NFC631KT Software for Wi-Fi Protected Setup Version 1.1.2 Setup Guide

Testing Equipments

Name	Product Code	Quantity
1. PC		1
2. NFC631 Reader/Writer KIT	NFC631KT	1

Contents:

NFC Reader/Writer

NFC Token

USB Cable

NFC631KT Software for Wi-Fi Protected Setup CD

4. Wireless LAN Card	WLI-CB-AMG54	1

Setting up general Environment

NFC631KT Software for Wi-Fi Protected Setup CD is bootable, and enables general PCs to work as WPS NFC Access Point and Station.

1. PC with RAM 512MB or more, CPU architecture i686, PCMCIA Card available, and CD-ROM available.
2. NFC Reader/Writer
3. USB Cable to connect NFC Reader/Writer with PC
4. NFC Token
5. Wireless LAN CardBus Card – WLI-CB-AMG54

Setup Instruction

1. Set NFC631KT Software for Wi-Fi Protected Setup CD in the PC
2. Insert WLI-CB-AMG54 CardBus card in the PC
3. Plug NFC Reader/Writer in the PC with an USB cable
   We are NOT able to support any other NFC Reader/Writer except ours

4. Power on PC
5. Wait a few minutes
6. The 'fedora log-in' screen will appear
7. Enter Username: **root**, no password is required

8. After a few minutes, a main desktop screen will appear.

9. Click [testbed_sta] icon for using WPS Station Application, or click [testbed_ap] icon for using WPS Access Point Appliction.

Optionally, user can use an NFC Token Reader/Writer utility. Click [NFCTokenRW] icon and follow to the terminal messages.

2

Launch AP Application

Important: Users should once pull out and insert WLAN CardBus Card if they switched the application between STA and AP. It may cause an application launch fail or an unstable behavior without this procedure.

1. Launch the AP Application
   Click [testbed_ap] icon on the desktop
2. Confirm the wireless/wired/bridge interface device name, and their IP address.
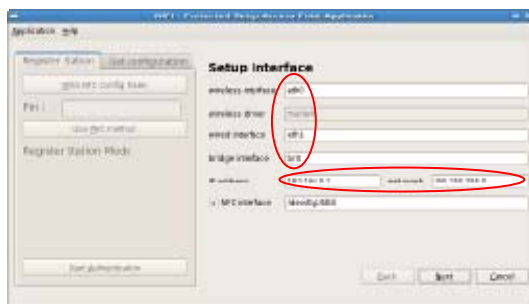

3. Click [Next]
4. Set SSID, Authentication type and Network key. Use [Generate] button if auto generation is necessary. User can choose 802.11a/b/g Channel and Frequency information.

5. Click [Next]

3
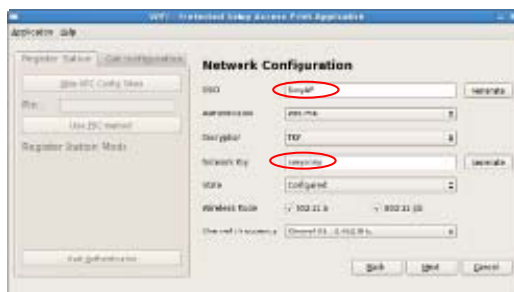
6. AP Setup Completed. The current settings are shown on the right side of the main dialog. If the setting does not show up in 10-20 seconds, click [Exit] and repeat the beginning of this step again.
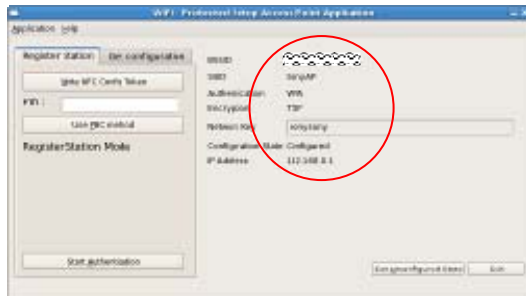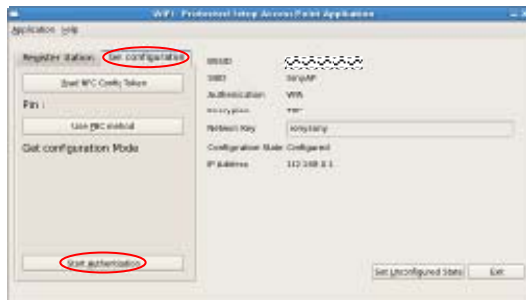
Testing AP as Enrollee – Get Configuration

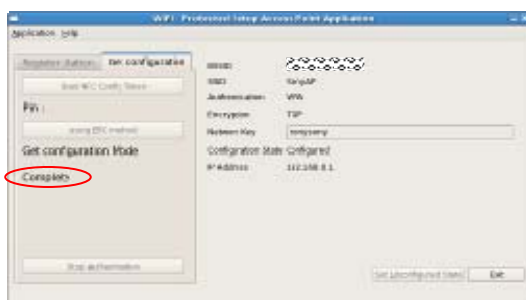Correspond to: Test Plan v1.3 - 4.1.6, 5.3.3, 5.3.4

1. Click [Get configuration] tab on the main dialog
2. Click [Start Authentication]

3. Touch NFC Password Token to the AP in 30 seconds

4. Touch the NFC Token to a Registrar Station
5. The WPS Authentication will complete in 2 minutes
6. AP will restart its internal settings and the new configuration is effective within 15 seconds.
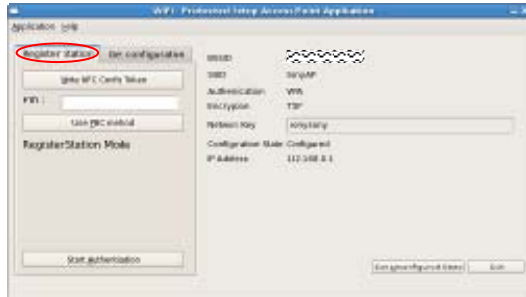
Testing AP as Registrar – NFC Password Token

Correspond to: Test Plan v1.3 - 4.2.5, 5.1.9

1. Click [Register Station] tab on the main dialog

2. Prepare an NFC Password Token from the Station

3. Click [Start Authentication]

4. Touch the NFC Password Token to the AP's NFC Reader/Writer

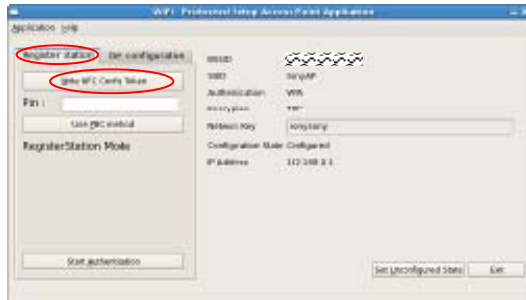5. WPS Authentication will complete in 2 minutes

6

Testing AP as Registrar – NFC Config Token

Correspond to: Test Plan v1.3 - 4.2.6, 5.1.10

1. Click [Register Station] tab on the main dialog
2. Prepare an NFC Password Token from the Station
3. Click [Write NFC Config Token]

4. Touch the AP with an NFC Config Token
5. The 'Complete' message will appear
6. Touch the target Station with the NFC Config Token
7. Configuration will be done in 10-15 seconds

Testing proxy AP function

Correspond to: Test Plan v1.3 - 5.3.3, 5.3.4

AP is working as proxy AP by default and no special procedure is required

Appendix: Auto Generate AP Settings - NFC Config Token

1. Click [Register Station] tab on the main dialog
2. Click [Set Unconfigured State]
3. Configuration state will be changed to 'Unconfigured' on the main dialog
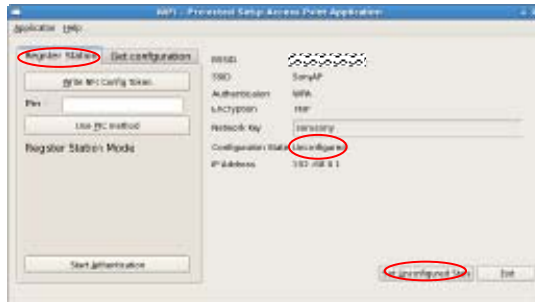
4. Click [Write NFC Config Token]
5. Touch the AP with an NFC Token
6. AP will restart in a few seconds and the auto generated settings appear on the main dialog
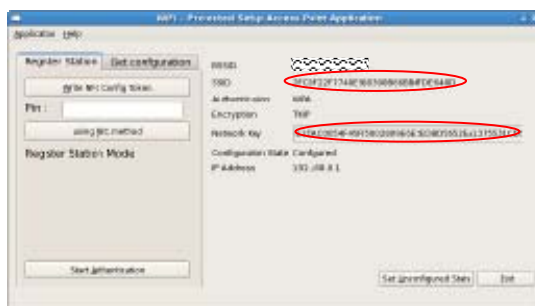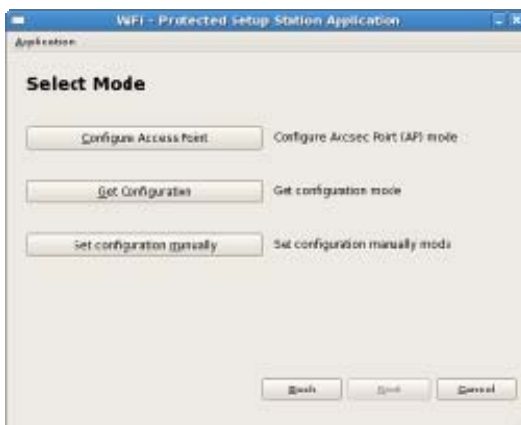
Launch Station Application

Important: Users should once pull out and insert Wireless LAN Card if they switched the application between STA and AP. It may cause an application launch fail or an unstable behavior without this procedure.

1. Launch the Station Application
   Click [testbed_sta] icon on the desktop
2. Confirm the wireless and the wired IP addresses. They must not be conflicted with peripheral testbed devices such as an AP or console devices.
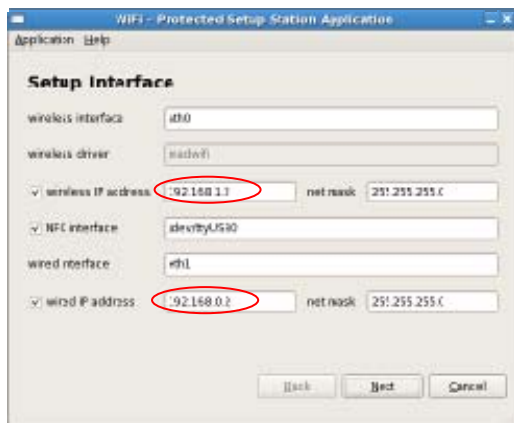
3. If the parameters are set properly, click [Next] button.
4. Setup completed. The following 'Select Mode' dialog will appear.

Testing Station as Enrollee – NFC Password Token

Correspond to: WPS Test Plan v1.3 - 4.2.5, 5.1.9, 5.3.3

1. Launch Station Application
2. Click [Get Configuration] button at the 'Select Mode dialog

3. Click [PIN] method
4. Select the registrar AP which is listed on the dialog. If the target AP is not listed, click [Update] button and wait for 10 seconds.

5. Click [Next]
6. Touch the Station's NFC Reader/Writer with an NFC Password Token in 30 seconds. In the event of the timeout, click [Retry] and touch the Token again..

7. If the Password is properly written, the following message will appear.

8. Touch a target AP with the NFC Password Token
9. Click [Next]
10. Wait a few seconds for the WPS Authentication
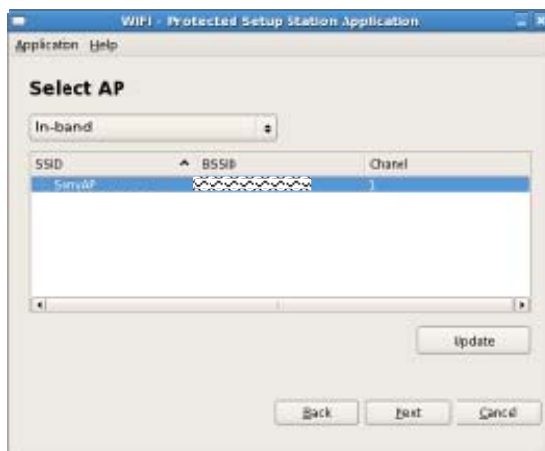11. If the WPS authentication succeeded, the 'Complete' message will appear. If not, 'Fail' message will appear

Testing Station as Enrollee – NFC Config Token

Correspond to: Test Plan v1.3 - 4.2.6, 5.1.10, 5.3.4

1. Launch Station Application
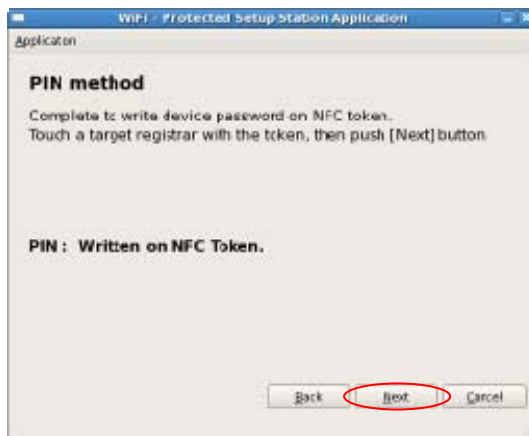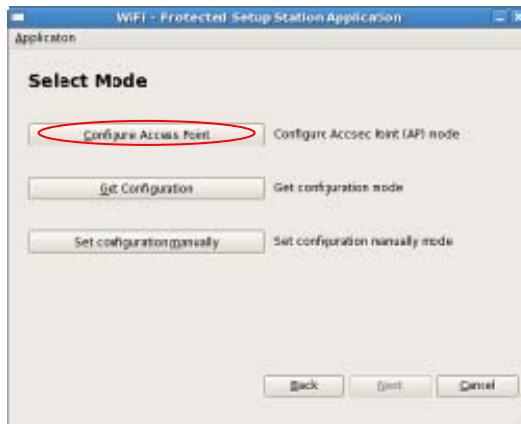2. Click [Get Configuration] button at the 'Select Mode' dialog
3. Prepare a Configuration Token form an AP Registrar before going to the following step
4. Click [NFC Config Token] on the Select Method dialog
5. Touch the NFC Config Token to the Station in 30 seconds. In the event of the timeout, click [Retry] and touch the Token again.
6. The 'Complete' message will appear

Testing Station as Registrar – Configure AP

Correspond to: Test Plan v1.3 - 4.1.6, 5.3.3, 5.3.4

1. Launch Station Application
2. Click [Configure Access Point] at the Select Mode dialog

3. Input SSID and PSK which are required to configure AP

   If necessary, Click [Generate] to make parameters automatically.

4. Click [Next] button
5. Click [PIN] at the 'Select Method' dialog
6. Select an appropriate AP which are listed on the 'Select AP' dialog
7. Prepare an NFC Password Token from the AP before going to the following step
8. Click [Next] button
9. Touch the NFC Password Token to the Station's NFC Reader/Writer
10. Wait a few seconds for the WPS Authentication
11. The 'Complete' message will appear if the WPS Authentication succeeded

Testing Station as Registrar – Register Another Station with NFC Password Token
Correspond to: Test Plan v1.3 - 5.3.3

1. Launch Station Application
2. Click [Configure Access Point] at the Select Mode dialog
3. Input SSID and PSK which are required to configure AP
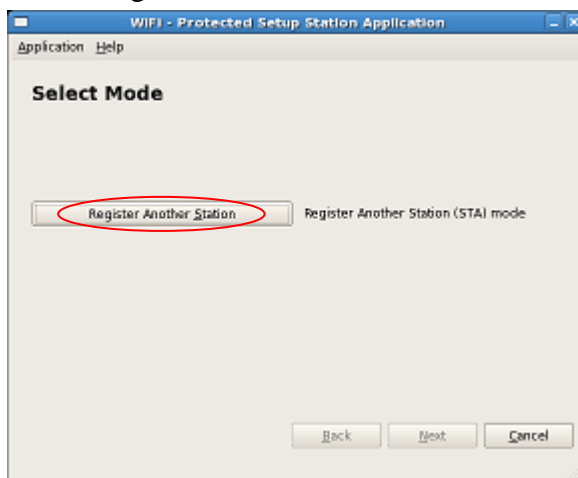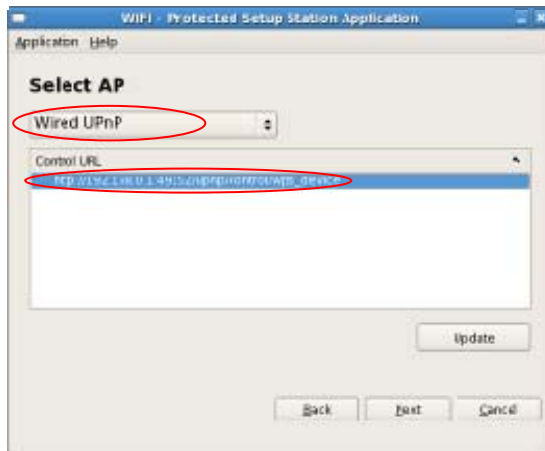   If necessary, Click [Generate] to make parameters automatically.
4. Click [Next] button
5. Click [PIN] at the 'Select Method' dialog
6. Select an appropriate AP which are listed on the 'Select AP' dialog
7. Prepare an NFC Password Token from the AP before going to the following step
8. Click [Next] button
9. Touch the NFC Password Token to the Station's NFC Reader/Writer
10. Wait a few seconds for the WPS Authentication
11. The 'Complete' message will appear if the WPS Authentication succeeded
12. Click [Next] button
13. Click [Register Another Station] button at the 'Select Mode' dialog

14. Click [PIN] button at the 'Select Method' dialog

15. Select [Wired UPnP] or [Wireless UPnP] and find an appropriate AP, and click the AP which is listed on the 'Select AP' dialog

16. Prepare NFC Password Token from the Enrollee Station before going to the following step
17. Click [Next] button
18. Touch the Enrollee's NFC Password Token to the Registrar Station
19. Wait a few seconds for the WPS Authentication
20. The 'Complete' message will appear

Testing Station as Registrar – Register Another Station with NFC Config Token

Correspond to: Test Plan v1.3 - 5.3.4

1. Launch Station Application
2. Click [Configure Access Point] at the Select Mode dialog
3. Input SSID and PSK which are required to configure AP

   If necessary, Click [Generate] to make parameters automatically.
4. Click [Next] button
5. Click [PIN] at the 'Select Method' dialog
6. Select an appropriate AP which are listed on the 'Select AP' dialog
7. Prepare an NFC Password Token from the AP before going to the following step
8. Click [Next] button
9. Touch the NFC Password Token to the Station's NFC Reader/Writer
10. Wait a few seconds for the WPS Authentication
11. The 'Complete' message will appear if the WPS Authentication succeeded
12. Click [Next] button
13. Click [Register Another Station] button at the 'Select Mode' dialog
14. Click [NFC Config Token] button at the 'Select Method' dialog
15. Touch an NFC Config Token in 30 seconds
16. The 'Complete' message will appear
17. Touch the target Enrollee Station with the NFC Config Token
18. Configuration will be done in a few seconds

Appendix: Setup Station manually

1. Launch Station Application
2. Click [Set Configuration manually]

3. Input SSID and PSK to be set as a default setting. This must be same as the AP setting.
4. Click [Next] button
5. The 'Complete' message will appear

Appendix: How to setup wireless interface for Wireshark Network Analyzer with Wi-Fi Protected Setup(WPS) protocol

About Wireshark, please refer to Wireshark website below

http://www.wireshark.org/

1. Set wireless interface to monitor mode to monitor wireless packet

   ex. # wlanconfig ath2 create wlandev wifi0 wlanmode monitor

   When you are testing with AP or Station, you MUST NOT set the same interface as AP

   or Station. For example, if you use "ath0" as AP, do not set "ath0" as monitor mode.

2. Start up interface

   ex. # ifconfig ath2 up

3. Launch Wireshark Network Analyzer

   Click [Wireshark Network Analyzer] icon on the desktop

4. You may use filter tag for WPS as follows.

   * For WPS Information Elements (IE) of Beacon and Probe Request/Response

   [wlan_mgt.wps]

   [wlan_mgt.wps.oui]

   [wlan_mgt.wps.tlv.version]

   [wlan_mgt.wps.tlv.wps_state]

   and so on…

   * For WPS EAP protocol

   [eap.wps]

   [eap.wps.vendor_id]

   [eap.wps.vendor_type]

   [eap.wps.op_code]

   [eap.wps.flags]

   [eap.wps.tlv.version]

   [eap.wps.tlv.msg_type]

   and so on…