in 9800-40 or 9800-80 Ewlc	To Check if it showing errors in CLI	Passed	
EWLCJ176S_SR_137	HA setup using RP option in 9800-L Ewlc	To configure HA setup using RP option in 9800-L Ewlc	Passed	
EWLCJ176S_SR_138	console logs flooding with "%CPOSLIBERROR_NOTIFY" Tracebacks	to check if 9800 console logs flooding with "%CPOSLIBERROR_NOTIFY" Tracebacks	Passed	
EWLCJ176S_SR_139	HA setup using RP option in EWC UI	To configure HA setup using RP option in EWC	Passed	
EWLCJ176S_SR_140	Check if it showing any errors in CLI of HA setup in Ewc	To configure HA setup using RP option in EWC	Passed	
EWLCJ176S_SR_141	HA setup using RMI option in EWC UI	To HA setup using RMI option in EWC UI	Passed	

EWLCJ176S_SR_142	Check if it showing any errors in CLI of HA(RMI) setup in Ewc	To configure HA setup using RMI option in EWC CLI	Passed	
EWLCJ176S_SR_143	Check HA setup with downgrade build version of 9800 EWLC & downgrade build version of 9105 or 9130 EWC	To Check & Configure HA setup using RP & RMI option	Passed	
EWLCJ176S_SR_144	Check HA setup with downgrade build version of 9105 or 9130 EWC	To Check & Configure HA setup using RP & RMI option	Passed	
EWLCJ176S_SR_145	Check HA Setup (EWLC & EWC) behaviour in DNA-C & PI	to check behaviour in DNA-C & PI of EWLC & DNA-c	Passed	
EWLCJ176S_SR_146	Prepare csv file for c9800 MAC filtering in Ewlc	C9800 MAC Filtering: Preparation of CSV file	Passed	
EWLCJ176S_SR_147	Prepare csv file for c9800 MAC filtering in CLI	C9800 MAC Filtering: Description not imported properly from CSV file	Passed	
EWLCJ176S_SR_148	Prepare csv file for c9800 MAC filtering in EWC	C9800 MAC Filtering: Description not imported properly from CSV file	Passed	
EWLCJ176S_SR_149	import Description properly from CSV file in CLI of eWC	C9800 MAC Filtering: import Description properly from CSV file	Passed	
EWLCJ176S_SR_150	Configure Application Visibility and Control (AVC) in EWLC Web GUI	C9800: Create and configure an AVC profile	Passed	

EWLCJ176S_SR_151	Application visibility in EWLC Web CLI	C9800: Application visibility ,check data availability in Web CLI	Passed	
EWLCJ176S_SR_152	Configure Application Visibility and Control (AVC) in EWC Web GUI	C9800: Application visibility shows "No data available" in Web GUI	Passed	
EWLCJ176S_SR_153	Application visibility in EWC Web CLI	C9800: Application visibility shows "No data available" in Web GUI	Passed	
EWLCJ176S_SR_154	create wlan with open security to associate android phones	Various Android 10 phones associate	Passed	
EWLCJ176S_SR_155	create wlan with dot1 Authentication to associate android phones	Various Android 10 phones to associate	Passed	
EWLCJ176S_SR_156	Create a WLAN with WPA+WPA2 security to associate android phones	Various Android 10 phones to associate	Passed	
EWLCJ176S_SR_157	Create a WLAN with Static WEP security to associate android phones	Various Android 10 phones to associate	Passed	
EWLCJ176S_SR_158	Create a WLAN with Static+ WEP+802.1x security to associate android phones	Various Android 10 phones to associate	Passed	
EWLCJ176S_SR_159	Create a WLAN with CKIP security to associate android phones	Various Android 10 phones to associate	Passed	
EWLCJ176S_SR_160	Create a WLAN with None+EAP Pass through security to associate android phones	Various Android 10 phones to associate	Passed	
EWLCJ176S_SR_161	join & configure 2600 series IOS AP in EWLC	To configure 2600 series IOS AP	Passed	

EWLCJ176S_SR_162	connect a client & check (AP & client) status	connect a client & check AP status	Passed	
EWLCJ176S_SR_163	check Flash on lightweight Wave 1 APs	to check Flash on lightweight Wave 1 APs if gets corrupted	Passed	
EWLCJ176S_SR_164	check Flash on lightweight Wave 1 APs in flex mode	Flash on lightweight Wave 1 APs gets corrupted	Passed	
EWLCJ176S_SR_165	Troubleshoot ,if Flash on lightweight Wave 1 APs gets corrupted	To troubleshoot if Flash on lightweight Wave 1 APs gets corrupted	Passed	
EWLCJ176S_SR_166	check Flash on lightweight Wave 1 APs in (monitor or sniffer or bridge)	Flash on lightweight Wave 1 APs gets corrupted	Passed	
EWLCJ176S_SR_167	join , configure 2600 series IOS AP & check FLASH Status in EWC	To configure 2600 series IOS AP in EWC	Passed	
EWLCJ176S_SR_168	Check 2600 AP status with downgrade build version of 9105 or 9130 EWC	To configure 2600 series IOS AP in downgrade version of 9800 Ewlc & 9105 0r 9130 EWC	Passed	
EWLCJ176S_SR_169	Create ACL & configure in 9800 EWLC	to Create ACL & configure	Passed	
EWLCJ176S_SR_170	configure flex profile & map ACL	to configure flex profile & map ACL	Passed	
EWLCJ176S_SR_171	CLI Flex Connect ACLs - URL Rules can be configured > 20 and "remove" issue from 21st URL Rule	CLI Flex Connect ACLs - URL Rules can be configured > 20 and "remove" issue from 21st URL Rule	Passed	
EWLCJ176S_SR_172	Create ACL & configure in 9105 & 9130 EWC	GUI Flex Connect ACLs - URL Rules can be configured > 20 and "remove" issue from 21st URL Rule	Passed	

EWLCJ176S_SR_173	GUI Flex Connect ACLs - URL Rules can be configured > 20 and "remove" issue from 21st URL Rule	GUI Flex Connect ACLs - URL Rules can be configured > 20 and "remove" issue from 21st URL Rule	Passed	
EWLCJ176S_SR_174	Check & configure with downgrade build version of 9800 EWLC	to configure with downgrade build version of 9800 EWLC	Passed	
EWLCJ176S_SR_175	Check & configure with downgrade build version of 9105 & 9130 EWC	to configure with downgrade build version of 9105 & 9130 EWC	Passed	
EWLCJ176_2S_SR_01	Checking the ip address of DHCP Client after joining to the controller.	To check whether the DHCP client getting IP or not after joined to the controller	Passed	
EWLCJ176_2S_SR_02	Verifying the Interface status of DHCP client	To verify the interface status of DHCP client	Passed	
EWLCJ176_2S_SR_03	configuring mode of access as switch port in catalyst ap & checking the DHCP Client IP	To check the DHCP client IP after configuring mode of access as switch port	Passed	
EWLCJ176_2S_SR_04	Verify HA setup details in Standby console	To verify HA setup details in Standby console	Passed	
EWLCJ176_2S_SR_05	Monitor ntp config in Standby unit from Active unit console	To monitor ntp config in Standby unit from Active unit console	Passed	
EWLCJ176_2S_SR_06	Check ntp configuration details in standby console	To check ntp config details in standby console	Passed	
EWLCJ176_2S_SR_07	Performing local switching for Windows clients with 9115 AP	To verify local switching traffic for windows client with 9115 AP	Passed	
EWLCJ176_2S_SR_08	Associate the mac client with local switching	To verify the client association in local switching	Passed	

EWLCJ176_2S_SR_09	Smart Account Creation, registration and activation.	To verify smart Account Creation, registration and activation.	Passed	
EWLCJ176_2S_SR_10	Validate license info on multiple reload	To validate license info on multiple reboot	Passed	
EWLCJ176_2S_SR_11	Validate license info after EWC upgrade	To validate license info after EWC upgrade	Passed	
EWLCJ176_2S_SR_12	Validate deauthenticate logs while continuous roaming	To verify the deauthentication logs received or not while performing continues roaming	Passed	
EWLCJ176_2S_SR_13	Validate deauthenticate logs in HA	To verify the deauthentication logs received or not while Primary goes down in HA pair	Passed	
EWLCJ176_2S_SR_14	Validate the deauthenticate logs in IRCM	To verify the deauthentication logs received or not while performing IRCM	Passed	
EWLCJ176_2S_SR_15	Perform the reload via 9130 AP UI	To verify the ap behaviour after giving the reload via GUI	Passed	
EWLCJ176_2S_SR_16	Verifying the internal AP's Association after the EWC reload	To check whether the internal AP properly associate with the EWC after reload	Passed	
EWLCJ176_2S_SR_17	Roam the Client between two controllers and verify any errors	To roam the Client between two controllers and verify any errors	Passed	
EWLCJ176_2S_SR_18	Roam the clients (10-50) between two controllers and verify any errors	To roam the clients (10-50) between two controllers and verify any errors	Passed	
EWLCJ176_2S_SR_19	Verify roaming between the controller with different radio types	To verify roaming between the controller with different radio types	Passed	

EWLCJ176_2S_SR_20	Verify client connectivity using 1800AP	To verify client connectivity using 1800AP	Passed	
EWLCJ176_2S_SR_21	Verify client connectivity using 1800AP	To verify client connectivity using 1800AP	Passed	
EWLCJ176_2S_SR_22	Configure 11ax for 1800 AP for 5ghz band	Configure 11ax for 1800 AP for 5ghz band	Passed	
EWLCJ176_2S_SR_23	Configure 11ax for 1800 AP for 24ghz band	Configure 11ax for 1800 AP for 24ghz band	Passed	
EWLCJ176_2S_SR_24	Verify Prime Infrastructure live logs	To verify Prime Infrastructure live logs	Passed	
EWLCJ176_2S_SR_25	Verify Prime Infrastructure Syslog's after upgrading to newer version	To verify Prime Infrastructure Syslog's after upgrading to newer version	Passed	
EWLCJ176_2S_SR_26	Validate Prime Infrastructure live alerts with example	Validate Prime Infrastructure live alerts with example	Passed	
EWLCJ176_2S_SR_27	Verify client count is showing properly or not	To verify client count is showing properly or not	Passed	
EWLCJ176_2S_SR_28	Validate total clients and verify each client parameters	To validate total clients and to verify each client parameters	Passed	
EWLCJ176_2S_SR_29	Roam the client from 9800-40 or 9800-80 to 9800-CL and verify client count status	To roam the client from 9800-40 or 9800-80 to 9800-CL and verify client count status	Passed	
EWLCJ176_2S_SR_30	Verify Smart Licensing is enabling or not and Register Device	To verify Smart Licensing is enabling or not and Register Device	Passed	
EWLCJ176_2S_SR_31	Validate license info in HA SSO RMI pair	To validate license info in HA SSO RMI pair	Passed	

EWLCJ176_2S_SR_32	Validate license info on multiple reload	To validate license info on multiple reboot	Passed	
EWLCJ176_2S_SR_33	Verify any crashes occurred when AIR-AP3802I-B-K9 is in Flex mode	To verify any crashes occurred when AIR-AP3802I-B-K9 is in Flex mode	Passed	
EWLCJ176_2S_SR_34	Verify any crashes occurred when AIR-AP3802E-B-K9 is in Flex mode	To verify any crashes occurred when AIR-AP3802E-B-K9 is in Flex mode	Passed	
EWLCJ176_2S_SR_35	Verify max number of wired clients supported on each LAN port for C9105AX AP is documented or not	To verify max number of wired clients supported on each LAN port for C9105AX AP is documented or not	Passed	
EWLCJ176_2S_SR_36	Verify max number of wired clients supported on each LAN port for C9105AXW AP is documented or not	To verify max number of wired clients supported on each LAN port for C9105AXW AP is documented or not	Failed	CSCvy89875
EWLCJ176_2S_SR_37	Verify Syslog log level shows updated data as configured in Japanese GUI	To Verify Syslog log level shows updated data as configured in Japanese GUI	Passed	
EWLCJ176_2S_SR_38	Verify edited Syslog log level shows with data as configured in Japanese GUI	To Verify edited Syslog log level shows with data as configured in Japanese GUI	Passed	
EWLCJ176_2S_SR_39	Verify by discarding Syslog log level data as configured in Japanese GUI	To Verify by discarding Syslog log level data as configured in Japanese GUI	Passed	
EWLCJ176_2S_SR_40	Verify the Transmit power values configured in RFID	To Verify the Transmit power values configured in RFID	Passed	

EWLCJ176_2S_SR_41	Verify the Transmit power range values configured in RFID	To Verify the Transmit power range values configured in RFID	Passed	
EWLCJ176_2S_SR_42	Verify smart licensing reservation in 9800 setup.	To Verify smart licensing reservation in 9800 setup.	Passed	
EWLCJ176_2S_SR_43	Verify by deleting the existing smart licensing reservation in 9800 setup.	To Verify by deleting the existing smart licensing reservation in 9800 setup.	Passed	
EWLCJ176_2S_SR_44	Verify HA support in smart licensing reservation in 9800 setup.	To Verify HA support in smart licensing reservation in 9800 setup.	Passed	
EWLCJ176_2S_SR_45	Verify Whether AP details are updated or not	To Verify Whether AP details are updated or not	Passed	
EWLCJ176_2S_SR_46	Verify Client details are updated in Wireshark	To Verify Client details are updated in Wireshark	Passed	
EWLCJ176_2S_SR_47	Verify whether eWC controller image is deleted from AP once installed	To Verify whether eWC controller image is deleted from AP once installed	Passed	
EWLCJ176_2S_SR_48	Convert EWC Back To Lightweight CAPWAP Mode	To Convert EWC Back To Lightweight CAPWAP Mode	Passed	
EWLCJ176_2S_SR_49	Verify that junk characters should not be added in Primary WLC name of AP output	To Verify that junk characters should not be added in Primary WLC name of AP output	Passed	

EWLCJ176_2S_SR_50	Verify by Shutting the Primary WLC port and Joining AP with Another WLC check junk characters are added in Primary WLC name	To Verify by Shutting the Primary WLC port and Joining AP with Another WLC check junk characters are added in Primary WLC name	Passed	
EWLCJ176_2S_SR_51	Verify by UnShut of Primary WLC port check junk characters are added in Primary WLC name	To Verify by unShut of Primary WLC port check junk characters are added in Primary WLC name	Passed	
EWLCJ176_2S_SR_52	The recommend and latest version is different with Cisco.com	To check ,The recommend and latest version is different with Cisco.com	Passed	
EWLCJ176_2S_SR_53	The recommend and latest version is different with Cisco.com	To check ,The recommend and latest version is different with Cisco.com	Passed	
EWLCJ176_2S_SR_54	The recommend and latest version is different with Cisco.com	to check, The recommend and latest version is different with Cisco.com	Passed	
EWLCJ176_2S_SR_55	The recommend and latest version is different with Cisco.com	to check, The recommend and latest version is different with Cisco.com	Passed	
EWLCJ176_2S_SR_56	The recommend and latest version is different with Cisco.com	to check, The recommend and latest version is different with Cisco.com	Passed	
EWLCJ176_2S_SR_57	The recommend and latest version is different with Cisco.com	to check, The recommend and latest version is different with Cisco.com	Passed	

EWLCJ176_2S_SR_58	The recommend and latest version is different with Cisco.com	to check, The recommend and latest version is different with Cisco.com	Passed	
EWLCJ176_2S_SR_59	WLC: GUI has multiple rendering issues with some web browsers even after reboot.	WLC: GUI has multiple rendering issues with some web browsers even after reboot.	Passed	
EWLCJ176_2S_SR_60	WLC: GUI has multiple rendering issues with some web browsers even after reboot.	WLC: GUI has multiple rendering issues with some web browsers even after reboot.	Passed	
EWLCJ176_2S_SR_61	WLC: GUI has multiple rendering issues with some web browsers even after reboot.	WLC: GUI has multiple rendering issues with some web browsers even after reboot.	Passed	
EWLCJ176_2S_SR_62	Wrong source ip address is shown in https access log	to check source ip address is shown in https access log	Passed	
EWLCJ176_2S_SR_63	Wrong source ip address is shown in https access log	to check source ip address is shown in https access log	Passed	
EWLCJ176_2S_SR_64	show interface status shows maximum link speed on auto-negotiation port	show interface status shows maximum link speed on auto-negotiation port	Passed	
EWLCJ176_2S_SR_65	show interface status shows maximum link speed on auto-negotiation port	show interface status shows maximum link speed on auto-negotiation port	Passed	
EWLCJ176_2S_SR_66	show interface status shows maximum link speed on auto-negotiation port	show interface status shows maximum link speed on auto-negotiation port	Passed	

EWLCJ176_2S_SR_67	show interface status shows maximum link speed on auto-negotiation port	show interface status shows maximum link speed on auto-negotiation port	Passed	
EWLCJ176_2S_SR_68	eWLC doc: single authentication support with mobility anchor	to configure single authentication support with mobility anchor	Passed	
EWLCJ176_2S_SR_69	eWLC doc: single authentication support with mobility anchor	to configure single authentication support with mobility anchor	Passed	
EWLCJ176_2S_SR_70	eWLC doc: single authentication support with mobility anchor	to Configure a WLAN Profile for Guest Access with Open Authentication (GUI)	Passed	
EWLCJ176_2S_SR_71	eWLC doc: single authentication support with mobility anchor	Configure a WLAN Profile For Guest Access with Open Authentication (CLI)	Passed	
EWLCJ176_2S_SR_72	eWLC doc: single authentication support with mobility anchor	Configure a WLAN Profile For Guest Access with Local Web Authentication in GUI	Passed	
EWLCJ176_2S_SR_73	eWLC doc: single authentication support with mobility anchor	Configure a WLAN Profile For Guest Access with Local Web Authentication in CLI	Passed	
EWLCJ176_2S_SR_74	eWLC doc: single authentication support with mobility anchor	to Configure a WLAN Profile for Guest Access with Central Web Authentication (GUI)	Passed	
EWLCJ176_2S_SR_75	The local authentication behaviour in the document is incorrect	to Enable local authentication for a Flex Connect AP Group in UI mode of WLC	Failed	CSCvy29392

EWLCJ176_2S_SR_76	The local authentication behaviour in the document is incorrect	to Enable local authentication for a Flex Connect AP Group in cli mode of WLC	Passed	
EWLCJ176_2S_SR_77	The local authentication behaviour in the document is incorrect	to Enable local authentication for a Flex Connect AP Group in EWLC	Passed	
EWLCJ176_2S_SR_78	The local authentication behaviour in the document is incorrect	Configuring Application Visibility and Control for Flex Connect (GUI)	Passed	
EWLCJ176_2S_SR_79	The local authentication behaviour in the document is incorrect	Configuring Application Visibility and Control for Flex Connect (CLI)	Passed	
EWLCJ176_2S_SR_80	Checking any duplex mismatch error in 9200 switch when connecting 4800 AP	Verifying any duplex mismatch error is generating in switch when connecting 4800 AP	Passed	
EWLCJ176_2S_SR_81	Checking any duplex mismatch error in 9200 switch when connecting 9105 AP after changing port to full duplex	Verifying any duplex mismatch error is generating in switch when connecting 9105 AP after changing port to full duplex	Passed	
EWLCJ176_2S_SR_82	Checking any duplex mismatch error in 9500 switch when connecting 9120 AP after changing port to full duplex	Verifying any duplex mismatch error is generating in switch when connecting 9120 AP after changing port to full duplex	Passed	
EWLCJ176_2S_SR_83	Checking any duplex mismatch error in 9400 switch when connecting 9120 AP after changing port to full duplex	Verifying any duplex mismatch error is generating in switch when connecting 9120 AP after changing port to full duplex	Passed	

EWLCJ176_2S_SR_84	Configuring 802.11r WLAN in eWLC having 9105 AP and passing traffic to client for 24 hours and check for any memory leaks or crash	To configuring 802.11r WLAN in eWLC having 9105 AP connecting a client and passing traffic for 24 hours and check the behaviour of the client and verify if any memory leak or crash happens	Passed	
EWLCJ176_2S_SR_85	Configuring 802.11r WLAN in eWLC having 9120 AP and passing traffic to client for 24 hours and check for any memory leaks or crash	To configuring 802.11r WLAN in eWLC having 9120 AP connecting a client and passing traffic for 24 hours and check the behaviour of the client and verify if any memory leak or crash happens	Passed	
EWLCJ176_2S_SR_86	Configuring 802.11r WLAN in eWLC having 9130 AP and passing traffic to client for 24 hours and check for any memory leaks or crash	To configuring 802.11r WLAN in eWLC having 9130 AP connecting a client and passing traffic for 24 hours and check the behaviour of the client and verify if any memory leak or crash happens	Passed	
EWLCJ176_2S_SR_87	Configuring 802.11r WLAN in eWLC having 4800 AP and passing traffic to client for 24 hours and check for any memory leaks or crash	To configuring 802.11r WLAN in eWLC having 4800 AP connecting a client and passing traffic for 24 hours and check the behaviour of the client and verify if any memory leak or crash happens	Passed	

EWLCJ176_2S_SR_88	Validating if the 9120 AP in EWC with 2.4 GHz sends Ack frame to the window client enabling SI	To validating if the 9120 AP in EWC with 2.4 GHz sends Ack frame to the window client enabling SI	Passed	
EWLCJ176_2S_SR_89	Validating if the 9130 AP in EWC with 2.4 GHz sends Ack frame to the window client enabling SI	To validating if the 9130 AP in EWC with 2.4 GHz sends Ack frame to the window client enabling SI	Passed	
EWLCJ176_2S_SR_90	Connecting different client to 9115 AP Joined in eWLC with WLAN security as dot1x enabling SI and capturing wireless packet	To connect different client to 9115 AP Joined in eWLC with WLAN security as dot1x enabling SI and capturing wireless packet to validate the full client authentication	Passed	
EWLCJ176_2S_SR_91	Connecting different client to 9120 AP Joined in eWLC with WLAN security as dot1x enabling SI and capturing wireless packet	To connect different client to 9120 AP Joined in eWLC with WLAN security as dot1x enabling SI and capturing wireless packet to validate the full client authentication	Passed	
EWLCJ176_2S_SR_92	Connecting different client to 9130 AP Joined in eWLC with WLAN security as dot1x enabling SI and capturing wireless packet	To connect different client to 9130 AP Joined in eWLC with WLAN security as dot1x enabling SI and capturing wireless packet to validate the full client authentication	Passed	
EWLCJ176_2S_SR_93	Configure with a ip server and hostname server with domain name lookup enabled	To Configure with a ip server and hostname server with domain name lookup enabled	Passed	

EWLCJ176_2S_SR_94	Configure with a ip server and two hostname server	To Configure with a ip server and two hostname server	Passed	
EWLCJ176_2S_SR_95	Configure with a ip server and NTP address	To Configure with a ip server and with NTP IP address	Passed	
EWLCJ176_2S_SR_96	Configure with two NTP servers with stratum level set	To Configure with two dns one hostname and one ip	Passed	
EWLCJ176_2S_SR_97	Apply default tags for AP and verify it is displayed in AP	To configure default tags for AP and verify it is displayed in AP	Passed	
EWLCJ176_2S_SR_98	Configure new tags and verify created tags are shown in AP	To configure tags for AP and verify it is displayed in AP	Passed	
EWLCJ176_2S_SR_99	Verify tags after reload	To configure and verify tags after AP and WLC reload	Passed	
EWLCJ176_2S_SR_100	Set AP tag Priority and verify AP tags are set based on priority	To configure AP Tag priority and verify tags are set based on priority	Passed	
EWLCJ176_2S_SR_101	Enable Clean air for 2.4 Ghz	To Enable Clean air for 2.4 Ghz	Passed	
EWLCJ176_2S_SR_102	Enable Clean air for 5.4 Ghz	To Enable Clean air for 5.4 Ghz	Passed	
EWLCJ176_2S_SR_103	Enable Event driven clean air RRM	To Enable Event driven clean air RRM	Passed	
EWLCJ176_2S_SR_104	Configure interference reporting for Clean air for 2.4ghz	To Configure interference reporting for Clean air	Passed	
EWLCJ176_2S_SR_105	Configure interference reporting for Clean air for 5ghz	To Configure interference reporting for Clean air for 5ghz	Passed	
EWLCJ176_2S_SR_106	Verify client connectivity for AP's in 5Ghz	To verify client connectivity Cat9100 series AP	Passed	

EWLCJ176_2S_SR_107	Verify client connectivity for AP's in 2.4ghz	Verify client connectivity for AP's in 5ghz	Passed	
EWLCJ176_2S_SR_108	Validate if the data clean-up job deletes the data except for data retention info in PI 3.8	Validate if the data clean-up job deletes the data except for data retention info in PI 3.8	Passed	
EWLCJ176_2S_SR_109	Validate if the data clean-up job deletes the data except for data retention info in PI 3.9	Validate if the data clean-up job deletes the data except for data retention info in PI 3.9	Passed	
EWLCJ176_2S_SR_110	Check reachable AP data is populated upon device addition to PI 3.8	To check reachable AP data is populated upon device addition to PI 3.8	Passed	
EWLCJ176_2S_SR_111	Check reachable AP data is populated upon device addition to PI 3.9	To check reachable AP data is populated upon device addition to PI 3.9	Passed	
EWLCJ176_2S_SR_112	Check reachable AP data is populated upon manual device addition to PI	To check reachable AP data is populated upon manual device addition to PI	Passed	
EWLCJ176_2S_SR_113	Check the client connectivity with AP in flex local mode	To check the client connectivity with AP in flex local mode	Passed	
EWLCJ176_2S_SR_114	Check the android client connectivity with AP in flex local mode	To check the client connectivity with AP in flex local mode	Passed	
EWLCJ176_2S_SR_115	Check the MAC client connectivity with AP in flex local mode	To check the client connectivity with AP in flex local mode	Passed	
EWLCJ176_2S_SR_116	Check the client connectivity with AP in flex local mode and AP roaming to secondary controller	To check the client connectivity with AP in flex local mode and AP roaming to secondary controller	Passed	

EWLCJ176_2S_SR_117	Check if rogue AP stats show own associated AP's with controller	To check if rogue AP stats show own associated AP's with controller	Passed	
EWLCJ176_2S_SR_118	Check if rogue AP stats show own associated 9130 AP's with controller	To check if rogue AP stats show own associated AP's with controller	Passed	
EWLCJ176_2S_SR_119	Check if rogue AP stats show own associated 9120 AP's with controller	To check if rogue AP stats show own associated AP's with controller	Passed	
EWLCJ176_2S_SR_120	Check if rogue AP stats show own associated 9105 AP's with controller	To check if rogue AP stats show own associated AP's with controller	Passed	
EWLCJ176_2S_SR_121	Check if rogue AP stats show own associated 4800 AP's with controller	To check if rogue AP stats show own associated AP's with controller	Passed	
EWLCJ176_2S_SR_122	Check if 9800L controller initializes with one master port interface	To check if 9800L controller initializes with one master port interface	Passed	
EWLCJ176_2S_SR_123	Check if 9800CL controller initializes with one master port interface	To check if 9800CL controller initializes with one master port interface	Passed	
EWLCJ176_2S_SR_124	Check if 9800-80/40 controller initializes with one master port interface	To check if 9800-80/40 controller initializes with one master port interface	Passed	
EWLCJ176_2S_SR_125	Check if the 4800 AP is able to reach default gateway and IP is assigned via DHCP	To check if the AP is able to reach default gateway and IP is assigned via DHCP	Passed	
EWLCJ176_2S_SR_126	Check if the 9120 AP is able to reach default gateway and IP is assigned via DHCP	To check if the AP is able to reach default gateway and IP is assigned via DHCP	Passed	

EWLCJ176_2S_SR_127	Check if the 9130 AP is able to reach default gateway and IP is assigned via DHCP	To check if the AP is able to reach default gateway and IP is assigned via DHCP	Passed	
EWLCJ176_2S_SR_128	Check if the 9105 AP is able to reach default gateway and IP is assigned via DHCP	To check if the AP is able to reach default gateway and IP is assigned via DHCP	Passed	
EWLCJ176_2S_SR_129	Clear the Job using CLI	Verify the messgses cleared or not using CLI	Passed	
EWLCJ176_2S_SR_130	Clear the job messages using GUI	Verify the messgses cleared or not using UI	Passed	
EWLCJ176_2S_SR_131	Configuring 11ax Access Points, Channel width, OFDMA & radio parameters for 5Ghz band.	Verify the crash happen while configue 11ax Access Points, Channel width, OFDMA & radio parameters for 5Ghz band.	Passed	
EWLCJ176_2S_SR_132	Modify the radio parameter	to check crash happen or not while modify the radio parameters	Passed	
EWLCJ176_2S_SR_133	checking 9120 ap boot status ,led status ,console output ap powered by either of AC adapter, PoE switch, or Power Injector.	Verify the status in ap while power up in 9120 ap	Passed	
EWLCJ176_2S_SR_134	checking 9130 ap boot status ,led status ,console output ap powered by either of AC adapter, PoE switch, or Power Injector.	Verify the status in ap while power up in 9130 ap	Passed	

EWLCJ176_2S_SR_135	checking 9115 ap boot status ,led status ,console output ap powered by either of AC adapter, PoE switch, or Power Injector.	Verify the status in ap while power up in 9115 ap	Passed	
EWLCJ176_2S_SR_136	checking 9105 ap boot status ,led status ,console output ap powered by either of AC adapter, PoE switch, or Power Injector.	Verify the status in ap while power up in 9105 ap	Passed	
EWLCJ176_2S_SR_137	Verfying BSSID on 3800/4800 ap's	Check Ap sending BSSID properly or not	Passed	
EWLCJ176_2S_SR_138	Verifying BSSID on 9120/9130/9115/9105 Ap's	Check Ap sending BSSID properly or not	Passed	

Related Documentation

Related Documentation

Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-5/config-guide/b_wl_17_5_cg.html

Cisco Catalyst 9800 Series Wireless Controller 17.5 Configuration Guide

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-5/config-guide/b_wl_17_5_cg.html

Cisco Catalyst 9800 Series Wireless Controller 17.5 Release Notes

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-5/release-notes/rn-17-5-9800.html

Release Notes for Cisco Digital Network Architecture Spaces

https://www.cisco.com/c/en/us/td/docs/wireless/cisco-dna-spaces/release-notes/cisco-dnaspaces-mar21.html

Cisco Catalyst 9600 Series Switches 17.5 Release Notes

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9600/software/release/17-5/release_notes/ol-17-5-9600.html

Release Notes Cisco Digital Network Architecture Center

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/%20dna-center/2-1-2/release_notes/b_cisco_dna_center_rn_2_1_2.html

PI 3.9 User Guide

https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-9/user/guide/bk_CiscoPrimeInfrastructure_3_9_0_UserGuide.html

ISE 3.0 Release Notes

https://www.cisco.com/c/en/us/td/docs/security/ise/3-0/release_notes/b_ise_30_rn.html