



Connected X Cyber Security

FNV2 Vehicle HotSpot and AP Client

Version .20

UNCONTROLLED COPY IF PRINTED

FORD CONFIDENTIAL



Feature Document
FNV2 Vehicle HotSpot and AP Client

Table of Contents

1.1	REVISION HISTORY:	3
1.2	WiFi HotSpot REQUIREMENTS	4
1.2.1	4
1.2.2	4
1.2.3	5
1.3	WiFi CLIENT REQUIREMENTS	6
1.3.1	6
1.3.2	6

CONFIDENTIAL



Feature Document
FNV2 Vehicle HotSpot and AP Client

1.1 Revision History:

Version	Revision Date	Description of Change	Affected Sections	Author
V0.1	5/08/2018	Initial Version	N/A	Scott MacArthur
V0.2	10/9/2018	Security Group Review	All	Scott Macarthur

CONFIDENTIAL



1.2 WiFi HotSpot Requirements

1.2.1

Encryption

The access point shall be configured only to accept connections using the WPA2 or higher security protocol. Configuring the hotspot without security, or with WPS or WPA protocols shall not be allowed.

Requirement ID: ###WiFi_00001###			
Rationale			
Encryption provides a basic level of security required by Ford policy			
Acceptance Criteria			V&V Method
<ul style="list-style-type: none">The results of "netsh wlan show networks" will show the associated SSID is encrypted with WPA2-Personal			DV
Notes			
Visit http://www.wi-fi.org for more information on WPA2/3			
Version	Date	Author	Change
1.0	5/08/18	smacarth/ mburris6	Initial version

1.2.2

Pre-Shared Keys

A default pre-shared key shall be generated from random letters and numbers with minimum length specified by security protocol used.

Requirement ID: ###WiFi_00002###			
Rationale			
A WiFi password will keep unauthorized users from accessing the vehicle hotspot.			
Acceptance Criteria			V&V Method
<ul style="list-style-type: none">When attempting to connect to the WiFi hotspot, the user should be prompted for a password.New modules have a unique random password by default (which users may be able to change).Review of PSK generation algorithm			DV
Notes			
Version	Date	Author	Change
1.0	5/08/18	smacarth/mburris6	Initial version



Feature Document FNV2 Vehicle HotSpot and AP Client

1.2.3

SSID

For AP mode, the shared SSID shall include a unique naming convention in the format "HotspotXXXX" where "XXXX" is the last four digits of the TCUs ESN.

Requirement ID: ###WiFi_00003###

Rationale

Having a unique SSID will prevent errors when trying to connect with multiple vehicles in range. This helps both in terms of having a unique SSID, but also makes dictionary attacks more difficult.

Acceptance Criteria

- Wi-Fi AP ID follows specified format

V&V Method

DV Testing

Notes

The Linux command "ifconfig" will show the WiFi chipset's MAC address and the results of "netsh wlan show networks" in Windows will show all available SSIDs.

Version	Date	Author	Change
1.0	5/10/18	smacarth/mburris6	Initial version



1.3 WiFi Client Requirements

1.3.1

HotSpot Authentication

While in WiFi mode, the client shall only connect to networks which have been approved by the vehicle owner or pre-populated by Ford. The list of owner-approved hotspots shall be erased during a master reset.

Requirement ID: ### WiFi_00005###			
Rationale			
Forcing the client to connect to trusted networks decreases the chances of a malicious actor from attacking the client.			
Acceptance Criteria			
Review code and/or configuration(s) to ensure only pre-approved networks are approved for connection.			Manual verification
Notes			
Version	Date	Author	Change
1.0	5/10/18	smacarth/mburris6	Initial version

1.3.2

Insecure Networks

WiFi client shall prompt the user for confirmation before attempting to connect to any network not secured with WPA2+.

Requirement ID: ### WiFi_00006###			
Rationale			
WiFi networks not using WPA2 are considered insecure and communications could be intercepted by a malicious 3rd party.			
Acceptance Criteria			V&V Method
<ul style="list-style-type: none">Connecting to a WiFi network not protected by WPA2 should prompt the user to confirm they want to connect to an insecure network.			DV
Notes			
Version	Date	Author	Change
1.0	5/10/18	smacarth/mburris6	Initial version