Test Results Summary for Cisco Wireless LAN Controller AireOS 8.0MR2 for Japan (Release Version AireOS 8.0.120.0)

First Published: September 03, 2015

Last Modified: September 08, 2015

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

Text Part Number:

© 2015 Cisco Systems, Inc. All rights reserved.

CONTENTS

CHAPTER 1 **Overview** 1

Cisco Wireless LAN Solution Test 1

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

Test Topology 8

Environment Matrix 8

What's New ? 10

Open Caveats 10

Resolved Caveats 11

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

CMX - Facebook WiFi 13

CMX Visitor Management 14

MSE HA 18

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

L3 Security 22

L2 Security 22

NCS Maps 23

Autonomous to LWAPP Migration 23

Link Aggregation Mode 23

High Availability 24

Roaming 25

AAA 26

Flexconnect Enhancements 27

H-REAP Fault tolerance 28

Dot1x and WEB-Auth Support 28

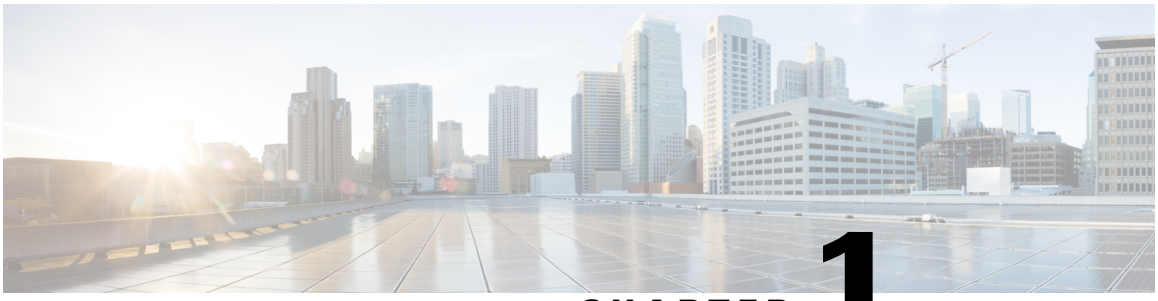
Multiple RADIUS Server Per SSID 29

Secure FTP 30
Backup and Restore 31
NBAR 31
HTTPS Support for Web-Auth 32
AVC Engine 34
AAA Override 35
Flexconnect Upgrade time reduction 35
11ac CCX Lite 37
3700 AP 38
2700 Autonomous AP 39
SSID Filtering 40
Flexconnect on Mesh 40
SR Test Cases 41

CHAPTER 5 SR/CFD Test cases 43
SR/CFD 43

CHAPTER 6 Adhoc Test cases 49
Adhoc Test cases 49

CHAPTER 7 Related Documentation 51
Related Documentation 51



CHAPTER 1

Overview

- Cisco Wireless LAN Solution Test, page 1

Cisco Wireless LAN Solution Test

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

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

- New features in 8.0MR2
- Customer found defects in selected wireless products
- High priority scenarios and basic regression features
- Inputs from Cisco SEs/ TAC

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

The following products are covered in the test execution:

- Cisco Wireless LAN Controller 5508
- Cisco Wireless LAN Controller 2500
- Cisco Wireless LAN Flex Controller 7500
- Cisco Wireless LAN Flex Controller 8500
- Cisco Catalyst 3850 Switch
- WiSM2 Controller
- Virtual Controller
- Access Point 3500

- Access Point 1700
- Access Point 3600
- Access Point 3700
- Access Point 2600
- Access Point 1530
- Access Point 1550
- Access Point 1600
- Access Point 2700
- Access Point 1570
- Access Point 702
- Cisco OEAP 602
- Cisco Prime Network Control System
- Cisco Prime Infrastructure
- ISE Virtual Appliance
- Cisco Secure ACS
- Cisco Mobility Service Engine (MSE)

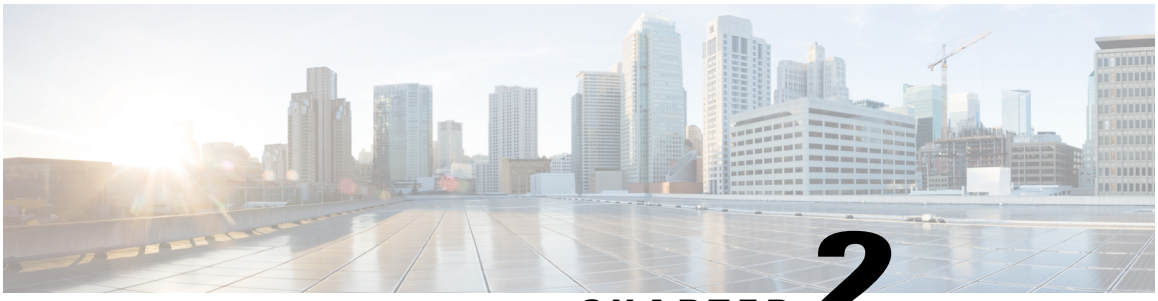
Acronyms

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

Acronym	Description
CCN	Channel Change Notification
CCX	Cisco Compatible Extensions
CDP	Cisco Discovery Protocol
CKIP	Cisco Key Integrity Protocol
CMX	Connected Mobile Experience
CVBF	Cisco Vector Beam Forming
CWA	Central Web Authentication
DCA	Dynamic Channel Assignment
DMZ	Demilitarized Zone
DNS	Domain Name System
DTIM	Delivery Traffic Indication Map
DSCP	Differentiated Services Code Point
DTLS	Datagram Transport Layer Security
EAP	Extensible Authentication Protocol
EULA	End User Licence Agreement
FLA	Flex Local Authentication
FLS	Flex Local Switching
FT	Fast Transition
FTP	File Transfer Protocol
FW	Firm Ware
HA	High Availability
H-REAP	Hybrid Remote Edge Access Point
IOS	Internetwork Operating System
ISE	Identity Service Engine
LAG	Link Aggregation
LEAP	Lightweight Extensible Authentication Protocol
LSS	Location Specific Services
LWAPP	Lightweight Access Point Protocol
MAP	Mesh Access Point
MCS	Modulation Coding Scheme
MFP	Management Frame Protection

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

Acronym	Description
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
WiSM	Wireless Service Module
WLAN	Wireless LAN
WLC	Wireless LAN Controller
WPA	Wi-Fi Protected Access



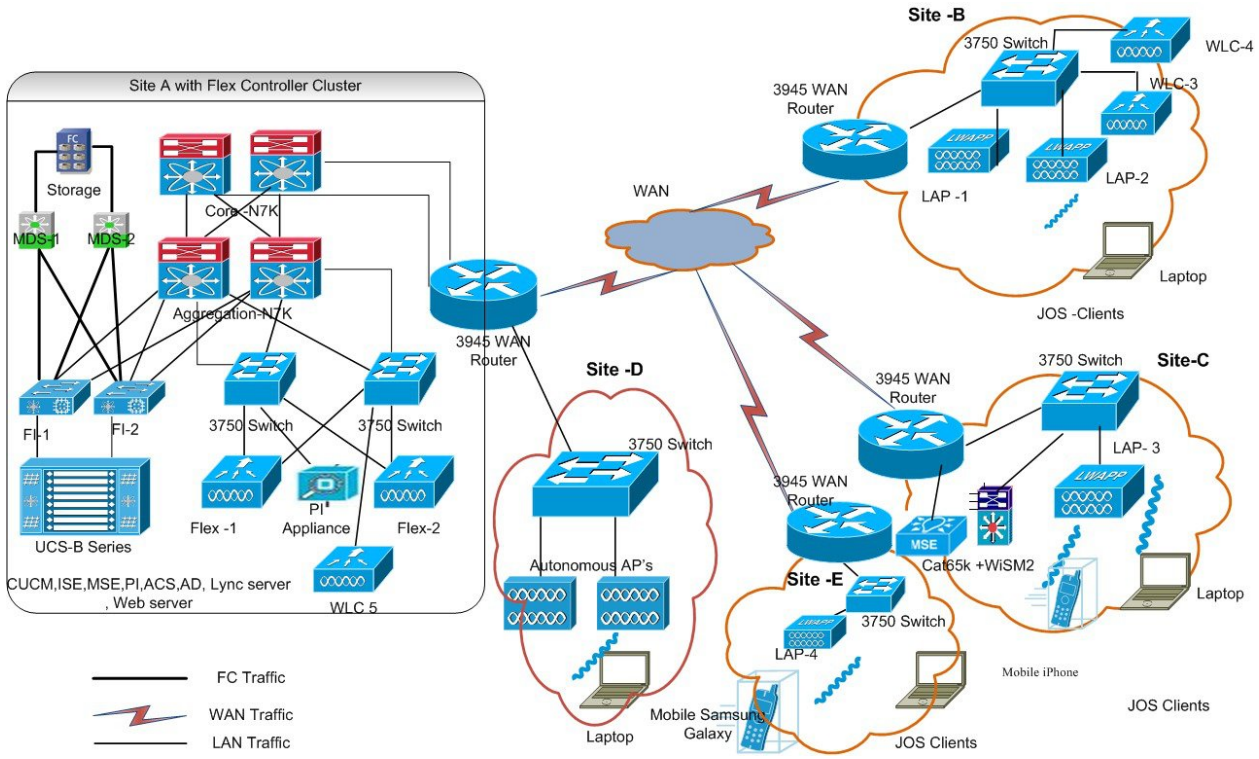
CHAPTER 2

Test Topology and Environment Matrix

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

Test Topology

Figure 1: Topology In Use



Environment Matrix

Category	Component	Version
Controller	Wireless LAN controller 5508	8.0.120.0
	Flex Controller 7500	8.0.120.0
	Wireless LAN Controller 2500	8.0.120.0
	Wireless LAN Controller 8500	8.0.120.0
	WiSM2	8.0.120.0
	Virtual controller	8.0.120.0

Category	Component	Version
Application	PI (Physical (UCS), VM)	2.2.0.0.158
	ISE(VM)	1.3
	Secure ACS (VM)	5.5.0.46
	MSE (Physical, VM)	8.0.120.0
	CMX (Physical (3365), VM)	10.1.2
	Cisco Jabber for Windows	11.0(1)
	Cisco Jabber for iPhone	11.0(1)
	MS Lync Client 2013	15.0
Call control	Cisco Unified Communications Manager	10.5.1-10000-7/10.5.1.1000-1(JP)
Access Point	Cisco AP 3500	15.3
	Cisco AP 3600	15.3
	Cisco AP 3700	15.3
	Cisco AP 2600	15.3
	Cisco AP 2700	15.3
	Cisco AP 1600	15.3
	Cisco AP 1700	15.3
	Cisco OEAP 602	15.3
	Cisco AP 702I	15.3
	Cisco AP 702W	15.3
	Cisco AP 1550	15.3
	Cisco AP 1530	15.3
	Cisco AP 1570	15.3
Switch	Cisco 3750V2 switch	15.0(2)SE2
	Cisco Cat 6509-E	15.1(1)SY1
	Cisco Cat 3850	03.07.01E
Chipset	5300, 6300 AGN	15.13.0.2
	Airport Extreme	7.7
	7260 AGN	17.16.1.2

Category	Component	Version
Client	Operating System(JOS)	Windows 7 Enterprise
		Windows 8 Enterprise
		Windows 8.1 Enterprise
		Windows XP Professional
	Apple Mac Book Pro (JP Locale)	Mac OS 10.10.4
	iPhone 5(JP Locale)	iOS 8.1.2(12B440)
	iPhone 6(JP Locale)	iOS 8.1.2(12B440)
	Samsung Galaxy S-II and S4	Android 4.3
	Wireless IP Phone 7925G	1.4.5.3
Active Directory	AD	Windows 2008R2Enterprise
Browsers	IE	9,10,11
	Opera	11.5
	Mozilla Firefox	40.0.3
	Safari	7.1.3
	Chrome	45.0

What's New ?

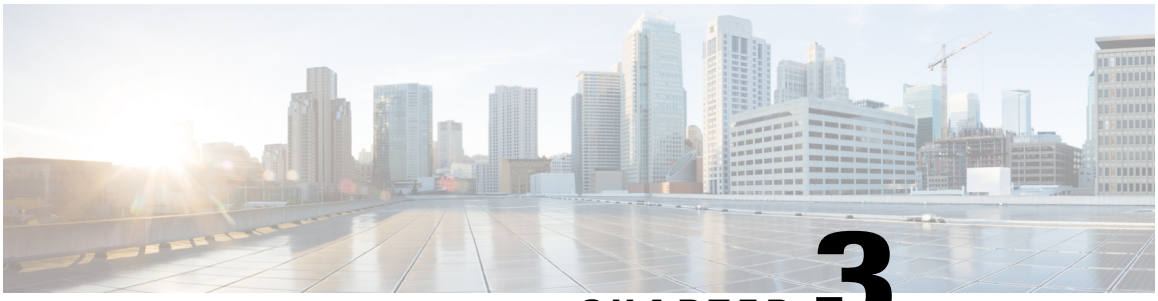
- CMX-Facebook Wifi
- CMX Visitor Connect
- MSE HA

Open Caveats

Defect ID	Title
CSCuv29025	Configuring Mobility domain name in UTF-8 character
CSCuv13395	Create a flexconnect group in WLC GUI
CSCuv30652	Enabling HTTPS redirection option in WLC GUI
CSCuv51964	Checking the search Filter options in WLAN page using UTF-8 character
CSCuq94587	Creating EAP profile name in UTF-8 character
CSCuv91244	Checking the Interface count entries in WLC GUI

Resolved Caveats

Defect ID	Title
CSCuv16895	Checking the MAP count in show mesh ap summary CLI command
CSCuv44023	Create a local policy in UTF - 8 characters
CSCuv79155	Checking the ARP timeout value in WLC GUI and CLI



CHAPTER 3

New Features - Test Summary

- CMX - Facebook WiFi, page 13
- CMX Visitor Management, page 14
- MSE HA, page 18

CMX - Facebook WiFi

Logical ID	Title	Description	Status	Defects
WLJ80MR2S_FB_WiFi_1	Redirection to Facebook Page	To verify redirection to facebook page for logging in is successful or not	Passed	
WLJ80MR2S_FB_WiFi_2	Authentication using facebook credentials	To verify successful authentication using facebook credentials	Passed	
WLJ80MR2S_FB_WiFi_3	Authentication using WiFi Code	To verify successful authentication using WiFi Code	Passed	
WLJ80MR2S_FB_WiFi_4	Get WiFi access using Skip-check-in	To verify whether user getting free wifi access using Skip check-in	Passed	
WLJ80MR2S_FB_WiFi_5	Restricting free internet access for unauthenticated Windows client	To verify denial of internet access for unauthenticated Windows users is successful or not	Passed	
WLJ80MR2S_FB_WiFi_6	Restricting free internet access for unauthenticated Android clients	To verify denial of internet access for unauthenticated Android users is successful or not	Passed	

WLJ80MR2S_FB_WiFi_7	Restricting free internet access for unauthenticated iOS clients	To verify denial of internet access for unauthenticated iOS users is successful or not	Passed	
WLJ80MR2S_FB_WiFi_8	Http Redirection for Continuing Browsing in iOS	To Verify Redirection to the Http page initially requested by the iOS user is successful or not	Passed	
WLJ80MR2S_FB_WiFi_9	Http Redirection for Continuing Browsing in Android Phone	To Verify Redirection to the Http page initially requested by the Android user is successful or not	Passed	
WLJ80MR2S_FB_WiFi_10	Https Redirection for Continuing Browsing in Windows Laptop	To Verify Redirection to the Https page initially requested by the Windows Laptop user is successful or not	Passed	
WLJ80MR2S_FB_WiFi_11	Setup the WiFi session length and check using Windows user	To verify whether the windows user not getting wifi access after session length time expires	Passed	
WLJ80MR2S_FB_WiFi_12	Setup the WiFi session length and check using Android user	To verify whether the Android user not getting wifi access after session length time expires	Passed	
WLJ80MR2S_FB_WiFi_13	Setup the WiFi session length and check using iOS user	To verify whether the iOS user not getting wifi access after session length time expires	Passed	
WLJ80MR2S_FB_WiFi_14	Show Logs tab	To Verify successful download of each individual log file listed in the show logs tab	Passed	
WLJ80MR2S_FB_WiFi_16	KNOWN Users	To verify whether authenticated users are listed in the user data tab or not	Passed	

CMX Visitor Management

Logical ID	Title	Description	Status	Defects

WLJ80MR2S_CMX_Visitor_01	Creating Template Fields in CMX Connect and Engage UI	To verify created New Template Field is listed in the Splash Templates Tab or not	Passed	
WLJ80MR2S_CMX_Visitor_02	Editing Template Fields in CMX Connect and Engage UI	To verify whether Editing the existing Template Field in CMX Connect and Engage UI is successful or not	Passed	
WLJ80MR2S_CMX_Visitor_03	Deleting Template Fields in CMX Connect and Engage UI	To verify whether Deleting the existing Template Field in CMX Connect and Engage UI is successful or not	Passed	
WLJ80MR2S_CMX_Visitor_04	Creating Social Connectors in CMX Connect and Engage UI	To verify created New Social Connector is listed in the Splash Templates Tab or not	Passed	
WLJ80MR2S_CMX_Visitor_05	Editing Social Connectors in CMX Connect and Engage UI	To verify whether Editing the existing Social Connectors in CMX Connect and Engage UI is successful or not	Passed	
WLJ80MR2S_CMX_Visitor_06	Deleting Social Connectors in CMX Connect and Engage UI	To verify whether Deleting the existing Social Connectors in CMX Connect and Engage UI is successful or not	Passed	
WLJ80MR2S_CMX_Visitor_07	Creating Splash Templates in CMX Connect and Engage UI	To verify creation of New Splash Template is successful or not	Passed	
WLJ80MR2S_CMX_Visitor_08	Editing Splash Templates in CMX Connect and Engage UI	To verify Editing the existing Splash Template is successful or not	Passed	
WLJ80MR2S_CMX_Visitor_09	Deleting Splash Templates in CMX Connect and Engage UI	To verify Deleting the existing Splash Template is successful or not	Passed	
WLJ80MR2S_CMX_Visitor_10	Splash Templates assigned to the Social Connectors	To verify displaying of Splash Templates assigned to the Social Connectors is successful or not	Passed	

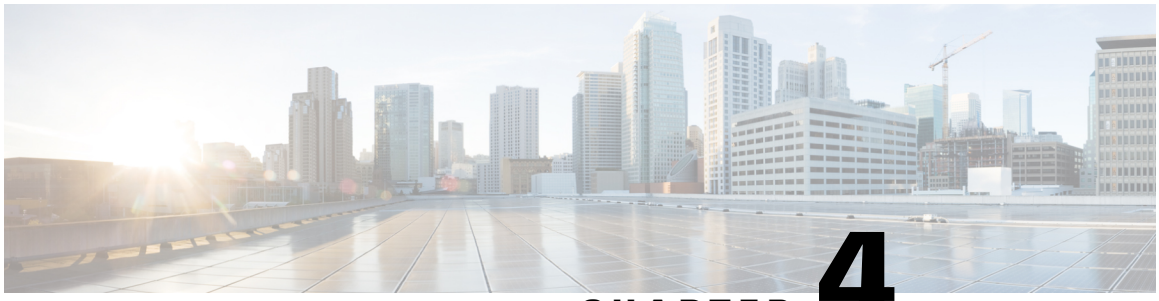
WLJ80MR2S_CMX_Visitor_11	Assigning a Splash Template to a floor	To verify assignation of Splash Template to a Floor is successful or not	Passed	
WLJ80MR2S_CMX_Visitor_12	Network Usage Graph	To verify whether the network usage is correctly calculated and updated in the graph or not	Passed	
WLJ80MR2S_CMX_Visitor_13	Classifying Visitors by setting time interval	To verify whether the visitors are classified according to the selected time filter or not	Passed	
WLJ80MR2S_CMX_Visitor_14	Classifying Visitors by setting location	To verify whether the visitors are classified according to the selected location filter or not	Passed	
WLJ80MR2S_CMX_Visitor_15	Statistics Retention Period	To verify whether the statistics are purged or not from the data store after the statistics Retention Period is expired	Passed	
WLJ80MR2S_CMX_Visitor_16	User Retention Period	To verify whether the users are removed or not from the data store after the User Retention Period is expired	Passed	
WLJ80MR2S_CMX_Visitor_17	Custom Portal Post Auth URL	To verify whether Custom Portal Post Auth URL works as expected	Passed	
WLJ80MR2S_CMX_Visitor_18	Resetting Custom Portal Post Auth URL	To verify whether Custom Portal Post Auth URL could be reset or not	Passed	
WLJ80MR2S_CMX_Visitor_19	"Global Dashboard Today's View"	To verify whether New and Repeat visitor's count is shown in today's view	Passed	
WLJ80MR2S_CMX_Visitor_20	Data Usage in dashboard	To verify whether data usage statistics (upload/Download) are shown or not as expected	Passed	
WLJ80MR2S_CMX_Visitor_21	Repeated Windows 7 Visitors	To verify whether repeated Windows 7 Visitors are displayed in the CMX Connect and Engage UI or not	Passed	

WLJ80MR2S_CMX_Visitor_22	Repeated Apple Macbook Visitors	To verify whether repeated Apple Macbook Visitors are displayed in the CMX Connect and Engage UI or not	Passed	
WLJ80MR2S_CMX_Visitor_23	Repeated Apple iPhone Visitors	To verify Whether repeated Apple iPhone Visitors are displayed in the CMX Connect and Engage UI or not	Passed	
WLJ80MR2S_CMX_Visitor_24	Repeated Samsung S4 mobile Visitors	To verify whether repeated Samsung S4 mobile Visitors are displayed in the CMX Connect and Engage UI or not	Passed	
WLJ80MR2S_CMX_Visitor_25	Active Windows 7 Visitors	To verify whether active Windows 7 Visitors are displayed in the CMX Connect and Engage UI or not	Passed	
WLJ80MR2S_CMX_Visitor_26	Active Apple Macbook Visitors	To verify whether active Apple Macbook Visitors are displayed in the CMX Connect and Engage UI or not	Passed	
WLJ80MR2S_CMX_Visitor_27	Active Apple iPhone Visitors	To verify whether active Apple iPhone Visitors are displayed in the CMX Connect and Engage UI or not	Passed	
WLJ80MR2S_CMX_Visitor_28	Active Samsung S4 mobile Visitors	To verify whether active Samsung S4 mobile Visitors are displayed in the CMX Connect and Engage UI or not	Passed	
WLJ80MR2S_CMX_Visitor_29	Classifying Visitor's Graph based on different time lapse	To verify whether Visitor graphs appear based on the selected time period lapse	Passed	
WLJ80MR2S_CMX_Visitor_30	Exporting Visitors as CSV	To verify whether Visitors log can be exported as CSV file or not	Passed	

MSE HA

Logical ID	Title	Description	Status	Defects
WLJ80MR2S_MSE_HA_01	Pairing of 2 MSEs for HA using PI	To verify the pairing of 2 MSEs for HA setup	Passed	
WLJ80MR2S_MSE_HA_02	Failover in case of primary failure-Automatic	To verify whether secondary MSE take over the place when primary fails where the failover type is configured as "Automatic"	Passed	
WLJ80MR2S_MSE_HA_03	Failover in case of primary failure-Manual	To verify whether secondary MSE take over the place when primary fails by trigerring the failover where the failover type is configured as "Manual"	Passed	
WLJ80MR2S_MSE_HA_04	Manual failover in case of Network failure	To verify the manual failover to the secondary in case of NW failure	Passed	
WLJ80MR2S_MSE_HA_05	Automatic failover in case of Network failure	To verify the failover to the secondary MSE in case of primary failure due to network outage	Passed	
WLJ80MR2S_MSE_HA_06	Manual failover in case of HW failure	To verify the failover in case of primary HW failure	Passed	
WLJ80MR2S_MSE_HA_07	Automatic failover in case of HW failure	To verify the failover in case of primary HW failure	Passed	
WLJ80MR2S_MSE_HA_08	Manual failback in case of primary Active	To verify the manual failback once the primary is up	Passed	
WLJ80MR2S_MSE_HA_09	Automatic failback in case of primary Active	To verify the automatic failback to primary MSE once the application is up	Passed	
WLJ80MR2S_MSE_HA_10	Manual Failback where primary MSE is RMAed	To verify the failback functionality to the newly installed primary MSE	Passed	

WLJ80MR2S_MSE_HA_12	Addition of license to the primary	To verify the addition of license to the primary appliance	Passed	
WLJ80MR2S_MSE_HA_13	Deletion of license from the primary	To verify the deletion of license to the primary appliance	Passed	



CHAPTER 4

Regression Features - Test Summary

- L3 Security, page 22
- L2 Security, page 22
- NCS Maps, page 23
- Autonomous to LWAPP Migration , page 23
- Link Aggregation Mode, page 23
- High Availability, page 24
- Roaming, page 25
- AAA, page 26
- Flexconnect Enhancements, page 27
- H-REAP Fault tolerance, page 28
- Dot1x and WEB-Auth Support, page 28
- Multiple RADIUS Server Per SSID, page 29
- Secure FTP, page 30
- Backup and Restore, page 31
- NBAR, page 31
- HTTPS Support for Web-Auth, page 32
- AVC Engine, page 34
- AAA Override, page 35
- Flexconnect Upgrade time reduction, page 35
- 11ac CCX Lite, page 37
- 3700 AP, page 38
- 2700 Autonomous AP, page 39
- SSID Filtering, page 40
- Flexconnect on Mesh, page 40

• SR Test Cases, page 41

L3 Security

Logical ID	Title	Description	Status	Defects
WLJ80MR2S_L3_01	Configuring Customized(Downloaded) web-auth using NCS	To check the Customized(Downloaded) web-auth configuration in NCS reflects in WLC.	Passed	
WLJ80MR2S_L3_02	CT2500: Customized(Downloaded) login page for the controller.	To verify the successful customized web login page with Internal Authentication.	Passed	
WLJ80MR2S_L3_03	CT2500: Download customized login page for the controller.	To verify the customized web login page bundle is downloaded successfully.	Passed	
WLJ80MR2S_L3_04	Customized web auth login page for the controller-Laptop	To verify the successful customized web login page with internal authentication	Passed	
WLJ80MR2S_L3_05	Downloading the customized login page	To verify the successful download of customized login page	Passed	
WLJ80MR2S_L3_06	Customized web login page for the controller	To verify the successful customized web login page with internal authentication	Passed	

L2 Security

Logical ID	Title	Description	Status	Defects

WLJ80MR2S_L2_07	Associating 7925G IP phone – WPA	To check whether the 7925G ip phone is associated successfully into the network through WPA authentication method	Passed	
WLJ80MR2S_L2_08	Authentication for the association of clients-WPA in 8500 / 7500 WLC	Checking for the Authentication of the clients when connected to an AP - 8500 / 7500 WLC.	Passed	
WLJ80MR2S_L2_09	Authentication for the association of clients-WPA in Virtual WLC	Checking for the Authentication of the clients when connected to an AP - Virtual WLC.	Passed	
WLJ80MR2S_L2_10	Authentication for the association of clients-WPA in 5508 / 2504 /WiSM2	Checking for the Authentication of the clients when connected to an AP - 5508 / 2504 / WiSM2	Passed	

NCS Maps

Logical ID	Title	Description	Status	Defects
WLJ80MR2S_MAP_11	Copy & Replace AP-Map	To verify the successful copy & replace	Passed	

Autonomous to LWAPP Migration

Logical ID	Title	Description	Status	Defects
WLJ80MR2S_Migration_12	Autonomous to LWAPP Migration	To migrate the autonomous AP to LWAPP using archive command in AAP CLI.	Passed	

Link Aggregation Mode

Logical ID	Title	Description	Status	Defects

WLJ80MR2S_LAG_13	Enable Link Aggregation on the controller- LAP Local	To verify the Light Weight Access Point Registration/Join status on controller	Passed	
WLJ80MR2S_LAG_14	Enable Link Aggregation on the controller -LAP H-REAP Mode Ports)	To verify the Light Weight Access Point Registration status when one port fails	Passed	
WLJ80MR2S_LAG_15	Client Association with Light Weight Access Point after Link Aggregation failover	To verify the successful association of wireless client with Light Weight Access Point	Passed	
WLJ80MR2S_LAG_16	LAG failover –Ping,FTP (Refer- CSCth12513)	To verify the successful PING,FTP packets during LAG failover	Passed	
WLJ80MR2S_LAG_17	LAG Port status Trap Log with SNMP Manager (Refer: CSCto58101 Delay in Port Up down causes issues with LAG working on WLC	To verify the successful LAG port status message in SNMP manager	Passed	
WLJ80MR2S_LAG_18	Active controller ports status when it is in Link Aggregation (LAG) failover	To check active controller ports status in Link Aggregation failover	Passed	

High Availability

Logical ID	Title	Description	Status	Defects
WLJ80MR2S_HA_19	Bringing HA pair up-WLC 5508	To verify whether the HA pair(ACTIVE:STANDBY) is up successfully	Passed	
WLJ80MR2S_HA_20	Bringing HA pair up-WLC 7500	To verify whether the HA pair(ACTIVE:STANDBY) is up successfully	Passed	
WLJ80MR2S_HA_21	Controller HA pair with different hardware models	To verify the role negotiation between the controllers with different hardware models	Passed	

WLJ80MR2S_HA_22	Controller HA pair with different software versions	To verify the role negotiation between the controllers with different software versions	Passed	
WLJ80MR2S_HA_23	Controller mode when the redundancy port loses connectivity	To verify the HA pair controller modes after disconnecting the redundancy port	Passed	
WLJ80MR2S_HA_24	Controller mode when the Gateway is not reachable to the STANDBY controller	To verify the HA pair controller modes when the Gateway is not reachable from the STANDBY controller	Passed	
WLJ80MR2S_HA_25	Controller mode when the Gateway is not reachable to the ACTIVE controller	To verify the HA pair controller modes when the Gateway is not reachable from the ACTIVE controller	Passed	
WLJ80MR2S_HA_26	Controller mode when the Gateway is not reachable to both the controllers	To verify the HA pair controller modes when the Gateway is not reachable to both the controllers	Passed	
WLJ80MR2S_HA_27	Controller modes(HA pair) after power failure	To verify the controller modes after power failure on both the controllers	Passed	
WLJ80MR2S_HA_28	HA mode after resetting the peer system from ACTIVE	To verify the HA mode after resetting the peer system from ACTIVE controller	Passed	
WLJ80MR2S_HA_29	Client status during AP SSO after active failover-Web Authentication	To check whether the Client gets disassociated and forced to re-join to the controller after AP SSO	Passed	

Roaming

Logical ID	Title	Description	Status	Defects
WLJ80MR2S_11r_30	11r Client Association with AKM PSK – FlexConnect Central Switch	To verify client's initial association to a wlan with 11r enabled with ft-psk AKM Suite in flexconnect central switching	Passed	

WLJ80MR2S_11r_31	11r Client Association with AKM PSK – FlexConnect Local Switch Central Auth	Verify client's initial association to a wlan with 11r enabled with ft-psk AKM Suite in flexconnect local switch central auth	Passed	
WLJ80MR2S_11r_32	Over the Air Intra-controller roaming – flexconnect Central Switch	To verify fast transition client roaming over the air within the same controller in flexconnect central auth.	Passed	
WLJ80MR2S_11r_33	Over the DS Intra-controller roaming – Flexconnect Central Switch VLAN Pooling	Verify fast transition client roaming over the DS within the same controller in flexconnect central switch	Passed	
WLJ80MR2S_11r_34	Open Security Over-the-Air Roaming - controller	Verify open security 11r Over-the-Air Roaming	Passed	
WLJ80MR2S_11r_35	Open Security Over-the-Air Roaming -NCS	Verify open security 11r Over-the-Air Roaming	Passed	
WLJ80MR2S_11r_36	Roaming of wireless data clients within APs of one Flex connect group when controller is Down	To check for the successful and seamless roaming of wireless data clients between APs of same Flex connect group when controller is “Down”	Passed	
WLJ80MR2S_11r_37	Roaming of wireless data clients within APs of one Flex connect group when controller is Up	To check for the successful and seamless roaming of wireless data clients between APs of same Flex connect group when controller is “Up”	Passed	
WLJ80MR2S_11r_38	Roaming of data clients between APs in same Flex connect group	To check for the seamless roaming from one AP to another from the same Flex Connect group	Passed	

AAA

Logical ID	Title	Description	Status	Defects

WLJ80MR2S_AAA_39	Performing MAC Filtering with Clients registered in ACS server- WiSM2 Controller	To check whether registered client is successfully authenticated and associated with WLANs enabled MAC Filtering	Passed	
WLJ80MR2S_AAA_40	Performing MAC Filtering with Clients registered in ACS server- 2500 Controller	To check whether registered client is successfully authenticated and associated with WLANs enabled MAC Filtering	Passed	
WLJ80MR2S_AAA_41	Performing MAC Filtering with Clients registered in ACS server- 7500 Controller	To check whether registered client is successfully authenticated and associated with WLANs enabled MAC Filtering	Passed	

Flexconnect Enhancements

Logical ID	Title	Description	Status	Defects
WLJ80MR2S_FLEX_42	WGB Association, WGB client registration through Flexconnect AP in connected mode.	To verify whether the WGB associates and the clients are registered to the controller through Flexconnect AP.	Passed	
WLJ80MR2S_FLEX_43	WGB Association, WGB client registration through Flexconnect AP in standalone mode	To verify whether the WGB associates and the clients are registered to the controller through Flexconnect AP in standalone mode.	Passed	
WLJ80MR2S_FLEX_44	WGB Association through Local authenticated WLAN.	To verify whether the WGB associates with the flexconnect through local authenticated WLAN	Passed	
WLJ80MR2S_FLEX_45	WGB disassociation from the controller	To verify whether the WGB disassociates from the controller upon deletion	Passed	

WLJ80MR2S_FLEX_46	WGB client deregistration with the flexconnect in standalone mode to connected mode	To verify whether the WGB disassociates from the controller upon deletion	Passed	
WLJ80MR2S_FLEX_47	Flexconnect AP reload in connected mode when WGB is associated-Central auth locally switched	To verify whether WGB and WGB clients re-associates to the controller after flexconnect AP reloads	Passed	
WLJ80MR2S_FLEX_48	Flexconnect AP reload in standalone mode when WGB is associated-Local authentication	To verify whether WGB and WGB clients re-associates to the controller after flexconnect AP reloads	Passed	
WLJ80MR2S_FLEX_49	WGB Clients roaming to a different flexconnect on the same controller	To verify the WGB client reassociates successfully to a different fleconnect after roaming within the controller	Passed	

H-REAP Fault tolerance

Logical ID	Title	Description	Status	Defects
WLJ80MR2S_Fault_50	HREAP fault tolerance between connected and standalone AP-2.4 GHz	To verify whether the client associated to flexconnect AP will get reassociated in case of fault tolerance	Passed	
WLJ80MR2S_Fault_51	HREAP fault tolerance between standalone and connected AP-2.4 GHz	To verify whether the client associated to flexconnect AP will get reassociated in case of fault tolerance	Passed	

Dot1x and WEB-Auth Support

Logical ID	Title	Description	Status	Defects

WLJ80MR2S_Web_52	Authentication of client(Apple Mac Book) with Security Static WEP and Web-Auth –2500,5508, WiSM2 and 7500 Controller.	Checking for the Authentication of the client when connected to a WLAN in which Static WEP and Web-Auth is enabled.	Passed	
WLJ80MR2S_Web_53	Authentication of clients(Apple Mac Book & Win 7) with Security Static WEP+Dot1x and Web-Auth using ISE-2500,5508, WiSM2 and 7500 Controller.	Checking for the Authentication of the clients when connected to a WLAN in which Static WEP+Dot1x and Web-Auth is enabled.	Passed	
WLJ80MR2S_Web_54	Authentication of clients(Apple Mac Book & Win 7) with Security Dot1x using ISE and WebAuth-2500,5508,WiSM2 and 7500 Controller.	Checking for the Authentication of the clients when connected to a WLAN in which Dot1x and Web-Auth is enabled.	Passed	

Multiple RADIUS Server Per SSID

Logical ID	Title	Description	Status	Defects
WLJ80MR2S_RAD_55	Performing Dot1x authentication over PPPoE AP with RADIUS servers configured(Primary)-2500,5508,WiSM2 and 7500 WLC	To verify whether Dot1x authentication can be performed successfully to the clients associated via the Primary RADIUS server over the PPPoE connection with the Vlan mapped	Passed	
WLJ80MR2S_RAD_56	Performing Dot1x authentication over PPPoE AP with RADIUS servers configured(Secondary)-2500,5508,WiSM2 and 7500 WLC	To verify whether Dot1x authentication can be performed successfully to the clients associated via the secondary RADIUS server over the PPPoE connection with the Vlan mapped	Passed	

WLJ80MR2S_RAD_57	Performing Dot1x authentication over PPPoE AP with RADIUS servers configured(Primary failover)- 2500,5508,WiSM2 and 7500 WLC	To verify whether Dot1x authentication can be performed successfully to the clients associated via the secondary RADIUS server over the PPPoE connection with the Vlan mapped	Passed	
WLJ80MR2S_RAD_58	Performing Dot1x authentication over FlexConnect AP with RADIUS servers configured(Primary)- 2500,5508,WiSM2 and 7500 WLC	To verify whether Dot1x authentication can be performed successfully to the clients associated via the Primary RADIUS server over the Flex AP connection with the Vlan mapped	Passed	
WLJ80MR2S_RAD_59	Performing Dot1x authentication over FlexConnect AP with RADIUS servers configured(Secondary)- 2500,5508,WiSM2 and 7500 WLC	To verify whether Dot1x authentication can be performed successfully to the clients associated via the secondary RADIUS server over the Flex AP connection with the Vlan mapped	Passed	
WLJ80MR2S_RAD_60	Performing Dot1x authentication over FlexConnect AP with RADIUS servers configured(Primary failover)- 2500,5508,WiSM2 and 7500 WLC	To verify whether Dot1x authentication can be performed successfully to the clients associated via the secondary RADIUS server over the Flex AP connection with the Vlan mapped	Passed	

Secure FTP

Logical ID	Title	Description	Status	Defects
WLJ80MR2S_SFTP_61	Transfer download of controller image with SFTP method- WLC 5500series , WiSM2 , 2500 series	To verify controller able to download the image using SFTP method and installs properly	Passed	

WLJ80MR2S_SFTP_62	Transfer of controller configuration with SFTP method – WLC 5500 , 2500 , WiSM2.	To verify controller able to download a configuration and upload the current configuration using SFTP transfer method	Passed	
WLJ80MR2S_SFTP_63	Transfer download of controller certificates with SFTP method – WLC Virtual and 7500	To verify controller is able to download all the supported certificates using SFTP transfer method	Passed	
WLJ80MR2S_SFTP_64	SFTP Transfer validation with other configuration items like, path, filename, server ip and port number – All Controllers	Verify controller validates properly the transfer parameters like server ip address, Port number, filename, and path. Transfer is aborted if any of the above configuration parameters are in-correct or server issues – All controllers	Passed	
WLJ80MR2S_SFTP_65	Transfer upload of other data type files with SFTP method - WLC 5500 series , 2500 and WiSM2	To verify controller is able to upload all the other supported data type files using SFTP transfer method- WLC 5500 , 2500 & WiSM2.	Passed	

Backup and Restore

Logical ID	Title	Description	Status	Defects
WLJ80MR2S_BnR_66	Performing Backup and restore in NCS	To verify the NCS successfully done a backup and restore	Passed	

NBAR

Logical ID	Title	Description	Status	Defects

WLJ80MR2S_NBAR_67	Apply an AVC profile with a rule to block an application and check if that application is dropped when tried to open and notification is sent via snmp trap	To verify AVC rule to drop an application works fine	Passed	
WLJ80MR2S_NBAR_68	AVC profile should work fine in AP SSO	To verify if AVC profile works fine after AP SSO	Passed	
WLJ80MR2S_NBAR_69	Application traffic flow from client to AP when AP in local mode and centrally switched flexconnect - 5508,7500 &2500 WLC	To verify the IP traffic flow from client to AP when AP is in local mode and centrally switched flexconnect	Passed	
WLJ80MR2S_NBAR_70	Configuring and verifying custom DSCP value for AVC	To verify if custom DSCP value is configured and applied successfully for a AVC rule	Passed	
WLJ80MR2S_NBAR_71	Bandwidth contract Rate limit applied per-SSID on downstream traffic	To verify if bandwidth contract applied per-SSID on downstream traffic works fine	Passed	
WLJ80MR2S_NBAR_72	Override Per-user bandwidth contract on downstream and upstream traffic	To verify if Override Per-user bandwidth contract on downstream and upstream traffic works fine	Passed	

HTTPS Support for Web-Auth

Logical ID	Title	Description	Status	Defects

WLJ80MR2S_HTTPS_73	Associating two clients(Win 7 & Macbook) to web-auth security and checking the redirection of HTTPS url in both clients in 7500 & 8500 WLC's.	To check whether HTTPS url gets redirected or not to web-auth login page when clients gets connected and browses the internet and also checking the Ping function works or not between them.	Passed	
WLJ80MR2S_HTTPS_74	Associating two clients(Win 7 & Win 8) to web-auth security and checking the redirection of HTTPS url in both clients in 7500 & 8500 WLC's.	To check whether HTTPS url gets redirected or not to web-auth login page when clients gets connected and browses the internet and also checking the Ping function works or not between them.	Passed	
WLJ80MR2S_HTTPS_75	Associating two clients(Win 7 & Win 8) to web-auth security and checking the redirection of HTTPS url in both clients in 5500, 2500 & WiSM2 WLC's.	To check whether HTTPS url gets redirected or not to web-auth login page when clients gets connected and browses the internet and also checking the Ping function works or not between them.	Passed	
WLJ80MR2S_HTTPS_76	Associating two clients(Apple MacBook & Win 8) to web-auth security and checking the redirection of HTTPS url in both clients in 5500, 2500 & WiSM2 WLC's.	To check whether HTTPS url gets redirected or not to web-auth login page when clients gets connected and browses the internet and also checking the Ping function works or not between them.	Passed	
WLJ80MR2S_HTTPS_77	Associating two clients(Iphone 5 & Samsung S4) to web-auth security and checking the redirection of HTTPS url in both clients in 7500 & 8500 WLC's.	To check whether HTTPS url gets redirected or not to web-auth login page when clients gets connected and browses the internet.	Passed	

WLJ80MR2S_HTTPS_78	Associating two clients(Iphone 5 & Samsung S4) to web-auth security and checking the redirection of HTTPS url in both clients in vWLC.	To check whether HTTPS url gets redirected or not to web-auth login page when clients gets connected and browses the internet.	Passed	

AVC Engine

Logical ID	Title	Description	Status	Defects
WLJ80MR2S_AVC_79	Check AVC visibility on upgrade from older release to 8.1 with changing protocol pack in WiSM2 & 5500 WLC's	This is to verify that after upgrade from an older release that supports older AVC engine to 8.1 does not break the basic classification functionality of AVC. The older release will be uploaded with the latest protocol pack 6.0 and then upgraded to 8.1	Passed	
WLJ80MR2S_AVC_80	Check AVC visibility on upgrade from older release to 8.1 with changing protocol pack in 8500 & 7500 WLC's	This is to verify that after upgrade from an older release that supports older AVC engine to 8.1 does not break the basic classification functionality of AVC. The older release will be uploaded with the latest protocol pack 6.0 and then upgraded to 8.1	Passed	
WLJ80MR2S_AVC_81	Check AVC visibility on downgrade from 8.1 to an older release with the latest protocol pack uploaded in 8.1 image in 5500 & 2500 WLC's.	This is to verify that after downgrade from 8.1 to an older release AVC functionality should not break and AVC config maintained across wlans. The 8.1 image by default will have 4.1 AVC protocol pack which will be upgraded to the latest 6.0 protocol pack before downgrading	Passed	

WLJ80MR2S_AVC_82	Check AVC visibility on downgrade from 8.1 to an older release with the latest protocol pack uploaded in 8.1 image in 8500 & 7500 WLC's.	This is to verify that after downgrade from 8.1 to an older release AVC functionality should not break and AVC config maintained across wlans. The 8.1 image by default will have 4.1 AVC protocol pack which will be upgraded to the latest 6.0 protocol pack before downgrading	Passed	
WLJ80MR2S_AVC_83	Verify AVC classifies multiple applications for multiple clients associated to a single WLC 5500	This is to verify that after upgrade to 8.1 multiple applications for multiple clients are classified as expected.	Passed	
WLJ80MR2S_AVC_84	Verify AVC classifies multiple applications for multiple clients associated to a single WLC 8500	This is to verify that after upgrade to 8.1 multiple applications for multiple clients are classified as expected.	Passed	

AAA Override

Logical ID	Title	Description	Status	Defects
WLJ80MR2S_AAA_85	Verify AVC profile AAA override from authentication server when wlan is configured for mac filtering	This is to verify that AVC profile is applied using AAA override from authentication server when the wlan is configured for mac filtering	Passed	
WLJ80MR2S_AAA_86	Check if after re-authentication AVC profile is still applied to the client.	This is to verify that AVC profile is applied using AAA override from authentication server even after session timeout is expired.	Passed	

Flexconnect Upgrade time reduction

Logical ID	Title	Description	Status	Defects

WLJ80MR2S_Flex_Change_87	Client authentication with AP after mode change to flexconnect_Central Switching	To verify whether client has been successfully authenticated after AP mode has been changed to flexconnect with central switching WLAN	Passed	
WLJ80MR2S_Flex_Change_88	Client authentication with AP after mode change to flexconnect_Local Switching, Central auth	To verify whether client has been successfully authenticated after AP mode has been changed to flexconnect with local switching, central auth WLAN	Passed	
WLJ80MR2S_Flex_Change_89	Software upgrade/downgrade	To verify whether the AP retains its flex configuration after software upgrade/downgrade	Passed	
WLJ80MR2S_Flex_Change_90	Intra-Controller roam, local switching WLAN	To verify the roaming within the controller is successful	Passed	
WLJ80MR2S_Flex_Change_91	Inter-Controller roam, central switching WLAN	To verify the inter-controller roaming is successful	Passed	
WLJ80MR2S_Flex_Change_92	AP mode change from local to flexconnect using WLC CLI	To verify whether changing the AP mode from local to flexconnect using WLC CLI is successful without rebooting the AP	Passed	
WLJ80MR2S_Flex_Change_93	AP mode change from local to flexconnect using WLC GUI	To verify whether changing the AP mode from local to flexconnect using WLC GUI is successful without rebooting the AP	Passed	
WLJ80MR2S_Flex_Change_94	Basic flex configuration after AP mode change	To verify whether basic flex configurations have been applied to AP after mode change	Passed	
WLJ80MR2S_Flex_Change_95	Client association with AP in standalone mode and FT	To verify whether client has been associated successfully to AP in standalone mode and fault tolerance	Passed	

WLJ80MR2S_Flex_Change_96	AP reboot in connected/standalone mode, for converted flex AP	To verify whether converted flex AP retains all config when AP is rebooted in connected/standalone mode	Passed	
WLJ80MR2S_Flex_Change_97	Client association with AP reboot in connected/standalone mode	To verify the client association with AP reboot in connected/standalone mode, for AP converted to flex	Passed	
WLJ80MR2S_Flex_Change_98	HA support for mode change	To verify the AP mode change in HA setup, whether AP mode is synched to standby	Passed	
WLJ80MR2S_Flex_Change_99	AP mode change with autoconversion on WLC	To verify the AP mode with autoconversion on WLC	Passed	
WLJ80MR2S_Flex_Change_100	AP mode change for few Aps	To verify whether change of AP mode for few Aps are successful	Passed	
WLJ80MR2S_Flex_Change_101	Mode change from local > flex > local	To verify whether changing the mode from local > flex > local for few times are working properly	Passed	
WLJ80MR2S_Flex_Change_102	Mode change to flexconnect then to submode wIPS	To verify the mode change to flexconnect and then to WIPS	Passed	

11ac CCX Lite

Logical ID	Title	Description	Status	Defects
WLJ80MR2S_11AC_CCX_103	Initial Client association with CCKM enabled-Macbook Pro	To verify the initial client association with CCKM enabled- Macbook Pro	Passed	

WLJ80MR2S_11AC_CCX_104	Fast reauthenctication of 11ac client with CCKM enabled-Samsung S4	To verify the Fast reauthentication of Samsung S4 with CCKM enabled under roaming conditions- Samsung S4	Passed	
WLJ80MR2S_11AC_CCX_105	Fast reauthenctication of 11ac client with CCKM enabled-Macbook Pro	To verify the Fast reauthentication of Samsung S4 with CCKM enabled under roaming conditions- Macbook Pro	Passed	
WLJ80MR2S_11AC_CCX_106	Fast reauthenctication of 11ac client with CCKM enabled-Netgear client	To verify the Fast reauthentication of Samsung S4 with CCKM enabled under roaming conditions- Netgear client	Passed	
WLJ80MR2S_11AC_CCX_107	EAP-FAST dot1x authentication with 11ac client Macbook Pro	To verify EAP-FAST dot1x authentication in 11ac interface-Macbook Pro	Passed	

3700 AP

Logical ID	Title	Description	Status	Defects
WLJ80MR2S_3700AAP_108	Client association with WPA	To check whether client association is successful with WPA	Passed	
WLJ80MR2S_3700AAP_109	Traffic flow between two wireless clients	To check the traffic flow between two wireless clients	Passed	
WLJ80MR2S_3700AAP_110	Client association with AES-CCMP	To check the client association with AES-CCMP	Passed	
WLJ80MR2S_3700AAP_111	Client association with Local radius server	To check the client association with Local radius server	Passed	
WLJ80MR2S_3700AAP_112	Data rates change	To verify the client association after changing the data rates	Passed	

WLJ80MR2S_3700AAP_113	Client association with WEP	To verify client association with WEP	Passed	
WLJ80MR2S_3700AAP_114	WGB Mode	To verify work group bridge mode	Passed	
WLJ80MR2S_3700AAP_115	Autonomous AP management access	To verify autonomous AP management access	Passed	
WLJ80MR2S_3700AAP_116	Monitoring of connected client	To verify the connected client in AP management page	Passed	
WLJ80MR2S_3700AAP_117	Trap logs for connected client	To verify whether trap logs are displayed or not for the clients connected	Passed	
WLJ80MR2S_3700AAP_118	Management users	To verify the management user creation	Passed	
WLJ80MR2S_3700AAP_119	Enabling/Disabling the radio	To verify whether status is reflected or not when radio is enabled/disabled	Passed	
WLJ80MR2S_3700AAP_120	Client association with TKIP	To verify client association with TKIP	Passed	

2700 Autonomous AP

Logical ID	Title	Description	Status	Defects
WLJ80MR2S_2700AAP_121	Client association with WPA	To verify client association is successful or not with WPA	Passed	
WLJ80MR2S_2700AAP_122	WGB Mode	To verify WGB association	Passed	
WLJ80MR2S_2700AAP_123	Autonomous AP management access	To verify the autonomous AP management access	Passed	
WLJ80MR2S_2700AAP_124	Traffic flow between two wireless clients	To verify traffic flow between two wireless clients	Passed	
WLJ80MR2S_2700AAP_125	Trap logs for connected client	To verify the trap logs for connected client	Passed	
WLJ80MR2S_2700AAP_126	Monitoring of connected client	To verify the connected client in AP management page	Passed	

WLJ80MR2S_2700AAP_127	Client Association with WEP	To verify client association is successful or not with WEP	Passed	

SSID Filtering

Logical ID	Title	Description	Status	Defects
WLJ80MR2S_SSID_Filtering_128	SSIDs could be excluded by checking box	To verify whether SSIDs list could be excluded by checking box	Passed	
WLJ80MR2S_SSID_Filtering_129	Clients on excluded SSID list will not show up on MSE DB	To verify whether Clients on excluded SSID list is not shown on MSE DB	Passed	
WLJ80MR2S_SSID_Filtering_130	Configure Maximum SSID on WLC and check if all show up for selection on SSID list	To verify whether Maximum set SSID on WLC which is displayed on the SSID exclusion list.	Passed	
WLJ80MR2S_SSID_Filtering_131	Exclusion list for SSID from multiple WLC	To verify whether Mutiple WLC SSID Filtering Parameters is configurable	Passed	
WLJ80MR2S_SSID_Filtering_132	Client MAC on allowed list but SSID excluded	To verify whether Client MAC allowed but SSID excluded will enable client tracking	Passed	

Flexconnect on Mesh

Logical ID	Title	Description	Status	Defects
WLJ80MR2S_Flex_Mesh_133	AP conversion from Flexconnect to Flex+bridge mode for RAP	To verify whether changing the RAP mode from Flexconnect to Flex+bridge works properly	Passed	

WLJ80MR2S_Flex_Mesh_134	AP conversion from Flexconnect to Flex+bridge mode for MAP	To verify whether changing the MAP mode from Flexconnect to Flex+bridge works properly	Passed	
WLJ80MR2S_Flex_Mesh_135	AP conversion from Flexconnect to Flex+bridge mode for RAP/MAP	To verify whether changing the mode from flexconnect to Flex+bridge works properly for RAP/MAP	Passed	
WLJ80MR2S_Flex_Mesh_136	Show commands for Flex+bridge mode	To verify all the show commands for Flex+bridge mode	Passed	
WLJ80MR2S_Flex_Mesh_137	AP mode after upgrade	To verify whether the AP mode retains after upgrading the WLC to latest software	Passed	
WLJ80MR2S_Flex_Mesh_138	Client status when Flex+bridge AP is in standalone mode	To verify the client status	Passed	

SR Test Cases

Button in Report Launch pad

Logical ID	Title	Description	Status	Defects
WLJ80MR2S_Reg_01	PI: Save/Run button in Report Launch pad	To verify whether "Save", "Run and Save" button is working in Report Launch pad in PI	Passed	

Map Location in Copy and Replace

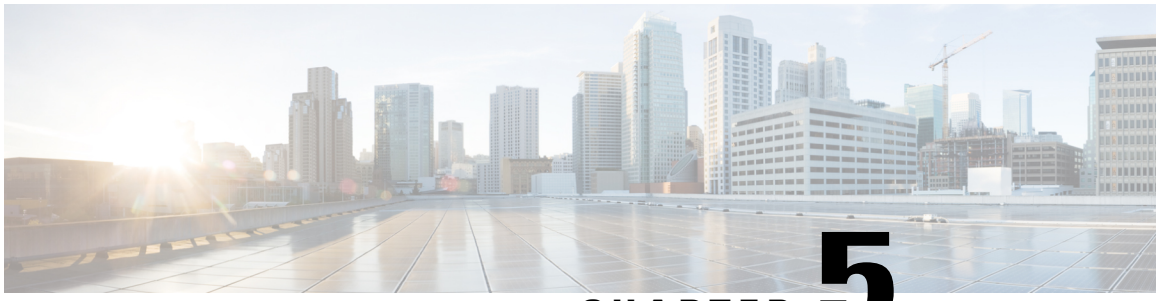
Logical ID	Title	Description	Status	Defects
WLJ80MR2S_Reg_02	Map Location in Copy and Replace	To verify the successful copy and replace with Map Location	Passed	

Upload File

Logical ID	Title	Description	Status	Defects
WLJ80MR2S_Reg_03	CT5508: Controller configuration Upload using TFTP server	To verify whether the configuration upload from a controller is successful	Passed	
WLJ80MR2S_Reg_04	CT7500: Controller configuration Upload using TFTP server	To verify whether the configuration upload from a controller is successful	Passed	
WLJ80MR2S_Reg_05	CT2504: Controller configuration Upload using TFTP server	To verify whether the configuration upload from a controller is successful	Passed	

HREAP

Logical ID	Title	Description	Status	Defects
WLJ80MR2S_Reg_06	HREAP fault tolerance between connected and standalone AP-2.4 GHz	To verify whether the client associated to flexconnect AP will get re-associated in case of fault tolerance	Passed	
WLJ80MR2S_Reg_07	HREAP fault tolerance between standalone and connected AP-2.4 GHz	To verify whether the client associated to flexconnect AP will get re-associated in case of fault tolerance	Passed	



CHAPTER 5

SR/CFD Test cases

- SR/CFD, page 43

SR/CFD

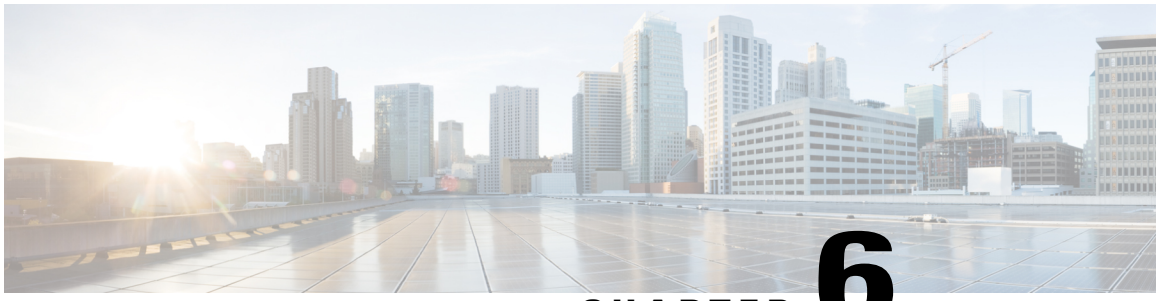
Logical ID	Title	Description	Status	Defects
WLJ80MR2S_SR_CFD_01	Optimized Roaming	To check whether optimized roaming gets activated and works fine	Passed	
WLJ80MR2S_SR_CFD_02	Audit status of AP associated to NGWC box in PI	To check the AP audit status in PI after doing WLC sync- IOS-XE	Passed	
WLJ80MR2S_SR_CFD_03	Audit status of AP associated to legacy WLCs in PI	To check the AP audit status in PI after doing WLC sync-AireOS	Passed	
WLJ80MR2S_SR_CFD_04	Command "show tech-support wireless" in NGWC	To check the execution of the command "show tech-support wireless" in both MC/MA	Passed	
WLJ80MR2S_SR_CFD_05	Location info rogue extended in WLC	To check the location rogue info extended/RSSI measurement in WLC/MSE	Passed	
WLJ80MR2S_SR_CFD_06	Critical Alarms in Monitor AP page	To verify the Monitor > AP page in PI shows correct critical alarms	Passed	

WLJ80MR2S_SR_CFD_07	Associating clients to L3 security-customized web auth.	To verify whether clients can able to see Customized web auth page while associated to web-auth security.	Passed	
WLJ80MR2S_SR_CFD_08	Upgrading WLC 7.6 to 8.0 image and associating clients to 5508 WLC.	To verify whether clients gets associated or not to WLC (which is upgraded to 8.0 image from 7.6) with Central auth and local switching enabled in WLAN.	Passed	
WLJ80MR2S_SR_CFD_09	Upgrading WLC 7.6 to 8.0 image and associating clients to 8500 WLC.	To verify whether clients gets associated or not to WLC (which is upgraded to 8.0 image from 7.6) with Central auth and local switching enabled in WLAN.	Passed	
WLJ80MR2S_SR_CFD_10	Joining 2700 AP to WLC via DHCP option 43.	To verify whether 2700 AP joins WLC or not via DHCP option 43.	Passed	
WLJ80MR2S_SR_CFD_11	Joining 3700 AP to WLC via DHCP option 43.	To verify whether 3700 AP joins WLC or not via DHCP option 43.	Passed	
WLJ80MR2S_SR_CFD_12	Enabling Optimized roaming and associating clients to WLC	To check whether clients gets associated or not to WLC once optimized roaming is enabled.	Passed	
WLJ80MR2S_SR_CFD_13	Enabling BPDU guard on AP port in Switch and joining 2700 AP to WLC.	To verify whether 2700 AP joins to WLC or not when BPDU guard is enabled on AP port in Switch.	Passed	
WLJ80MR2S_SR_CFD_14	Enabling BPDU guard on AP port in Switch and joining 3700 AP to WLC.	To verify whether 3700 AP joins to WLC or not when BPDU guard is enabled on AP port in Switch.	Passed	
WLJ80MR2S_SR_CFD_15	Joining 2700 AP to WLC via DNS resolution	To verify whether 2700 AP joins WLC or not via DNS resolution.	Passed	
WLJ80MR2S_SR_CFD_16	Joining 3700 AP to WLC via DNS resolution.	To verify whether 3700 AP joins WLC or not via DNS resolution.	Passed	

WLJ80MR2S_SR_CFD_17	Performing configuration rollback to WLC from PI.	To verify whether configuration gets retained or not in WLC once performing configuration rollback in PI	Passed	
WLJ80MR2S_SR_CFD_18	MSE Backup operation getting failed with permission denied error	To check whether MSE backup operation can be done without any errors	Passed	
WLJ80MR2S_SR_CFD_19	Native VLAN field in AP Flexconnect of WLC GUI	To check whether the native vlan id checkbox is available or not for AP's 2700/1700 in AP > flexconnect tab in 7500/2500/vWLC/5500 WLC's GUI.	Passed	
WLJ80MR2S_SR_CFD_23	Monitoring Active Clients when connected to 1702 AP	To verify whether Active clients connected to 1702 AP are displayed in the MSE or not	Passed	
WLJ80MR2S_SR_CFD_24	Monitoring Active Clients when connected to 1570 AP	To verify whether Active clients connected to 1570 AP are displayed in the MSE or not	Passed	
WLJ80MR2S_SR_CFD_25	Device Port Summary for 5508 WLC	To verify that the Device Port Summary is displayed for 5508 WLC or not	Passed	
WLJ80MR2S_SR_CFD_26	Device Port Summary for 8500 WLC	To verify that the Device Port Summary is displayed for 8500 WLC or not	Passed	
WLJ80MR2S_SR_CFD_27	Checking the Syslog filter in PI	To verify whether the syslog filters are displayed properly after adding new filters	Passed	
WLJ80MR2S_SR_CFD_28	Create and delete Context aware notification using PI	To verify whether context aware notification is able to create and edit in PI	Passed	

WLJ80MR2S_SR_CFD_30	Create and delete MSE user groups through MSE GUI.	To verify whether user groups on MSE is able to create and delete successfully	Passed	
WLJ80MR2S_SR_CFD_31	Create and delete MSE user groups through PI	To verify whether user groups on MSE is able to create and delete successfully through PI	Passed	
WLJ80MR2S_SR_CFD_33	Create a duplicate wlan-template without any configuration mismatch from the original template using PI.	To verify whether the duplicate template is able to create successfully without any configuration mismatch from the original wlan-template using PI or not	Passed	
WLJ80MR2S_SR_CFD_34	Monitoring the audit status for the deployed wlan template from PI	To verify whether the created wlan template is deployed successfully in controller and check the audit status	Passed	
WLJ80MR2S_SR_CFD_35	Checking the MSE physical appliance's timestamp in Japanese browser when time zone is Asia/Tokyo.	To verify whether the MSE physical appliance's timestamp is showing correctly in Japanese language browser when the time zone is set to Asia/Tokyo.	Passed	
WLJ80MR2S_SR_CFD_36	Checking the MSE virtual appliance's timestamp in Japanese browser when time zone is Asia/Tokyo.	To verify whether the MSE virtual appliance's timestamp is showing correctly in Japanese language browser when the time zone is set to Asia/Tokyo.	Passed	
WLJ80MR2S_SR_CFD_37	Prime Infrastructure 2.2 Number of Aps supported	To Check whether count for maximum number of AP's supported is displayed	Passed	
WLJ80MR2S_SR_CFD_38	PI2.2 Task Permission of Rogue Location in User Group	To check whether a User who does not allow Rogue Location permission on the configuration can see rogue APs on PI maps	Passed	

WLJ80MR2S_SR_CFD_41	Client AP Association History graph	To check whether Client AP Association History graph is consitent with other graphs	Passed	



CHAPTER 6

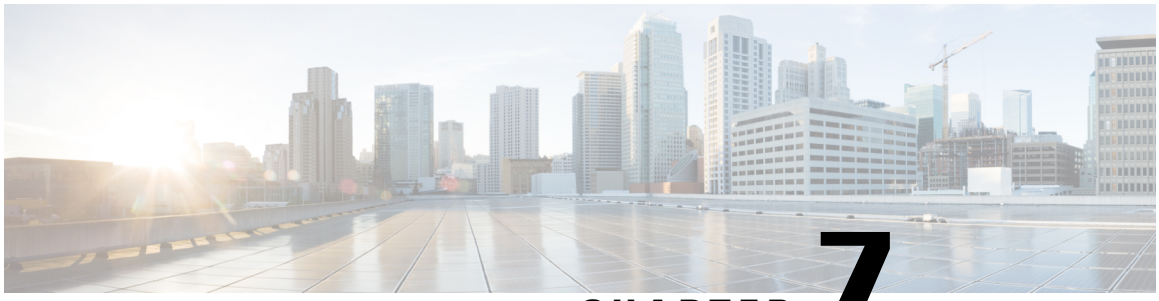
Adhoc Test cases

- Adhoc Test cases, page 49

Adhoc Test cases

Logical ID	Title	Description	Status	Defect ID
WLJ80MR2S_Failed_01	Create a flexconnect group in WLC GUI	To check whether the error message is displaying correctly or not, when creating a flexconnect group name with no strings.	Failed	CSCuv13395
WLJ80MR2S_Failed_02	Checking the MAP count in show mesh ap summary CLI command	To check whether MAP count is shown correctly or not in CLI command show mesh ap summary	Failed	CSCuv16895
WLJ80MR2S_Failed_03	Configuring Mobility domain name in UTF-8 character	To check whether Mobility domain name is created or not in UTF-8 character in WLC GUI	Failed	CSCuv29025
WLJ80MR2S_Failed_04	Enabling HTTPS redirection option in WLC GUI	To check whether HTTPS redirection option is able to enable via WLC GUI or not.	Failed	CSCuv30652
WLJ80MR2S_Failed_05	Create a local policy in UTF - 8 characters	To check whether local policy name in UTF - 8 characters is able to create and displays correctly in its edit page or not.	Failed	CSCuv44023
WLJ80MR2S_Failed_06	Checking the search Filter options in WLAN page using UTF-8 character	To check whether search filter option works or not in WLAN Page of WLC GUI using UTF-8 character	Failed	CSCuv51964

WLJ80MR2S_Failed_07	Checking the ARP timeout value in WLC GUI and CLI	To check whether ARP timeout value is same or not in both WLC GUI and CLI	Failed	CSCuv79155
WLJ80MR2S_Failed_08	Creating EAP profile name in UTF-8 character	To check whether EAP profile name is created or not in UTF-8 character in WLC GUI.	Failed	CSCuq94587
WLJ80MR2S_Failed_09	Checking the Interface count enteries in WLC GUI	To check whether Interface count enteries are shown correctly or not in WLC GUI	Failed	CSCuv91244



CHAPTER 7

Related Documentation

- Related Documentation, page 51

Related Documentation

ACS User Guide

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

ISE 1.3 Admin Guide

http://www.cisco.com/c/en/us/td/docs/security/ise/1-3/admin_guide/b_ise_admin_guide_13.html

PI 2.2 User Guide

http://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/2-2/user/guide/pi_ug.pdf

WLC 8.0 Configuration Guide

http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-0/configuration-guide/b_cg80.pdf

MSE Reference Guide

http://www.cisco.com/en/US/docs/wireless/mse/3310/quick/guide/MSE3310_GSG.html

Related Documentation