

CONFIDENTIAL TRADE SECRET

FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE® MEMBERS

– DO NOT COPY –



Wi-Fi CERTIFIED Wi-Fi Protected Setup™
Test Plan
Version 2.0.20

10900-B Stonelake Boulevard, Suite 126
Austin, TX 78759

Phone: 512.498.9434 • Fax: 512.498.9435 • Email: certifications@wi-fi.org
www.wi-fi.org

Latest version available at <https://www.wi-fi.org/members/certifications-testing/test-plans>

© 2018 Wi-Fi Alliance. All Rights Reserved.

This document contains confidential trade secrets intended solely for use by only authorized Wi-Fi Alliance members.
For the latest up-to-date information, please refer to the Wi-Fi Alliance website's members-only area.



WI-FI ALLIANCE PROPRIETARY AND CONFIDENTIAL – SUBJECT TO CHANGE WITHOUT NOTICE

Wi-Fi Alliance owns the copyright in this document and reserves all rights therein. This document and any related materials may only be used by Wi-Fi Alliance members for their internal use, such as quality assurance and pre-certification activities, and for their participation in approved Wi-Fi Alliance activities, such as the Wi-Fi Alliance certification program, unless otherwise permitted by Wi-Fi Alliance through prior written consent. A user of this document may duplicate and distribute copies of the document in connection with the authorized uses described above, provided any duplication in whole or in part includes the copyright notice and the disclaimer text set forth herein. Unless prior written permission has been received from Wi-Fi Alliance, any other use of this document and all other duplication and distribution of this document are prohibited. Wi-Fi Alliance regards the unauthorized use, duplication or distribution of this document by a member as a material breach of the member's obligations under the organization's rules and regulations, which may result in the suspension or termination of Wi-Fi Alliance membership. Unauthorized use, duplication, or distribution by nonmembers is an infringement of the Wi-Fi Alliance's copyright. Distribution of this document to persons or organizations who are not members of Wi-Fi Alliance is strictly prohibited. TO PREVENT UNAUTHORIZED ACCESS, DO NOT STORE ON COMPUTER ANY LONGER THAN REQUIRED.

THIS DOCUMENT IS PROVIDED "AS IS" AND WITHOUT WARRANTY OF ANY KIND. TO THE GREATEST EXTENT PERMITTED BY LAW, WI-FI ALLIANCE DISCLAIMS ALL EXPRESS, IMPLIED AND STATUTORY WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF TITLE, NONINFRINGEMENT, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. WI-FI ALLIANCE DOES NOT WARRANT THAT THIS DOCUMENT IS COMPLETE OR WITHOUT ERROR AND DISCLAIMS ANY WARRANTIES TO THE CONTRARY. NOTHING IN THIS DOCUMENT CREATES ANY WARRANTIES WHATSOEVER REGARDING THE SUITABILITY OR NON-SUITABILITY OF A PRODUCT OR A SERVICE FOR CERTIFICATION UNDER ANY CERTIFICATION PROGRAM OF WI-FI ALLIANCE OR ANY THIRD PARTY.



Table of Contents

1	Overview	9
1.1	Scope and Purpose	9
1.2	Definition of Devices under test (DUT).....	9
1.2.1	Access Points (APUT).....	9
1.2.2	Mobile Access Points (MAPUT)	9
1.2.3	Station (STAUT).....	9
1.2.4	Stand-Alone External Registrar (SAERUT).....	9
1.2.5	DUT general capabilities description.....	10
1.3	References	10
1.4	Definitions	10
2	Test tools, methodology and approach	13
2.1	Basic system test configuration	13
2.2	NFC Method Instructions	14
2.3	APUT Testing instructions when Ethernet port not available	14
3	Requirements for Wi-Fi Alliance certification	16
3.1	General requirements	16
3.2	Applicability of tests	16
3.2.1	APUT tests.....	16
3.2.2	MAPUT tests.....	18
3.2.3	STAUT tests.....	19
3.2.4	SAERUT tests.....	21
4	AP tests	22
4.1	Configure APUT.....	22
4.1.1	Check APUT's WSC Protocol frame format and correctness of self-generated SSID and PSK	22
4.1.2	Configure APUT using PIN method through an ER that connects via 802.11	25
4.1.3	Configure APUT using PIN method through an ER that connects via Ethernet	27
4.1.4	Configure APUT to use open networking (no security) using PIN method through an ER and add a STA using the internal Registrar	28
4.1.5	Check PBC Walk Time is correctly implemented	29
4.1.6	Configure APUT using NFC tag method with password token through an external Registrar	31
4.1.7	Manually configure APUT to disable broadcasting of the SSID.....	32
4.1.8	Manually configure APUT to use open networking (no security) and add a STA using internal registrar.....	33
4.1.9	Disable WSC if the APUT is manually configured for WEP.....	34
4.1.10	WSC fails if the APUT is configured for WEP by a WSC 1.0 external Registrar	35
4.1.11	Disable WSC if the APUT is manually configured for WPA/TKIP only, unless the APUT is configured for mixed mode	36
4.1.12	APUT correctly handles WPA/TKIP configuration from a WSC 1.0 ER	36
4.1.13	APUT correctly uses AuthorizedMACs subelement in the WFA Vendor Extension attribute in Beacons/DMG Beacons and Probe Responses .	37



4.1.14	APUT detects and mitigates against brute-force attack on static PIN by external Registrars	39
4.2	Add devices	41
4.2.1	Manually configure APUT and add device using PIN method, and then add device using PBC method.....	41
4.2.2	Add devices using PIN method, and then add device using PBC method to out-of-box APUT	44
4.2.3	Add devices using multiple external Registrars and internal Registrar..	45
4.2.4	Mixed mode test with PIN including whitespace and manually add a legacy WPA device	47
4.2.5	Add device using NFC tag method with password token	48
4.2.6	Add device using NFC tag method with configuration token	49
4.2.7	Add device using PIN Method when AP has MAC Address filtering enabled	51
4.2.8	Protocol Extensibility	51
4.2.9	Test reassembly of WSC IEs	53
4.2.10	Add device when EAP-WSC fragmentation is used	54
4.2.11	Add device using NFC connection handover method	55
4.2.12	Refuse to add erroneous device using NFC connection handover method	56
4.2.13	Check correctness of APUT association procedure	56
4.2.14	Overlapped PBC sessions	58
4.3	WSC 1.0 backwards compatibility tests for APUT	60
4.3.1	Configure APUT using PIN method through a WSC 1.0 external Registrar	60
4.3.2	Add WSC 1.0 device using PIN method, and then add WSC 1.0 device using PBC method to OOB APUT	61
4.4	Additional tests for Mobile AP	62
4.4.1	Protocol extensibility with STA	62
4.4.2	Protocol extensibility with external Registrar	63
4.4.3	Configure APUT to use open networking (no security) using PIN method through an external Registrar and add a STA using internal Registrar ..	64
4.4.4	Add devices using multiple external Registrars and internal Registrar..	65
4.4.5	Configure APUT using PIN method through a WSC 1.0 external Registrar	67
5	STA tests	69
5.1	Add to AP as an Enrollee	69
5.1.1	Add to AP using PIN Config method through an external Registrar and check frame format	69
5.1.2	Add to AP using PBC method through internal Registrar	71
5.1.3	Add to AP using PIN Config method through an external Registrar that connects to the AP via 802.11.....	73
5.1.4	Add to AP using PIN Config method through an external Registrar that connects to the AP via Ethernet.....	73
5.1.5	Add to AP using PIN method and open networking setting through an external Registrar	75



5.1.6	Add to AP using PBC method and open network settings through internal Registrar	75
5.1.7	Two (2) minute timeout with multiple push button events for PBC method	76
5.1.8	Overlapped PBC sessions	77
5.1.9	Add to AP using NFC tag method with password token through internal registrar	79
5.1.10	Add to AP using NFC tag method with configuration token containing standalone NDEF record through internal registrar	80
5.1.11	Protocol extensibility	81
5.1.12	Add to AP when WSC IE and EAP-WSC is fragmented	82
5.1.13	Add to AP using PIN Configuration method through internal Registrar ..	83
5.1.14	Check correctness of STAUT association procedure	84
5.1.15	(Moved to test 5.4.5)	86
5.1.16	Add to AP using NFC connection handover method through internal Registrar	86
5.1.17	Refuse to add to erroneous AP using NFC connection handover method through internal Registrar	86
5.1.18	Add to AP using PBC method through external Registrar	87
5.1.19	STAUT selects WPA2 with mixed-mode AP	88
5.1.20	WSC fails if the STAUT is provisioned with WEP credential by a WSC 1.0 Registrar	89
5.2	Act as Registrar and configure AP	90
5.2.1	Manually configure AP, and then enroll with Registrar using PIN Config method	90
5.2.2	Configure the AP to use passphrase using PIN	91
5.2.3	Configure the AP to use open networking settings using PIN	93
5.3	Act as Registrar and add devices	93
5.3.1	Registrar configuring AP using registrar defaults and add device using both 4-digit and 8-digit PIN method	94
5.3.2	Registrar enrolling configured open AP and add device using PIN method	95
5.3.3	Registrar adding device using NFC tag method with password token ..	96
5.3.4	Registrar adding device using NFC tag method with configuration token	97
5.3.5	Registrar adding device using NFC connection handover method	98
5.3.6	Registrar refusing to add erroneous device using NFC connection handover method	99
5.3.7	Overlapped PBC sessions	99
5.3.8	STAUT acting as External Registrar correctly uses AuthorizedMACs subelement in the WFA Vendor Extension attribute in SetSelectedRegistrar UPnP action	101
5.3.9	Protocol extensibility for STAUT which also implements Registrar	102
5.4	WSC 1.0 backwards compatibility tests for STAUT	103
5.4.1	Add to WSC 1.0 AP using PBC method through internal Registrar	103



5.4.2	Add to WSC 1.0 AP using PIN Configuration method through internal Registrar	104
5.4.3	Add to WSC 1.0 AP using PIN Config method through WSC 1.0 external Registrar	105
5.4.4	Add to WSC 2.0 AP using PIN Config method through WSC 1.0 external Registrar	106
5.4.5	Able to be Enrolled by WSC 1.0 external Registrars that use null terminated password.....	107
5.5	Use Registrar handshake to discover AP settings and use those settings to associate.....	108
5.5.1	Discover settings of an AP in Configured state and associate	108
5.5.2	Discover settings of an AP configured to use open networking, and associate.....	109
5.5.3	Detect AP is in Not Configured state and not associate automatically	110
6	Stand-Alone External Registrar (SAERUT) tests	111
6.1	Stand-Alone External Registrar configuring and enrolling an AP and enrolling STA via PIN	111
6.1.1	SAERUT enroll and configure AP for Security	111
6.1.2	SAERUT enroll manually configured AP using PIN method.....	112
6.1.3	SAERUT enroll and configure AP using Registrar's configuration and then enroll STAs using both 4-digit and 8-digit PIN method.....	113
6.1.4	SAERUT enrolls and configures open AP and then enroll STA using PIN method	114
6.1.5	SAERUT correctly uses AuthorizedMACs subelement in the WFA Vendor Extension attribute in SetSelectedRegistrar UPnP action.....	115
6.1.6	Protocol extensibility for SAERUT	117
6.2	Stand-Alone External Registrar enrolling STA via PBC	119
6.2.1	SAERUT enroll AP using PIN method, and then enroll STA using PBC method	119
6.2.2	Overlapped PBC sessions	120
6.3	Stand-Alone External Registrar enrolling STA via NFC	121
Appendix A: Vendor equipment list and contacts		122
A.1	WSC 2.0 equipment.....	122
A.1.1	802.11 (A, B, G, N) Access Points	122
A.1.2	802.11 (A, B, G, N) Stations.....	123
A.1.3	802.11ad (60GHz, DMG) Test bed Devices.....	124
A.1.4	NFC Tags.....	124
A.2	WSC 1.0 equipment.....	124
Appendix B: UpnP Information Element.....		125
Appendix C: (Normative) STAUT test cases for devices supporting only WSC Push Button Configuration method.....		126
C.1	Test case list	126
C.2	STAUT tests	127
C.2.1	Add to AP using PBC method through internal Registrar	127
C.2.2	Two (2) minute timeout with multiple push button events for PBC method	130



C.2.3 Overlapped PBC sessions	131
C.2.4 Protocol extensibility.....	132
C.2.5 Add to AP when WSC IE and EAP-WSC is fragmented.....	133
C.2.6 Add to WSC 1.0 AP using PBC method through internal Registrar.....	134
Appendix D: Change history table.....	135



Table of Tables

Table 1: General capabilities declaration	10
Table 2: APUT tests	16
Table 3: MAPUT tests	18
Table 4: STAUT tests	19
Table 5: SAERUT tests	21
Table 6: STAUT tests for WSC PBC only DUTs	126

Table of Figures

Figure 1: Wi-Fi Test Suite system test configuration	14
--	----



1 Overview

1.1 Scope and Purpose

The goal of Wi-Fi Alliance (WFA) is to ensure the interoperability among Wi-Fi and products that support the features of Wi-Fi Protected Setup from multiple manufacturers, and to promote this technology within the business and consumer markets. To achieve this goal, Wi-Fi Alliance has developed the following test plan.

This test plan exercises various combinations of the wireless network usage models and the WSC configuration methods. The usage models consist of:

- Setting up the network (initial network setup)
- Adding additional clients

The Wi-Fi Simple Configuration (WSC) configuration methods include: Pin Input Config (PIN) method, Push Button Config (PBC) method and Near Field Communication Contactless Token Config (NFC) method. Each of these three methods utilizes the EAP protocol and/or UPnP protocol as applicable.

The test plan will also verify the conformance of the device's WSC protocol operations according to WSC Protocol Specification.

1.2 Definition of Devices under test (DUT)

1.2.1 Access Points (APUT)

The APUT is an infrastructure-mode 802.11 Access Point that functions as a WSC AP. A Registrar, which has the authority to issue and revoke Domain Credentials, shall be integrated into the APUT as an Internal Registrar. The APUT also can be an Enrollee, which can register itself to an external Registrar.

1.2.2 Mobile Access Points (MAPUT)

The MAPUT is a Mobile AP that functions as a WSC AP. A Registrar, which has the authority to issue and revoke Domain Credentials, shall be integrated into the MAPUT as a built-in Registrar. The MAPUT may optionally be an Enrollee, which can register itself to an external Registrar. The MAPUT may support configuration by an external Registrar or it may support both configuration by an external Registrar and addition of enrollees by an external Registrar. Note that a MAPUT that does not support configuration by an external Registrar will not interoperate with STAs that always join using the station's registrar; the station may join not using Wi-Fi Simple Configuration.

1.2.3 Station (STAUT)

The STAUT is an 802.11 non-AP STA, which functions as a WSC Enrollee device. If the STAUT has a built-in External Registrar, the STAUT's External Registrar function shall be tested.

1.2.4 Stand-Alone External Registrar (SAERUT)

The SAERUT is a stand-alone external Registrar which may communicate with an AP over Ethernet and/or 802.11 connection using UPnP messages. SAERUT testing is only



applicable outside DMG. By stand-alone it is meant that the external Registrar functionality is not integrated with a STA's wireless functionality.

1.2.5 DUT general capabilities description

The general characteristics of the DUT are entered in the WFA Web registration system and will be summarized in Table 1.

Table 1: General capabilities declaration

Item	Vendor Answer
DUT Type	AP, MAP, STA, SAER
Device Model Number	
Primary Product Category	
Secondary Product Category	
Device Serial Number	
Device Firmware Version	
Is 802.11a Device	Yes/No
Is 802.11b Device	Yes/No
Is 802.11g Device	Yes/No
Is 802.11n Device	Yes/No
Is 802.11ac Device	Yes/no
Is 802.11ad Device	Yes/No
For MAPs, does the AP support an External Registrar?	Yes/No/Not Applicable
For Stations, does the device support an External Registrar (choose one)	COER/OCOER/CEER, NO/Not applicable
Does the device support PBC?	Yes/No
Does the device support NFC?	Yes/No
For NFC support, does the device support NFC tags?	Yes/No/Not applicable
For NFC support, does the device support NFC connection handover?	Yes/No/Not applicable
Does the device have an Ethernet Port (APs, MAPs, and SAERs only)	Yes/No/Not applicable
Does the device support WPA?	Yes/No
Does the device support WEP?	Yes/No
Does the device support open (i.e. no security) Wi-Fi network?	Yes/No

1.3 References

- [1] [Wi-Fi Simple Configuration Specification](#), Wi-Fi Alliance
- [2] [Wi-Fi CERTIFIED Wi-Fi Direct Test Plan](#), Wi-Fi Alliance
- [3] [Wi-Fi CERTIFIED Miracast Test Plan](#), Wi-Fi Alliance

1.4 Definitions

AP: An infrastructure-mode 802.11 Access Point

Credential: A data structure issued by a Registrar to an Enrollee, allowing the latter to gain access to the network

Device: An independent physical or logical entity capable of communicating with other Devices across a LAN or WLAN

Domain: A set of one or more Devices governed by a common authority for the purpose of gaining access to one or more WLANs



Directional Multi-Gigabit (DMG): A frequency band wherein the operating channel center frequency is above 45 GHz

Enrollee: A Device seeking to join a WLAN Domain. Once an Enrollee obtains a valid credential, it becomes a Member

External Registrar (ER): A Registrar for an AP's Domain that runs on a device separate from the AP.

Configuration Only External Registrar (COER): A Registrar for an AP's Domain that runs on a device separate from the AP which is used for configuration of the AP only.

Configuration and Enrollee External Registrar (CEER): A Registrar for an AP's Domain that runs on a device separate from the AP which is used for configuration of the AP and to enroll other enrollees.

Obtain Credentials Only External Registrar (OCOER): A Registrar for an AP's Domain that runs on a device separate from the AP which implements the Registrar handshake for discovery of an AP's settings, but which cannot configure the AP nor add enrollees.

In-band: Data transfer using the WLAN communication channel

Internal Registrar (IR): A Registrar for an AP's Domain that runs on the AP

Member: A WLAN Device possessing Domain credentials

Mobile AP: A device with access point functionality powered by an internal battery.

NFC Device: NFC Forum compliant contactless device that support the following Modus Operandi: Initiator, Target, and Reader/Writer. It may also support card emulator.

NFC Interface: Contactless interface of an NFC Device.

NFC Tag: NFC Forum compliant contactless memory card or Tag embedded within an AP/STA that can be read or written by an NFC Device and may be powered by the RF field.

Out-Of-Band: Data transfer using a communication channel other than the WLAN

Proxy: An AP is able to proxy 802.11 management packets, such as probe requests, from an 802.11 STA to an external Registrar by encapsulating them in UPnP messages and sending them via Ethernet or 802.11 connection to the external Registrar

PushButton Configuration (PBC): A configuration method triggered by pressing a physical or logical button on the Enrollee and on the Registrar

Registrar: An entity with the authority to issue and revoke Domain Credentials. A Registrar may be integrated into an AP, or it may be separate from the AP. A Registrar may not have WLAN capability. A given Domain may have multiple Registrars.

Registration Protocol: A Registration Protocol is a (logically) three party in-band protocol to assign a Credential to the Enrollee. The protocol operates between the Enrollee and the Access Point, via the auspices of the Registrar

STA: An 802.11 non-AP station



Stand-Alone External Registrar: An External Registrar which is not integrated with a STA's wireless functionality.

Static PIN: A PIN that never changes (printed on label, taken from UI, etc.), or a PIN that once generated persists if unused or persists to be reused two or more times is static. For example, if the PIN is generated on the AP's UI and can be used more than one try or it stays valid indefinitely, it is considered a static PIN.

UPnP: Universal Plug and Play is a set of networking protocols for primarily residential networks without enterprise class devices that permits networked devices, such as personal computers, printers, Internet gateways, Wi-Fi access points and mobile devices to seamlessly discover each other's presence on the network and establish functional network services for data sharing, communications, and entertainment.

WLAN: A Wi-Fi network when operating outside or within DMG or a WiGig network when operating within DMG

WSC State: Identifies the Wi-Fi Simple Configuration State of an AP, as having security Configured or Not Configured as defined in the Wi-Fi Simple Configuration specification [1]

2 Test tools, methodology and approach

Two sniffers are required to execute the tests:

- A wireless sniffer capable of capturing and decoding EAP protocol frame is required for the testing involving exchanging the WSC protocol message through the EAP protocol. An example of such a sniffer is the AiroPeek software.
- An Ethernet sniffer is required to assess UPnP messages.

For out-of-band test cases that require NFC tags, the following tags and memory sizes are supported by this certification:

NFC Forum Tag Type	Memory Capacity
Type 1	479 bytes
Type 3	>1 kB
Type 4	>2 kB

Note the above list is not meant to be exclusive. Any NFC Forum compliant tag with a sufficient memory capacity can be used.

2.1 Basic system test configuration

The basic test configuration for infrastructure tests outside DMG is depicted in the following figure:

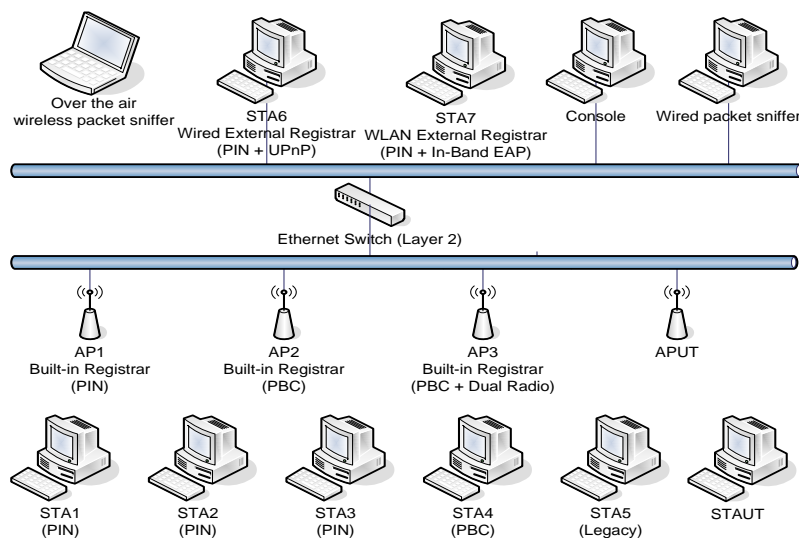


Figure 1: Wi-Fi Test Suite system test configuration

The following attributes of test bed devices should be noted:

- APx is a dual-radio WSC AP that out-of-box operates simultaneously in both 2.4GHz and 5GHz bands.
- STAx, as an External Registrar that connects via 802.11, is capable of issuing multiple credentials to an Enrollee.
 - Some test bed devices are able to use a higher WSC version number than the current version.
 - Some test bed devices are able to add unknown WSC attributes to information elements.
 - Some test bed devices are able to add the Manufacturer, Model Name, Model Number, Serial Number, and Device Name attributes with zero length data fields.
 - Some test bed devices are able to fragment WSC information elements and EAP-WSC messages.
- Note: the designations of APs and STAs apply only to this diagram and not the test bed equipment. See Appendix A of the test bed equipment for the designations for the test bed equipment used in the certification testing.

2.2 NFC Method Instructions

- For these instructions, the word “exchange” means that the NFC Tag based static handover method or NFC Interface based negotiated handover method will be used.
- For optimal magnetic field overlap, align the coils in each device parallel to each other.
- Attempt to make the exchange work a maximum of 3 times. If the exchange fails 3 times in a row, then consider the test failed.
- If the DUT or the test bed equipment has an indicator for failure of the exchange, wait for the failure notice before retrying.
- If the DUT or test bed equipment does not have an indicator for failure of the exchange, wait at least 15 seconds to retry. WSC can take up to 15 seconds to complete the connection.

2.3 APUT Testing instructions when Ethernet port not available

Note: If APUT doesn't have an Ethernet port to configure the settings required as per the test cases, please use a wireless client (use any Wi-Fi Protected Setup testbed STA) and follow the below steps to configure the AP.

- Turn on the APUT
- Turn on the Wireless client and cause it to associate to APUT.
- Access the APUT GUI/telnet from wireless client laptop using APUT IP address.
- Configure the test cases parameters and confirm the settings with the sniffer.
- Follow the steps mentioned in the test cases





3 Requirements for Wi-Fi Alliance certification

The following items describe the necessary features that are required for a DUT to pass Wi-Fi Protected Setup certification.

All tests marked optional become mandatory if that feature is implemented on the DUT.

3.1 General requirements

- For a device under test seeking certification outside DMG, the device under test shall be Wi-Fi CERTIFIED for either the WPA2 test plan or 11n certified test plan before being submitted for Wi-Fi Protected Setup certified.
- For a device under test seeking Wi-Fi CERTIFIED WiGig within DMG, passing the relevant tests in this test plan is a mandatory prerequisite. The device under test shall first pass the relevant tests in the WiGig Test Plan before running the tests in this test plan.

3.2 Applicability of tests

The member submitting the DUT for Wi-Fi Protected Setup certification shall indicate which category of device the DUT is: APUT, MAPUT, STAUT, or SAERUT.

If the submitted device is an APUT, then the test cases in Table 2 shall be performed.

If the submitted device is an MAPUT, then the test cases in Table 3 shall be performed.

If the submitted device is a STAUT, then the test cases in Table 4 shall be performed.

If the submitted device is a SAERUT, then the test cases in Table 5 shall be performed.

3.2.1 APUT tests

Table 2: APUT tests

Name	Test case	Applicability Mandatory / Optional / Conditional (M/O/C)	If implemented in submission, then Vendor must indicate	If implemented, displayed in certificate.
Check APUT's WSC Protocol frame format and correctness of self-generated SSID and PSK	4.1.1	M		
Configure APUT using PIN method through an ER that connects via 802.11	4.1.2	M (outside DMG) N/A (within DMG)		
Configure APUT using PIN method through an ER that connects via Ethernet	4.1.3	M (outside DMG) N/A (within DMG)		
Configure APUT to use open networking (no security) using PIN method through an ER and add a STA using the internal Registrar	4.1.4	M (outside DMG) N/A (within DMG)		
Check PBC Walk Time is correctly implemented	4.1.5	M		
Configure APUT using NFC tag method with password token through an external Registrar	4.1.6	O (outside DMG) N/A (within DMG)	Y	
Manually configure APUT to disable broadcasting of the SSID	4.1.7	O (outside DMG) N/A (within DMG)	Y	



Name	Test case	Applicability Mandatory / Optional / Conditional (M/O/C)	If implemented in submission, then Vendor must indicate	If implemented, displayed in certificate.
Manually configure APUT to use open networking (no security) and add a STA using internal registrar	4.1.8	M		
Disable WSC if the APUT is manually configured for WEP	4.1.9	O (outside DMG) N/A (within DMG)	Y	
WSC fails if the APUT is configured for WEP by a WSC 1.0 external Registrar	4.1.10	O (outside DMG) N/A (within DMG)	Y	
APUT correctly handles WPA/TKIP configuration from a WSC 1.0 ER	4.1.12	M (outside DMG) N/A (within DMG)		
APUT correctly uses AuthorizedMACs subelement in the WFA Vendor Extension attribute in Beacons/DMG Beacons and Probe Responses	4.1.13	M		
APUT detects and mitigates against brute-force attack on static PIN by external Registrars	4.1.14	O (outside DMG) N/A (within DMG)	Y	
Manually configure APUT and add device using PIN method, and then add device using PBC method	4.2.1	M		
Add devices using PIN method, and then add device using PBC method to out-of-box APUT	4.2.2	M		
Add devices using multiple external Registrars and internal Registrar	4.2.3	M (outside DMG) N/A (within DMG)		
Mixed mode test with PIN including whitespace and manually add a legacy WPA device	4.2.4	M (outside DMG) N/A (within DMG)		
Add device using NFC tag method with password token	4.2.5	O (outside DMG) N/A (within DMG)	Y	
Add device using NFC tag method with configuration token	4.2.6	O (outside DMG) N/A (within DMG)	Y	
Add device using PIN Method when AP has MAC Address filtering enabled	4.2.7	O (outside DMG) N/A (within DMG)	Y	
Protocol Extensibility	4.2.8	M		
Test reassembly of WSC IE	4.2.9	M		
Add device when EAP-WSC fragmentation is used	4.2.10	M		
Add device using NFC connection handover method	4.2.11	O (outside DMG) N/A (within DMG)	Y	
Refuse to add erroneous device using NFC connection handover method	4.2.12	O (outside DMG) N/A (within DMG)	Y	
Check correctness of APUT association procedure	4.2.13	M		
Overlapped PBC sessions	4.2.14	M		
Configure APUT using PIN method through a WSC 1.0 external Registrar	4.3.1	M (outside DMG) N/A (within DMG)		
Add WSC 1.0 device using PIN method, and then add WSC 1.0	4.3.2	M (outside DMG) N/A (within DMG)		



Name	Test case	Applicability Mandatory / Optional / Conditional (M/O/C)	If implemented in submission, then Vendor must indicate	If implemented, displayed in certificate.
device using PBC method to OOB APUT				

3.2.2 MAPUT tests

Table 3: MAPUT tests

Name	Test case	Applicability Mandatory / Optional / Conditional (M/O/C)	If implemented in submission, then Vendor must indicate	If implemented, displayed in certificate.
Check MAPUT's WSC Protocol frame format and correctness of self-generated SSID and PSK	4.1.1	M		
Configure MAPUT using PIN method through an ER that connects via 802.11	4.1.2	O (outside DMG) N/A (within DMG)	Y	
Check PBC Walk Time is correctly implemented	4.1.5	M		
Configure MAPUT using NFC tag method with password token through an external Registrar	4.1.6	O (outside DMG) N/A (within DMG)	Y	
Manually configure MAPUT to disable broadcasting of the SSID	4.1.7	O (outside DMG) N/A (within DMG)	Y	
Manually configure MAPUT to use open networking (no security) and add a STA using internal registrar	4.1.8	M		
Disable WSC if the MAPUT is manually configured for WEP	4.1.9	O (outside DMG) N/A (within DMG)	Y	
WSC fails if the MAPUT is configured for WEP by a WSC 1.0 external Registrar	4.1.10	O (outside DMG) N/A (within DMG)	Y	
MAPUT correctly handles WPA/TKIP configuration from a WSC 1.0 ER	4.1.12	O (outside DMG) N/A (within DMG)	Y	
MAPUT correctly uses AuthorizedMACs subelement in the WFA Vendor Extension attribute in Beacons and Probe Responses	4.1.13	M		
MAPUT detects and mitigates against brute-force attack on static PIN by external Registrars	4.1.14	O (outside DMG) N/A (within DMG)	Y	
Manually configure MAPUT and add device using PIN method, and then add device using PBC method	4.2.1	M		
Add devices using PIN method, and then add device using PBC method to out-of-box MAPUT	4.2.2	M		
Mixed mode test with PIN including whitespace and manually add a legacy WPA device	4.2.4	M (outside DMG) N/A (within DMG)		
Add device using NFC tag method with password token	4.2.5	O (outside DMG) N/A (within DMG)	Y	
Add device using NFC tag method with configuration token	4.2.6	O (outside DMG) N/A (within DMG)	Y	



Name	Test case	Applicability Mandatory / Optional / Conditional (M/O/C)	If implemented in submission, then Vendor must indicate	If implemented, displayed in certificate.
Add device using PIN Method when MAPUT has MAC Address filtering enabled	4.2.7	O (outside DMG) N/A (within DMG)	Y	
Test reassembly of WSC IEs	4.2.9	O	Y	
Add device when EAP-WSC fragmentation is used	4.2.10	M		
Add device using NFC connection handover method	4.2.11	O (outside DMG) N/A (within DMG)	Y	
Refuse to add erroneous device using NFC connection handover method	4.2.12	O (outside DMG) N/A (within DMG)	Y	
Check correctness of MAPUT association procedure	4.2.13	M		
Overlapped PBC sessions	4.2.14	M		
Add WSC 1.0 device using PIN method, and then add WSC 1.0 device using PBC method to OOB APUT	4.3.2	M (outside DMG) N/A (within DMG)		
Protocol extensibility with STA	4.4.1	M (outside DMG) Execute 4.2.8 (within DMG)		
Protocol extensibility with external Registrar	4.4.2	O (outside DMG) N/A (within DMG)	Y	
Configure APUT to use open networking (no security) using PIN method through an external Registrar and add a STA using internal Registrar	4.4.3	O (outside DMG) N/A (within DMG)	Y	
Add devices using multiple external Registrars and internal Registrar	4.4.4	O (outside DMG) N/A (within DMG)	Y	
Configure MAPUT using PIN method through a WSC 1.0 external Registrar	4.4.5	O (outside DMG) N/A (within DMG)	Y	

3.2.3 STAUT tests

Table 4: STAUT tests

Name	Test case	Applicability Mandatory / Optional / Conditional (M/O/C)	If implemented in submission, then Vendor must indicate	If implemented, displayed in certificate.
Add to AP using PIN Config method through an external Registrar and check frame format	5.1.1	M outside DMG N/A within DMG		
Add to AP using PBC method through internal Registrar	5.1.2	O	Y	
Add to AP using PIN Config method through an external Registrar that connects to the AP via 802.11	5.1.3	M outside DMG N/A within DMG		
Add to AP using PIN Config method through an external Registrar that connects to the AP via Ethernet	5.1.4	M outside DMG N/A within DMG		
Add to AP using PIN method and open networking setting through an external Registrar	5.1.5	M outside DMG N/A within DMG		
Add to AP using PBC method and open network settings through internal Registrar	5.1.6	O	Y	
Two (2) minute timeout with multiple push button events for PBC method	5.1.7	O	Y	



Name	Test case	Applicability Mandatory / Optional / Conditional (M/O/C)	If implemented in submission, then Vendor must indicate	If implemented, displayed in certificate.
Overlapped PBC sessions	5.1.8	O	Y	
Add to AP using NFC tag method with password token through internal registrar	5.1.9	O outside DMG N/A within DMG	Y	
Add to AP using NFC tag method with configuration token containing standalone NDEF record through internal registrar	5.1.10	O outside DMG N/A within DMG	Y	
Protocol extensibility	5.1.11	M		
Add to AP when WSC IE and EAP-WSC is fragmented	5.1.12	M		
Add to AP using PIN Configuration method through internal Registrar	5.1.13	M		
Check correctness of STAUT association procedure	5.1.14	M		
Add to AP using NFC connection handover method through internal Registrar	5.1.16	O outside DMG N/A within DMG	Y	
Refuse to add to erroneous AP using NFC connection handover method through internal Registrar	5.1.17	O outside DMG N/A within DMG	Y	
Add to AP using PBC method through external Registrar	5.1.18	O outside DMG N/A within DMG	Y	
STAUT selects WPA2 with mixed-mode AP	5.1.19	M outside DMG N/A within DMG		
WSC fails if the STAUT is provisioned with WEP credential by a WSC 1.0 Registrar	5.1.20	O outside DMG N/A within DMG	Y	
Manually configure AP, and then enroll with Registrar using PIN Config method	5.2.1	O (COER and CEER only) outside DMG N/A within DMG	Y	
Configure the AP to use passphrase using PIN	5.2.2	O (COER and CEER only) outside DMG N/A within DMG	Y	
Configure the AP to use open networking settings using PIN	5.2.3	O (COER and CEER only) outside DMG N/A within DMG	Y	
Registrar configuring AP using registrar defaults and add device using both 4-digit and 8-digit PIN method	5.3.1	O (CEER only) outside DMG N/A within DMG	Y	
Registrar enrolling configured open AP and add device using PIN method	5.3.2	O (CEER only) outside DMG N/A within DMG	Y	
Registrar adding device using NFC tag method with password token	5.3.3	O (CEER only) outside DMG N/A within DMG	Y	
Registrar adding device using NFC tag method with configuration token	5.3.4	O (CEER only) outside DMG N/A within DMG	Y	
Registrar adding device using NFC connection handover method	5.3.5	O (CEER only) outside DMG N/A within DMG	Y	
Registrar refusing to add erroneous device using NFC connection handover method	5.3.6	O (CEER only) outside DMG N/A within DMG	Y	
Overlapped PBC sessions	5.3.7	O (CEER only) outside DMG N/A within DMG	Y	
STAUT acting as External Registrar correctly uses AuthorizedMACs subelement in the WFA Vendor Extension attribute in SetSelectedRegistrar UPnP action	5.3.8	O (CEER only) outside DMG N/A within DMG	Y	
Protocol extensibility for STAUT which also implements Registrar	5.3.9	O (CEER only) outside DMG N/A within DMG	Y	



Name	Test case	Applicability Mandatory / Optional / Conditional (M/O/C)	If implemented in submission, then Vendor must indicate	If implemented, displayed in certificate.
Add to WSC 1.0 AP using PBC method through internal Registrar	5.4.1	O outside DMG N/A within DMG	Y	
Add to WSC 1.0 AP using PIN Configuration method through internal Registrar	5.4.2	M outside DMG N/A within DMG		
Add to WSC 1.0 AP using PIN Config method through WSC 1.0 external Registrar	5.4.3	M outside DMG N/A within DMG		
Add to WSC 2.0 AP using PIN Config method through WSC 1.0 external Registrar	5.4.4	M outside DMG N/A within DMG		
Able to be Enrolled by WSC 1.0 external Registrars that use null terminated password	5.4.5	M outside DMG N/A within DMG		
Discover settings of an AP in Configured state and associate	5.5.1	O (OCOER only) outside DMG N/A within DMG	Y	
Discover settings of an AP configured to use open networking, and associate	5.5.2	O (OCOER only) outside DMG N/A within DMG	Y	
Detect AP is in Not Configured state and not associate automatically	5.5.3	O (OCOER only) outside DMG N/A within DMG	Y	

3.2.4 SAERUT tests

Table 5: SAERUT tests

Name	Test case	Applicability Mandatory / Optional / Conditional (M/O/C)	If implemented in submission, then Vendor must indicate	If implemented, displayed in certificate.
SAERUT enroll and configure AP for Security	6.1.1	M		
SAERUT enroll manually configured AP using PIN method	6.1.2	M		
SAERUT enroll and configure AP using Registrar's configuration and then enroll STAs using both 4-digit and 8-digit PIN method	6.1.3	M		
SAERUT enrolls and configures open AP and then enroll STA using PIN method	6.1.4	M		
SAERUT correctly uses AuthorizedMACs subelement in the WFA Vendor Extension attribute in SetSelectedRegistrar UPnP action	6.1.5	M		
Protocol extensibility for SAERUT	6.1.6	M		
SAERUT enroll AP using PIN method, and then enroll STA using PBC method	6.2.1	M		
Overlapped PBC sessions	6.2.2	O	Y	



4 AP tests

Throughout section 4, except within the test Applicability, the term APUT refers to either the AP or the Mobile AP under test.

4.1 Configure APUT

4.1.1 Check APUT's WSC Protocol frame format and correctness of self-generated SSID and PSK

Test Applicability: Mandatory for APUT. Mandatory for MAPUT.

Channel Assignment: For 5GHz only APs and for dual band APs, use channel 36. For 2.4GHz only APs, use channel 1. For 60 GHz only APs, configure the AP to use channel 2. For dual band 2.4 GHz/60 GHz APs, configure the AP(s) to use channels 1 and 2 in each band, respectively. For tri-band 2.4 GHz/5 GHz/60 GHz APs, configure the AP(s) to use channels 1, 36 and 2 in each band, respectively.

Test Goal: The test verifies the APUT sets the correct WSC IE content in the Beacon and Probe Response frames outside of DMG and in the DMG Beacon or Probe Response frames within DMG, including the WSC version value and WSC State. If APUT is reset to out-of-box state with WSC State set to Not Configured and its Internal Registrar initiates a new WSC session, the new PSK must be different from the one used in the previous session.

Test Requirement: The APUT must support WSC Protocol

Test bed Devices:

1. A wireless packet sniffer device.
2. Outside DMG STA1W / Inside DMG STA14 which supports PIN Config method and is acting as an Enrollee. This station has the ability to correctly validate that the APUT which implements WSC version 2.0 does not add the unwanted zero padding in SSID/Network Key attribute. This station also has the capability to verify that APUT sets the Authentication Type and Encryption Type attributes in Encrypted Settings of M8 messages correctly.
3. Outside DMG STA2 / Inside DMG STA12
4. Outside DMG, STA8 which is a legacy station and does not support any WSC Config methods (WSC must be disabled). Inside DMG, STA13 is a 60 GHz STA that has WSC disabled.
5. "Console" PC attached to the APUT via Ethernet.

Test Procedure:

1. Turn on the APUT.
2. Reset the APUT to out-of-box configuration.



3. Turn on the wireless sniffer and start to monitor the traffic to/from the APUT.
4. If the APUT's out-of-box WSC State is Not Configured, the Beacon packet from the APUT outside of DMG and the DMG Beacon or Probe Response packets within DMG from the APUT must contain the WSC IE with the Version attribute set to 0x10 and the Version2 subelement in the WFA Vendor Extension attribute set to 0x20 and WSC State set to Not Configured (0x01). If the APUT's out-of-box configuration is set to Configured, the Beacon packet from the APUT must contain the WSC IE with version 0x10 and the Version2 subelement in the WFA Vendor Extension attribute set to 0x20 and WSC State set to Configured (0x02). Check on the sniffer.
5. Turn on STA1W/STA14 and invoke WSC application to join WLAN.
6. The Probe Response frame from the APUT must include the following mandatory, variable length string attributes: Manufacturer, Model Name, Model Number, Serial Number, Device Name. These attributes must not use NULL-padding, i.e., the last octet of the attribute value must not be 0x00.
7. Read the displayed PIN on STA1W/STA14 and enter the PIN in the Internal Registrar of the APUT. No additional user action is allowed at APUT (e.g. enabling WSC or enabling "PIN mode") in order to continue.
8. Repeat Step 5 to 7 with the STA2/STA12.
9. Start pings from the Console to STA1W/STA14 and the STA2/STA12; the pings must succeed within 90 seconds.
10. On the sniffer device, verify that the M2 messages that the APUT sends include the following mandatory, variable length string attributes: Manufacturer, Model Name, Model Number, Serial Number, and Device Name. These attributes must not use NULL-padding, i.e., the last octet of the attribute value must not be 0x00.
11. On the sniffer device, verify that the M2 message that the APUT sends includes the following attributes: Authentication Type Flags and Encryption Type Flags. The values for these attributes must reflect the authentication and encryption types supported by the APUT. The Authentication Type Flags value must include following bits depending on APUT capabilities: 0x0001 Open (mandatory), 0x0020 WPA2-Personal (mandatory). The Encryption Type Flags value must include the following bits depending on APUT capabilities: 0x0001 None (mandatory), 0x0008 AES (mandatory)
12. On the sniffer device, verify that the M2 message that the APUT sends includes the Connection Type Flags attribute. The Connection Type Flags value must be 0x01(ESS).
13. On the sniffer device, verify that the M2 message that the APUT sends includes the Configuration Methods attribute. The Configuration Methods attribute in the WSC IE must reflect the correct configuration methods that the Internal Registrar supports. Check on the sniffer to verify that the list of supported method in the IE is a bitwise OR of values from the list below:

0x0004 Label PIN



0x0010	External NFC Tag
0x0020	Integrated NFC Tag
0x0040	NFC Interface
0x0100	Keypad
0x0280	Virtual Push Button
0x0480	Physical Push Button
0x2008	Virtual Display PIN
0x4008	Physical Display PIN

The APUT must support every Config method that it advertises as a bitwise OR in the M2 message.

0x0004

0x0010 – The APUT must support and External NFC Tag.

0x0020 – The APUT must support an Integrated NFC Tag.

0x0040 – The APUT must support an NFC interface.

0x0100 – The APUT must support PIN using a Keypad on the APUT

0x0280 – The APUT must have a Virtual Push Button (in the UI) and support it.

0x0480 – The APUT must have a Physical Push Button (on the APUT) and support it.

0x2008 – The APUT must have a PIN in the Virtual UI and support it.

0x4008 – The APUT must have a PIN on the physical display on the APUT and support it.

14. On the sniffer device, verify that the M2 message that the APUT sends includes the Device Password ID attribute. The Device Password ID value must be 0x0000(Default(PIN)).
15. Outside of DMG, the Beacon packet from the APUT must contain the WSC IE with WSC State set to Configured (0x02). Check on the sniffer.
16. The APUT UI must display the SSID. Retrieve the SSID.
17. The APUT UI must display the PSK or passphrase or both. Retrieve the PSK or passphrase.
18. Add STA8/STA13 manually (WSC not enabled) using the SSID and PSK retrieved from the APUT.
19. The APUT must include the WSC IE in its Probe Response to STA8/STA13. Check on the sniffer.



20. Start pings from STA8/STA13 to the STA1W/STA14; pings must succeed within 90 seconds.
21. If out-of-box WSC State was Not Configured in step 4 then continue through steps 22 to 29. If out-of-box WSC State was Configured in step 4 then the test completed and stop this test here.
22. Reset the APUT to the out-of-box configuration.
23. Ping from STA8/STA13 to the STA1W/STA14 for 30 seconds. The Ping command must fail.
24. Read the displayed PIN on STA1W/STA14 and enter the PIN in the Internal Registrar of the APUT. No additional user action is allowed at APUT (e.g. enabling WSC or enabling "PIN mode") in order to continue.
25. Start ping from the Console to STA1W/STA14 it must succeed within 90 seconds.
26. STA8/STA13 must be in a disconnected state.
27. Retrieve the PSK or passphrase from the APUT UI. This PSK or passphrase must be different from the one retrieved in the step 10.
28. Change STA8/STA13 configuration using manual legacy methods to the PSK/passphrase and SSID retrieved from the APUT.
29. Start ping from STA8/STA13 to STA1W/STA14; it must succeed within 90 seconds.

Test Pass/Fail Criterion: The APUT must send the correct Beacon/DMG Beacon and Probe Response frames. The APUT must generate different PSK after being reset for out-of-box configuration. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as 'must' is not fulfilled.

4.1.2 Configure APUT using PIN method through an ER that connects via 802.11

Test Applicability: Mandatory for APUT. Mandatory for MAPUT if configuration by external Registrar supported.

Channel Assignment: For 5GHz only APs and for dual band APs, use channel 40. For 2.4GHz only APs, use channel 6.

Test Goal: This test verifies that the APUT implements the PIN method correctly to act as an Enrollee. The APUT must be configurable by an external Registrar that connects via 802.11.

Test Requirement: The APUT must support the PIN Config method. The APUT must be able to act as an Enrollee and register itself with an external Registrar.

Test bed Devices:



1. STA4, which is an External Registrar that connects via 802.11
2. STA8, which does not support any WSC methods (WSC is disabled).
3. A wireless packet sniffer device.
4. “Console” PC attached to the APUT via Ethernet.

Test Procedure:

1. Turn on the APUT.
2. Reset the APUT to out-of-box Configuration.
3. Turn on STA4, which is acting as the ER.
4. On the sniffer device, verify that the Probe Response message that the APUT sends includes the Config method attribute in the WSC IE must reflect the correct configuration methods that the APUT supports as an Enrollee for adding an ER. Check on the sniffer to verify that the list of supported method in the IE is a bitwise OR of values from the list below:

0x0004	Label PIN
0x0010	External NFC Tag
0x0020	Integrated NFC Tag
0x0040	NFC Interface
0x0080	PushButton
0x0100	Keypad
0x0280	Virtual Push Button
0x0480	Physical Push Button
0x2008	Virtual Display PIN
0x4008	Physical Display PIN

The APUT must support every Config method that it advertises as a bitwise OR in the WSC IE.

0x0004

0x0010 – The APUT must support and External NFC Tag.

0x0020 – The APUT must support an Integrated NFC Tag.

0x0040 – The APUT must support an NFC interface.

0x0080 – The APUT cannot use push button to add an External Registrar. If this option is set this test must FAIL.

0x0100 – The APUT must support PIN using a Keypad on the APUT



0x0280 – The APUT cannot use push button to add an External Registrar. If this option is set this test must FAIL.

0x0480 – The APUT cannot use push button to add an External Registrar. If this option is set this test must FAIL.

0x2008 – The APUT must have a PIN in the Virtual UI and support it.

0x4008 – The APUT must have a PIN on the physical display on the APUT and support it.

5. The Registrar on STA4 will be configured with the new parameters (SSID = “scaptest4.1.2ssid” and WPA2-PSK = “scaptest4.1.2psk”) which should be entered when prompted
6. Read the PIN from the APUT and enter the PIN at STA4’s ER when prompted by the ER.
7. Start ping from STA4 to the Console; it must succeed within 90 seconds.
8. Manually configure STA8 with the new parameters (SSID = “scaptest4.1.2ssid” and WPA2-PSK = “scaptest4.1.2psk”).
9. Start ping from STA8 to STA4; it must succeed within 90 seconds.
10. The Beacon packet from the APUT must contain the WSC IE with WSC State set to Configured (0x2). Check on the sniffer.

Test Pass/Fail Criterion: In step 4 and step 10, the WSC State must be set correctly in the WSC IE. Both Ping commands must be successful. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.

4.1.3 Configure APUT using PIN method through an ER that connects via Ethernet

Test Applicability: Mandatory for APUT. Skip for MAPUT.

Channel Assignment: For 5GHz only APs and for dual band APs, use channel 44. For 2.4GHz only APs, use channel 11.

Test Goal: The test verifies that the APUT implements the PIN method to act as an Enrollee with an external Registrar and supports use of a passphrase.

Test Requirement: The APUT must support the PIN Config method and the APUT must be able to act as an Enrollee and register itself with an external Registrar that connects via Ethernet.

Test bed Devices:

1. STA1L which is an External Registrar that connects via Ethernet.
2. STA8, which does not support any WSC methods (WSC is disabled).



3. A wireless packet sniffer device, which is able to capture the wireless packets including the Beacon packet

Test Procedure:

1. Turn on the APUT.
2. Reset the APUT to out-of-box Configuration.
3. Turn on STA1L.
4. Configure STA1L' Registrar with the configuration settings (SSID = "scaptest4.1.3ssid" and WPA2-PSK = "scaptest4.1.3psk"), which should be entered when prompted.
5. Read the PIN from the APUT and enter the PIN at STA1L' Registrar when prompted.
6. Manually configure the STA8 with the parameters (SSID = "scaptest4.1.3ssid" and WPA2-PSK passphrase= "scaptest4.1.3psk").
7. Start pings from STA8 to STA1L; pings must succeed within 90 seconds.
8. The Beacon packet from the APUT must contain the WSC IE with WSC State set to Configured (0x2). Check on the sniffer.
9. The APUT must be capable of displaying the passphrase. The passphrase must be "scaptest4.1.3psk".

Test Pass/Fail Criterion: If both Ping commands are successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as 'must' is not fulfilled.

4.1.4 Configure APUT to use open networking (no security) using PIN method through an ER and add a STA using the internal Registrar

Test Applicability: Mandatory for APUT. Skip for MAPUT.

Channel Assignment: For 2.4GHz only APs and for dual band APs, use channel 1. For 5GHz only APs, use channel 48.

Test Goal: The test verifies that the APUT can be configured to use open networking setting by an external Registrar and that a STA can be added using the internal Registrar.

Test Requirement: The APUT must support PIN Config method

Test bed Devices:

1. STA1L which is an External Registrar that connects via Ethernet.
2. STA8 does not support any WSC methods (WSC is disabled).



3. STA2, which is a WSC Station.

Test Procedure:

1. Turn on the APUT.
2. Reset the APUT to out-of-box Configuration.
3. Turn on STA1L, which is acting as external Registrar
4. The Registrar on STA1L will be configured to use open network settings (SSID = “scaptest4.1.4ssid”) which should be entered when prompted
5. Read the PIN from the APUT and enter the PIN at STA1L when prompted by the Registrar.
6. Start ping from STA1L to the Console; it must succeed within 90 seconds.
7. Enter the PIN for STA2 at the internal Registrar of the APUT. No additional user action is allowed at APUT (enabling WSC or enabling "PIN mode") in order to continue.
8. Start pings from STA2 to STA1L; pings must succeed within 90 seconds.
9. Manually associate STA8 with the APUT using open networking settings (SSID = “scaptest4.1.4ssid”).
10. Start pings from STA8 to STA1L; pings must succeed within 90 seconds.

Test Pass/Fail Criterion: If both Ping commands are successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.

4.1.5 Check PBC Walk Time is correctly implemented

Test Applicability: Mandatory for APUT. Mandatory for MAPUT.

Channel Assignment: For 2.4GHz only APs and for dual band APs, use channel 6. For 5GHz only APs, use channel 36. For 60 GHz only APs, configure the AP to use channel 2. For dual band 2.4 GHz/60 GHz APs, configure the AP(s) to use channels 6 and 2 in each band, respectively. For tri-band 2.4 GHz/5 GHz/60 GHz APs, configure the AP(s) to use channels 6, 36 and 2 in each band, respectively.

Test Goal: The test verifies that the APUT implements the 2 minute Walk Time and resets the timer appropriately. If the period between the time when the WSC button on APUT is pushed and the time when the WSC button on STA is pushed is longer than 2 minutes, the APUT must not succeed in this WSC session.

Test Requirement: The APUT must support PBC method

Test bed Devices:



1. A wireless sniffer device
2. Outside DMG STA5 / Inside DMG STA14, which supports PBC method and is acting as an Enrollee.
3. “Console” PC attached to the APUT via Ethernet.

Test Procedure:

1. Turn on the APUT
2. Reset the APUT to out-of-box Configuration
3. Turn on the wireless sniffer device, set it to monitor the wireless traffic to/from the APUT
4. Outside DMG, using the wireless sniffer device monitor the APUT Beacon. The Device Password ID attribute in the WSC IE of the Beacon frame must NOT be present, and the Selected Registrar flag is either NOT present, or if present, is set to zero (false).
5. Within DMG, using the wireless sniffer device monitor the APUT DMG Beacon and Probe Response frames. The Device Password ID attribute in the WSC IE of the DMG Beacon (if WSC IE present) and Probe Response frames must NOT be present, and the Selected Registrar flag is either NOT present, or if present, is set to zero (false).
6. Push the WSC button (which may be a physical button or a soft button on the AP UI) on the APUT. No additional user action is allowed at APUT (enabling WSC or enabling "Push Button mode") in order to continue.
7. Using the wireless sniffer device:
 - a. Outside DMG: monitor the APUT Beacon. The SelectedRegistrar flag in the WSC IE of the Beacon frame must be present and have value TRUE. The Device Password ID attribute needs to be set to PushButton (0x0004).
 - b. Within DMG: monitor the APUT DMG Beacon and Probe Response frames. The SelectedRegistrar flag in the WSC IE of the DMG Beacon (if WSC IE present) and Probe Response frames must be present and have value TRUE. The Device Password ID attribute must be set to PushButton (0x0004).
8. Wait 1 minute.
9. Push the WSC button on the APUT. No additional user action is allowed at APUT (e.g. enabling WSC or enabling "Push Button mode") in order to continue.
10. Using the wireless sniffer:
 - a. Outside DMG: monitor the APUT Beacon. The SelectedRegistrar flag in the WSC IE of the Beacon frame must be present and have value TRUE. The Device Password ID attribute needs to be set to PushButton (0x0004). The beacon must maintain this state for 2 minutes from the button push in Step 8. After 2 minutes the Device Password ID attribute in



the WSC IE of the Beacon frame must NOT be present, and the Selected Registrar flag is either NOT present, or if present, is set to zero (false).

- b. Within DMG: monitor the APUT DMG Beacon and Probe Response frames. The SelectedRegistrar flag in the WSC IE of the DMG Beacon (if WSC IE present) and Probe Response frames must be present and have value TRUE. The Device Password ID attribute must be set to PushButton (0x0004). The DMG Beacon (if WSC IE present) and Probe Response frames must maintain this state for 2 minutes from the button push in Step 8. After 2 minutes, the Device Password ID attribute in the WSC IE of the DMG Beacon (if WSC IE present) and Probe Response frames must NOT be present, and the Selected Registrar flag is either NOT present, or if present, is set to zero (false).
11. After the 2 minutes in Step 9 have expired push the WSC button on STA5/STA14.
 12. STA5/STA14 must not indicate success.
 13. Wait 1 minute.
 14. Push the WSC button on APUT. No additional user action is allowed at APUT (enabling WSC or enabling "Push Button mode") in order to continue.
 15. Start ping from STA5/STA14 to the Console; it must succeed within 90 seconds.

Test Pass/Fail Criterion: If The Ping command is successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as 'must' is not fulfilled.

4.1.6 Configure APUT using NFC tag method with password token through an external Registrar

Test Applicability: Mandatory for APUT if NFC tag is implemented. Mandatory for MAPUT if NFC tag is implemented and configuration by external Registrar supported.

Test Goal: This test verifies that the APUT implements the NFC tag method with password token to act as an Enrollee. The APUT must be configurable by external Registrar using NFC tag method with password token.

Test Requirement: The APUT must support the NFC tag method with password token. The APUT must be able to act as an Enrollee and register itself with an external Registrar. The APUT must provide a writable NFC tag if the NFC tag method with password token is implemented by creating a password token on a writable NFC tag.

Test bed Devices:

1. STA9 which is an external Registrar that connects via 802.11 and supports NFC tag method with password token.



2. STA7 which does not support any WSC methods.
3. The writable test bed NFC tag type 4
4. A wireless sniffer.

Test Procedure:

1. Turn on the APUT.
2. Reset the APUT to out-of-box Configuration.
3. Turn on the STA9, which is acting as external Registrar.
4. When prompted, configure the Registrar on STA9 with the parameters (SSID = “scaptest4.1.6ssid” and WPA2-PSK = “scaptest4.1.6psk”).
5. Start a WSC NFC password token registration process on APUT following the vendor directions.
6. Touch the NFC Interface of the STA9 with the Password Token
7. Manually configure the STA7 with the parameters (SSID = “scaptest4.1.6ssid” and WPA2-PSK = “scaptest4.1.6psk”)
8. Start ping from the STA7 to the STA9; it must succeed within 90 seconds.
9. Using the wireless packet sniffer, verify that the Beacon packet from the APUT contains the WSC IE with WSC State set to Configured (0x2).

Test Pass/Fail Criterion: If The Ping command is successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.

4.1.7 Manually configure APUT to disable broadcasting of the SSID

Test Applicability: Mandatory for APUT if it has the ability to disable broadcasting of the SSID. Mandatory for MAPUT if it has the ability to disable broadcasting of the SSID.

Channel Assignment: For 2.4GHz only APs and for dual band APs, use channel 11. For 5GHz only APs, use channel 44.

Test Goal: The test verifies that the APUT disables WSC if the user disables broadcasting of the SSID.

Test Requirement: The APUT must disable WSC when the user manually disables broadcasting of the SSID.

Test bed Devices:

1. A wireless packet sniffer device, which is able to capture the wireless packets including the Beacon and Probe Response packet

**Test Procedure:**

1. Turn on the APUT.
2. Reset the APUT to out of box Configuration.
3. On the UI of the APUT disable broadcasting of the SSID.
4. The UI must inform the user that WSC will be disabled and require confirmation or require explicit user operation to continue.
5. As soon as WSC is disabled the beacons and probe responses transmitted by the APUT must not include the WSC IE.
6. Start the wireless packet sniffer device; verify that the APUT's beacons do not include the WSC IE.

Test Pass/Fail Criterion: If in the last step 6 the beacons do not include the WSC IE, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as 'must' is not fulfilled.

4.1.8 Manually configure APUT to use open networking (no security) and add a STA using internal registrar

Test Applicability: Mandatory for APUT. Mandatory for MAPUT.

Channel Assignment: For 2.4GHz only APs and for dual band APs, use channel 1. For 5GHz only APs, use channel 48. For 60 GHz only APs, configure the AP to use channel 2. For dual band 2.4 GHz/60 GHz APs, configure the AP(s) to use channels 1 and 2 in each band, respectively. For tri-band 2.4 GHz/5 GHz/60 GHz APs, configure the AP(s) to use channels 1, 46 and 2 in each band, respectively.

Test Goal: The test verifies that the APUT can be manually configured to use open networking setting (no security) and that a STA can be added using the internal registrar. The APUT must notify the user and require user acknowledgement when security is disabled.

Test Requirement: The APUT must support PIN Configuration method.

Test bed Devices:

1. Outside DMG STA1W / Inside DMG STA12, which supports PIN Configuration method and is acting as an Enrollee. The STA1W/STA12 has the ability to correctly validate all WSC Attributes marked as R (required) in the Credential Attribute delivered in message M8 (including the Network Key which in this case must be a zero-length attribute).
2. "Console" PC attached to the APUT via Ethernet.



Test Procedure:

1. Turn on the APUT.
2. Reset the APUT to Out of Box Configuration.
3. On the UI of the APUT, configure the APUT with new security settings SSID = “scaptest4.1.8ssid” and open (no security).
4. The internal Registrar must inform the user that security is not set and require confirmation or require explicit user operation to create this open network.
5. Turn on the STA1W/STA12.
6. Read the PIN displayed on the STA1W/STA12 and enter the PIN in the internal Registrar on the APUT.
7. Start ping from the Console to STA1W/STA12; it must succeed within 90 seconds.

Test Pass/Fail Criterion: If the Ping command is successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.

4.1.9 Disable WSC if the APUT is manually configured for WEP

Test Applicability: Mandatory for APUT if WEP supported. Mandatory for MAPUT if WEP supported.

Channel Assignment: For 2.4GHz only APs and for dual band APs, use channel 11. For 5GHz only APs, use channel 44.

Test Goal: The test verifies that the APUT disables WSC if the APUT is manually configured for WEP

Test Requirement: The APUT must disable WSC when the APUT is manually configured for WEP

Test bed Devices:

1. A wireless packet sniffer device, which is able to capture the wireless packets including the Beacon and Probe Response packet

Test Procedure:

1. Turn on the APUT.
2. Reset the APUT to out of box Configuration.



3. Disable 11n mode on the APUT as 11n mode prevents WEP from being used. On the UI of the APUT enable WEP
4. The UI must inform the user that WSC will be disabled and require confirmation or require explicit user operation to continue.
5. As soon as WSC is disabled the beacons and probe responses transmitted by the APUT must not include the WSC IE.
6. Start the wireless packet sniffer device; verify that the APUT's beacons do not include the WSC IE.

Test Pass/Fail Criterion: If in the last step 6 the beacons do not include the WSC IE, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as 'must' is not fulfilled

4.1.10 WSC fails if the APUT is configured for WEP by a WSC 1.0 external Registrar

Test Applicability: Mandatory for APUT if WEP supported. Mandatory for MAPUT if WEP supported and configuration by external Registrar supported.

Channel Assignment: For 2.4GHz only APs and for dual band APs, use channel 11. For 5GHz only APs, use channel 44.

Test Goal: The test verifies that the APUT returns a WSC_NACK if an attempt is made to configure the APUT for WEP by a WSC 1.0 external registrar

Test Requirement: The APUT must return a WSC_NACK if an attempt is made to configure the APUT for WEP by a WSC 1.0 external registrar

Test bed Devices:

1. STA3 which is an External Registrar that connects via 802.11 in WSC 1.0 mode that is capable of configuring APs for WEP.
2. A wireless packet sniffer device, which is able to capture the wireless packets including the EAP packets.

Test Procedure:

1. Turn on the APUT.
2. Reset the APUT to out of box Configuration.
3. Turn on the STA3's ER.
4. Configure the STA3's ER for WEP.
5. Read the PIN from the APUT



6. Using the APUT's PIN use the STA3's ER to configure the APUT for WEP
7. Use the sniffer to verify that the response to M8 is WSC_NACK.
8. If WSC_NACK is observed TEST PASS else TEST Fail

Test Pass/Fail Criterion: If in step 8 WSC_NACK is observed the test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as 'must' is not fulfilled

4.1.11 Disable WSC if the APUT is manually configured for WPA/TKIP only, unless the APUT is configured for mixed mode

Obsoleted January 1, 2014

4.1.12 APUT correctly handles WPA/TKIP configuration from a WSC 1.0 ER

Test Applicability: Mandatory for APUT. Mandatory for MAPUT if configuration by external Registrar supported.

Channel Assignment: For 2.4GHz only APs and for dual band APs, use channel 11. For 5GHz only APs, use channel 44.

Test Goal: The test verifies that the APUT is configured either for mixed mode or will reject WSC configuration request if an attempt is made to configure the APUT for WPA/TKIP only by a WSC 1.0 external registrar.

Test Requirement: The APUT must be configured for mixed mode if an attempt is made to configure the APUT for WPA/TKIP only by a WSC 1.0 external registrar

Test bed Devices:

1. STA8 which is an External Registrar that connects via 802.11 in WSC 1.0 mode that is capable of configuring an APUT for WPA/TKIP only
2. STA5
3. STA1W that is capable of being configured for WPA/TKIP only
4. A wireless packet sniffer device, which is able to capture the wireless packets including the Association request packet
5. "Console" PC attached to the APUT via Ethernet.

Test Procedure:



1. Turn on the APUT.
2. Reset the APUT to out of box Configuration.
3. Turn on the test bed external registrar
4. Configure the STA8's ER for WPA/TKIP only with new security settings (SSID = "scaptest4.1.12ssid" and WPA-Personal passphrase = "scaptest4.1.12psk").
5. Read the PIN from the APUT
6. Use STA8's ER to configure the APUT for WPA/TKIP only
7. If APUT does not support mixed mode, use the sniffer to verify that the response to M8 is WSC_NACK. If WSC_NACK is observed TEST PASS else TEST continues
8. Manually configure STA5 with new security settings SSID = "scaptest4.1.12ssid" and WPA2-Personal = "scaptest4.1.12psk"
9. Manually configure STA1W with new security settings SSID = "scaptest4.1.12ssid" and WPA-Personal = "scaptest4.1.12psk"
10. Start pings from the Console to STA5 and STA1W; they must succeed within 90 seconds

Test Pass/Fail Criterion: If either WSC_NACK is observed in step 7 or successful Ping has been observed in the step 10, the test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as 'must' is not fulfilled

4.1.13 APUT correctly uses AuthorizedMACs subelement in the WFA Vendor Extension attribute in Beacons/DMG Beacons and Probe Responses

Test Applicability: Mandatory for APUT. Mandatory for MAPUT.

Channel Assignment: For 5GHz only APs and for dual band APs, use channel 48. For 2.4GHz only APs, use channel 6. For 60 GHz only APs, configure the AP to use channel 2. For dual band 2.4 GHz/60 GHz APs, configure the AP(s) to use channels 6 and 2 in each band, respectively. For tri-band 2.4 GHz/5 GHz/60 GHz APs, configure the AP(s) to use channels 6, 48 and 2 in each band, respectively.

Test Goal: The test verifies that the APUT implements the PIN method to act as an internal registrar and is able to add the Enrollee or Wildcard MAC address to the AuthorizedMACs subelement in the WFA Vendor Extension attribute in Beacon/DMG Beacon and Probe Response frames, and remove the wildcard MAC address (if present) from Beacon/DMG Beacon and Probe Response frames after the registration process has completed successfully.

Test Requirement: The APUT must support PIN method. The APUT may support selection of the STA to commence the PIN registration process from a list on its user interface.

**Test bed Devices:**

1. Outside DMG STA1W / Inside DMG STA14, which supports PIN Config method as an Enrollee.
2. Outside DMG STA2 / Inside DMG STA13, which supports PIN Config method as an Enrollee.
3. A wireless packet sniffer device.

Test Procedure:

1. Turn on the APUT
2. Reset the APUT to out-of-box configuration
3. Turn on the sniffer.
4. Turn on STA1W/STA14 and start a WSC PIN registration process.
5. Turn on STA2/STA13 and start a WSC PIN registration process. STA2/STA13 must use a different PIN to STA1W/STA14.
6. If the APUT user interface allows selection of a particular STA to begin the registration process from a list then select STA1W/STA14, otherwise skip this step.
7. Read the PIN displayed on STA1W/STA14 and enter the PIN in the internal Registrar on the APUT. No additional user action is allowed at APUT (e.g. enabling WSC or enabling "PIN mode") in order to continue.
8. Start ping from STA1W/STA14 to the Console; it must succeed within 90 seconds.
9. Start ping from STA2/STA13 to the Console; it must not succeed.
10. If the ping from STA1W/STA14 succeeded, check the sniffer trace for the following.
 - a. Outside of DMG: If the APUT user interface allowed selection of STA1W/STA14 to commence the registration process then the AuthorizedMACs subelement in the WFA Vendor Extension attribute with the MAC address of STA1W/STA14 must be present, and the MAC address of STA2/STA13 must not be present, in Beacons and Probe Responses from the APUT that follow the commencement of the PIN registration process on the APUT. If the APUT user interface did not allow selection of STA1W/STA14 then the AuthorizedMACs subelement in the WFA Vendor Extension attribute in Beacons and Probe Responses sent by the APUT must contain the wildcard MAC address (FF:FF:FF:FF:FF:FF) after the PIN has been entered on the APUT, and in this case following a successful PIN method registration by STA1W/STA14 the AuthorizedMACs subelement in the WFA Vendor Extension attribute must not include the wildcard MAC address in the Beacons and Probe Responses sent by the APUT.



- b. Within DMG: If the APUT user interface allowed selection of STA1W/STA14 to commence the registration process, then the AuthorizedMACs subelement in the Wi-Fi Alliance Vendor Extension attribute with the MAC address of STA1W/STA14 must be present, and the MAC address of STA2/STA13 must not be present, in Probe Response frames and may be present in DMG Beacon frames from the APUT that follow the commencement of the PIN registration process on the APUT. If the APUT user interface did not allow selection of STA1W/STA14, then the AuthorizedMACs subelement in the Wi-Fi Alliance Vendor Extension attribute in DMG Beacon frames (if WSC IE exists) and Probe Response frames sent by the APUT must contain the wildcard MAC address (FF:FF:FF:FF:FF:FF) after the PIN has been entered on the APUT, and in this case following a successful PIN method registration by STA1W/STA14 the AuthorizedMACs subelement in the Wi-Fi Alliance Vendor Extension attribute must not include the wildcard MAC address in the DMG Beacon (if WSC IE exists) and Probe Response frames sent by the APUT.

Test Pass/Fail Criterion: If the Ping command to STA1W/STA14 is successful and the Ping command to STA2/STA13 is unsuccessful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.

4.1.14 APUT detects and mitigates against brute-force attack on static PIN by external Registrars

Test Applicability: Mandatory for APUT if static PIN implemented. Mandatory for MAPUT if static PIN implemented.

Channel Assignment: For 2.4GHz only APs and for dual band APs, use channel 11. For 5GHz only APs, use channel 44.

Test Goal: The test verifies that the APUT detects and mitigates against a brute force attack on its static PIN by an attacker acting as an External Registrar. The APUT must detect the attack after at most 10 failed PIN attempts by all External Registrars using the same PIN or different PINs with no time limitation to enter the PINs. The APUT must then enter and advertise Setup Locked state, indefinitely preventing the use of the AP’s correct PIN to add External Registrars to the network. Once in the indefinitely locked state, the PIN must only be unlocked by the user’s intervention.

Test Requirement: The APUT must support an External Registrar connected via 802.11. The APUT must have a static PIN. The APUT must detect a brute-force attack after at most 10 unsuccessful PIN attempts using the same PIN or different PINs. The APUT may temporarily enter the locked state for a vendor defined time after which the APUT will allow the use of its PIN without any user intervention, or the APUT may enter the indefinitely locked state before 10 incorrect PINs are entered at the ER. For this test’s purposes, an indefinite lock is assumed to occur if any lock lasts more than 30



minutes. If no lock lasts 30 minutes, then the test will be terminated and the test passed if the sum of all lock times exceeds 60 minutes. NOTE: the limitation of 30 or 60 minutes is purely for the efficiency of the test environment, and does not preclude the requirement for the APUT to enter an indefinite lockdown state after at most 10 failed PIN attempts.

Test bed Devices:

1. STA1W which is an External Registrar that connects via 802.11. This ER allows selection of the AP with which it will attempt to run the registration protocol, and allows an operator to make attempts using different PINs. Note that the External Registrar may also make multiple attempts using the same PIN if the PIN is incorrect.
2. A wireless packet sniffer device, which is capable of capturing wireless packets including the Beacon and Probe Response packets.

Test Procedure:

1. Prepare eleven different valid PINs (i.e., with correct checksum digit), which are not the same as the APUT static PIN. These are termed incorrect PINs in the steps below.
2. Turn on the APUT.
3. Reset the APUT to out-of-box Configuration.
4. Turn on the STA1W.
5. Turn on the wireless sniffer and start to monitor the traffic to & from the APUT.
6. If there was a previous incorrect PIN, after 10 seconds cancel that PIN attempt.
7. Enter the incorrect PIN at the STA1W's ER when prompted, and select the APUT as the AP with which to run the registration protocol.
8. Check the beacon to see if the APUT is in the locked state. If not locked, go to step 6.
9. Wait and record the time duration between the start of the locked state and the end of the locked state; this is the lock duration. If the lock duration is greater than 30 minutes, go to step 13.
10. If this lock duration is less than 30 minutes (the APUT unlocks at this point, or we would still be waiting to see if the lock state goes past 30 minutes), add up all the lock durations to this point. If the sum of the lock times exceeds 60 minutes, enter enough incorrect PINs to force the APUT into a locked state. Proceed to step 13.
11. If all 11 incorrect PINs have been entered, no lock time has exceeded 30 minutes and the sum of all lock times is less than 60 minutes, STOP testing and FAIL the test.
12. Return to step 6 and enter the next incorrect PIN.
13. Using the APUT's correct PIN, enter this PIN into the External Registrar. Verify the following on the wireless sniffer device. The APUT must be in a Setup Locked state.. In Setup Locked state the Beacon and Probe Response frames



transmitted by the APUT must include an AP Setup Locked attribute in the WSC IE. Also in Setup Locked state if the APUT allows operation as an Enrollee to be started by sending WSC message M1, and the External Registrar sends WSC message M2, the APUT must reply to M2 with a WSC_NACK with a configuration error value equal to Setup Locked (15).

Test Pass/Fail Criterion: The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled in step 13, or the test fails in step 11. Otherwise the test is determined as a PASS.

4.2 Add devices

4.2.1 Manually configure APUT and add device using PIN method, and then add device using PBC method

Test Applicability: Mandatory for APUT. Mandatory for MAPUT.

Channel Assignment: For 2.4GHz only APs use channel 11. For dual band APs, use channel 11 for steps 1 to 20 and channel 40 for steps 21 to 25. For 5GHz only APs, use channel 40. For 60 GHz only APs, configure the AP to use channel 2. For dual band 2.4 GHz/60 GHz APs, configure the AP(s) to use channels 11 and 2 in each band, respectively. For tri-band 2.4 GHz/5 GHz/60 GHz APs, configure the AP(s) to use channels 11, 40 and 2 in each band, respectively.

Test Goal:

- Outside of DMG: The test verifies that the APUT implements the PIN and PBC method to act as an internal Registrar. The configured APUT must be able to add a STA device to its WLAN using PIN method and then add a STA device using PBC method. This test also verifies that the correct PIN must be used and a bad checksum is correctly identified. A legacy station validates that the manual configuration does not change after adding devices with WSC. The test also verifies that a dual band AP includes the RF Bands and UUID-E attributes in its Beacons and Probe Responses in both bands.
- Within DMG: The test verifies that the APUT implements the PIN and PBC method to act as an internal Registrar. The configured APUT must be able to add a STA device to its WLAN using PIN method and then add a STA device using PBC method. This test also verifies that the correct PIN must be used and a bad checksum is correctly identified. The test also verifies that a dual band AP includes the RF Bands and UUID-E attributes in its Beacon and Probe Response frames in both bands.

Test Requirement: The APUT must support PIN and PBC method

Test bed Devices:



1. Outside DMG STA2 / Inside DMG STA13, which supports PIN Config method and is acting as an Enrollee
2. Outside DMG STA4 / Inside DMG STA14, which supports PBC method and is acting as an Enrollee
3. Outside DMG: STA8, which does not support any WSC method.
4. A wireless packet sniffer device, which is able to capture the wireless packet including the Beacon/DMG Beacon and Probe Response frame
5. “Console” PC attached to the APUT via Ethernet.

Test Procedure:

1. Turn on the APUT
2. Reset the APUT to out-of-box Configuration
3. On the UI of the APUT, configure the APUT with new security settings (SSID = “scaptest4.2.1ssid” and WPA(2)-PSK = “scaptest4.2.1psk”).
4. Outside of DMG: Turn on STA8 and set security setting to the manually configured APUT settings (SSID = “scaptest4.2.1ssid” and WPA(2)-PSK = “scaptest4.2.1psk”). Within DMG: Skip
5. Outside of DMG: Start ping from STA8 to the Console; it must succeed within 90 seconds. Within DMG: Skip
6. Turn on STA2/STA13 and start WSC PIN enrollment.
7. Enter PIN of 12345671 (invalid checksum PIN) in the internal Registrar on the APUT. No additional user action is allowed at APUT (e.g. enabling WSC or enabling "PIN mode") in order to continue.
8. Internal Registrar must report an invalid PIN
9. Enter PIN of 12345670 (if the STA2/STA13's PIN is 12345670 then use PIN 24681353) in the internal Registrar on the APUT. No additional user action is allowed at APUT (e.g. enabling WSC or enabling "PIN mode") in order to continue.
10. Start ping from the Console to STA2/STA13; it must fail.
11. Read the PIN displayed on STA2/STA13 and enter the PIN in the internal Registrar on the APUT. No additional user action is allowed at APUT (e.g. enabling WSC or enabling "PIN mode") in order to continue.
12. On the wireless packet sniffer device, verify that the Selected Registrar flag is TRUE, Device Password ID is Zero and Selected Registrar Configuration Methods attributes in the WSC IE of the Beacon and Probe Response frame are present and indicate PIN when APUT activates the registration protocol to accept new Enrollee.



13. Start ping from STA2/STA13 to the Console; it must succeed within 90 seconds (AP must be configured at this point).
14. Turn on STA4/STA14.
15. Push the WSC button on the APUT. No additional user action is allowed at APUT (enabling WSC or enabling "Push Button mode") in order to continue.
16. On the wireless packet sniffer device,
 - a. Outside of DMG: verify that the Selected Registrar flag is TRUE, Device Password ID is 4 and Selected Registrar Configuration Methods attributes in the WSC IE of the Beacon and Probe Response frame include PBC. If the APUT is dual band capable, the WSC IE of the Beacon and Probe Response must also contain the RF Bands and UUID-E attributes.
 - b. Within DMG: verify that the Selected Registrar flag is TRUE, Device Password ID is 4 and Selected Registrar Configuration Methods attributes in the WSC IE of the DMG Beacon (if WSC IE exists) and Probe Response frame include PBC. If the APUT is dual band capable, the WSC IE of the DMG Beacon and Probe Response frame must also contain the RF Bands and UUID-E attributes.
17. Push the WSC button on STA4/STA14.
18. Start ping from STA4/STA14 to STA2/STA13; it must succeed within 90 seconds.
19. Outside of DMG: Verify ping from STA8 to the Console; it must succeed within 90 seconds. Within DMG: skip.
20. On the wireless packet sniffer device,
 - a. Outside of DMG: verify that the Device Password ID and Selected Registrar Configuration Methods attributes in the WSC IE of the Beacon and Probe Response frame are NOT present after the successful WSC handshake, and the Selected Registrar flag is either NOT present, or if present, is set to zero (false). Single band APUTs finish the test here. Dual band APUTs continue.
 - b. Within DMG: verify that the Device Password ID and Selected Registrar Configuration Methods attributes in the WSC IE of the DMG Beacon (if WSC IE exists) and Probe Response frame are NOT present after the successful WSC handshake, and the Selected Registrar flag is either NOT present, or if present, is set to zero (false). Single band APUTs finish the test here. Multi band APUTs continue.
21. Restart or configure STA4/STA14 so that it is no longer associated to the APUT, and start the wireless sniffer device in channel 40.
22. Push the WSC button on STA4/STA14.
23. Push the WSC button on the APUT. No additional user action is allowed at APUT (e.g. enabling WSC or enabling "Push Button mode") in order to continue.
24. Start ping from STA4/STA14 to STA2/STA13; it must succeed within 90 seconds.



25. On the wireless packet sniffer device check the Beacons and Probe Responses that were sent by the AP after the button was pressed on the AP and before the registration protocol started. The WSC IE of the Beacon and Probe Response must contain the RF Bands and UUID-E attributes.

Test Pass/Fail Criterion: If the Ping commands are successful where required, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.

4.2.2 Add devices using PIN method, and then add device using PBC method to out-of-box APUT

Test Applicability: Mandatory for APUT. Mandatory for MAPUT.

Channel Assignment: For 5GHz only APs and for dual band APs, use channel 48. For 2.4GHz only APs, use channel 6. For 60 GHz only APs, configure the AP to use channel 2. For dual band 2.4 GHz/60 GHz APs, configure the AP(s) to use channels 6 and 2 in each band, respectively. For tri-band 2.4 GHz/5 GHz/60 GHz APs, configure the AP(s) to use channels 6, 48 and 2 in each band, respectively.

Test Goal: The test verifies that the APUT implements the PIN and PBC method to act as an internal Registrar from its out-of-box state. The APUT must be able to add 2 STAs device to its WLAN using PIN method and then add STA device using PBC method. The APUT must be able to tolerate the inclusion of an extraneous hyphen (dash) during the PIN entry and must be able to handle a 4-digit PIN entry.

Test Requirement: The APUT must support PIN and PBC method

Test bed Devices:

1. Outside DMG STA2 / Inside DMG STA13, which supports PIN Config method and is acting as an Enrollee
2. Outside DMG STA4 / Inside DMG STA12, which supports PIN Config method and will generate a 4-digit PIN and is acting as an Enrollee
3. Outside DMG STA5 / Inside DMG STA14, which supports PBC method and is acting as an Enrollee.

Test Procedure:

1. Turn on the APUT
2. Reset the APUT to out-of-box configuration
3. Turn on STA2/STA13.
4. Read the PIN displayed on STA2/STA13 and enter the PIN in the internal Registrar on the APUT. No additional user action is allowed at APUT (enabling



WSC or enabling "PIN mode") in order to continue. NOTE: enter the PIN by inserting a hyphen (dash) between the first four digits and the last four digits (e.g., nnnn-nnnn)

5. Start ping from STA2/STA13 to the Console; it must succeed within 90 seconds.
6. Turn on STA4/STA12.
7. Read the 4-digit PIN displayed on STA4/STA12 and enter the 4-digit PIN in the internal Registrar on the APUT.
8. Ping from STA4/STA12 to the Console must succeed within 90 seconds.
9. Turn on STA5/STA14.
10. Push the WSC button on STA5/STA14.
11. Push the WSC button on the APUT. No additional user action is allowed at APUT (enabling WSC or enabling "Push Button mode") in order to continue.
12. Start ping from STA5/STA14 to STA2/STA13; it must succeed within 90 seconds.

Test Pass/Fail Criterion: If the both of Ping commands are successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as 'must' is not fulfilled.

4.2.3 Add devices using multiple external Registrars and internal Registrar

Test Applicability: Mandatory for APUT. Skip for MAPUT.

Channel Assignment: For 2.4GHz only APs and for dual band APs, use channel 11. For 5GHz only APs, use channel 44.

Test Goal: The test verifies that the APUT supports interchangeable use of the internal registrar, an external Registrar connected via Ethernet and an external Registrar connected via 802.11 to add enrollees.

Test Requirement: The APUT must support external Registrars connected via Ethernet and via 802.11. The APUT must support PIN Config method.

Test bed Devices:

1. STA4, which supports PIN Config method and is an External Registrar that connects via 802.11.
2. STA2, which supports PIN Config method and is an Enrollee
3. STA5, which supports PIN Config method and is an Enrollee
4. STA3, which supports PIN Config method and is an Enrollee



5. STA1L, which supports PIN Config method and is as an External Registrar that connects via Ethernet. STA1L has the ability to show the list of enrollees based on the received Probe Request proxied by APUT and let users to select a target enrollee from the list. Also STA1L is capable of adding a selected enrollee's MAC address in the AuthorizedMACs subelement in the WFA Vendor Extension attribute in SetSelectedRegistrar UPnP action and send it to the APUT
6. A wired packet sniffer device, which is able to capture the UPnP packets exchanged between an External Registrar and APUT over the Ethernet connection
7. A wireless packet sniffer device, which is capable to capture the wireless packet including the Beacon and Probe Response packets

Test Procedure:

1. Turn on the APUT
2. Reset the APUT to out-of-box Configuration
3. Turn on STA1L, which is acting as external Registrar.
4. The Registrar on STA1L will be configured with the new wireless configuration settings (SSID = "scaptest4.2.3ssid" and WPA(2)-PSK = "scaptest4.2.3psk"), which should be entered when prompted
5. Read the PIN from the APUT and enter the PIN at STA1L when prompted by the Registrar.
6. The Registrar on STA1L will display status on completion. The status must be success.
7. Turn on STA4, which is acting as external Registrar
8. Read the PIN from the APUT and enter the PIN at the external Registrar on STA4 when prompted by the Registrar.
9. Start ping from STA4 to STA1L; it must succeed within 180 seconds.
10. Turn on the wired and wireless sniffer devices and start to monitor the traffic to/from the APUT
11. Turn on STA2, which is acting as an Enrollee. Then start a WSC PIN registration process per the Test bed vendor direction
12. Enter the PIN from STA2 into the external Registrar on STA1L.
13. Start ping from STA2 to STA1L; it must succeed within 180 seconds.
14. Verify the following on the wired sniffer. The APUT must proxy the received Probe Request from STA2.
15. Verify the following on the wireless sniffer device. After the PIN has been entered into the external Registrar on STA1L, and while the WSC handshake is in progress, the Beacon and Probe Response frames transmitted by the APUT



must include an AuthorizedMACs subelement in the WFA Vendor Extension attribute in the WSC IE. Said AuthorizedMACs subelement in the WFA Vendor Extension attribute must include the MAC address of STA2. The AuthorizedMACs subelement in the WFA Vendor Extension attribute must not be present in the Beacon and Probe Response frames sent by the APUT after the registration for STA2 has concluded successfully. Note that depending on delays between the external Registrar on STA1L and the APUT it may take up to five seconds for the AuthorizedMACs subelement in the WFA Vendor Extension attribute to be removed from Beacons and Probe Responses sent by the APUT after the registration has concluded.

16. Turn off STA1L.
17. Turn on STA5, which is acting as an Enrollee
18. Enter the PIN from STA5 into the external Registrar on STA4. No additional user action is allowed at APUT (e.g. enabling WSC or enabling "PIN mode") in order to continue.
19. Start ping from STA4 to STA5; it must succeed within 180 seconds.
20. Turn on STA3, which is acting as an Enrollee
21. Enter the PIN from STA3 into the internal Registrar on APUT
22. Start ping from STA2 to STA3; it must succeed within 180 seconds.

Test Pass/Fail Criterion: If all of PING commands are successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as 'must' is not fulfilled.

4.2.4 Mixed mode test with PIN including whitespace and manually add a legacy WPA device

Test Applicability: Mandatory for APUT. Mandatory for MAPUT.

Channel Assignment: For 2.4GHz only APs and for dual band APs, use channel 6. For 5GHz only APs, use channel 40.

Test Goal:

- The test verifies that the APUT can support WPA/WPA2 mixed mode. For APUTs that support WPA2 only or WPA2 and open configurations, use WPA2.
- A legacy STA which uses only WPA-Personal can be manually added to the APUT's WLAN. Skip this if the APUT supports only WPA2 or WPA2 and open configurations.
- The APUT must be able to tolerate the inclusion of an extraneous space during the PIN entry.

Test Requirement: The APUT must mixed-mode (WPA+WPA2).

**Test bed Devices:**

1. STA3, which supports PIN Config method and is acting as an Enrollee
2. STA8, which uses WPA only

Test Procedure:

Note: skip steps 7 and 8 if the APUT supports only WPA2 or WPA2 and open configurations.

1. Turn on the APUT
2. Reset the APUT to out-of-box Configuration. The default out-of-box configuration must be either open or WPA2 security.
3. Configure APUT to support mixed mode if supported. The APUT must not support mixed mode as an out-of-box configuration. If not supported configure for WPA2.
4. Turn on STA3, which is acting as an Enrollee
5. Enter the PIN from STA3 at internal Registrar on APUT. NOTE: enter the PIN by inserting a space between the first four digits and the last four digits (e.g., nnnn nnnn) No additional user action is allowed at APUT (enabling WSC or enabling "PIN mode") in order to continue.
6. Start ping from STA3 to the Console; it must succeed within 90 seconds.
7. Retrieve the SSID and PSK from the UI on the APUT.
8. Manually configure STA8 with the SSID and PSK of the APUT using WPA-Personal.
9. Start ping from STA8 to STA3; it must succeed within 90 seconds.

Test Pass/Fail Criterion: If both of PING commands are successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as 'must' is not fulfilled.

4.2.5 Add device using NFC tag method with password token

Test Applicability: Mandatory for APUT if NFC tag is implemented. Mandatory for MAPUT if NFC tag is implemented.

Test Goal: The test verifies that the APUT implements the NFC tag method with password token to act as an internal Registrar. The configured APUT must be able to add a STA device to its WLAN using NFC tag method with password token.

Test bed Devices:

1. STA11 which supports NFC tag method with password token and is acting as an Enrollee.



2. The writable test bed NFC tag type 1, type 3 and type 4.

Test Procedure:

1. Turn on the APUT.
2. Reset the APUT to out-of-box Configuration.
3. Turn on the Test bed STA.
4. Create a Password Token for the Test bed STA by selecting the password token generation function on the UI of the Test bed STA and touching the NFC Interface with the writable Test bed NFC Tag Type1.
5. Touch the APUT with the created Password Token.
6. Test bed STA is requested to connect to APUT.
7. Start ping from the Test bed STA to Console; it must succeed within 90 seconds.
8. Reset the APUT to out-of-box Configuration.
9. Create a Password Token for the Test bed STA by selecting the password token generation function on the UI of the Test bed STA and touching the NFC Interface with the writable Test bed NFC Tag Type3.
10. Touch the APUT with the created Password Token.
11. Test bed STA is requested to connect to APUT.
12. Start ping from the Test bed STA to Console; it must succeed within 90 seconds.
13. Reset the APUT to out-of-box Configuration.
14. Create a Password Token for the Test bed STA by selecting the password token generation function on the UI of the Test bed STA and touching the NFC Interface with the writable Test bed NFC Tag Type4.
15. Touch the APUT with the created Password Token.
16. Test bed STA is requested to connect to APUT.
17. Start ping from the Test bed STA to Console; it must succeed within 90 seconds.

Test Pass/Fail Criterion: If The Ping command is successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.

4.2.6 Add device using NFC tag method with configuration token

Test Applicability: Mandatory for APUT if NFC tag is implemented. Mandatory for MAPUT if NFC tag is implemented.



Test Goal: The test verifies that the APUT implements the NFC tag method with configuration token to act as an internal Registrar. The configured APUT must be able to add a STA device to its WLAN using NFC tag method with configuration token.

Test bed Devices:

1. STA9 which supports NFC tag method with configuration token and is acting as an Enrollee.
2. The writable test bed NFC tag type 1, type 3 and type 4.

Test Procedure:

1. Turn on the APUT.
2. Reset the APUT to out-of-box Configuration.
3. Turn on the Test bed STA.
4. Create a configuration token by selecting the configuration token generation function on the UI and touching the NFC Interface of the APUT with the writable Test bed NFC Tag Type1.
5. Touch the Test bed STA with the created configuration token.
6. Start ping from the Test bed STA to the Console; it must succeed within 90 seconds.
7. Reset the APUT to out-of-box Configuration.
8. Create a configuration token by selecting the configuration token generation function on the UI and touching the NFC Interface of the APUT with the writable Test bed NFC Tag Type3.
9. Touch the Test bed STA with the created configuration token.
10. Start ping from the Test bed STA to the Console; it must succeed within 90 seconds.
11. Reset the APUT to out-of-box Configuration.
12. Create a configuration token by selecting the configuration token generation function on the UI and touching the NFC Interface of the APUT with the writable Test bed NFC Tag Type4.
13. Touch the Test bed STA with the created configuration token.
14. Start ping from the Test bed STA to the Console; it must succeed within 90 seconds.

Test Pass/Fail Criterion: If The Ping command is successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as 'must' is not fulfilled.



4.2.7 Add device using PIN Method when AP has MAC Address filtering enabled

Test Applicability: Mandatory for APUT if user specified white list (addresses that are allowed) MAC Address Filtering is implemented. Mandatory for MAPUT if user specified white list (addresses that are allowed) MAC Address Filtering is implemented.

Test Goal: The test verifies that the APUT allows a STA to be added when MAC Address filtering is enabled or WSC gets disabled.

Test Requirement: The APUT must support MAC address filtering

Test bed Devices:

1. STA3, which supports PIN

Test Procedure:

1. Turn on the APUT.
2. Reset the APUT to out of box Configuration.
3. Turn on MAC Address filtering and do not add any MAC addresses to the allowed list
4. Use a sniffer to determine if the WSC IE is still being included in the beacon, if not TEST PASS, else continue to step 5.
5. Read the PIN from STA3 and enter the WSC PIN on the APUT.
6. Start ping from STA3 to the Console; it must succeed within 90 seconds.
7. Reboot the APUT
8. After the APUT is rebooted, start ping from STA3 to the Console. The ping must succeed within 90 seconds.

Test Pass/Fail Criterion: If the Ping command is successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as 'must' is not fulfilled.

4.2.8 Protocol Extensibility

Test Applicability:

Outside of DMG: Mandatory for APUT. Skip for MAPUT.

Within DMG: Mandatory for both APUT and MAPUT.

Channel Assignment: For 2.4GHz only APs and for dual band APs, use channel 11. For 5GHz only APs, use channel 40. For 60 GHz only APs, configure the AP to use channel 2. For dual band 2.4 GHz/60 GHz APs, configure the AP(s) to use channels 11



and 2 in each band, respectively. For tri-band 2.4 GHz/5 GHz/60 GHz APs, configure the AP(s) to use channels 11, 40 and 2 in each band, respectively.

Test Goal: The test verifies that the APUT supports protocol extensibility by accepting higher version number and new attributes.

Test Requirement: The APUT must support WSC Protocol

Test bed Devices:

1. Outside DMG STA2 / Inside DMG STA12 that can be configured to advertise different version number, add a new attribute and include some attributes with zero length data fields.
2. Outside of DMG, STA4 which is an External Registrar that connects via 802.11 and can be configured to advertise different version number and to add a new attribute.

Test Procedure:

1. Turn on the APUT
2. Reset the APUT to out-of-box Configuration
3. On the UI of the APUT, configure the APUT with new security settings (SSID = “scaptest4.2.8-ssid” and WPA(2)-Personal passphrase = “scaptest4.2.8-psk”).
4. Turn on STA2/STA12 and configure it to advertise version 5.7 and to add a new attribute (i.e., an attribute that is not defined in WSC 2.0 specification) to all messages.
5. Read the displayed PIN on STA2/STA12 and enter the PIN in the internal Registrar of the APUT.
6. Start ping from Console to STA2/STA12; it must succeed within 90 seconds.
7. Outside of DMG: Perform steps 8-13.
8. Disconnect STA2/STA12 from the APUT and remove the provisioned network from STA2/STA12.
9. Start STA4 external Registrar and configure it to advertise version 5.7 and to add a new attribute (i.e., an attribute that is not defined in WSC 2.0 specification) to all messages.
10. The APUT is configured using STA4 external Registrar with new security settings (SSID = “scaptest4.2.8-er” and WPA(2)-Personal passphrase = “scaptest4.2.8-psk-er”). Read the PIN from the APUT and enter the PIN at STA4 external Registrar when prompted by the Registrar. The APUT must change its configuration (SSID and passphrase) to match with the new configuration from the Registrar.
11. Reset STA2/STA12.



12. Start WSC provisioning on STA2/STA12 and enter the PIN displayed on STA2/STA12 to STA4 external Registrar.
13. Start ping from the Console to STA2/STA12; it must succeed within 90 seconds.

Test Pass/Fail Criterion:

Outside of DMG: If both ping commands succeed, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as 'must' is not fulfilled.

Within DMG: If the ping command succeeds, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as 'must' is not fulfilled.

4.2.9 Test reassembly of WSC IEs**Test Applicability:**

- Outside of DMG: Mandatory for APUT. Mandatory for MAPUT if configuration and enrollee addition by external Registrar supported.
- Within DMG: Mandatory for APUT. Mandatory for MAPUT.

Channel Assignment: For 2.4GHz only APs and for dual band APs, use channel 11. For 5GHz only APs, use channel 40. For 60 GHz only APs, configure the AP to use channel 2. For dual band 2.4 GHz/60 GHz APs, configure the AP(s) to use channels 11 and 2 in each band, respectively. For tri-band 2.4 GHz/5 GHz/60 GHz APs, configure the AP(s) to use channels 11, 40 and 2 in each band, respectively.

Test Goal:

- Outside of DMG: The test verifies that the APUT implements reassembly of WSC IEs in Probe Request frames and sends out correctly constructed UPnP event with the TLVs from the reassembled WSC IEs.
- Within DMG: The test verifies that the APUT implements reassembly of WSC IEs in Probe Request frames.

Test Requirement: The APUT must support WSC Protocol

Test bed Devices:

1. Outside DMG: STA4.
2. Outside DMG: STA1L which is an External Registrar that connects via Ethernet.
3. Inside DMG: STA13 and STA14 which support PBC and are acting as Enrollee.

Test Procedure:

1. Turn on the APUT



2. Reset the APUT to out-of-box Configuration
3. On the UI of the APUT, configure the APUT with new security settings (SSID = “scaptest4.2.9ssid” and WPA(2)-PSK = “scaptest4.2.9psk”).
4. Outside of DMG: Start STA1L external Registrar and subscribe it to receive UPnP events from the APUT.
5. Use STA4/STA14 to create a Probe Request frame with two WSC IEs (the first one including only the first octet of the TLVs and the second including rest of the TLV data). Outside of DMG: The APUT must proxy information from this Probe Request frame to the subscribed external Registrar.
6. Outside of DMG: Verify that STA4 shows up on the external Registrar UI.
7. Within DMG: Perform the following steps:
 - a. Initiate WSC Push Button Configuration Method on STA13
 - b. Wait for 30 seconds and initiate WSC Push Button Configuration Method on STA14
 - c. Wait for 30 seconds and initiate WSC Push Button Configuration Method on APUT
 - d. Start ping for 30 seconds from APUT to both STA13 and STA14. The ping must fail.

Test Pass/Fail Criterion:

- Outside of DMG: If the Enrollee shows up with correct properties on the external Registrar, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.
- Within DMG: If the ping command in step 7.d fails, this test is determined as PASS. Otherwise it is determined as FAIL.

4.2.10 Add device when EAP-WSC fragmentation is used

Test Applicability: Mandatory for APUT. Mandatory for MAPUT.

Channel Assignment: For 5GHz only APs and for dual band APs, use channel 48. For 2.4GHz only APs, use channel 6. For 60 GHz only APs, configure the AP to use channel 2. For dual band 2.4 GHz/60 GHz APs, configure the AP(s) to use channels 6 and 2 for each band, respectively. For tri-band 2.4 GHz/5 GHz/60 GHz APs, configure the AP(s) to use channels 6, 48 and 2 for each band, respectively.

Test Goal: The test verifies that the APUT implements EAP-WSC reassembly. The APUT must be able to add STA device to its WLAN using PIN method when the STA fragments some of the EAP-WSC messages.

Test Requirement: The APUT must support PIN method



Test bed Devices:

1. Outside DMG STA2 / Inside DMG STA12, which supports EAP-WSC fragmentation

Test Procedure:

1. Turn on the APUT
2. Reset the APUT to out-of-box configuration
3. Turn on STA2/STA12 and configure it to fragment EAP-WSC messages.
4. Read the PIN displayed on STA2/STA12 and enter the PIN in the internal Registrar on the APUT. The APUT must be able to complete WSC protocol with fragmented EAP-WSC messages.
5. Start ping from STA2/STA12 to the Console; it must succeed within 90 seconds.

Test Pass/Fail Criterion: If the Ping command is successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.

4.2.11 Add device using NFC connection handover method

Test Applicability: Mandatory for APUT if NFC connection handover is implemented. Mandatory for MAPUT if NFC connection handover is implemented

Test Goal: The test verifies that the APUT implements the NFC connection handover method to act as an internal Registrar. The configured APUT must be able to add a STA device to its WLAN using NFC connection handover method.

Test bed Devices:

1. STA10 which supports NFC connection handover method and is acting as an Enrollee.

Test Procedure:

1. Turn on the APUT.
2. Reset the APUT to out-of-box Configuration.
3. Turn on the test bed STA.
4. If necessary, activate the NFC function on the APUT per vendor directions.
5. Touch the APUT NFC Interface with the test bed STA NFC Interface
6. Start ping from Console to the test bed STA; it must succeed within 90 seconds.



Test Pass/Fail Criterion: If the ping command is successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.

4.2.12 Refuse to add erroneous device using NFC connection handover method

Test Applicability: Mandatory for APUT if NFC connection handover is implemented. Mandatory for MAPUT if NFC connection handover is implemented

Test Goal: The test verifies that the APUT implements the NFC connection handover method to act as an internal Registrar. The configured APUT must be able to refuse the addition of a STA device to its WLAN using NFC connection handover method, when the public key information received from the device differs for NFC and WLAN.

Test bed Devices:

1. STA11 which supports NFC connection handover method and is acting as an Enrollee. Operation of test bed STA is changed to offer incorrect public key information over NFC (compute correct public key hash of the correct public key and change at least 1 bit of the computed public key hash and offer this in the NFC message).

Test Procedure:

1. Turn on the APUT.
2. Reset the APUT to out-of-box Configuration.
3. Turn on the test bed STA.
4. If necessary, activate the NFC function on the APUT per vendor directions.
5. Touch the APUT NFC Interface with the test bed STA NFC Interface
6. Start ping from Console to the test bed STA; it must NOT succeed within 90 seconds.

Test Pass/Fail Criterion: If the ping command is NOT successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.

4.2.13 Check correctness of APUT association procedure

Test Applicability: Mandatory for APUT. Mandatory for MAPUT.

Channel Assignment: For 5GHz only APUTs and for dual band APUTs, use channel 40. For 2.4GHz only APUTs, use channel 6. For 60 GHz only APs, configure the AP to use channel 2. For dual band 2.4 GHz/60 GHz APs, configure the AP(s) to use channels 6 and 2 for each band, respectively. For tri-band 2.4 GHz/5 GHz/60 GHz APs, configure the AP(s) to use channels 6, 40 and 2 for each band, respectively.

Test Goal: The test verifies that the APUT implements the WSC association procedure correctly.

**Test Requirement:**

- Outside of DMG: The APUT must support PIN Configuration method. The APUT must include the WSC IE in the 802.11 Association Response frame. The APUT must ignore the Privacy subfield of the Capability information field in the Association Request frame. The APUT must ignore the RSN IE and the WPA IE if present in the Association Request frame. If the APUT supports WMM it must continue to comply with the WMM requirements. The APUT must be backwards compatible and accept association from a version 1.0 WSC STA.
- Within DMG: The APUT must support PIN Configuration method. The APUT must include the WSC IE in the 802.11 Association Response frame. The APUT must ignore the DMG Privacy subfield of the DMG Parameters field of the Capability information field in the Association Request frame. The APUT must ignore the RSN IE if present in the Association Request frame.

Test bed Devices:

1. STA4/STA14, which implements WSC version 2.0 and supports PIN Configuration method.
 - a. Outside of DMG: STA4 includes the RSN IE in the Association Request frame in addition to the WSC IE and sets the Privacy subfield of the Capability information field to 1.
 - b. Within DMG: STA14 includes the RSN IE in the Association Request frame in addition to the WSC IE and sets the DMG Privacy subfield of the DMG Parameters field of the Capability information field to 1.
2. STA5/STA13, which implements WSC version 2.0 and supports PIN Configuration method.
 - a. Outside of DMG: STA5 does not include the RSN IE in the Association Request frame and sets the Privacy subfield of the Capability information field to 0. STA5 supports WMM and has WMM enabled.
 - b. Within DMG: STA13 does not include the RSN IE in the Association Request frame and sets the DMG Privacy subfield of the DMG Parameters field of the Capability information field to 0.
3. Outside of DMG: STA8, which implements WSC version 1.0 and supports PIN Configuration method. STA8 does not include the WSC IE in the Association Request frame.
4. A wireless packet sniffer device, which is able to capture the wireless packets including the Association Response frame

**Test Procedure:**

1. Turn on the APUT.
2. Reset the APUT in out of box Configuration.
3. On the UI of the APUT configure the APUT with new security settings SSID = “scaptest4.2.12ssid” and WPA2-PSK = “scaptest4.2.12psk”.
4. Outside of DMG: If the APUT supports WMM make sure WMM is enabled.
5. Turn on STA4/STA14 and start a WSC PIN registration process.
6. Start the wireless packet sniffer device.
7. Enter the PIN of STA4/STA14 into the APUT internal Registrar.
8. Start ping from the Console to STA4/STA14; it must succeed within 90 seconds.
9. Stop the wireless packet sniffer device; verify that the first Association Response frame transmitted by the APUT includes the WSC IE.
10. Repeat steps 5, 6, 7, 8 and 9 with STA5/STA13. Outside of DMG: Additionally, in step 9, verify that the Association Response frame includes the WMM Parameter Element as per WMM Specification.
11. Outside of DMG: Repeat steps 5, 6, 7, 8 and 9 with STA8.

Test Pass/Fail Criterion: If the Association Response frames include the WSC IE and if all the Ping commands are successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.

4.2.14 Overlapped PBC sessions

Test Applicability Mandatory for APUT. Mandatory for MAPUT.

Channel Assignment: For 2.4GHz only APUTs, use channel 11. For 5GHz only APUTs, use channel 48. For dual band APUTs, use channels 11 and 48. For 60 GHz only APs, configure the AP to use channel 2. For dual band 2.4 GHz/60 GHz APs, configure the AP(s) to use channels 11 and 2 for each band, respectively. For tri-band 2.4 GHz/5 GHz/60 GHz APs, configure the AP(s) to use channels 11, 48 and 2 for each band, respectively.

Test Goal: The test verifies the STA can’t join an APUT’s WLAN using PBC method through the APUT’s internal Registrar, if another PBC WSC session by another STA exists. Once the other PBC WSC session is removed, the STA must be able to join the APUT’s WLAN. Once the STA joins the APUT’s WLAN, the APUT must stop any current PBC WSC session(s).

Test Requirement: The APUT must support PBC method

**Test bed Devices:**

1. Outside DMG STA5 / Inside DMG STA13, which supports PBC method and is acting as an Enrollee.
2. Outside DMG STA1W / Inside DMG STA14, which supports PBC method and is acting as an Enrollee.

Test Procedure:

1. Turn on the APUT and reset it to out-of-box configuration.
2. Turn on STA5/STA13.
3. Turn on STA1W/STA14.
4. Initiate the WSC Push Button Configuration Method on STA5/STA13.
5. Wait for 1 minute and initiate the WSC Push Button Configuration Method on STA1W/STA14.
6. Push the WSC button on APUT.
7. Start ping from the Console to STA1W/STA14. The ping must fail.
8. Wait for 1 minute.
9. Push the WSC button again on the APUT.
10. Start pings from the Console to STA5/STA13 and STA1W/STA14. The pings must fail.
11. Wait for 2 minutes. The pings that were started in step 10 must continue to fail throughout this 2 minute period.
12. Stop pings from the console to STA5/STA13 and STA1W/STA14.
13. Initiate the WSC Push Button Configuration Method on STA1W/STA14.
14. Push the WSC button again on the APUT.
15. Start ping from the Console to STA1W/STA14; it must succeed within 90 seconds.
16. Outside of DMG: perform steps 17-19, otherwise test end here.
17. Make sure that STA5/STA13 is configured for dual band. Right after the pings succeed in step 15, initiate the WSC Push Button Configuration Method on STA5/STA13.
18. Start ping from the Console to STA5/STA13. The ping must fail.
19. Wait for 2 minutes. The pings that were started in step 17 must continue to fail throughout this 2 minute period.

Test Pass/Fail Criterion: The test is determined as a FAIL if any condition described as 'must' is not fulfilled otherwise the test passes.



4.3 WSC 1.0 backwards compatibility tests for APUT

These tests are run with STA and ER test devices from the WSC 1.0 test bed (see Appendix A).

4.3.1 Configure APUT using PIN method through a WSC 1.0 external Registrar

Test Applicability: Mandatory for APUT if the APUT is un-configured when OOB. Skip for MAPUT.

Channel Assignment: For 5GHz only APs and for dual band APs, use channel 44. For 2.4GHz only APs, use channel 11.

Test Goal: This test verifies that the APUT is backwards compatible with a WSC 1.0 external Registrar. The test verifies that the APUT implements the PIN method to act as an Enrollee with an external Registrar and supports use of a passphrase. The test also verifies that the AP adds the wildcard MAC Address (FF:FF:FF:FF:FF:FF) in an AuthorizedMACs subelement in the WFA Vendor Extension attribute, and removes it, on behalf of the WSC 1.0 external Registrar.

Test Requirement: The APUT must support the PIN Config method and the APUT must be able to act as an Enrollee and register itself with an external Registrar.

Test bed Devices:

1. SAER1, which is a WSC 1.0 external Registrar that connects via Ethernet
2. STA8, which does not support any WSC methods.
3. STA3, which supports PIN config method.
4. A wireless packet sniffer device, which is able to capture the wireless packets including the Beacon packet

Test Procedure:

1. Turn on the APUT.
2. Reset the APUT to OOB Configuration.
3. Turn on SAER1, which is acting as external Registrar
4. The Registrar on SAER1 will be configured with the new wireless configuration settings (SSID = “scaptest4.3.1ssid” and WPA(2)-PSK = “scaptest4.3.1psk”), which should be entered when prompted.
5. Read the PIN from the APUT and enter the PIN at SAER1 when prompted by the Registrar.
6. Manually configure STA8 with the new parameters (SSID = “scaptest4.3.1ssid” and WPA(2)-PSK passphrase= “scaptest4.3.1psk”).



7. Ping from STA8 to SAER1 must succeed within 90 seconds.
8. Start the wireless packet sniffer device.
9. The Beacon packet from the APUT must contain the WSC IE with WSC State set to Configured (0x2). Check on the sniffer.
10. APUT must be capable of displaying the passphrase. The passphrase must be “scaptest4.3.1psk”.
11. Turn on STA3.
12. Read the PIN displayed on STA3 and enter the PIN in the Registrar on SAER1.
13. Ping from STA3 to SAER1 must succeed within 90 seconds.
14. If the Ping was successful, check the sniffer trace. The APUT must have included the AuthorizedMACs subelement in the WFA Vendor Extension attribute with wildcard MAC Address in Beacons and Probe Responses from the time the SelectedRegistrar attribute was included in these frames with SelectedRegistrar flag set to TRUE. After the successful handshake by STA3, the APUT must have removed the wildcard MAC address from the AuthorizedMACs subelement in the WFA Vendor Extension attribute, or must have removed the AuthorizedMACs subelement in the WFA Vendor Extension attribute, from Beacons and Probe Responses when the SelectedRegistrar attribute was removed from these frames or the SelectedRegistrar flag set to FALSE. Note that some WSC v1.0 external registrars may set the SelectedRegistrar flag to TRUE when the user navigates to the registrar user interface before the PIN is entered, and may set the SelectedRegistrar flag to FALSE some time (up to 2 minutes) after the WSC handshake has concluded.

Test Pass/Fail Criterion: If both Ping commands are successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.

4.3.2 Add WSC 1.0 device using PIN method, and then add WSC 1.0 device using PBC method to OOB APUT

Test Applicability: Mandatory for APUT. Mandatory for MAPUT.

Channel Assignment: For 5GHz only APs and for dual band APs, use channel 48. For 2.4GHz only APs, use channel 6.

Test Goal: This test verifies that the APUT is backwards compatible with WSC 1.0 STAs. The test verifies that the APUT implements the PIN and PBC method to act as an internal Registrar from its OOB state. The APUT must be able to add STA device to its WLAN using PIN method and then add STA device using PBC method.

Test Requirement: The APUT must support PIN and PBC method

**Test bed Devices:**

1. STA8, which supports PIN Config method and is acting as an Enrollee
2. STA6, which supports PBC method and is acting as an Enrollee.

Test Procedure:

1. Turn on the APUT
2. Reset the APUT to OOB configuration
3. Turn on STA8.
4. Read the PIN displayed on STA8 and enter the PIN in the internal Registrar on the APUT.
5. Ping from STA8 to the Console must succeed within 90 seconds.
6. Turn on STA6.
7. Push the WSC button on STA6.
8. Push the WSC button on the APUT
9. Ping from STA6 to STA8 must succeed within 90 seconds.

Test Pass/Fail Criterion: If the both of Ping commands are successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.

4.4 Additional tests for Mobile AP

These tests apply only to MAPUT.

4.4.1 Protocol extensibility with STA

This test was developed from test 4.2.8.

Test Applicability: Mandatory for MAPUT.

Channel Assignment: For 2.4GHz only APs and for dual band APs, use channel 11. For 5GHz only APs, use channel 40.

Test Goal: The test verifies that the APUT supports protocol extensibility by accepting higher version number and new attributes from a STA.

Test Requirement: The APUT must support WSC Protocol

Test bed Devices:

1. STA2 that can be configured to advertise different version number, add a new attribute and include some attributes with zero length data fields.

**Test Procedure:**

1. Turn on the APUT
2. Reset the APUT to out-of-box Configuration
3. On the UI of the APUT, configure the APUT with new security settings (SSID = “scmaptest4.4.1-ssid” and WPA(2)-Personal passphrase = “scmaptest4.4.1-psk”).
4. Turn on STA2 and configure it to advertise version 5.7 and to add a new attribute (i.e., an attribute that is not defined in WSC 2.0 specification) to all messages.
5. Read the displayed PIN on STA2 and enter the PIN in the internal Registrar of the APUT.
6. Start ping from the Console to STA2; it must succeed within 90 seconds.

Test Pass/Fail Criterion: If the ping command succeeds, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.

4.4.2 Protocol extensibility with external Registrar

Test Applicability: Mandatory for MAPUT if configuration by external Registrar is supported

Channel Assignment: For 2.4GHz only APs and for dual band APs, use channel 11. For 5GHz only APs, use channel 40.

Test Goal: The test verifies that the APUT supports protocol extensibility by accepting higher version number and new attributes from an external Registrar.

Test Requirement: The APUT must support WSC Protocol and configuration by an external Registrar

Test bed Devices:

1. STA8 which is a legacy station and does not support any WSC methods.
2. STA4 which is an External Registrar that connects via 802.11 and is configured to advertise different version number and a new attribute.

Test Procedure:

1. Turn on the APUT
2. Reset the APUT to out-of-box Configuration
3. Start STA4 external Registrar and configure it to advertise version 5.7 and to add a new attribute (i.e., an attribute that is not defined in WSC 2.0 specification) to all messages.



4. The APUT is configured using STA4 external Registrar with new security settings (SSID = “scmaptest4.4.2-er” and WPA(2)-Personal passphrase = “scmaptest4.4.2-psk-er”). Read the PIN from the APUT and enter the PIN at STA4 external Registrar when prompted by the Registrar. The APUT must change its configuration (SSID and passphrase) to match with the new configuration from the Registrar.
5. Manually configure STA8 with the new parameters (SSID = “scmaptest4.4.2-er” and WPA(2)-PSK = “scmaptest4.4.2-psk-er”).
6. Start ping from the Console to STA8; it must succeed within 90 seconds.

Test Pass/Fail Criterion: If the ping command succeeds, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.

4.4.3 Configure APUT to use open networking (no security) using PIN method through an external Registrar and add a STA using internal Registrar

Test Applicability: Mandatory for MAPUT if configuration by external Registrar supported.

Channel Assignment: For 2.4GHz only APs and for dual band APs, use channel 1. For 5GHz only APs, use channel 48.

Test Goal: The test verifies that the APUT can be configured to use open networking setting by an external Registrar and that a STA can be added using the internal Registrar.

Test Requirement: The APUT must support PIN Config method

Test bed Devices:

1. STA5, which supports PIN Config method and is an External Registrar that connects via 802.11
2. STA8, which does not support any WSC methods.
3. STA1W, which is a WSC STA.

Test Procedure:

1. Turn on the APUT.
2. Reset the APUT to out-of-box Configuration.
3. Turn on STA5, which is acting as external Registrar
4. The Registrar on STA5 will be configured to use open network settings (SSID = “scmaptest4.4.3ssid”) which should be entered when prompted



5. Read the PIN from the APUT and enter the PIN at STA5 when prompted by the Registrar.
6. Start ping from STA5 to the Console; it must succeed within 90 seconds.
7. Enter the PIN for STA1W at the internal Registrar of the APUT. No additional user action is allowed at APUT (enabling WSC or enabling "PIN mode") in order to continue.
8. Start ping from STA1W to the Console; it must succeed within 90 seconds.
9. Manually associate STA8 with the APUT using open networking settings (SSID = "scmaptest4.4.3ssid").
10. Start ping from STA8 to STA5; it must succeed within 90 seconds.

Test Pass/Fail Criterion: If both Ping commands are successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as 'must' is not fulfilled.

4.4.4 Add devices using multiple external Registrars and internal Registrar

Test Applicability: Mandatory for MAPUT if configuration and enrollee addition by external Registrar supported.

Channel Assignment: For 2.4GHz only APs and for dual band APs, use channel 11. For 5GHz only APs, use channel 44.

Test Goal: The test verifies that the APUT supports multiple external Registrars connected via 802.11 to add enrollees.

Test Requirement: The APUT must support multiple external Registrars connected via 802.11. The APUT must support PIN Config method.

Test bed Devices:

1. STA4, which supports PIN Config method and is an External Registrar that connects via 802.11
2. STA2, which supports PIN Config method and is as an Enrollee
3. STA5, which supports PIN Config method and is as an Enrollee
4. STA3, which supports PIN Config method and is as an Enrollee
5. STA1W, which supports PIN Config method and is an External Registrar that connects via 802.11.
6. A wireless packet sniffer device, which is capable to capture the wireless packet including the Beacon and Probe Response packets

Test Procedure:



1. Turn on the APUT
2. Reset the APUT to out-of-box Configuration
3. Turn on STA1W, which is acting as external Registrar.
4. The Registrar on STA1W will be configured with the new wireless configuration settings (SSID = "scmaptest4.4.ssid" and WPA(2)-PSK = "scmaptest4.4.psk"), which should be entered when prompted
5. Read the PIN from the APUT and enter the PIN at STA1W when prompted by the Registrar.
6. The Registrar on STA1 will display status on completion. The status must be success.
7. Turn on STA4, which is acting as external Registrar
8. Read the PIN from the APUT and enter the PIN at the external Registrar on STA4 when prompted by the Registrar.
9. Start ping from STA4 to STA1W; it must succeed within 180 seconds.
10. Turn on the wireless sniffer devices and start to monitor the traffic to/from the APUT
11. Turn on STA2, which is acting as an Enrollee. Then start a WSC PIN registration process per the Test bed vendor direction
12. Enter the PIN from STA2 into the external Registrar on STA1W.
13. Start ping from STA2 to STA1W; it must succeed within 180 seconds.
14. Verify the following on the wireless sniffer device. After the PIN has been entered into the external Registrar on STA1W, and while the WSC handshake is in progress, the Beacon and Probe Response frames transmitted by the APUT must include an AuthorizedMACs subelement in the WFA Vendor Extension attribute in the WSC IE. The AuthorizedMACs subelement in the WFA Vendor Extension attribute must not be present in the Beacon and Probe Response frames sent by the APUT after the registration for STA2 has concluded successfully. Note that depending on delays between the external Registrar on STA1W and the APUT it may take up to five seconds for the AuthorizedMACs subelement in the WFA Vendor Extension attribute to be removed from Beacons and Probe Responses sent by the APUT after the registration has concluded.
15. Turn off STA1W.
16. Turn on STA5, which is acting as an Enrollee
17. Enter the PIN from STA5 into the external Registrar on STA4. No additional user action is allowed at APUT (e.g. enabling WSC or enabling "PIN mode") in order to continue.
18. Start ping from STA4 to STA5; it must succeed within 180 seconds.
19. Turn on STA3, which is acting as an Enrollee



20. Enter the PIN from STA3 into the internal Registrar on APUT
21. Start ping from STA2 to STA3; it must succeed within 180 seconds.

Test Pass/Fail Criterion: If all of PING commands are successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.

4.4.5 Configure APUT using PIN method through a WSC 1.0 external Registrar

Test Applicability: Mandatory for MAPUT if configuration and enrollee addition by external Registrar supported.

Channel Assignment: For 5GHz only APs and for dual band APs, use channel 44. For 2.4GHz only APs, use channel 11.

Test Goal: This test verifies that the APUT is backwards compatible with a WSC 1.0 external Registrar. The test verifies that the APUT implements the PIN method to act as an Enrollee with an external Registrar and supports use of a passphrase. The test also verifies that the APUT adds the wildcard MAC Address (FF:FF:FF:FF:FF:FF) in an AuthorizedMACs subelement in the WFA Vendor Extension attribute, and removes it, on behalf of the WSC 1.0 external Registrar.

Test Requirement: The APUT must support the PIN Config method and the APUT must be able to act as an Enrollee and register itself with an external Registrar.

Test bed Devices:

1. STA8, which is a WSC 1.0 External Registrar that connects via 802.11.
2. STA6, which does not support any WSC methods (WSC must be disabled).
3. STA3, which supports PIN config method.
4. A wireless packet sniffer device, which is able to capture the wireless packets including the Beacon packet.

Test Procedure:

1. Turn on the APUT.
2. Reset the APUT to OOB Configuration.
3. Turn on STA8, which is acting as external Registrar.
4. Configure the Registrar on STA8 with the new wireless configuration settings (SSID = “scmaptest4.4.5ssid” and WPA(2)-PSK = “scmaptest4.4.5psk”), which should be entered when prompted.



5. Read the PIN from the APUT and enter the PIN at STA8's Registrar when prompted by the Registrar.
6. Manually configure STA6 with the new parameters (SSID = "scaptest4.4.5ssid" and WPA(2)-PSK passphrase= "scaptest4.4.5psk").
7. Ping from STA6 to STA8 must succeed within 90 seconds.
8. Start the wireless packet sniffer device.
9. The Beacon packet from the APUT must contain the WSC IE with WSC State set to Configured (0x2). Check on the sniffer.
10. APUT must be capable of displaying the passphrase. The passphrase must be "scaptest4.4.5psk".
11. Turn on STA3.
12. Read the PIN displayed on STA3 and enter the PIN in the Registrar on STA8.
13. Ping from STA3 to STA8 must succeed within 90 seconds.
14. Stop the wireless packet sniffer and check the sniffer trace. The APUT must have included the AuthorizedMACs subelement in the WFA Vendor Extension attribute with wildcard MAC Address in Beacons and Probe Responses from the time the SelectedRegistrar attribute was included in these frames with SelectedRegistrar flag set to TRUE. After the successful handshake by STA3, the APUT must have removed the wildcard MAC address from the AuthorizedMACs subelement in the WFA Vendor Extension attribute, or must have removed the AuthorizedMACs subelement in the WFA Vendor Extension attribute, from Beacons and Probe Responses when the SelectedRegistrar attribute was removed from these frames or the SelectedRegistrar flag set to FALSE. The WSC V1.0 external registrar must set the SelectedRegistrar flag to FALSE within 2 minutes after the WSC handshake has completed.

Test Pass/Fail Criterion: If both Ping commands are successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as 'must' is not fulfilled.



5 STA tests

5.1 Add to AP as an Enrollee

5.1.1 Add to AP using PIN Config method through an external Registrar and check frame format

Test Applicability: Mandatory for all STAUTs, with the exception of STAUTs operating within DMG where the test is not applicable.

Channel Assignment: For 5GHz only STAUTs and for dual band STAUTs, configure the AP to use channel 36. For 2.4GHz only STAUTs, configure the AP to use channel 1.

Test Goal: The test verifies that the STAUT implements the PIN Config method as an Enrollee. The STAUT must be able to join an AP's WLAN through an external Registrar using PIN method. The external Registrar must deliver two network credentials, 1 for a network that is present and 1 that is not present. The STAUT must connect using the credentials for the network that is present. If transmitted during the WSC registration process the probe request is also validated for the correct format of the WSC IE.

Test Requirement: The STAUT must support PIN Config method.

Test bed Devices:

1. AP3, which supports PIN Config method.
2. STA1W, which is an External Registrar that connects via 802.11 and has a test mode allowing it to deliver an extra network credential to an enrollee (correct credential is the 2nd credential)
3. A wireless packet sniffer device.

Test Procedure:

1. Turn on the AP in out-of-box mode
2. Turn on the STA.
3. Turn on the sniffer device and start to monitor the traffic to/from the STAUT
4. Enter the PIN of the AP into Registrar on the STA. Use default configuration
5. Set the STA into its test mode
6. Turn on STAUT and start a WSC PIN registration process per vendor direction
7. Enter the PIN of STAUT into Registrar on the STA.
8. Start ping from Console to STAUT; it must succeed within 90 seconds.
9. If the STAUT transmits a Probe Request frame during the WSC registration process, verify on the sniffer device that the Probe Request frame from the STAUT includes following mandatory, variable length string attributes: Manufacturer, Model Name, Model Number, and Device Name. These attributes



must not use NULL-padding, i.e., the last octet of the attribute value must not be 0x00. Verify that the Probe Request contains the WSC Version2 subelement in the WFA Vendor Extension attribute.

The STAUT must support all the Config Methods it advertises in the Probe Request. On the sniffer device, verify that the Probe Request message that the STAUT sends includes the Config method attribute in the WSC IE and that it reflects the correct configuration methods of the STAUT.

Check on the sniffer to verify that the list of supported method in the IE is a bitwise OR of values from the list below:

0x0010	External NFC Tag
0x0020	Integrated NFC Tag
0x0040	NFC Interface
0x0080	PushButton
0x0100	Keypad
0x0280	Virtual Push Button
0x0480	Physical Push Button
0x2008	Virtual Display PIN
0x4008	Physical Display PIN

Every STAUT must support the PIN method and the WSC IE in the Probe Request must include Label (0x0004) and/or Display (0x0008).

Any STAUT claiming to support a Display must include either Virtual Display PIN (0x2008) or Physical Display PIN (0x4008). The display or virtual PIN methods must correspond to the features supported by the STAUT.

Any STAUT claiming to support Pushbutton (0x0080) must include either or both of the Virtual Push Button (0x0280) Physical Push Button (0x0480) attributes.

The STAUT must support every Config method that it advertises as a bitwise OR in the WSC IE.

0x0010 – The STAUT must support and External NFC Tag.

0x0020 – The STAUT must support an Integrated NFC Tag.

0x0040 – The STAUT must support an NFC interface.

0x0080 – The STAUT must have a push button and support it.

0x0100 – The STAUT must support PIN using a Keypad on the STAUT

0x0280 – The STAUT must have a Virtual Push Button (in the UI) and support it.



0x0480 – The STAUT must have a Physical Push Button (on the STAUT) and support it.

0x2008 – The STAUT must support a PIN in the Virtual UI of the STAUT.

0x4008 – The STAUT must support a PIN on the physical display of the STAUT

10. Verify on the sniffer device that the M1 message from the STAUT includes following mandatory, variable length string attributes: Manufacturer, Model Name, Model Number, Serial Number, and Device Name. These attributes must not use NULL-padding, i.e., the last octet of the attribute value must not be 0x00. The STAUT must support all the Configuration Methods it advertises in the M1 message.
11. On the sniffer device, verify that the M1 message that the STAUT sends includes the following attributes: Authentication Type Flags and Encryption Type Flags. The values for these attributes must reflect the authentication and encryption types supported by the STAUT. The Authentication Type Flags value must include the following bits depending on STAUT capabilities: 0x0001 Open (mandatory), 0x0020 WPA2-Personal (mandatory). The Encryption Type Flags value must include the following bits depending on STAUT capabilities: 0x0001 None (mandatory), 0x0008 AES (mandatory). The STAUT must include the WSC State set to 0x01 (Not Configured).

Test Pass/Fail Criterion: If the PING command is successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.

5.1.2 Add to AP using PBC method through internal Registrar

Test Applicability: Mandatory for STAUT if PBC is implemented.

Channel Assignment: For 5GHz only STAUTs, configure the AP to use channel 40. For 2.4GHz only STAUTs, configure the AP to use channel 6. For dual band 2.4GHz/5GHz STAUTs, configure the AP to use channels 6 and 40 respectively. For 60GHz only STAUTs, configure the AP to use channel 2. For dual band 2.4GHz/60GHz STAUTs, configure the AP(s) to use channels 6 and 2 respectively. For tri-band 2.4GHz/5GHz/60GHz STAUTs, configure the AP(s) to use channels 6, 40 and 2 respectively.

Test Goal: The test verifies that the STAUT implements the PBC method as an Enrollee. The STAUT must be able to join an AP’s WLAN through the AP’s internal Registrar using PBC method. This test also checks that a STAUT with at least 2 radios does not incorrectly identify the PBC active state of an AP with at least 2 radios as an overlapping session.

Test Requirement: The STAUT must support PBC method.

**Test bed Devices:**

1. AP is one of the following:
 - a. Outside DMG AP2 – a dual-radio 2.4GHz/5GHz WSC AP, which supports PBC method.
 - b. Inside DMG AP12 or AP13, which supports the WSC PBC method.
2. A wireless packet sniffer device.

Test Procedure:

1. Turn on the AP in out-of-box mode. If AP is operating within DMG, enable WSC.
2. Turn on the STAUT. If the STAUT only supports single band, confirm that it sees the AP. If the STAUT scans in more than one band, confirm that it sees the APs in all scanned bands.
3. Push WSC button on the AP.
4. Push WSC button on the STAUT or start a WSC PBC registration process per vendor direction.
5. On the wireless packet sniffer device, verify that the Probe Request frame transmitted by the STAUT includes the WSC IE. Also verify that the WSC IE includes all of the required attributes (Version, Request Type, Configuration Methods, UUID, Primary Device Type, RF Bands, Association State, Configuration Error, Device Password ID, Version2 subelement in the WFA Vendor Extension, Manufacturer, Model Name, Model Number, Device Name. The STAUT must support all the Configuration Methods it advertises in the Probe Request.
6. On the sniffer device, verify the M1 message from STAUT. The Message must include the WSC State set to 0x01 (Not Configured).
7. Start ping from Console to STAUT; it must succeed within 90 seconds.
8. If outside DMG, check the Beacon or Probe Response of AP. The message must include the WSC State set to Configured (0x02)

Test Pass/Fail Criterion: If the Ping command is successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.



5.1.3 Add to AP using PIN Config method through an external Registrar that connects to the AP via 802.11

Test Applicability: Mandatory for all STAUTs, with the exception of STAUTs operating within DMG where the test is not applicable.

Channel Assignment: For 5GHz only STAUTs and for dual band STAUTs, configure the AP to use channel 40. For 2.4GHz only STAUTs, configure the AP to use channel 11.

Test Goal: The test verifies that the STAUT implements the PIN Config method as an Enrollee. The STAUT must be able to join an AP's WLAN using PIN method through an external Registrar that connects to the AP via 802.11.

Test Requirement: The STAUT must support PIN Config method.

Test bed Devices:

1. AP1, which supports PIN Config method
2. STA1W, which is acting as an external Registrar that connects via 802.11

Test Procedure:

1. Turn on the AP.
2. Turn on STA1W.
3. The Registrar on STA1W will be configured with the new parameters (SSID = "scstatest5.1.3ssid" and WPA2-PSK = "scstatest5.1.3psk") which should be entered when prompted
4. Enter the PIN of the AP into the ER when prompted by the ER.
5. Wait for the ER to indicate completion.
6. Turn on STAUT and start a WSC PIN registration process per vendor direction.
7. On the test bed ER enter the PIN from the STAUT.
8. Start ping from Console to STAUT; it must succeed within 90 seconds.

Test Pass/Fail Criterion: If the Ping command is successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as 'must' is not fulfilled.

5.1.4 Add to AP using PIN Config method through an external Registrar that connects to the AP via Ethernet

Test Applicability: Mandatory for all STAUTs, with the exception of STAUTs operating within DMG where the test is not applicable.



Channel Assignment: For 5GHz only STAUTs and for dual band STAUTs, configure the AP to use channel 44. For 2.4GHz only STAUTs, configure the AP to use channel 1.

Test Goal: The test verifies that the STAUT implements the PIN Config method as an Enrollee. The STAUT must be able to join an AP's WLAN using PIN method through an external Registrar that connects to the AP via Ethernet.

Test Requirement: The STAUT must support PIN Config method.

Test bed Devices:

1. AP4, which supports PIN Config method
2. STA1L which is an External Registrar that connects via Ethernet using UpnP. Test bed ER that connects via Ethernet has the ability to show the list of enrollees based on the received Probe Request proxied by Test bed AP and let users to select a target enrollee from the list. Also the Test bed STA is capable to add a selected enrollee's MAC address in the AuthorizedMACs subelement in the WFA Vendor Extension attribute in SetSelectedRegistrar UpnP action and send it to the Test bed AP.
3. A wireless packet sniffer device, which is able to capture the wireless packet including the Probe Request packet.

Test Procedure:

1. Turn on the Test bed AP.
2. Turn on the STA1L.
3. Configured STA1L's Registrar with the new parameters (SSID = "scstatest5.1.4ssid" and WPA2-Personal PASS PHRASE = "scstatest5.1.4psk") which should be entered when prompted
4. Enter the PIN of the Test bed AP at STA1L's Registrar when prompted by the Registrar.
5. Wait for STA1L's Registrar to indicate completion.
6. Turn on STAUT and start a WSC PIN registration process per vendor direction.
7. If the STAUT transmits a Probe Request frame during the WSC registration process, on the wireless packet sniffer, verify that the Probe Request frame transmitted by the STAUT includes the WSC IE.
8. Enter the PIN from the STAUT in STA1L's Registrar.
9. Start ping from STA1L to STAUT; it must succeed within 90 seconds.

Test Pass/Fail Criterion: If the Ping command is successful, this test is determined as PASS. Otherwise, it is determined as FAIL. The test is determined as a FAIL if any condition described as 'must' is not fulfilled.



5.1.5 Add to AP using PIN method and open networking setting through an external Registrar

Test Applicability: Mandatory for all STAUTs, with the exception of STAUTs operating within DMG where the test is not applicable.

Channel Assignment: For 5GHz only STAUTs and for dual band STAUTs, configure the AP to use channel 48. For 2.4GHz only STAUTs, configure the AP to use channel 6.

Test Goal: The test verifies that the STAUT can be configured to use open network settings to join an AP's WLAN using PIN method through an external Registrar.

Test Requirement: The STAUT must support PIN Config method.

Test bed Devices:

1. AP3, which supports PIN Config method
2. STA1W which is an External Registrar that connects via 802.11.

Test Procedure:

1. Turn on AP3.
2. Turn on the ER.
3. The Registrar on the ER will be configured with the open network settings (SSID = "scstatest5.1.5ssid") which should be entered when prompted.
4. Enter the PIN of AP3 at the ER when prompted by the Registrar.
5. Wait for the ER to indicate completion.
6. Turn on STAUT and start a WSC PIN registration process per vendor direction.
7. On the ER enter the PIN from the STAUT.
8. Start ping from the ER station to STAUT; it must succeed within 90 seconds.

Test Pass/Fail Criterion: If the Ping command is successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as 'must' is not fulfilled.

5.1.6 Add to AP using PBC method and open network settings through internal Registrar

Test Applicability: Mandatory for STAUT if PBC implemented.

Channel Assignment: For 2.4GHz only STAUTs and for dual band 2.4GHz/5GHz STAUTs, configure the AP to use channel 1. For 5GHz only STAUTs, configure the AP



to use channel 36. For 60GHz only STAUTs, configure the AP to use channel 2. For dual band 2.4GHz/60GHz STAUTs, configure the AP(s) to use channels 6 and 2 respectively. For tri-band 2.4GHz/5GHz/60GHz STAUTs, configure the AP(s) to use channels 6, 40 and 2 respectively.

Test Goal: The test verifies that the STAUT can be configured to use open network settings to join an AP's WLAN using PBC method through AP's internal Registrar.

Test Requirement: The STAUT must support PBC method.

Test bed Devices:

1. AP is one of the following:
 - a. Outside DMG AP2, which supports PBC method.
 - b. Inside DMG AP12, which supports the WSC PBC method.
2. A wireless packet sniffer device.

Test Procedure:

1. Turn on the AP and turn on WSC if the AP is operating within DMG.
2. Configure the AP with the open network settings (SSID = "scstatest5.1.6ssid").
3. Turn on the STAUT.
4. Push the WSC button on the AP.
5. Push the WSC button on STAUT.
6. Start ping from Console to STAUT; it must succeed within 90 seconds.
7. On the sniffer device, verify the M1 message from STAUT. The message must include the WSC State set to 0x01 (Not Configured).

Test Pass/Fail Criterion: If the Ping command is successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as 'must' is not fulfilled.

5.1.7 Two (2) minute timeout with multiple push button events for PBC method

Test Applicability: Mandatory for STAUT if PBC implemented

Channel Assignment: For 2.4GHz only STAUTs and for dual band 2.4GHz/5GHz STAUTs, configure the AP to use channel 6. For 5GHz only STAUTs, configure the AP to use channel 40. For 60GHz only STAUTs, configure the AP to use channel 2. For dual band 2.4GHz/60GHz STAUTs, configure the AP(s) to use channels 6 and 2



respectively. For tri-band 2.4GHz/5GHz/60GHz STAUTs, configure the AP(s) to use channels 6, 40 and 2 respectively.

Test Goal: The test verifies that the STAUT exercises the push button 2 minutes timer correctly. As long as the period between when the user pushes the WSC button on the AP and when the user pushes the WSC button on the STAUT is less than 2 minutes, the STAUT must be able to join the AP's WLAN using PBC method through the AP's internal Registrar.

Test Requirement: The STAUT must support PBC method

Test bed Devices:

1. AP is one of the following:
 - a. Outside DMG AP1 , which supports PBC method.
 - b. Inside DMG AP12 or AP13, which supports the WSC PBC method.

Test Procedure:

1. Turn on the AP and turn on WSC if the AP is operating within DMG.
2. Turn on the STAUT.
3. Push the WSC button on STAUT.
4. Wait 90 seconds.
5. Push the WSC button on STAUT again. NOTE: in some station implementations using a “soft” button, the button is not available to push until the 120-second timer has expired. In these cases, the button may be pushed as soon as it is available as long as the 90 seconds has elapsed in the previous step.
6. Wait for 1 minute.
7. Push the WSC button on the AP.
8. Start ping from Console to STAUT; it must succeed within 90 seconds.

Test Pass/Fail Criterion: If the PING command is successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.

5.1.8 Overlapped PBC sessions

Test Applicability: Mandatory for STAUT if PBC implemented

Channel Assignment: For 2.4GHz only STAUTs and for dual band 2.4GHz/5GHz STAUTs, configure the AP to use channel 11. For 5GHz only STAUTs, configure the AP to use channel 48. For 60GHz only STAUTs, configure the AP to use channel 2. For



dual band 2.4GHz/60GHz STAUTs, configure the AP(s) to use channels 11 and 2 respectively. For tri-band 2.4GHz/5GHz/60GHz STAUTs, configure the AP(s) to use channels 11, 48 and 2 respectively.

Test Goal: The test verifies the STAUT can't join an AP's WLAN using PBC method through the AP's internal Registrar, if another PBC WSC session by another AP exists. Once other PBC WSC session is removed, the STAUT must be able to join the AP's WLAN.

Test Requirement: The STAUT must support PBC method

Test bed Devices:

1. AP-I is one of the following:
 - a. Outside DMG AP1, which supports the WSC PBC method.
 - b. Inside DMG AP12, which supports the WSC PBC method.
2. AP-II is one of the following:
 - a. Outside DMG AP2, which supports the WSC PBC method.
 - b. Inside DMG AP11, which supports the WSC PBC method.

Test Procedure:

1. Turn on AP-II and turn on WSC if the AP is operating within DMG.
2. Turn on AP-I and turn on Wi-Fi Protected Setup if the AP is operating within DMG.
3. Turn on the STAUT. STAUT discovers AP-I and AP-II.
4. Push the WSC button on AP-I.
5. Wait for 1 minute and push the WSC button on AP-II.
6. Push the WSC button on STAUT
7. STAUT must indicate PBC session overlap.
8. Start ping from Console to STAUT. The ping must fail.
9. Wait for at least 2 minutes or until the STAUT allows the WSC PBC button to be pushed
10. Push the WSC button on the STAUT. Push the WSC button on AP-II, also.
11. Start ping from Console to STAUT; it must succeed within 90 seconds.

Test Pass/Fail Criterion: The STAUT must indicate that the WSC process fails after pushing the button on STAUT for the first time. The test is determined as a FAIL if any condition described as 'must' is not fulfilled.



5.1.9 Add to AP using NFC tag method with password token through internal registrar

Test Applicability: Mandatory for STAUT if NFC tag is implemented, with the exception of STAUTs operating within DMG where the test is not applicable.

Test Goal: The test verifies the STAUT implements the NFC tag method with password token as an Enrollee. The STAUT must be able to join an AP's WLAN through the AP's internal Registrar using NFC tag method with password token. The STAUT must fail the registration protocol if presented a different password token.

Test bed Devices:

1. AP9 which has an internal registrar and supports NFC tag method with password token.
2. STA9 which supports NFC tag method with password token.
3. The writable test bed NFC tag type 1, type 3 and type 4.

Test Procedure:

1. Turn on the Test bed STA.
2. Create a Password Token for the Test bed STA by selecting the password token generation function on the UI of the Test bed STA and touching the NFC Interface with the writable Test bed NFC Tag Type1.
3. Turn off the Test bed STA.
4. Turn on the Test bed AP.
5. Turn on STAUT and create a Password Token for the STAUT by selecting the password token generation function on the UI of the STAUT and touching the NFC Interface with the writable Test bed NFC Tag Type3.
6. Touch the NFC Interface of the Test bed AP with the Test bed STA password token.
7. STAUT is requested to connect to Test bed AP.
8. Wait 90 seconds.
9. Start ping from Console to STAUT; the console must not receive any ping responses within 90 seconds
10. Restart the Test bed AP.
11. Restart the WSC NFC password token registration process on STAUT as per vendor direction and touch the NFC Interface of STAUT with the writable Test bed NFC Tag Type1.
12. Touch the NFC Interface of the Test bed AP with the writable Test bed NFC Tag Type1.



13. STAUT is requested to connect to Test bed AP.
14. Start ping from Console to STAUT; it must succeed within 90 seconds.
15. Restart the Test bed AP.
16. Restart the WSC NFC password token registration process on STAUT as per vendor direction and touch the NFC Interface of STAUT with the writable Test bed NFC Tag Type3.
17. Touch the NFC Interface of the Test bed AP with the writable Test bed NFC Tag Type3.
18. Attempt to connect STAUT to Test bed AP.
19. Start ping from Console to STAUT; it must succeed within 90 seconds.
20. Restart the Test bed AP.
21. Restart the WSC NFC password token registration process on STAUT as per vendor direction and touch the NFC Interface of STAUT with the writable Test bed NFC Tag Type4.
22. Touch the NFC Interface of the Test bed AP with the writable Test bed NFC Tag Type4.
23. Attempt to connect STAUT to Test bed AP.
24. Start ping from Console to STAUT; it must succeed within 90 seconds.

Test Pass/Fail Criterion: If steps 9, 14, 19, and 24 are met, then pass; else fail.

5.1.10 Add to AP using NFC tag method with configuration token containing standalone NDEF record through internal registrar

Test Applicability: Mandatory for STAUT if NFC is implemented with NFC Interface, with the exception of STAUTs operating within DMG where the test is not applicable.

Test Goal: The test verifies the STAUT implements the NFC tag method with configuration token as an Enrollee when the configuration token contains a standalone NDEF record. The STAUT must be able to join an AP's WLAN through the AP's internal Registrar using NFC tag method with configuration token. The STAUT must fail the registration protocol if presented a configuration token with an incorrect NDEF record.

Test bed Devices:

1. AP8 which has an internal registrar and supports NFC Method with configuration token containing a standalone NDEF record.
2. The writable test bed NFC tag type 1, type 3 and type 4.

**Test Procedure:**

1. Turn on the Test bed AP.
2. Create a Configuration Token by executing the configuration token generation function on the Test bed AP and touching the NFC Interface with the writable Test bed NFC Tag Type1.
3. Start a WSC NFC configuration token registration process per vendor directions and touch the STAUT with the Configuration Token.
4. Start ping from Console to STAUT; it must succeed within 90 seconds.
5. Manually configure the Test bed AP with new wireless configuration settings (SSID = “scstatest5.1.10ssid_type3” and WPA(2)-PSK = “scstatest5.1.10psk_type3”).
6. Create a Configuration Token by executing the configuration token generation function on the Test bed AP and touching the NFC Interface with the writable Test bed NFC Tag Type3.
7. Start a WSC NFC configuration token registration process per vendor directions and touch the STAUT with the Configuration Token.
8. Start ping from Console to STAUT; it must succeed within 90 seconds.
9. Manually configure the Test bed AP with new wireless configuration settings (SSID = “scstatest5.1.10ssid_type4” and WPA(2)-PSK = “scstatest5.1.10psk_type4”).
10. Create a Configuration Token by executing the configuration token generation function on the Test bed AP and touching the NFC Interface with the writable Test bed NFC Tag Type4.
11. Start a WSC NFC configuration token registration process per vendor directions and touch the STAUT with the Configuration Token.
12. Start ping from Console to STAUT; it must succeed within 90 seconds.

Test Pass/Fail Criterion: If the first Ping command fails and rest of Ping commands are successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.

5.1.11 Protocol extensibility

Test Applicability: Mandatory for all STAUTs

Channel Assignment: For 5GHz only STAUTs and for 2.4GHz/5GHz dual band STAUTs, configure the AP to use channel 36. For 2.4GHz only STAUTs, configure the AP to use channel 1. For 60GHz only STAUTs, configure the AP to use channel 2. For multiband 2.4GHz/5GHz/60GHz STAUTs, configure the AP(s) to use channel 1, 36, and 2 respectively.



Test Goal: The test verifies that the STAUT supports protocol extensibility by accepting higher version number and new attributes.

Test Requirement: The STAUT must support PIN Config method.

Test bed Devices:

1. AP that can be configured to advertise different version numbers, add a new attribute and include some attributes with zero length data fields. Choose one of the following:
 - a. Outside DMG: AP1.
 - b. Inside DMG: 60GHz WSC AP12.

Test Procedure:

1. Turn on the Test bed AP in out-of-box mode and turn on WSC if the AP is operating within DMG. Configure it to advertise version 5.7 and to add a new attribute (i.e., an attribute that is not defined in WSC 2.0 specification) to all messages.
2. Turn on STAUT and start a WSC PIN registration process per vendor direction
3. Enter the PIN of STAUT into AP's Internal Registrar.
4. Start ping from Console to STAUT; it must succeed within 90 seconds.
5. For AP1: in the Beacon frame, check that:
 - a. Version 5.7 is advertised, and a new attribute (i.e., an attribute that is not defined in WSC 2.0 specification) is added
 - b. The WSC State must be set to Configured (0x02).

Test Pass/Fail Criterion: If the PING command is successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as 'must' is not fulfilled.

5.1.12 Add to AP when WSC IE and EAP-WSC is fragmented

Test Applicability: Mandatory for all STAUTs

Channel Assignment: For 5GHz only STAUTs and for dual band 2.4GHz/5GHz STAUTs, configure the AP to use channel 36. For 2.4GHz only STAUTs, configure the AP to use channel 1. For 60GHz only STAUTs, configure the AP to use channel 2. For multiband 2.4GHz/5GHz/60GHz STAUTs, configure the AP(s) to use channel 1, 36, and 2 respectively.



Test Goal: The test verifies that the STAUT implements reassembly of WSC IE and EAP-WSC. The STAUT must be able to join an AP's WLAN using PIN method when the AP is fragmenting attributes in WSC IEs and EAP-WSC messages.

Test Requirement: The STAUT must support PIN Config method.

Test bed Devices:

1. AP, which supports PIN Config method and fragmentation of WSC IE and EAP-WSC messages. Chosse one of the following:
 - a. Outside DMG: AP2.
 - b. Inside DMG: 60GHz WSC AP12.

Test Procedure:

1. Turn on the Test bed AP in out-of-box mode and turn on WSC if the AP is operating within DMG. Configure it to fragment WSC IEs within a Probe Response frames. In addition, configure it to fragment some EAP-WSC messages.
2. Turn on STAUT and start a WSC PIN registration process per vendor direction
3. Enter the PIN of STAUT into Registrar on the Test bed AP.
4. Start ping from Console to STAUT; it must succeed within 90 seconds.

Test Pass/Fail Criterion: If the PING command is successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as 'must' is not fulfilled.

5.1.13 Add to AP using PIN Configuration method through internal Registrar

Test Applicability: Mandatory for all STAUTs

Channel Assignment: For 5GHz only STAUTs and for dual band 2.4GHz/5GHz STAUTs, configure the AP use channel 40. For 2.4GHz only STAUTs, configure the AP to use channel 6. For 60GHz only STAUTs, configure the AP to use channel 2. For multiband 2.4GHz/5GHz/60GHz STAUTs, configure the AP(s) to use channel 6, 40, and 2 respectively.

Test Goal: The test verifies that the STAUT implements the PIN Configuration method as an Enrollee. The STAUT must be able to join an AP's WLAN through the AP's internal Registrar using PIN method when the AP's WSC State is Not Configured.

Test Requirement: The STAUT must support PIN Configuration method.

**Test bed Devices:**

1. AP, which supports PIN Configuration method. The test bed AP is Not Configured. Choose one of the following:
 - a. Outside DMG: AP3.
 - b. Inside DMG: 60GHz WSC AP11.
2. A wireless packet sniffer device

Test Procedure:

1. Turn on the test bed AP in un-configured state and turn on WSC if the AP is operating within DMG.
 - a. For AP3: check the WSC State is set to Not Configured (0x01) in the Beacon.
2. Turn on the STAUT and start a WSC PIN registration process per vendor direction.
 - a. For Qualcomm device operating within DMG: if Probe Response is transmitted, check the WSC State is set to Not Configured (0x01).
3. Enter the PIN of STAUT into the test bed AP Internal Registrar.
4. If within DMG, on the wireless packet sniffer device, verify that the Probe Request frame transmitted by the STAUT includes the WSC IE. Also verify that the WSC IE includes all of the required attributes (Version, Request Type, Configuration Methods, UUID, Primary Device Type, RF Bands, Association State, Configuration Error, Device Password ID, Version2 subelement in the WFA Vendor Extension, Manufacturer, Model Name, Model Number, Device Name). The STAUT must support all the Configuration Methods it advertises in the Probe Request.
5. If within DMG, on the sniffer device, verify the M1 message from STAUT. The Message must include the WSC State set to 0x01 (Not Configured).
6. For AP3: the WSC State in the Beacon must be set to Configured (0x02).
7. Start ping from Console to STAUT; it must succeed within 90 seconds.

Test Pass/Fail Criterion: If the Ping command is successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as 'must' is not fulfilled.

5.1.14 Check correctness of STAUT association procedure

Test Applicability: Mandatory for all STAUTs



Channel Assignment: For 5GHz only STAUTs and for dual band 2.4GHz/5GHz STAUTs, configure the AP to use channel 40. For 2.4GHz only STAUTs, configure the AP to use channel 6. For 60GHz only STAUTs, configure the AP to use channel 2. For multiband 2.4GHz/5GHz/60GHz STAUTs, configure the AP(s) to use channel 6, 40, and 2 respectively.

Test Goal: The test verifies that the STAUT implements the WSC association procedure correctly. The STAUT must be able to join an AP's WLAN through the AP's internal Registrar using PIN method.

Test Requirement: The STAUT must support PIN Configuration method. The STAUT must include the WSC IE in the 802.11 Association Request frame.

Test bed Devices:

1. AP, which supports PIN Configuration method. Choose one of the following:
 - a. Outside DMG: AP4.
 - b. Inside DMG: 60GHz WSC AP11.
2. A wireless packet sniffer device

Test Procedure:

1. Turn on the test bed AP in un-configured mode and turn on WSC if the AP is operating within DMG.
2. Manually configure test bed AP with new security settings SSID = "scstatest5.1.14ssid" and WPA2-PSK = "scstatest5.1.14psk"
3. Turn on the STAUT and start a WSC PIN registration process per vendor direction.
4. Start the wireless packet sniffer device.
5. Enter the PIN of STAUT into the test bed AP Internal Registrar.
6. Start ping from Console to STAUT; it must succeed within 90 seconds.
7. Stop the wireless packet sniffer device; verify that the first Association Request frame transmitted by the STAUT includes the WSC IE.

Test Pass/Fail Criterion: If the Association Request frame includes the WSC IE and if the Ping command is successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as 'must' is not fulfilled.



5.1.15 (Moved to test 5.4.5)

5.1.16 Add to AP using NFC connection handover method through internal Registrar

Test Applicability: Mandatory for STAUT if NFC connection handover is implemented, with the exception of STAUTs operating within DMG where the test is not applicable.

Test Goal: The test verifies the STAUT implements the NFC connection handover method as an Enrollee. The STAUT must be able to join an AP's WLAN through the AP's internal Registrar using NFC connection handover method.

Test bed Devices:

1. AP9 which has an internal registrar and supports NFC connection handover method.

Test Procedure:

1. Turn on the test bed AP.
2. Manually configure the test bed AP with new wireless configuration settings (SSID = "scstatest5.1.16ssid" and WPA(2)-PSK = "scstatest5.1.16psk") when prompted
3. Turn on the STAUT.
4. If necessary, activate the NFC function on the STAUT per vendor directions.
5. Touch the AP NFC Interface with the STAUT NFC Interface
6. Start ping from Console to the STAUT; it must succeed within 90 seconds.

Test Pass/Fail Criterion: If the Ping command is successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as 'must' is not fulfilled.

5.1.17 Refuse to add to erroneous AP using NFC connection handover method through internal Registrar

Test Applicability: Mandatory for STAUT if NFC connection handover is implemented, with the exception of STAUTs operating within DMG where the test is not applicable.

Test Goal: The test verifies the STAUT implements the NFC connection handover method as an Enrollee. The STAUT must be able to refuse joining an AP's WLAN through the AP's internal Registrar using NFC connection handover method, when the public key information received from the AP differs for NFC and WLAN.

Test bed Devices:

1. AP8 which has an internal registrar and supports NFC connection handover method with NFC Interface. Operation of test bed AP is changed to offer incorrect public key information over NFC (compute correct public key hash of the correct public key and change at least 1 bit of the computed public key hash and offer this in the NFC message).

**Test Procedure:**

1. Turn on the test bed AP.
2. Manually configure the test bed AP with new wireless configuration settings (SSID = “scstatest5.1.16ssid” and WPA(2)-PSK = “scstatest5.1.16psk”)
3. Turn on the STAUT.
4. If necessary, activate the NFC function on the STAUT per vendor directions.
5. Touch the AP NFC Interface with the STAUT NFC Interface
6. Start ping from Console to the STAUT; it must NOT succeed within 90 seconds.

Test Pass/Fail Criterion: If the Ping command is NOT successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.

5.1.18 Add to AP using PBC method through external Registrar

Test Applicability: Mandatory for STAUT if PBC implemented, with the exception of STAUTs operating within DMG where the test is not applicable.

Channel Assignment: For 5GHz only STAUTs and for dual band 2.4GHz/5GHz STAUTs, configure the AP to use channel 44. For 2.4GHz only STAUTs, configure the AP to use channel 1.

Test Goal: The test verifies that the STAUT implements the PBC method as an Enrollee. The STAUT must be able to join an AP’s WLAN using PBC method through an external Registrar.

Test Requirement: The STAUT must support PBC method.

Test bed Devices:

1. AP1, which supports PBC method
2. STA1L, which supports PBC method and is an External Registrar that connects via 802.11. Test bed External Registrar has the ability to show the list of enrollees based on the received Probe Request proxied by Test bed AP and let users to select a target enrollee from the list. Also the Test bed External Registrar is capable to add a selected enrollee’s MAC address in the AuthorizedMACs subelement in the WFA Vendor Extension attribute in SetSelectedRegistrar UPnP action and send it to the Test bed AP.
3. A wireless packet sniffer device, which is able to capture the wireless packet including the Probe Request packet.

Test Procedure:

1. Turn on the Test bed AP.



2. Turn on the Test bed ER.
3. Configure Test bed ER with the new parameters (SSID = “scstatest5.1.17ssid” and WPA2-Personal PASS PHRASE = “scstatest5.1.17psk”) which should be entered when prompted
4. Enter the PIN of the Test bed AP at the Test bed ER when prompted by the Registrar.
5. Wait for the Test bed ER to indicate completion
6. Turn on STAUT and start a WSC PBC registration process per vendor direction
7. On the wireless packet sniffer device, verify that the Probe Request frame transmitted by the STAUT includes the WSC IE
8. Initiate PBC Method on the Test bed External Registrar.
9. Start ping from the Test bed External Registrar to STAUT; it must succeed within 90 seconds.

Test Pass/Fail Criterion: If the Ping command is successful, this test is determined as PASS. Otherwise, it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.

5.1.19 STAUT selects WPA2 with mixed-mode AP

Test Applicability: Mandatory for all STAUTs, with the exception of STAUTs operating within DMG where the test is not applicable.

Channel Assignment: For 5GHz only STAUTs and for dual band 2.4GHz/5GHz STAUTs, configure the AP use channel 40. For 2.4GHz only STAUTs, configure the AP use channel 6.

Test Goal: The test verifies that the STAUT must be able to select WPA2 and join an AP’s WLAN through the AP’s internal Registrar using PIN method when the AP is configured for mixed mode.

Test Requirement: The STAUT must support PIN Configuration method and be able to end up selecting WPA2.

Test bed Devices:

1. AP2, which supports PIN Configuration method. The test bed AP also can be configured for mixed mode.
2. A wireless packet sniffer device, which is able to capture the wireless packets including the Association request frame.

Test Procedure:



1. Turn on the test bed AP and configure for mixed mode.
2. Turn on the STAUT and start a WSC PIN registration process per vendor direction.
3. Start the wireless packet sniffer device.
4. Enter the PIN of STAUT into the test bed AP IR.
5. Start ping from Console to STAUT; it must succeed within 90 seconds.
6. Stop the wireless packet sniffer device; verify that the Association Request frame transmitted by the STAUT after the provisioning includes the RSN IE, which indicates that the STAUT has been configured for WPA2.

Test Pass/Fail Criterion: If the Association Request frame includes the RSN IE, which indicates that the STAUT has been configured for WPA2 and if the Ping command is successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as 'must' is not fulfilled.

5.1.20 WSC fails if the STAUT is provisioned with WEP credential by a WSC 1.0 Registrar

Test Applicability: Mandatory for STAUT if WEP supported, with the exception of STAUTs operating within DMG where the test is not applicable.

Channel Assignment: For 5GHz only STAUTs and for dual band 2.4GHz/5GHz STAUTs, configure the AP to use channel 40. For 2.4GHz only STAUTs, configure the AP to use channel 6.

Test Goal: The test verifies that the STAUT returns WSC_NACK in response to message M8 if an attempt is made to provision a WEP credential by a WSC 1.0 Registrar. Alternatively the STAUT may choose not to associate and run the WSC protocol with a WEP configured AP.

Test Requirement: The STAUT must support PIN Configuration method. The STAUT must fail the WSC process and must reject the credential if it gets provisioned with a WEP credential.

Test bed Devices:

1. AP4, which implements WSC version 1.0 and which is capable of provisioning a WEP credential.
2. A wireless packet sniffer device, which is able to capture the wireless packets including the EAP packets.

Test Procedure:



1. Turn on the test bed AP. Disable 11n mode on the AP (11n mode prevents WEP from being used).
2. Configure the test bed AP with WEP settings (SSID = “scstatest5.1.19ssid” and WEP key = “scsta”).
3. Turn on the STAUT and start a WSC PIN registration process per vendor direction.
4. Start the wireless packet sniffer device.
5. Enter the PIN of the STAUT into the test bed AP IR.
6. Capture at least 60 seconds of wireless traffic or until a failure is indicated either on the AP’s IR or on the STAUT.
7. Examine the sniffer trace. If the STAUT does not associate to the test bed AP throughout the test, then PASS.
8. If message M8 is found the STAUT’s response must be WSC_NACK.

Test Pass/Fail Criterion: If in step 7, STAUT does not associate to the test bed AP or if in step 8, WSC_NACK is observed this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.

5.2 Act as Registrar and configure AP

These tests apply to COER and CEER STAUTs. Skip if OCOER or for testing within DMG.

5.2.1 Manually configure AP, and then enroll with Registrar using PIN Config method

Test Applicability: Mandatory for COER and CEER STAUTs. Skip if OCOER or for testing within DMG.

Channel Assignment: For 2.4GHz only STAUTs and for dual band 2.4GHz/5GHz STAUTs, configure the AP to use channel 6. For 5GHz only STAUTs, configure the AP to use channel 44.

Test Goal: The test verifies that the AP wireless configuration settings established by the user are not silently overwritten by the WSC methods. This test also verifies that the correct PIN must be used and a bad checksum is correctly identified.

Test Requirement: The STAUT must support PIN Config method and be capable of acting as an external Registrar.

Test bed Devices:

1. AP3, which supports PIN Config method and is acting as an Enrollee
2. STA7, which does not support any WSC method



3. A wireless packet sniffer device.

Test Procedure:

1. Turn on the AP.
2. Manually configure the AP with new wireless configuration settings (SSID = “scstatest5.2.1ssid” and WPA(2)-PSK = “scstatest5.2.1psk”) when prompted
3. Manually configure test bed station with new wireless configuration settings (SSID = “scstatest5.2.1ssid” and WPA2-PSK = “scstatest5.2.1psk”)
4. Ensure ping from the test bed station to Console operates correctly.
5. Turn on STAUT and start a WSC PIN registration process per vendor direction
6. Enter PIN of 12345671 in the Registrar of STAUT
7. Registrar must report an invalid PIN
8. Enter PIN of 12345670 (if the STAUT’s PIN is 12345670, then use PIN 24681353) in the Registrar of STAUT
9. Ping from Console to STAUT must fail
10. Enter the PIN of the AP in the ER of STAUT. If any options are presented by the Registrar the existing configuration setting must be selected (if there are default selections the existing configuration must be the default).

Note: An ER is allowed to change an already configured AP as long as the user is notified and given a choice NOT to change the AP configuration.
11. To confirm the existing configuration has been preserved, ping from the test bed station to STAUT; it must succeed within 90 seconds.
12. On the sniffer device, verify that the M2 message sent by the STAUT includes the follow mandatory, variable length string attributes: Manufacturer, Model Name, Model Number, Serial Number, and Device Name. These attributes must not use NULL-padding, i.e., the last octet of the attribute value must not be 0x00.

Test Pass/Fail Criterion: If the PING command is successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.

5.2.2 Configure the AP to use passphrase using PIN

Test Applicability: Mandatory for COER and CEER STAUTs. Skip if OCOER or for testing within DMG.

Channel Assignment: For 5GHz only STAUTs and for dual band 2.4GHz/5GHz STAUTs, configure the AP to use channel 40. For 2.4GHz only STAUTs, configure the AP to use channel 1.



Test Goal: The test verifies that the STAUT is able to configure an AP to use PASS PHRASE using PIN Config method. If the Registrar on STAUT supports saving of a profile or text file containing the passphrase and SSID then this functionality is also tested by reloading this information and using it to manually configure a legacy station that does not support any WSC method.

Test Requirement: The STAUT must support PIN Config method and be capable of acting as an external Registrar.

Test bed Devices:

1. AP1, which supports PIN Config method and is acting as an Enrollee
2. STA7, which does not support any WSC method

Test Procedure:

1. Turn on the AP.
2. Turn on the STAUT
3. Configure the STAUT with new wireless configuration settings (SSID = “scstatest5.2.ssid” and passphrase = “scstatest5.2.psk”) when prompted
4. Enter the PIN of the AP at the ER STAUT when prompted
5. Start ping from Console to STAUT; it must succeed within 90 seconds.
6. Manually configure the test bed station with the wireless configuration settings (SSID = “scstatest5.2.ssid” and passphrase = “scstatest5.2.psk”)
7. Start ping from the test bed station to STAUT; it must succeed within 90 seconds.
8. If the ER on STAUT does not support saving of the SSID and passphrase to a profile or text file and ping is successful then PASS, otherwise save the SSID and passphrase.
9. De-authenticate the test bed station and clear its wireless configuration.
10. Reset or restart the ER on STAUT and reload the profile saved earlier or open the text file saved earlier in which the SSID and passphrase were stored.
11. Manually configure the S test bed station with the wireless configuration settings from the Registrar on STAUT
12. Start ping from the test bed station to AP; it must succeed within 90 seconds.

Test Pass/Fail Criterion: For a STAUT with Registrar that does not support saving the SSID and passphrase, if the PING command is successful at Step 7, this test is determined as PASS. Otherwise it is determined as FAIL. For a STAUT with Registrar that does support saving the SSID and passphrase, if the PING command is successful at Step 12, this test is determined as PASS. Otherwise it is determined as fail. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.



5.2.3 Configure the AP to use open networking settings using PIN

Test Applicability: Mandatory for COER and CEER STAUTs. Skip if OCOER or for testing within DMG.

Channel Assignment: For 5GHz only STAUTs and for dual band 2.4GHz/5GHz STAUTs, configure the AP to use channel 44. For 2.4GHz only STAUTs, configure the AP to use channel 11.

Test Goal: The test verifies that the STAUT is able to configure an AP to use open network settings using PIN Config method.

Test Requirement: The STAUT must support PIN Config method and be capable of acting as an external Registrar.

Test bed Devices:

1. AP2, which supports PIN Config method and is acting as an Enrollee
2. STA7, which does not support any WSC method

Test Procedure:

1. Turn on the AP.
2. Turn on the STAUT
3. Configure the STAUT' ER with the open network settings (SSID = "scstatest5.2.3ssid")
4. Enter the AP's PIN at the ER on STAUT
5. The ER must inform the user that security is not set and require confirmation or require explicit user operation to create this open network.
6. Start ping from Console to STAUT; it must succeed within 90 seconds.
7. Manually associate the test bed station with the AP.
8. Start ping from the test bed station to STAUT; it must succeed within 90 seconds

Test Pass/Fail Criterion: If the PING command is successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as 'must' is not fulfilled.

5.3 Act as Registrar and add devices

These tests apply to CEER STAUTs. Skip if COER or OCOER or for testing within DMG.



5.3.1 Registrar configuring AP using registrar defaults and add device using both 4-digit and 8-digit PIN method

Test Applicability: Mandatory for CEER STAUTs. Skip if COER or OCOER or for testing within DMG.

Channel Assignment: For 2.4GHz only STAUTs and for dual band 2.4GHz/5GHz STAUTs, configure the AP to use channel 1. For 5GHz only STAUTs, configure the AP to use channel 36.

Test Goal: The test verifies that the STAUT implements the Registrar function. The STAUT must be able to configure an AP with its default settings and add a STA device to the AP's WLAN using PIN method.

Test Requirement: The STAUT must support PIN Config method and be capable of acting as an External Registrar

Test bed Devices:

1. AP1, which supports PIN Config method. The test bed AP has the ability to correctly validate that STAUT which implements WSC version 2.0 does not add the unwanted zero padding in SSID/Network Key attribute. Test bed AP also has a capability to verify that STAUT sets the Authentication Type and Encryption Type attributes in Encrypted Settings of M8 messages correctly. Test bed AP has also a capability to verify that the STAUT used the correct MAC address of the Enrollee and that The NewWLANEventMAC value of the PutWLANResponse UPnP actions must be the MAC address of STA2.
2. STA2, which supports PIN Config method and is acting as an Enrollee.
3. STA7, which is legacy station and does not support WSC methods.
4. STA5, which supports 4-digit PIN Config method and is acting as an Enrollee.
5. A wireless packet sniffer device.

Test Procedure:

1. Turn on the test bed AP. Put AP in un-configured state.
2. Turn on the STAUT.
3. Enter the SSID and passphrase into the STAUT's ER
 - SSID: scstatest5.3.1ssid
 - Passphrase: scstatest5.3.1psk
4. Enter the PIN of the test bed AP at the ER on STAUT.
5. Start ping from Console to STAUT; it must succeed within 90 seconds.
6. Turn on STA2.
7. Enter the 8-digit PIN of STA2 at the ER on STAUT.



8. Start ping from STA2 to STAUT; it must succeed within 90 seconds.
9. In the UI of the test bed AP, retrieve the wireless configuration settings (SSID and WPA2-PSK)
10. Turn on STA7.
11. Manually configure STA7 with retrieved wireless configuration settings from the AP and select to use WPA2 Personal.
12. Start ping from STA7 to STA2; it must succeed within 90 seconds.
13. Turn on STA5.
14. Enter the 4-digit PIN of STA5 at the ER on STAUT.
15. Start ping from STA5 to STAUT; it must succeed within 90 seconds.

Test Pass/Fail Criterion: If all of the PING commands are successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.

5.3.2 Registrar enrolling configured open AP and add device using PIN method

Test Applicability: Mandatory for CEER STAUTs. Skip if COER or OCOER or for testing within DMG.

Channel Assignment: For 2.4GHz only STAUTs and for dual band 2.4GHz/5GHz STAUTs, configure the AP to use channel 6. For 5GHz only STAUTs, configure the AP to use channel 48.

Test Goal: The test verifies that the STAUT implements the Registrar function. The STAUT must be able to register an AP configured with open network settings and add a STA device to the AP’s WLAN using PIN method with the original network settings.

Verify that in the discovery process for UPnP, the NewWLANEventMAC MAC address was used in PutWLANResponse actions. See Appendix B for an example of the UPnP frame.

Test Requirement: The STAUT must support PIN Config method and be capable of acting as an external Registrar

Test bed Devices:

1. AP2, which supports PIN Config method
2. STA2, which supports PIN Configuration method and is acting as an Enrollee. The test bed STA1 has the ability to correctly validate all WSC Attributes marked as R (required) in the Credential Attribute delivered in message M8 (including the Network Key which in this case must be a zero-length attribute).



3. STA7, which is legacy station and does not support WSC methods

Test Procedure:

1. Turn on the AP.
2. Configure the AP with the open network settings (SSID = “scstatest5.3.2ssid”)
3. Turn on STAUT and start a WSC PIN registration process per vendor direction
4. Enter the PIN of the AP at the ER on STAUT.
5. Start ping from Console to STAUT; it must succeed within 90 seconds.
6. Turn on the sniffer device and start to monitor the traffic to/from the test bed AP.
7. Turn on STA2.
8. Enter the PIN of STA2 at the ER on STAUT.
9. Start ping from STA2 to STAUT; it must succeed within 90 seconds.
10. Examine the sniffer trace and look for a TCP packet from the STAUT to the AP which contains the NewWLANEventMAC field with the MAC address of STA2 as the value.
11. Turn on STA7.
12. Manually configure STA7 with open network settings (SSID = “scstatest5.3.2ssid”)
13. Start ping from STA7 to STA2; it must succeed within 90 seconds.

Test Pass/Fail Criterion: If all of the PING commands are successful and the correct NewWLANEventMAC was used in PutWLANResponse actions, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.

5.3.3 Registrar adding device using NFC tag method with password token

Test Applicability: Mandatory for CEER STAUTs with NFC tag implemented. Skip if COER or OCOER regardless of NFC implementation or for testing within DMG.

Test Goal: The test verifies that the STAUT implements the Registrar function using NFC tag method with password token. The STAUT must be able to add a STA device to the AP’s WLAN using NFC tag method with password token.

Test bed Devices:

1. AP10 which supports NFC tag method with password token.
2. STA 11 which supports NFC tag method with password token and is acting as an Enrollee.



3. The writable test bed NFC tag type 4.

Test Procedure:

1. Turn on the Test bed AP and reset to out-of-box configuration.
2. Turn on the STAUT
3. Enter the PIN of the Test bed AP at the Registrar on STAUT.
4. Start ping from Console to STAUT; it must succeed within 90 seconds.
5. Turn on the Test bed STA.
6. Create a Password Token for the Test bed STA by selecting the password token generation function on the UI of the Test bed STA and touching the NFC Interface with the writable Test bed NFC Tag.
7. Follow the vendor directions to start a WSC NFC password token registration process on STAUT and touch the NFC Interface with the created Password Token.
8. Start ping from Console to the Test bed STA; it must succeed within 90 seconds.

Test Pass/Fail Criterion: If both Ping commands are successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.

5.3.4 Registrar adding device using NFC tag method with configuration token

Test Applicability: Mandatory for CEER STAUTs with NFC tag implemented. Skip if COER or OCOER regardless of NFC implementation or for testing within DMG.

Test Goal: The test verifies that the STAUT implements the Registrar function using NFC tag method with configuration token. The STAUT must be able to add a STA device to the AP’s WLAN using NFC tag method with configuration token.

Test bed Devices:

1. AP8 which supports NFC tag method with configuration token.
2. STA11 which supports NFC tag method with configuration token and is acting as an Enrollee.
3. The writable test bed NFC tag type 4.

Test Procedure:

1. Turn on the Test bed AP and reset to out-of-box configuration.
2. Turn on the STAUT.



3. Enter the PIN of the Test bed AP at the Registrar on STAUT.
4. Start ping from Console to STAUT; it must succeed within 90 seconds.
5. Create a Configuration Token on the STAUT following the vendor directions.
6. Turn on the Test bed STA and start the configuration token registration process.
7. Touch the Test bed STA with the Configuration Token when prompted.
8. Start ping from Console to the Test bed STA; it must succeed within 90 seconds.

Test Pass/Fail Criterion: If both Ping commands are successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.

5.3.5 Registrar adding device using NFC connection handover method

Test Applicability: Mandatory for CEER STAUTs with NFC connection handover implemented. Skip if COER or OCOER regardless of NFC implementation or for testing within DMG.

Test Goal: The test verifies that the STAUT implements the Registrar function using NFC connection handover method. The STAUT must be able to add a STA device to the AP’s WLAN using NFC connection handover method.

Test bed Devices:

1. AP10 which supports NFC connection handover method.
2. STA9 which supports NFC connection handover method and is acting as an Enrollee.

Test Procedure:

1. Turn on the Test bed AP.
2. Reset the Test bed AP to out-of-box configuration.
3. Turn on the STAUT.
4. Enter the PIN of the test bed AP at the Registrar on STAUT.
5. Start ping from the Console to STAUT; it must succeed within 90 seconds.
6. If necessary, activate the NFC function on the STAUT per vendor directions.
7. Touch the STAUT NFC Interface with the test bed STA NFC Interface.
8. Start ping from the Console to test bed STA; it must succeed within 90 seconds.

Test Pass/Fail Criterion: If both ping commands are successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.



5.3.6 Registrar refusing to add erroneous device using NFC connection handover method

Test Applicability: Mandatory for CEER STAUTs with NFC connection handover implemented. Skip if COER or OCOER regardless of NFC implementation or for testing within DMG.

Test Goal: The test verifies that the STAUT implements the Registrar function using NFC connection handover method. The STAUT must be able to refuse to add an erroneous STA device to the AP's WLAN using NFC connection handover method, when the public key information received from the device differs for NFC and WLAN.

Test bed Devices:

1. AP8 which supports NFC connection handover method.
2. STA9 which supports NFC connection handover method and is acting as an Enrollee. Operation of test bed STA is changed to offer incorrect public key information over NFC (compute correct public key hash of the correct public key and change at least 1 bit of the computed public key hash and offer this in the NFC message).

Test Procedure:

1. Turn on the test bed AP.
2. Reset the test bed AP to out-of-box configuration.
3. Turn on the STAUT.
4. Enter the PIN of the test bed AP at the Registrar on STAUT.
5. Start ping from the Console to STAUT; it must succeed within 90 seconds.
6. If necessary, activate the NFC function on the STAUT per vendor directions.
7. Touch the STAUT NFC Interface with the test bed STA NFC Interface.
8. Start ping from the Console to test bed STA; it must NOT succeed within 90 seconds.

Test Pass/Fail Criterion: If the first ping command is successful and the second ping command is NOT successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as 'must' is not fulfilled.

5.3.7 Overlapped PBC sessions

Test Applicability Mandatory for CEER STAUTs with PBC Implemented. Skip if COER or OCOER regardless of PBC implementation or for testing within DMG.

Channel Assignment: For 5GHz only STAUTs and for dual band 2.4GHz/5GHz STAUTs, configure the AP to use channel 48. For 2.4GHz only STAUTs, configure the AP to use channel 6.

Test Goal: The test verifies the STA can't join an AP's WLAN using PBC method through the STAUT's External Registrar, if another PBC WSC session by another STA



exists. Once other PBC WSC session is removed, the STA must be able to join the AP's WLAN.

Test Requirement: The STAUT must implement PBC method and be capable of acting as an external Registrar

Test bed Devices:

1. STA3, which supports PBC method and is acting as an Enrollee.
2. STA4, which supports PBC method and is acting as an Enrollee.
3. AP3

Test Procedure:

1. Turn on the test bed AP and reset to un-configured.
2. Turn on STA3.
3. Turn on STA4.
4. Turn on the STAUT.
5. Put the AP's PIN into the STAUT's ER to configure the AP.
 - SSID: scstatest5.3.6ssid
 - Passphrase: scstatest5.3.6psk
6. Initiate the WSC Push Button Configuration Method on STA3.
7. Wait for 1 minute and initiate the WSC Push Button Configuration Method on STA4.
8. Initiate the WSC Push Button Configuration Method on the ER on STAUT.
9. Start ping from Console to STA4. The ping must fail.
10. Wait for 1 minute.
11. Initiate the WSC Push Button Configuration Method on the ER on the STAUT.
12. Start pings from Console to STA3 and STA4. The pings must fail.
13. Wait for 2 minutes. The pings that were started in step 12 must continue to fail throughout this 2 minute period.
14. Stop pings from console to STA3 and STA4.
15. Initiate the WSC Push Button Configuration Method on STA4.
16. Initiate the WSC Push Button Configuration Method on the ER on the STAUT again.
17. Start ping from Console to STA4; it must succeed within 90 seconds.



Test Pass/Fail Criterion: If the PING command fails in the step 9 & 12 and succeeds in the step 17 this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.

5.3.8 STAUT acting as External Registrar correctly uses AuthorizedMACs subelement in the WFA Vendor Extension attribute in SetSelectedRegistrar UPnP action

Test Applicability: Mandatory for CEER STAUTs. Skip if COER or OCOER or for testing within DMG.

Channel Assignment: For 5GHz only STAUTs and for dual band 2.4GHz/5GHz STAUTs, configure the AP to use channel 48. For 2.4GHz only STAUTs, configure the AP to use channel 6.

Test Goal: The test verifies that the STAUT implements the PIN method to act as an external registrar and is able to add the Enrollee or Wildcard MAC address to the AuthorizedMACs subelement in the WFA Vendor Extension attribute in its SetSelectedRegistrar message, and remove the wildcard MAC address (if present) from its SetSelectedRegistrar message after the registration process has completed successfully.

Test Requirement: The STAUT must support PIN method and be capable of acting as an external Registrar. The STAUT may support selection of the STA to commence the PIN registration process from a list on its user interface.

Test bed Devices:

1. STA1W, which supports PIN Config method as an Enrollee.
2. STA5, which supports PIN Config method as an Enrollee.
3. AP4.
4. A wireless packet sniffer device.

Test Procedure:

1. Turn on the AP.
2. Reset AP to un-configured.
3. Turn on STAUT and start a WSC PIN registration process per vendor direction.
4. Configure the STAUT with the network settings (SSID = “scstatest5.3.7ssid” and passphrase = “scstatest5.3.7psk”)
5. Enter the PIN of AP at the STAUT’s ER.
6. Ping from Console to STAUT must succeed within 90 seconds.
7. Turn on the sniffer.



8. Turn on STA1W and start a WSC PIN registration process.
9. Turn on STA5 and start a WSC PIN registration process. STA5 must use a different PIN to STA1W.
10. If the STAUT user interface allows selection of a particular STA to begin the registration process from a list then select STA1W, otherwise skip this step.
11. Read the PIN displayed on STA1W and enter the PIN at the STAUT's ER.
12. Start ping from STA1W to the Console; it must succeed within 90 seconds.
13. Start ping from STA5 to the Console; it must not succeed.
14. If the ping from STA1W succeeded, check the sniffer trace for the following. If the STAUT user interface allowed selection of STA1W to commence the registration process then the AuthorizedMACs subelement in the WFA Vendor Extension attribute with the MAC address of STA1W must be present, and the MAC address of STA5 must not be present, in Beacons and Probe Responses from AP that follow the commencement of the PIN registration process on the STAUT. If the STAUT user interface did not allow selection of STA1W then the AuthorizedMACs subelement in the WFA Vendor Extension attribute in Beacons and Probe Responses sent by AP must contain the wildcard MAC address (FF:FF:FF:FF:FF:FF) after the PIN has been entered on the STAUT, and in this case after five seconds following a successful PIN method registration by STA1W the AuthorizedMACs subelement in the WFA Vendor Extension attribute must not include the wildcard MAC address in the Beacons and Probe Responses sent by AP.

Test Pass/Fail Criterion: If the Ping command to STA1 is successful and the Ping command to STA2 is unsuccessful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as 'must' is not fulfilled.

5.3.9 Protocol extensibility for STAUT which also implements Registrar

Test Applicability: Mandatory for CEER STAUTs. Skip if COER or OCOER or for testing within DMG.

Channel Assignment: For 5GHz only STAUTs and for dual band 2.4GHz/5GHz STAUTs, configure the AP to use channel 36. For 2.4GHz only STAUTs, configure the AP to use channel 1.

Test Goal: The test verifies that the STAUT Registrar supports protocol extensibility by accepting higher version number and new attributes from AP and STA.

Test Requirement: The STAUT must support PIN Config method and be capable of acting as an external Registrar.

**Test bed Devices:**

1. AP1 that can be configured to advertise different version numbers and to add a new attribute.
2. STA2 that can be configured to advertise different version number, add a new attribute and include some attributes with zero length data fields.

Test Procedure:

1. Turn on the Test bed AP in out-of-box mode and configure it to advertise version 5.7 and to add a new attribute (i.e., an attribute that is not defined in WSC 2.0 specification) to all messages.
2. Turn on STAUT and using its ER start a WSC PIN registration process per vendor direction.
3. Configure the ER STAUT with new wireless configuration settings (SSID = “scstatest5.3.8ssid” and passphrase = “scstatest5.3.8psk”) when prompted
4. Enter the PIN of the Test bed AP at the ER STAUT when prompted
5. Start ping from Console to STAUT; it must succeed within 90 seconds.
6. Turn on STA2 and configure it to advertise version 5.7 and to add a new attribute (i.e., an attribute that is not defined in WSC 2.0 specification) to all messages.
7. Read the displayed PIN on STA2 and enter the PIN at the ER STAUT.
8. Start ping from the Console to STA2; it must succeed within 90 seconds.

Test Pass/Fail Criterion: If the PING commands are successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.

5.4 WSC 1.0 backwards compatibility tests for STAUT

These tests are run with AP and external Registrar test devices from the WSC 1.0 test bed (see Appendix A), except where noted otherwise. These tests are not applicable for testing within DMG.

5.4.1 Add to WSC 1.0 AP using PBC method through internal Registrar

Test Applicability: Mandatory for all STAUTs if PBC is implemented, with the exception of STAUTs operating within DMG where the test is not applicable.

Channel Assignment: For 5GHz only STAUTs, configure the AP to use channel 40. For 2.4GHz only STAUTs, configure the AP to use channel 6. For dual band 2.4GHz/5GHz STAUTs, configure the AP to use channels 6 and 40 respectively.

Test Goal: This test verifies that the STAUT is backwards compatible with a WSC 1.0 AP. The test verifies that the STAUT implements the PBC method as an Enrollee. The



STAUT must be able to join an AP's WLAN through the AP's internal Registrar using PBC method. This test also checks that a dual-radio STAUT does not incorrectly identify the PBC active state of a dual-radio AP as an overlapping session.

Test Requirement: The STAUT must support PBC method.

Test bed Devices:

1. AP6

Test Procedure:

1. Turn on the AP and set its WSC State to configured.
2. Turn on the STAUT. If the STAUT scans both bands confirm that it sees the AP in both bands.
3. Push WSC button on the AP.
4. Push WSC button on the STAUT or start a WSC PBC registration process per vendor direction.
5. Ping from Console to STAUT must succeed within 90 seconds.

Test Pass/Fail Criterion: If the Ping command is successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as 'must' is not fulfilled.

5.4.2 Add to WSC 1.0 AP using PIN Configuration method through internal Registrar

Test Applicability: Mandatory for all STAUTs, with the exception of STAUTs operating within DMG where the test is not applicable.

Channel Assignment: For 5GHz only STAUTs and for dual band 2.4GHz/5GHz STAUTs, configure the AP to use channel 40. For 2.4GHz only STAUTs, configure the AP to use channel 6.

Test Goal: The test verifies that the STAUT implements the PIN Configuration method as an Enrollee. The STAUT must be able to join a WSC 1.0 AP's WLAN through the AP's internal Registrar using PIN method.

Test Requirement: The STAUT must support PIN Configuration method.

Test bed Devices:

1. AP5

**Test Procedure:**

1. Turn on the test bed AP in Out of the Box mode.
2. Turn on the STAUT and start a WSC PIN registration process per vendor direction.
3. Enter the PIN of STAUT into the test bed AP internal Registrar.
4. Start ping from Console to STAUT; it must succeed within 90 seconds.

Test Pass/Fail Criterion: If the Ping command is successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.

5.4.3 Add to WSC 1.0 AP using PIN Config method through WSC 1.0 external Registrar

Test Applicability: Mandatory for all STAUTs, with the exception of STAUTs operating within DMG where the test is not applicable.

Channel Assignment: For 5GHz only STAUTs and for dual band 2.4GHz/5GHz STAUTs, configure the AP to use channel 40. For 2.4GHz only STAUTs, configure the AP to use channel 11.

Test Goal: This test verifies that the STAUT is backwards compatible with WSC 1.0 ER and WSC 1.0 AP. The test verifies that the STAUT implements the PIN Config method as an Enrollee. The STAUT must be able to join an AP’s WLAN using PIN method through an external Registrar.

Test Requirement: The STAUT must support PIN Config method.

Test bed Devices:

1. AP7
2. STA8 - WSC 1.0 External Registrar that connects via 802.11

Test Procedure:

1. Turn on the AP.
2. Turn on the STA8.
3. The Registrar on the STA8 will be configured with the new parameters (SSID = “scstatest5.4.3ssid” and WPA2-PSK = “scstatest5.4.3psk”) which should be entered when prompted
4. Enter the PIN of the AP at the STA8 when prompted by the Registrar.
5. Wait for the Registrar on the STA8 to indicate completion



6. Turn on STAUT and start a WSC PIN registration process per vendor direction
7. On the STA8 enter the PIN from the STAUT.
8. Ping from Console to STAUT must succeed within 90 seconds.

Test Pass/Fail Criterion: If the Ping command is successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.

5.4.4 Add to WSC 2.0 AP using PIN Config method through WSC 1.0 external Registrar

Test Applicability: Mandatory for all STAUTs, with the exception of STAUTs operating within DMG where the test is not applicable.

Channel Assignment: For 5GHz only STAUTs and for dual band 2.4GHz/5GHz STAUTs, configure the AP to use channel 40. For 2.4GHz only STAUTs, configure the AP to use channel 11.

Test Goal: This test verifies that the STAUT is backwards compatible with WSC 1.0 ER and WSC 2.0 AP. The test verifies that the STAUT implements the PIN Config method as an Enrollee. The STAUT must be able to join an AP’s WLAN using PIN method through an external Registrar.

Test Requirement: The STAUT must support PIN Config method.

Test bed Devices:

1. AP4, which supports PIN Config method
2. STA8 which is an External Registrar that connects via 802.11

Test Procedure:

1. Turn on the WSC 2.0 AP.
2. Turn on the STA8.
3. The Registrar on the STA8 will be configured with the new parameters (SSID = “scstatest5.4.4ssid” and WPA(2)-PSK = “scstatest5.4.4psk”) which should be entered when prompted
4. Enter the PIN of the WSC 2.0 AP at the STA8 when prompted by the Registrar.
5. Wait for the Registrar on the STA8 to indicate completion
6. Turn on STAUT and start a WSC PIN registration process per vendor direction
7. On the STA8 enter the PIN from the STAUT.
8. Ping from Console to STAUT must succeed within 90 seconds.



Test Pass/Fail Criterion: If the Ping command is successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.

5.4.5 Able to be Enrolled by WSC 1.0 external Registrars that use null terminated password

Test Applicability: Mandatory for all STAUTs, with the exception of STAUTs operating within DMG where the test is not applicable.

Channel Assignment: For 2.4GHz only STAUTs and for dual band 2.4GHz/5GHz STAUTs, configure the AP to use channel 11. For 5GHz only STAUTs, configure the AP to use channel 44.

Test Goal: The test verifies that the STAUT supports null terminated password which might be provided by WSC 1.0 external Registrars.

Test Requirement: The STAUT must support PIN Config method.

Test bed Devices:

1. AP4
2. SAER1 which supports PIN Config method and is acting as a WSC 1.0 ER that uses null padding in the passphrase.

Test Procedure:

1. Turn on the test bed AP
2. Reset the test bed AP to un-configured mode.
3. Turn on the test bed WSC 1.0 external Registrar.
4. The test bed external Registrar will be configured with the new wireless configuration settings (SSID = “scstatest5.4.5ssid” and WPA2-PSK = “scstatest5.4.5psk”), which should be entered when prompted
5. Read the PIN from the AP and enter the PIN at the STA used as ER when prompted by the Registrar.
6. The test bed ER will display status on completion. The status must be success.
7. Turn on the STAUT, which is acting as an Enrollee
8. Enter the PIN from the STAUT into the external Registrar.
9. Start ping from console to the STAUT; it must succeed within 90 seconds.



Test Pass/Fail Criterion: If all of PING commands are successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.

5.5 Use Registrar handshake to discover AP settings and use those settings to associate

This test applies only to OCOER STAUTs. Skip if COER or CEER or for testing within DMG.

5.5.1 Discover settings of an AP in Configured state and associate

Test Applicability: Mandatory for OCOER STAUTs. Skip if COER or CEER or for testing within DMG.

Channel Assignment: For 2.4GHz only STAUTs and for dual band 2.4GHz/5GHz STAUTs, configure the AP to use channel 6. For 5GHz only STAUTs, configure the AP to use channel 44.

Test Goal: The test verifies that the STAUT can discover the settings of an AP which is in Configured state and associate using those settings. This test also verifies that the correct PIN must be used and a bad checksum is correctly identified.

Test Requirement: The STAUT must support PIN Config method and be capable of using the Registrar handshake to discover the AP's settings.

Test bed Devices:

1. AP3, which supports PIN Config method and is acting as an Enrollee
2. A wireless packet sniffer device.

Test Procedure:

1. Turn on the test bed AP.
2. Manually configure the AP with new wireless configuration settings (SSID = “scstatest5.5.1ssid” and WPA(2)-PSK = “scstatest5.5.1psk”).
3. Turn on STAUT and start a WSC PIN registration process per vendor direction
4. Enter PIN of 12345671 in the UI of the STAUT
5. Registrar must report an invalid PIN
6. Enter PIN of 12345670 (if the STAUT's PIN is 12345670, then use PIN 24681353) in the UI of the STAUT
7. Ping from Console to STAUT must fail
8. Enter the PIN of the AP in the UI of the STAUT.
9. Ping from the test bed station to STAUT; it must succeed within 90 seconds.



10. On the sniffer device, verify that the M2 message sent by the STAUT includes the follow mandatory, variable length string attributes: Manufacturer, Model Name, Model Number, Serial Number, and Device Name. These attributes must not use NULL-padding, i.e., the last octet of the attribute value must not be 0x00.

Test Pass/Fail Criterion: If the PING command is successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.

5.5.2 Discover settings of an AP configured to use open networking, and associate

Test Applicability: Mandatory for OCOER STAUTs. Skip if COER or CEER or for testing within DMG.

Channel Assignment: For 5GHz only STAUTs and for dual band 2.4GHz/5GHz STAUTs, configure the AP to use channel 44. For 2.4GHz only STAUTs, configure the AP to use channel 11.

Test Goal: The test verifies that the STAUT can discover the open settings of an AP which is in Configured state and associate using those settings.

Test Requirement: The STAUT must support PIN Config method and be capable of using the Registrar handshake to discover the AP’s settings.

Test bed Devices:

1. AP2, which supports PIN Config method and is acting as an Enrollee

Test Procedure:

1. Turn on the test bed AP.
2. Manually configure the AP with open network settings (SSID = “scstatest5.5.2ssid”).
3. Turn on STAUT and start a WSC PIN registration process per vendor direction
4. Enter the AP’s PIN in the UI of the STAUT
5. Start ping from Console to STAUT; it must succeed within 90 seconds.

Test Pass/Fail Criterion: If the PING command is successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.



5.5.3 Detect AP is in Not Configured state and not associate automatically

Test Applicability: Mandatory for OCOER STAUTs. Skip if COER or CEER or for testing within DMG.

Channel Assignment: For 5GHz only STAUTs and for dual band 2.4GHz/5GHz STAUTs, configure the AP to use channel 40. For 2.4GHz only STAUTs, configure the AP to use channel 1.

Test Goal: The test verifies that the STAUT can detect that an AP is in Not Configured state and that it informs the user and does not automatically associate to the AP.

Test Requirement: The STAUT must support PIN Config method and be capable of detecting that an AP is in Not Configured state.

Test bed Devices:

1. AP2, which supports PIN Config method and is acting as an Enrollee

Test Procedure:

1. Turn on the test bed AP in Not Configured state.
2. Turn on STAUT and start a WSC PIN registration process per vendor direction
3. Enter the PIN of the AP in the UI of the STAUT
4. STAUT must detect that the AP is in Not Configured state and inform the user. It may discover the AP's settings but may not associate automatically. The STAUT may then direct the user to join the AP manually or direct the user to use PBC mode to join the AP if the STAUT implements PBC.

Test Pass/Fail Criterion: The STAUT must detect that the AP is in Not Configured state, for example by scanning, and it must indicate this to the user. The STAUT may proceed with the Registrar handshake and discover the AP's settings but it must not automatically join the AP.



6 Stand-Alone External Registrar (SAERUT) tests

6.1 Stand-Alone External Registrar configuring and enrolling an AP and enrolling STA via PIN

These tests apply only to SAERUTs.

6.1.1 SAERUT enroll and configure AP for Security

Test Applicability: Mandatory for SAERUT

Channel Assignment: For 5GHz only STAUTs and for dual band STAUTs, configure the AP to use channel 40. For 2.4GHz only STAUTs, configure the AP to use channel 1.

Test Goal: The test verifies that the SAERUT is able to configure an AP to use a passphrase using PIN Config method. If the SAERUT supports saving of a profile or text file containing the passphrase and SSID then this functionality is also tested by reloading this information and using it to manually configure a legacy station that does not support any WSC method.

Test Requirement: The SAERUT must support PIN Config method

Test bed Devices:

1. AP1, which supports PIN Config method and is acting as an Enrollee. The test bed AP has the ability to correctly validate that SAERUT which implements WSC version 2.0 does not add the unwanted zero padding in SSID/Network Key attribute. Test bed AP also has a capability to verify that SAERUT sets the Authentication Type and Encryption Type attributes in Encrypted Settings of M8 messages correctly.
2. STA7, which does not support any WSC method

Test Procedure:

1. Turn on the Test bed AP.
2. Turn on SAERUT (if SAERUT is connected via Ethernet, connect to test bed) and start a WSC PIN registration process per vendor direction.
3. Configure the SAERUT with new wireless configuration settings (SSID = “scsaertest6.1.1ssid” and passphrase = “scstatest6.1.1psk”) when prompted
4. Enter the PIN of the Test bed AP at the SAERUT when prompted
5. If the SAERUT is an ER connected via 802.11, ping from SAERUT to the AP; it must succeed within 90 seconds. ERs connected via Ethernet skip this step.
6. Manually configure the test bed station with the wireless configuration settings (SSID = “scsaertest6.1.1ssid” and passphrase = “scsaertest6.1.1psk”)
7. Ping from the test bed station to SAERUT must succeed within 90 seconds.



8. If the SAERUT does not support saving of the SSID and passphrase to a profile or text file and ping is successful then PASS, otherwise save the SSID and passphrase in a profile or text file.
9. De-authenticate the test bed station and clear its wireless configuration.
10. Reset or restart the SAERUT and reload the profile saved earlier or open the text file saved earlier in which the SSID and passphrase were stored.
11. Manually configure the test bed station with the wireless configuration settings from the profile or text file saved earlier by the SAERUT
12. Start ping from the test bed station to SAERUT; it must succeed within 90 seconds.

Test Pass/Fail Criterion: For a SAERUT that does not support saving the SSID and passphrase to a profile or text file, if the PING command is successful at Step 7, this test is determined as PASS. Otherwise it is determined as FAIL. For a SAERUT that does support saving the SSID and passphrase to a profile or text file, if the PING command is successful at Step 12, this test is determined as PASS. Otherwise it is determined as fail. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.

6.1.2 SAERUT enroll manually configured AP using PIN method

Test Applicability: Mandatory for SAERUT

Channel Assignment: For 2.4GHz only STAUTs and for dual band STAUTs, configure the AP to use channel 6. For 5GHz only STAUTs, configure the AP to use channel 44.

Test Goal: The test verifies that the AP wireless configuration settings established by the user are not silently overwritten by the WSC methods. This test also verifies that the correct PIN must be used and a bad checksum is correctly identified.

Test Requirement: The SAERUT must support PIN Config method

Test bed Devices:

1. AP3, which supports PIN Config method and is acting as an Enrollee
2. STA7, which does not support any WSC method

Test Procedure:

1. Turn on the AP.
2. Manually configure the AP with new wireless configuration settings (SSID = “scsaertest6.1.2ssid” and WPA2-PSK = “scsaertest6.1.2psk”) when prompted



3. Manually configure the test bed station with new wireless configuration settings (SSID = “scsaertest6.1.2ssid” and WPA2-PSK = “scsaertest6.1.2psk”)
4. Ensure ping from the test bed station to the AP succeeds.
5. Turn on SAERUT (if SAERUT is connected via Ethernet, connect to test bed) and start a WSC PIN registration process per vendor direction.
6. Enter PIN of 12345671 in the SAERUT
7. SAERUT must report an invalid PIN
8. Enter the PIN of the AP in the SAERUT. If any options are presented by the SAERUT the existing configuration setting must be selected (if there are default selections the existing configuration must be the default).
9. To confirm the existing configuration has been preserved, ping from the test bed Station to AP must succeed within 90 seconds.

Test Pass/Fail Criterion: If the PING command is successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.

6.1.3 SAERUT enroll and configure AP using Registrar’s configuration and then enroll STAs using both 4-digit and 8-digit PIN method

Test Applicability: Mandatory for SAERUT

Channel Assignment: For 2.4GHz only STAUTs and for dual band STAUTs, configure the AP to use channel 1. For 5GHz only STAUTs, configure the AP to use channel 36.

Test Goal: The test verifies that the SAERUT must be able to configure an AP with the SAERUT settings and then enroll a STA using PIN method, and allow a legacy STA to be added to the WLAN manually.

Test Requirement: The SAERUT must support PIN Config method

Test bed Devices:

1. AP2, which supports PIN Config method.
2. STA3, which supports 8-digit PIN Config method and is acting as an Enrollee.
3. STA4, which supports 4-digit PIN Config method and is acting as an Enrollee.
4. STA7, which is legacy station and does not support WSC methods.

Test Procedure:

1. Turn on the AP.
2. Set the test bed AP WSC State to Not Configured..



3. Turn on SAERUT (if SAERUT is connected via Ethernet, connect to test bed) and start a WSC PIN registration process per vendor direction.
4. Configure the SAERUT with the network settings (SSID = “scsaertest6.1.3ssid” and passphrase = “scsaertest6.1.3psk”)
5. Enter the PIN of the AP at the SAERUT.
6. If the SAERUT is connected via 802.11, ping from SAERUT to the AP; it must succeed within 90 seconds. ERs connected via Ethernet skip this step.
7. Turn on STA3.
8. Enter the 8-digit PIN of STA3 at the SAERUT.
9. Ping from STA3 to SAERUT must succeed within 90 seconds.
10. In the UI of the AP, and confirm new wireless configuration settings (SSID = “scsaertest6.1.3ssid” and passphrase = “scsaertest6.1.3psk”)
11. Turn on STA7.
12. Manually configure STA7 with retrieved wireless configuration settings from the AP and select to use WPA2 Personal.
13. Pinging from STA7 to STA3 must succeed within 90 seconds.
14. Turn on STA1W.
15. Enter the 4-digit PIN of STA4 at the SAERUT.
16. Ping from STA4 to SAERUT must succeed within 90 seconds.

Test Pass/Fail Criterion: If all of the PING commands are successful, this test is determined as PASS. Otherwise, it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.

6.1.4 SAERUT enrolls and configures open AP and then enroll STA using PIN method

Test Applicability: Mandatory for SAERUT

Channel Assignment: For 2.4GHz only STAUTs and for dual band STAUTs, configure the AP to use channel 6. For 5GHz only STAUTs, configure the AP to use channel 48.

Test Goal: The test verifies that the Stand-Alone External Registrar must be able to configure an AP with open network settings and enroll a STA using PIN method, and allow a legacy STA to be added to the WLAN manually.

Test Requirement: The SAERUT must support PIN Config method

Test bed Devices:

1. AP4, which supports PIN Config method



2. STA4, which supports PIN Configuration method and is acting as an Enrollee. The test bed STA1 has the ability to correctly validate all WSC Attributes marked as R (required) in the Credential Attribute delivered in message M8 (including the Network Key which in this case must be a zero-length attribute).
3. STA7, which is legacy station and does not support WSC methods

Test Procedure:

1. Turn on the AP.
2. Turn on SAERUT (if SAERUT is connected via Ethernet, connect to test bed) and start a WSC PIN registration process per vendor direction.
3. Configure the SAERUT with the open network settings (SSID = "scsaertest6.1.4ssid")
4. Enter the PIN of the AP at the SAERUT
5. The SAERUT must inform the user that security is not set and require confirmation or require explicit user operation to create this open network.
6. If SAERUT is connected via 802.11, then ping from Console to SAERUT must succeed within 90 seconds. Skip this step for ERs connected via Ethernet.
7. Turn on STA4.
8. Enter the PIN of STA4 at the SAERUT.
9. Ping from STA4 to SAERUT must succeed within 90 seconds.
10. Turn on STA7.
11. Manually configure STA7 with open network settings (SSID = "scsaertest6.1.4ssid")
12. Ping from STA7 to STA4 must succeed within 90 seconds.

Test Pass/Fail Criterion: If all of the PING commands are successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as 'must' is not fulfilled.

6.1.5 SAERUT correctly uses AuthorizedMACs subelement in the WFA Vendor Extension attribute in SetSelectedRegistrar UPnP action

Test Applicability: Mandatory for SAERUT

Channel Assignment: For 5GHz only STAUTs and for dual band STAUTs, configure the AP to use channel 48. For 2.4GHz only STAUTs, configure the AP to use channel 6.

Test Goal: The test verifies that the SAERUT implements the PIN method to act as an external registrar and is able to add the Enrollee or Wildcard MAC address to the AuthorizedMACs subelement in the WFA Vendor Extension attribute in its



SetSelectedRegistrar message, and remove the wildcard MAC address (if present) from its SetSelectedRegistrar message after the registration process has completed successfully

Test Requirement: The SAERUT must support PIN method. The SAERUT may support selection of the STA to commence the PIN registration process from a list on its user interface.

Test bed Devices:

1. STA2, which supports PIN Config method as an Enrollee.
2. STA5, which supports PIN Config method as an Enrollee.
3. AP1.
4. A wireless packet sniffer device.

Test Procedure:

1. Turn on the AP
2. Reset the AP to out-of-box configuration
3. Turn on SAERUT (if SAERUT is connected via Ethernet, connect to test bed) and start a WSC PIN registration process per vendor direction.
4. Configure the SAERUT with the network settings (SSID = “scstatest6.1.5ssid” and passphrase = “scstatest6.1.5psk”)
5. Enter the PIN of the AP at the SAERUT.
6. If SAERUT is connected via 802.11, then ping from Console to SAERUT must succeed within 90 seconds. Skip this step for ERs connected via Ethernet.
7. Turn on the sniffer.
8. Turn on STA2 and start a WSC PIN registration process.
9. Turn on STA5 and start a WSC PIN registration process. STA5 must use a different PIN to STA2.
10. If the SAERUT user interface allows selection of a particular STA to begin the registration process from a list then select STA2, otherwise skip this step.
11. Read the PIN displayed on STA2 and enter the PIN at the SAERUT.
12. Start ping from STA2 to the SAERUT; it must succeed within 90 seconds.
13. Start ping from STA5 to the SAERUT; it must not succeed.
14. If the ping from STA2 succeeded, check the sniffer trace for the following. If the SAERUT user interface allowed selection of STA2 to commence the registration process then the AuthorizedMACs subelement in the WFA Vendor Extension attribute with the MAC address of STA2 must be present, and the MAC address



of STA5 must not be present, in Beacons and Probe Responses from the AP that follow the commencement of the PIN registration process on the SAERUT. If the SAERUT user interface did not allow selection of STA2 then the AuthorizedMACs subelement in the WFA Vendor Extension attribute in Beacons and Probe Responses sent by the AP must contain the wildcard MAC address (FF:FF:FF:FF:FF:FF) after the PIN has been entered on the SAERUT, and in this case after five seconds following a successful PIN method registration by STA2 the AuthorizedMACs subelement in the WFA Vendor Extension attribute must not include the Wildcard MAC address in the Beacons and Probe Responses sent by the AP.

Test Pass/Fail Criterion: If the Ping command to STA1 is successful and the Ping command to STA2 is unsuccessful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.

6.1.6 Protocol extensibility for SAERUT

Test Applicability: Mandatory for SAERUT

Channel Assignment: For 2.4GHz only STAUTs and for dual band STAUTs, configure the AP to use channel 6. For 5GHz only STAUTs, configure the AP to use channel 36.

Test Goal: The test verifies that the SAERUT supports protocol extensibility by accepting higher version number and new attributes from AP and STA.

Test Requirement: The SAERUT must support PIN Config method.

Test bed Devices:

1. AP1 that can be configured to advertise different version numbers and to add a new attribute.
2. STA2 that can be configured to advertise different version number, add a new attribute and include some attributes with zero length data fields.

Test Procedure:

1. Turn on the Test bed AP in out-of-box mode and configure it to advertise version 5.7 and to add a new attribute (i.e., an attribute that is not defined in WSC 2.0 specification) to all messages.
2. Turn on SAERUT (if SAERUT is connected via Ethernet, connect to test bed) and start a WSC PIN registration process per vendor direction.
3. Configure the SAERUT with new wireless configuration settings (SSID = “scstatest6.1.6ssid” and passphrase = “scstatest6.1.6psk”) when prompted



4. Enter the PIN of the Test bed AP at the SAERUT when prompted
5. If the SAERUT is an ER connected via 802.11, ping from SAERUT to the AP; it must succeed within 90 seconds. ERs connected via Ethernet skip this step.
6. Turn on STA2 and configure it to advertise version 5.7 and to add a new attribute (i.e., an attribute that is not defined in WSC 2.0 specification) to all messages.
7. Read the displayed PIN on STA2 and enter the PIN at the SAERUT.
8. Start ping from the Console to STA2; it must succeed within 90 seconds.

Test Pass/Fail Criterion: If the PING commands are successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as 'must' is not fulfilled.



6.2 Stand-Alone External Registrar enrolling STA via PBC

These tests apply only to SAERUTs.

6.2.1 SAERUT enroll AP using PIN method, and then enroll STA using PBC method

Test Applicability: Mandatory for SAERUT if PBC is implemented

Channel Assignment: For 2.4GHz only STAUTs and for dual band STAUTs, configure the AP to use channel 11. For 5GHz only STAUTs, configure the AP to use channel 40.

Test Goal: The test verifies that the SAERUT implements the PIN and PBC method. The configured SAERUT must be able to add a STA device to the WLAN using PIN method and then add a STA device using PBC method. This test also verifies that the correct PIN must be used and a bad checksum is correctly identified.

Test Requirement: The SAERUT must support PIN and PBC method

Test bed Devices:

1. AP2, which supports PIN Config method
2. STA3, which supports PBC method and is acting as an Enrollee

Test Procedure:

1. Turn on the AP
2. Reset the AP to out-of-box Configuration
3. On the UI of the AP, configure the AP with new security settings (SSID = "scsaertest6.2.1ssid" and WPA2-PSK = "scsaertest6.2.1psk").
4. Turn on SAERUT (if SAERUT is connected via Ethernet, connect to test bed AP) and start a WSC PIN registration process per vendor direction.
5. Enter the PIN of the AP at the SAERUT
6. If SAERUT is connected via 802.11, then ping from Console to SAERUT must succeed within 90 seconds. Skip this step for ERs connected via Ethernet.
7. Turn on the test bed station.
8. Push the WSC button on the SAERUT
9. Push the WSC button on the test bed station.
10. Ping from the test bed station to SAERUT must succeed within 90 seconds.



Test Pass/Fail Criterion: If the both of Ping commands are successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.

6.2.2 Overlapped PBC sessions

Test Applicability Mandatory for SAERUT if PBC implemented.

Test Goal: The test verifies the STA can't join an AP's WLAN using PBC method through the SAERUT's External Registrar, if another PBC WSC session by another STA exists. Once other PBC WSC session is removed, the STA must be able to join the AP's WLAN.

Test Requirement: The SAERUT must implement PBC method

Test bed Devices:

1. STA1W, which supports PBC method and is acting as an Enrollee.
2. STA4, which supports PBC method and is acting as an Enrollee.
3. AP3

Test Procedure:

1. Turn on the test bed AP.
2. On the UI of the test bed AP, configure the AP with new security settings (SSID = “scsaertest6.2.2ssid” and WPA2-PSK = “scsaertest6.2.2psk”).
3. Turn on STA1W.
4. Turn on STA4.
5. Turn on the SAERUT. Enter the PIN of the test bed AP at the SAERUT.
6. Initiate the WSC Push Button Configuration Method on STA1W.
7. Wait for 1 minute and initiate the WSC Push Button Configuration Method on STA4.
8. Initiate the WSC Push Button Configuration Method on SAERUT.
9. Start ping from SAERUT to STA4. The ping must fail.
10. Wait for 1 minute.
11. Initiate the WSC Push Button Configuration Method on the SAERUT.
12. Start pings from SAERUT to STA1W and STA4. The pings must fail.
13. Wait for 2 minutes. The pings that were started in step 12 must continue to fail throughout this 2 minute period.
14. Stop all pings.



15. Initiate the WSC Push Button Configuration Method on STA4.
16. Initiate the WSC Push Button Configuration Method on the SAERUT again.
17. Start ping from SAERUT to STA4; it must succeed within 90 seconds.

Test Pass/Fail Criterion: If the PING command fails in step 9 and step 12 and succeeds in step 17, this test is determined as PASS. Otherwise it is determined as FAIL.

6.3 Stand-Alone External Registrar enrolling STA via NFC

NFC for SAERs is not supported at this time.



Appendix A: Vendor equipment list and contacts

Melvin Simmons or Amber Buscemi

TESSCO Technologies

11126 McCormick Road

Hunt Valley, Maryland 21031

wifialliance@tessco.com

(Note: The distributor does **NOT** supply technical support and cannot answer technical questions regarding this equipment. A contact person for each device listed herein may be able to direct technical questions to the correct resource.)

A.1 WSC 2.0 equipment

A.1.1 802.11 (A, B, G, N) Access Points

AP #	Product Name/Model	HW Model	SW Version	Contact
AP1	Atheros	AR5KAP-0096WPS	2.6.15-9.2.0-wps2-2010-11-11	Wfa_external_support@mailman.atheros.com
AP2	Broadcom	BCM94718NR	Boot Loader Version: CFE 5.10.128.2 OS Version: Linux 5.70.63.1 WL Driver Version: 5.60.134	wfa-support-list@broadcom.com
AP3	Marvell	CD-88W-AP95-AO	Wireless Version: 5.0.8.11-W8366 System Version: AP95-5.0.9.7-HW-6281GTWGE LSP Version: 2010.11.05-LSP-2.6.29-RC7	wifilab-support@marvell.com
AP4	MediaTek	RT3800PDAP3	SDK Version: 3.3.3.0 Driver Version: 2.4.3.1	wfa-support@mediatek.com
AP8	Broadcom	BCM94708RDB_NFC	boot loader: CFE 6.37.14.54 (r425351) OS: Linux 2.6 6.31.58.0 wl driver: 6.31.58 (r451532)	wfa-support-list@broadcom.com
AP9	Mediatek	RT3883-6605NFC-AP	SDK: 3.3.3.0 driver: 2.4.2.6	wfa-support@mediatek.com
AP10	Qualcomm	AR5BXB-0092DA	kernel: 3.11.0-15-generic driver: master-2014-02-10-0-g4cf7c29	Wfa_external_support@mailman.atheros.com



			hostapd: v2.2-devel-wps-nfc-5	
AP11	Peraso	PRSW120	A.1.1804.004545	support-wifi60ghz@perasotech.com
AP12	Qualcomm	CA-65-YA181	IPQ8064.ILQ.5.2.0.1-000000011-P-1	WFA_60G_Support_Group@qti.qualcomm.com
AP13	Sibeam (Lattice Semiconductor)	SB6501	0.8.0.0.60560 60560	list-wigig-sw@latticesemi.com

A.1.2 802.11 (A, B, G, N) Stations

STA#	Product Name/Model	HW version	SW Version	OS	Contact
STA1L	Atheros	AR5BXB-0092DA	wpa_cli: v0.8.x-athr-wps2-2010-12-22, Driver: 9.1.0_P2P_1.14	Ubuntu 2.6.31-20	Wfa_external_support@mailman.atheros.com
STA1W	Atheros	AR5BXB-0092DA	Driver: 9.2.0.113 Jumpstart: 4.0.0.7	Windows 7 32-bit	Wfa_external_support@mailman.atheros.com
STA2	Broadcom	BCM943224HMS	wpsenr: 1.55.6	Fedora 2.6.29.4-167	wfa-support-list@broadcom.com
STA3	Marvell	RD-88W-PLUG-8787-B0	wpsapp: 10.063 Driver: SD8787-14.57.7.p7-M2614130.p001-GPL-(FP57)		wifilab-support@marvell.com
STA4	MediaTek	RT3592	RaConfig: 3.1.5.2033 Driver: 3.1.9013.6023 DLL: 1.0.9.1001 EEPROM: 1.2 Firmware: 0.26	Windows 7 32-bit	wfa-support@mediatek.com
STA5	Realtek	RTL8192DE	Driver: 1014.1.708.2011 Utility: 700.1635.421.2011	Windows 7 32-bit	wfa_help@realtek.com
STA9	Broadcom	Nexus 10	SigmaNFC-1.18-nexus-full.bz2	Fedora	wfa-support-list@broadcom.com
STA10	Qualcomm	AR5BXB-0092DA	kernel: 3.2.0-57-generic-pae driver: master-2013-11-04-0-g81a6c91 wpa_supplicant: 2.2-devel-wps-nfc-5	Ubuntu	Wfa_external_support@mailman.atheros.com



STA11	Mediatek	MT6620-6605NFC-STA	20140207_wps p2pnfcsta_sigm a	Windows XP	wfa-support@mediatek.com
-------	----------	--------------------	-------------------------------------	---------------	--

A.1.3 802.11ad (60GHz, DMG) Test bed Devices

STA #	Product Name/Model	HW version	SW Version	Contact
STA12	Intel	MaplePeak	4.0.10278.29	wigig-support@intel.com
STA13	Peraso	PRSW120	A.1.1804.004545	support-wifi60ghz@perasotech.com
STA14	Qualcomm	CA-65-YA181	IPQ8064.ILQ.5.2.0. 1-000000011-P-1	WFA_60G_Support_Group@qti.qualcomm.com

A.1.4 NFC Tags

NFC Forum Tag Type	Product Name	Memory Capacity
Type 1	Topaz512	512 bytes*
Type 3	FeliCa Standard	>1 kB
Type 4	Mifare DESFire	>2 kB

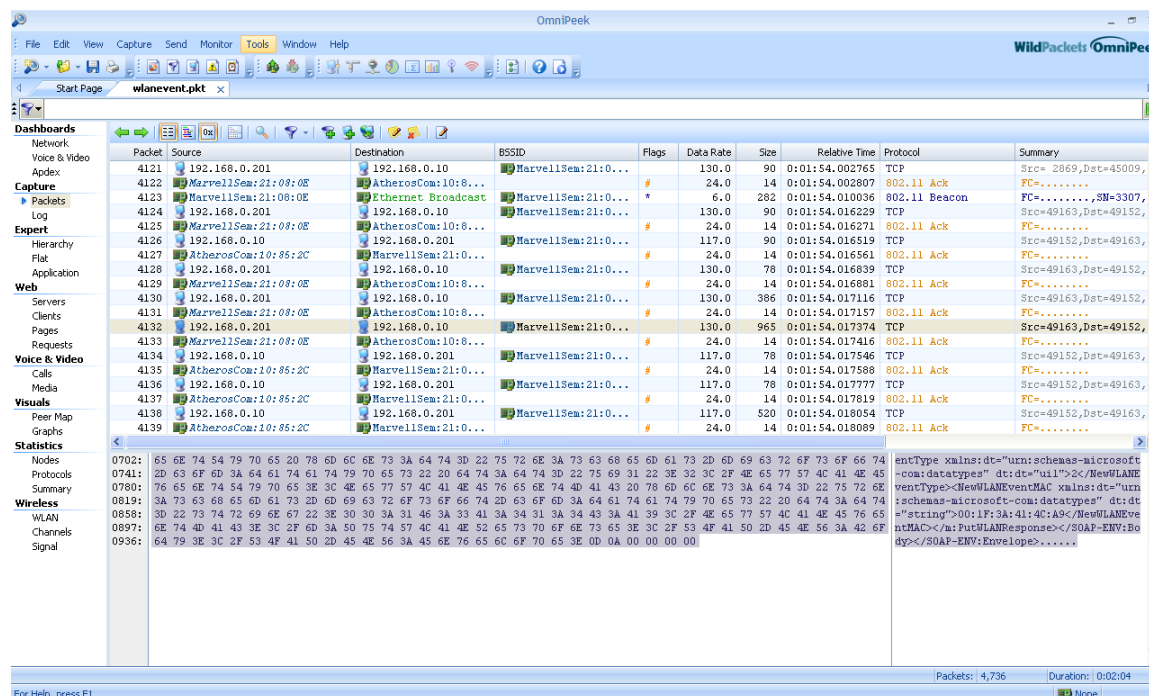
*User available memory after formatting is approximately 456 bytes for Topaz 512 NFC Type 1 Tag

A.2 WSC 1.0 equipment

AP# / STA#	Product Name/Model	HW version	SW Version	Contact
AP5	Atheros	AR5KAP-0096WFA	7.3.0.385	Wfa_external_support@mailman.atheros.com
AP6	Broadcom	BCM94718NR	WL=5.10.136.0, OS = 5.22.76.0	wfa-support-list@broadcom.com
AP7	Marvell	CD-88W-AP95-A0	5.0.6.2C	wifilab-support@marvell.com
STA6	Atheros	AR5KXB-0092DA or AR5BXB-0092DA	XP OS Driver: 7.7.0.448 Jumpstart: 2.1.0.26	Wfa_external_support@mailman.atheros.com
STA7	Broadcom	BCM943224HMS	XP OS 5.10.112.3	wfa-support-list@broadcom.com
STA8	Intel	633AN_HMWWB	XP OS Driver: 13.3.0.24	wfa.external.support@intel.com
SAER1	Microsoft wired ER		Windows 7 Ultimate	wfasupport@microsoft.com

Appendix B: UpnP Information Element

Here is an example of the TCP packet to look for in test 5.3.2. Here we are using the Marvell AP and the Atheros wireless ER. By looking at the ASCII translation of the packet, one can obtain the MAC address. Packet 4132 is the TCP packet containing the UpnP IE. The way to find this packet is to look at the ASCII translation to the right of the Hex codes, and look for the entry NewWLANEventMAC field. The MAC address can be seen as a group of string characters just before the /NewWLANEventMAC entry.



The screenshot shows the OmniPeek network analysis tool interface. The packet list on the left shows packet 4132 selected. The packet details on the right show the packet is a TCP ACK from 192.168.0.201 to 192.168.0.10. The ASCII translation on the right shows the UpnP IE structure, including the NewWLANEventMAC field with the MAC address 00:1F:3A:41:4C:A9.

Packet	Source	Destination	BSSID	Flags	Data Rate	Size	Relative Time	Protocol	Summary
4121	192.168.0.201	192.168.0.10	MarvellSem:21:0...		130.0	90	0:01:54.002765	TCP	Src= 2869,Dst=45009,
4122	MarvellSem:21:08:0E	AtherosCom:10:8...	MarvellSem:21:0...	#	24.0	14	0:01:54.002807	802.11 Ack	FC=.....
4123	MarvellSem:21:08:0E	Ethernet Broadcast	MarvellSem:21:0...	*	6.0	282	0:01:54.010036	802.11 Beacon	FC=.....,SN=3307,
4124	192.168.0.201	192.168.0.10	MarvellSem:21:0...		130.0	90	0:01:54.016229	TCP	Src=49163,Dst=49152,
4125	MarvellSem:21:08:0E	AtherosCom:10:8...	MarvellSem:21:0...	#	24.0	14	0:01:54.016271	802.11 Ack	FC=.....
4126	192.168.0.10	192.168.0.201	MarvellSem:21:0...		117.0	90	0:01:54.016519	TCP	Src=49152,Dst=49163,
4127	RtherosCom:10:85:2C	MarvellSem:21:0...	MarvellSem:21:0...	#	24.0	14	0:01:54.016561	802.11 Ack	FC=.....
4128	192.168.0.201	192.168.0.10	MarvellSem:21:0...		130.0	78	0:01:54.016839	TCP	Src=49163,Dst=49152,
4129	MarvellSem:21:08:0E	AtherosCom:10:8...	MarvellSem:21:0...	#	24.0	14	0:01:54.016881	802.11 Ack	FC=.....
4130	192.168.0.201	192.168.0.10	MarvellSem:21:0...		130.0	386	0:01:54.017116	TCP	Src=49163,Dst=49152,
4131	MarvellSem:21:08:0E	AtherosCom:10:8...	MarvellSem:21:0...	#	24.0	14	0:01:54.017157	802.11 Ack	FC=.....
4132	192.168.0.201	192.168.0.10	MarvellSem:21:0...		130.0	965	0:01:54.017374	TCP	Src=49163,Dst=49152,
4133	MarvellSem:21:08:0E	AtherosCom:10:8...	MarvellSem:21:0...	#	24.0	14	0:01:54.017416	802.11 Ack	FC=.....
4134	192.168.0.10	192.168.0.201	MarvellSem:21:0...		117.0	78	0:01:54.017546	TCP	Src=49152,Dst=49163,
4135	RtherosCom:10:85:2C	MarvellSem:21:0...	MarvellSem:21:0...	#	24.0	14	0:01:54.017588	802.11 Ack	FC=.....
4136	192.168.0.10	192.168.0.201	MarvellSem:21:0...		117.0	78	0:01:54.017777	TCP	Src=49152,Dst=49163,
4137	RtherosCom:10:85:2C	MarvellSem:21:0...	MarvellSem:21:0...	#	24.0	14	0:01:54.017819	802.11 Ack	FC=.....
4138	192.168.0.10	192.168.0.201	MarvellSem:21:0...		117.0	520	0:01:54.018054	TCP	Src=49152,Dst=49163,
4139	AtherosCom:10:85:2C	MarvellSem:21:0...	MarvellSem:21:0...	#	24.0	14	0:01:54.018089	802.11 Ack	FC=.....

The ASCII translation for packet 4132 shows the following structure:

```

entType xmlns:dt="urn:schemas-microsoft-com:datatypes" dt:dt="u11">2</NewWLANEventMAC>
<NewWLANEventMAC xmlns:dt="urn:schemas-microsoft-com:datatypes" dt:dt="string">00:1F:3A:41:4C:A9</NewWLANEventMAC>
</SOAP-ENV:Envelope>
  
```



Appendix C: (Normative) STAUT test cases for devices supporting only WSC Push Button Configuration method

The test cases in this section are applicable to a device under test (DUT) that only supports WSC Push Button Configuration (PBC) method. DUTs only passing test cases listed in this section will not carry the Wi-Fi CERTIFIED™ Wi-Fi Protected Setup™ certification. A DUT applying for Wi-Fi CERTIFIED Wi-Fi Direct® (refer to section 3.1 of [2]) or Wi-Fi CERTIFIED Miracast™ (refer to section 3.1.1 in [3]) certification that only supports WSC Push Button Configuration method shall pass test cases listed in this section to meet the pre-requisite requirements for these certification programs.

C.1 Test case list

Table 6 summarizes the test cases for STAUT devices supporting only WSC PBC method.

Table 6: STAUT tests for WSC PBC only DUTs

Name	Test case ID	Test case mapping to section 5	Applicability Mandatory / Optional / Conditional (M/O/C)
Add to AP using PBC method through internal Registrar	C.2.1	5.1.2	M
Two (2) minute timeout with multiple push button events for PBC method	C.2.2	5.1.7	M
Overlapped PBC sessions	C.2.3	5.1.8	M
Protocol extensibility	C.2.4	5.1.11	M
Add to AP when WSC IE and EAP-WSC is fragmented	C.2.5	5.1.12	M
Add to WSC 1.0 AP using PBC method through internal Registrar	C.2.6	5.4.1	M



C.2 STAUT tests

C.2.1 Add to AP using PBC method through internal Registrar

Test Applicability: Mandatory.

Channel Assignment: For 5GHz only STAUTs, configure the AP to use channel 40. For 2.4GHz only STAUTs, configure the AP to use channel 6. For dual band 2.4GHz/5GHz STAUTs, configure the AP to use channels 6 and 40 respectively.

Test Goal: The test verifies that the STAUT implements the PBC method as an Enrollee. The STAUT must be able to initiate and complete WSC handshake successfully through the AP's internal Registrar using PBC method. This test also checks that a STAUT with at least 2 radios does not incorrectly identify the PBC active state of an AP with at least 2 radios as an overlapping session.

Test Requirement: The STAUT must support PBC method.

Test bed Devices:

1. AP (AP2) is a dual-radio 2.4GHz/5GHz WSC AP, which supports PBC method.
2. A wireless packet sniffer device.

Test Procedure:

1. Turn on the AP in out-of-box mode with WSC enabled.
2. Turn on the STAUT. If the STAUT only supports single band, confirm that it sees the AP. If the STAUT scans in more than one band, confirm that it sees the APs in all scanned bands.
3. Push WSC button on the AP.
4. Push WSC button on the STAUT or start a WSC PBC registration process per vendor direction.
5. On the wireless packet sniffer device, verify that the Probe Request frame transmitted by the STAUT includes the WSC IE. Also verify that the WSC IE includes all of the required attributes (Version, Request Type, Configuration Methods, UUID, Primary Device Type, RF Bands, Association State, Configuration Error, Device Password ID, Version2 subelement in the WFA Vendor Extension, Manufacturer, Model Name, Model Number, Device Name).
6. The STAUT must support all the Config Methods it advertises in the Probe Request. On the sniffer device, verify that the Probe Request message that the STAUT sends includes the Config method attribute in the WSC IE and that it reflects the correct configuration methods of the STAUT.

Check on the sniffer to verify that the list of supported method in the IE is a bitwise OR of values from the list below:

0x0010	External NFC Tag
0x0020	Integrated NFC Tag
0x0040	NFC Interface



0x0080	PushButton
0x0100	Keypad
0x0280	Virtual Push Button
0x0480	Physical Push Button
0x2008	Virtual Display PIN
0x4008	Physical Display PIN

A STAUT supporting Pushbutton (0x0080) must include either or both of the Virtual Push Button (0x0280) Physical Push Button (0x0480) attributes.

The STAUT must support every Config method that it advertises as a bitwise OR in the WSC IE.

0x0010 – The STAUT must support and External NFC Tag.

0x0020 – The STAUT must support an Integrated NFC Tag.

0x0040 – The STAUT must support an NFC interface.

0x0080 – The STAUT must have a push button and support it.

0x0100 – The STAUT must support PIN using a Keypad on the STAUT

0x0280 – The STAUT must have a Virtual Push Button (in the UI) and support it.

0x0480 – The STAUT must have a Physical Push Button (on the STAUT) and support it.

0x2008 – The STAUT must support a PIN in the Virtual UI of the STAUT.

0x4008 – The STAUT must support a PIN on the physical display of the STAUT

7. Verify on the sniffer device that the M1 message from the STAUT includes following mandatory, variable length string attributes: Manufacturer, Model Name, Model Number, Serial Number, and Device Name. These attributes must not use NULL-padding, i.e., the last octet of the attribute value must not be 0x00. The STAUT must support all the Configuration Methods it advertises in the M1 message.
8. On the sniffer device, verify that the M1 message that the STAUT sends includes the following attributes: Authentication Type Flags and Encryption Type Flags. The values for these attributes must reflect the authentication and encryption types supported by the STAUT. The Authentication Type Flags value must include the following bits depending on STAUT capabilities: 0x0001 Open (mandatory), 0x0020 WPA2-Personal (mandatory). The Encryption Type Flags value must include 0x0008 AES (mandatory). The STAUT must include the WSC State set to 0x01 (Not Configured).
9. Check the Beacon or Probe Response of AP. The message must include the WSC State set to Configured (0x02).



10. On the wireless packet sniffer device, verify that the WSC handshake (M1-M8) completed successfully, and the test bed AP/registrar transmitted Deauthentication frame to the STAUT/enrollee.

Test Pass/Fail Criterion: If the WSC handshake is successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as 'must' is not fulfilled.



C.2.2 Two (2) minute timeout with multiple push button events for PBC method

Test Applicability: Mandatory.

Channel Assignment: For 2.4GHz only STAUTs and for dual band 2.4GHz/5GHz STAUTs, configure the AP to use channel 6. For 5GHz only STAUTs, configure the AP to use channel 40.

Test Goal: The test verifies that the STAUT exercises the push button 2 minutes timer correctly. As long as the period between when the user pushes the WSC button on the AP and when the user pushes the WSC button on the STAUT is less than 2 minutes, the STAUT must be able to initiate and complete WSC handshake using PBC method through the AP's internal Registrar.

Test Requirement: The STAUT must support PBC method

Test bed Devices:

1. AP (AP1) is a dual-radio 2.4GHz/5GHz WSC AP, which supports PBC method.
2. A wireless packet sniffer device.

Test Procedure:

1. Turn on the AP with WSC enabled.
2. Turn on the STAUT.
3. Push the WSC button on STAUT.
4. Wait 90 seconds.
5. Push the WSC button on STAUT again. NOTE: in some station implementations using a "soft" button, the button is not available to push until the 120-second timer has expired. In these cases, the button may be pushed as soon as it is available as long as the 90 seconds has elapsed in the previous step.
6. Wait for 1 minute.
7. Push the WSC button on the AP.
8. On the wireless packet sniffer device, verify that the WSC handshake (M1-M8) is completed successfully. And the test bed AP/registrar transmitted Deauthentication frame to the STAUT/enrollee.

Test Pass/Fail Criterion: If the WSC handshake is successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as 'must' is not fulfilled.



C.2.3 Overlapped PBC sessions

Test Applicability: Mandatory.

Channel Assignment: For 2.4GHz only STAUTs and for dual band 2.4GHz/5GHz STAUTs, configure the AP to use channel 11. For 5GHz only STAUTs, configure the AP to use channel 48.

Test Goal: The test verifies the STAUT cannot initiate and complete WSC handshake successfully using PBC method through the AP's internal Registrar, if another PBC WSC session by another AP exists. Once other PBC WSC session is removed, the STAUT must be able to initiate and complete WSC handshake successfully.

Test Requirement: The STAUT must support PBC method.

Test bed Devices:

1. AP-I (AP1) which supports the WSC PBC method.
2. AP-II (AP2) which supports the WSC PBC method.
3. A wireless packet sniffer device.

Test Procedure:

1. Turn on AP-II with WSC enabled.
2. Turn on AP-I with WSC enabled.
3. Turn on the STAUT. STAUT discovers AP-I and AP-II.
4. Push the WSC button on AP-I.
5. Wait for 1 minute and push the WSC button on AP-II.
6. Push the WSC button on STAUT.
7. STAUT must indicate PBC session overlap.
8. On the wireless packet sniffer device, verify that the STAUT does not initiate WSC handshake with either AP-I or AP-II.
9. Wait for at least 2 minutes or until the STAUT allows the WSC PBC button to be pushed
10. Push the WSC button on the STAUT. Push the WSC button on AP-II, also.
11. On the wireless packet sniffer device, verify that the WSC handshake (M1-M8) completed successfully. And the test bed AP/registrar transmitted Deauthentication frame to the STAUT/enrollee.

Test Pass/Fail Criterion: The STAUT must indicate that the WSC process fails after pushing the button on STAUT for the first time. The test is determined as a FAIL if any condition described as 'must' is not fulfilled.



C.2.4 Protocol extensibility

Test Applicability: Mandatory.

Channel Assignment: For 5GHz only STAUTs and for 2.4GHz/5GHz dual band STAUTs, configure the AP to use channel 36. For 2.4GHz only STAUTs, configure the AP to use channel 1.

Test Goal: The test verifies that the STAUT supports protocol extensibility by accepting higher version number and new attributes.

Test Requirement: The STAUT must support PBC method.

Test bed Devices:

1. AP (AP1) which supports WSC PBC method and that can be configured to advertise different version numbers, add a new attribute and include some attributes with zero length data fields.
2. A wireless packet sniffer device.

Test Procedure:

1. Turn on the Test bed AP in out-of-box mode with WSC enabled. Configure it to advertise version 5.7 and to add a new attribute (i.e., an attribute that is not defined in WSC 2.0 specification) to all messages.
2. Turn on the STAUT; push WSC button on the STAUT or start a WSC PBC registration process per vendor direction.
3. Push WSC button on the AP.
4. On the wireless packet sniffer device, verify that the WSC handshake (M1-M8) completed successfully And the test bed AP/registrar transmitted Deauthentication frame to the STAUT/enrollee.
5. On the wireless packet sniffer device, capture the Beacon frame from AP1 and verify the following is true else fix the test bed AP configuration and execute the test again:
 - a. Version 5.7 is advertised, and a new attribute (i.e., an attribute that is not defined in WSC 2.0 specification) is added
 - b. The WSC State must be set to Configured (0x02).

Test Pass/Fail Criterion: If the WSC handshake is successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as 'must' is not fulfilled.



C.2.5 Add to AP when WSC IE and EAP-WSC is fragmented

Test Applicability: Mandatory.

Channel Assignment: For 5GHz only STAUTs and for dual band 2.4GHz/5GHz STAUTs, configure the AP to use channel 36. For 2.4GHz only STAUTs, configure the AP to use channel 1.

Test Goal: The test verifies that the STAUT implements reassembly of WSC IE and EAP-WSC. The STAUT must be able to initiate and complete WSC handshake successfully with the test bed AP using PBC method when the AP is fragmenting attributes in WSC IEs and EAP-WSC messages.

Test Requirement: The STAUT must support PBC method.

Test bed Devices:

1. AP (AP2) which supports the WSC PBC method, and fragmentation of WSC IE and EAP-WSC messages.
2. A wireless packet sniffer device.

Test Procedure:

1. Turn on the Test bed AP in out-of-box mode with WSC enabled. Configure it to fragment WSC IEs within Probe Response frames. In addition, configure it to fragment some EAP-WSC messages.
2. Turn on the STAUT; push WSC button on the STAUT or start a WSC PBC registration process per vendor direction.
3. Push WSC button on the AP.
4. On the wireless packet sniffer device, verify that the WSC handshake (M1-M8) completed successfully. And the test bed AP/registrar transmitted Deauthentication frame to the STAUT/enrollee.

Test Pass/Fail Criterion: If the WSC handshake is successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as 'must' is not fulfilled.



C.2.6 Add to WSC 1.0 AP using PBC method through internal Registrar

Test Applicability: Mandatory.

Channel Assignment: For 5GHz only STAUTs, configure the AP to use channel 40. For 2.4GHz only STAUTs, configure the AP to use channel 6. For dual band 2.4GHz/5GHz STAUTs, configure the AP to use channels 6 and 40 respectively.

Test Goal: This test verifies that the STAUT is backwards compatible with a WSC 1.0 AP. The test verifies that the STAUT implements the PBC method as an Enrollee. The STAUT must be able to initiate and complete WSC handshake successfully through the AP's internal Registrar using PBC method. This test also checks that a dual-radio STAUT does not incorrectly identify the PBC active state of a dual-radio AP as an overlapping session.

Test Requirement: The STAUT must support PBC method.

Test bed Devices:

1. AP (AP6) which supports the WSC PBC method.
2. A wireless packet sniffer device.

Test Procedure:

1. Turn on the AP and set its WSC State to configured.
2. Turn on the STAUT. If the STAUT scans both bands confirm that it sees the AP in both bands.
3. Push WSC button on the AP.
4. Push WSC button on the STAUT or start a WSC PBC registration process per vendor direction.
5. On the wireless packet sniffer device, verify that the WSC handshake (M1-M8) completed successfully. And the test bed AP/registrar transmitted Deauthentication frame to the STAUT/enrollee.

Test Pass/Fail Criterion: If the WSC handshake is successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as 'must' is not fulfilled.



Appendix D: Change history table

Version	Date yyyy-mm-dd	Remarks
2.0.0	2010-12-22	Initial Release.
2.0.1	2011-02-04 2011-02-07	1.2.1, changed AP to APUT Added in contact information in appendix. Upgraded Ralink Station SW to correct bug in ACK length calculation.
2.0.2	2011-02-24	Section 2.2 – Added 5.3.2 – Removed step 5
2.0.3	2011-03-10 2011-04-11	– Use Ralink AP instead of Atheros AP. The Atheros AP does not always include selected registrar flag when used with the Windows external registrar. – Added Channel Assignment. Clarified between Ethernet and 802.11 External Registrars.
2.0.4	2011-04-20 2011-04-21 2011-04-25 2011-05-03 2011-05-18 2011-05-26 2011-06-01 2011-06-07 2011-06-16 2011-06-29	Appendix A – Changed Realtek's technical support contact. Appendix A – Added TESSCO's contact information. Appendix A – Changed Intel's technical support contact. Appendix A – Changed Realtek's technical support contact. – Fixed typo. Moved test 5.1.15 to test 5.4.5. Added test 5.3.8 – protocol extensibility test for STAUT which implement registrars. Added test 6.1.6 – protocol extensibility test for SAERUT. – Clarified step 7 so that STAUTs that choose not to associate and run the WSC protocol with a WEP configured AP pass. Appendix A – Changed Broadcom's technical support contact. Appendix A – Fixed Broadcom's wpsenr version number. Appendix A – Changed Atheros' technical support contact. – Replaced Ralink ER with Atheros ER. Appendix A – Updated Broadcom's firmware. Fixes an issue with slow enrollees.
2.0.5	2011-07-06 2011-08-03 2011-08-12	and 5.4.1 – Changed channel requirements. Appendix A – Replaced Realtek station with new Realtek station and driver. 5.1.1 – Modified test for STAUTs that do not transmit probe requests when WPS hasn't started or do not include the WSC IE in probe requests when WPS hasn't started. 5.3.6 – Clarified that this test is mandatory for a STAUT that implements a registrar and if the STAUT implements PB for that registrar.



		Appendix A – Updated Ralink AP with new firmware. Fixes an issue with slow enrollees.
2.0.6	2011-08-24	Appendix A – Marvell station has two hardware versions, A0 and A1. Either can be used.
	2011-09-01	Appendix A – Noted that Windows 7 are 32-bit versions.
	2011-09-08	Appendix A – Updated Marvell station with new software. Fixes an issue with LDPC.
	2011-09-27	Appendix A – Changed Ralink's technical support contact.
	2011-09-30	5.1.8 – If the elapsed time has been more than 2 minutes, push the WSC button on AP4, also.
2.0.7	2011-11-09	5.1.7 – Replace Ralink AP with Atheros AP. 5.1.8 – Replace Ralink AP with Broadcom AP.
	2011-11-14	and 4.1.2 – Added Label PIN to Configuration Methods.
	2011-11-29	– Added note about Ers changing already configured Aps.
	2011-12-01	Appendix A – Updated Ralink AP's firmware. Fixed issue where Ralink AP was not setting authorizedMAC subelement when using PBC.
2.0.8	2011-12-12	– Added note about disabling 11n to enable WEP.
	2012-1-26	Change test 4.1.14 to enforce the test for “brute force” attack to “indefinitely lockout the APUT's static PIN and prevent the addition of an ER to a network”. Added definition of static PIN.
2.0.9	2012-9-13	Added Section 5.5 for OCOER
	2012-10-23	6.1.2, step 4 – Corrected typo. Pings should be from test bed station to AP.
2.0.10	2012-11-15	Appendix A – For STA6, added hardware model AR5BXB-0092DA as an option.
	2012-12-19	Appendix A – Updated Microsoft's email.
	2013-01-14	Appendix A – Corrected model number for Atheros WPS1 AP.
	2013-03-12	– Placed a note stating this test case was moved to 5.4.5
	2013-03-20	Appendix A – For STA8, replaced the Intel 6200 with the Intel 6300 (633AN_HMWVB). The driver remains the same.
	2013-05-31	step 6 – Clarified when sniffer check should be performed.
	2013-06-25	Appendix A – Ralink AP firmware updated to 2.4.3.1
2.0.11		Internal draft, not released
2.0.12	2014-04-08	Adding in NFC
		Swapped sections 2 and 3 to match the test plan template.
		Added test requirement tables to section 3.



		<p>Deleted obsolete test 4.1.11; WPA/TKIP alone no longer allowed.</p> <p>Test 4.4.5, added criterion to require the SetRegister flag to be set to false within 2 minutes.</p> <p>Added changes that were lost from versions 2.0.9 to 2.0.11: 4.1.5 and 4.2.1 – Allow the Selected Registrar flag to be present and set to false when WPS is not active. 5.1.1 – Fixed typos. 4.1.11 – Fixed typo. 4.1.10 – Replaced Ralink station with Marvell station. 4.2.4—modified test to allow APUT to support only WPA2 or WPA2 and open configurations. 5.1.4 – Added note to skip step 7 if the STAUT doesn't use probe requests. 4.3.1 – Added note to skip test if APUT is configured when OOB. 5.1.19, change “may” to “must” for station not associating to a WEP configured AP. 5.4.1 – Set Broadcom AP to configured state. Fixed for matting of section 6 heading. Corrected model name of Atheros Aps. – Changed STA1W to STA4. Appendix A – Replaced the Marvell station with the Marvell RD-88W-PLUG-8787-B0. Updated the Marvell station's drivers.</p>
2.0.13	2014-05-07	Renamed Ralink to MediaTek.
	2014-06-12	steps 9 and 10 – Corrected mislabeled steps.
	2014-07-15	Appendix A – Added Broadcom NFC station's model number.
	2014-07-17	Added section 2.3.
2.0.14	2014-08-13	<p>Fixed overlapping AP and STA numbers between nonNFC and NFC devices; now all devices have unique numbers.</p> <p>Change SW for AP7, Marvell WSC1 AP.</p>
2.0.15	2014-08-27	2.1 – Modified image and text so that there is no misunderstanding about which devices support which features.
	2015-01-05	4.2.14 – Added additional steps to ensure that the APUT ends the PBC session(s) once a STA joins the WLAN.
2.0.16	2015-03-19	4.1.1 and 5.1.1 – Removed mention of Enterprise security.
	2015-08-27	3.2.3 – Corrected typo.
2.0.17	2016-10-10	Added support for testing within DMG (60GHz)
2.0.18	2018-07-09	Added support for WiGig Release 2
2.0.19	2018-11-29	Added test cases in Appendix C for STAUTs that only supports WSC PBC method.
2.0.20	2019-05-20	Allow the Qualcomm AP to be used in place of the Sbeam AP.