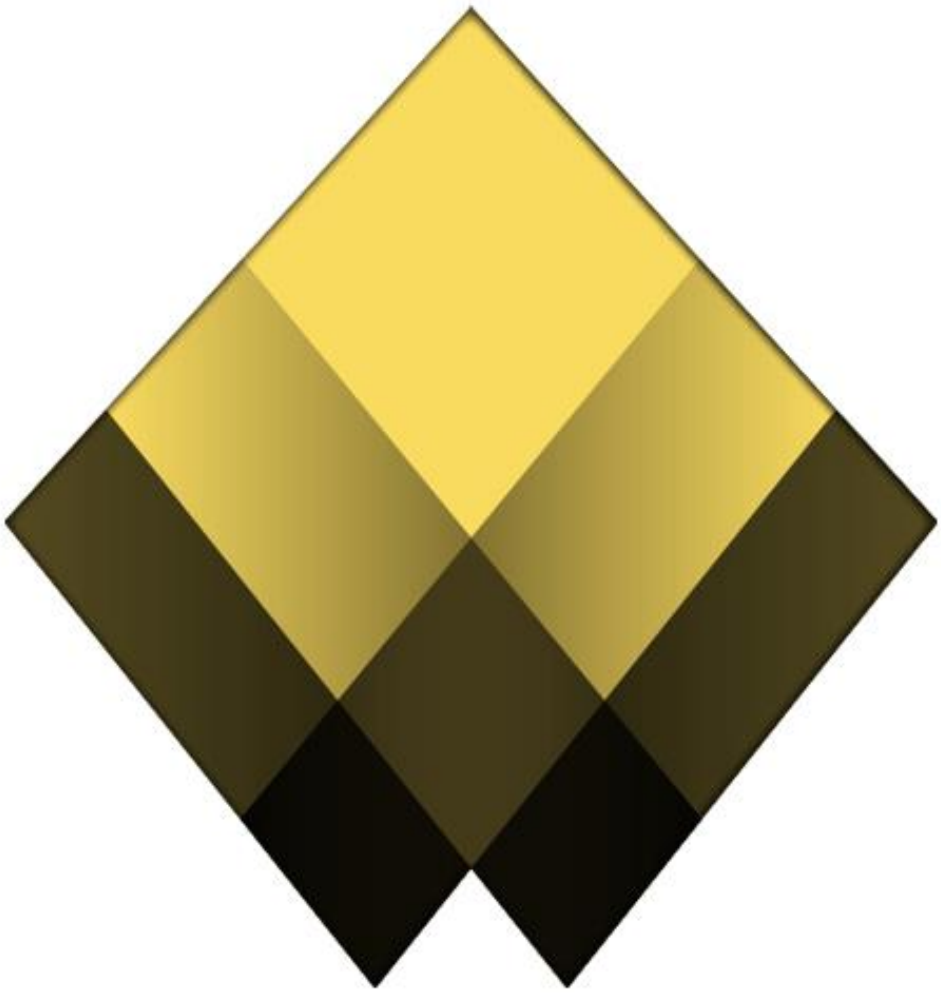


PROFESSIONAL
ACRYLIC
WiFi

Quick Help

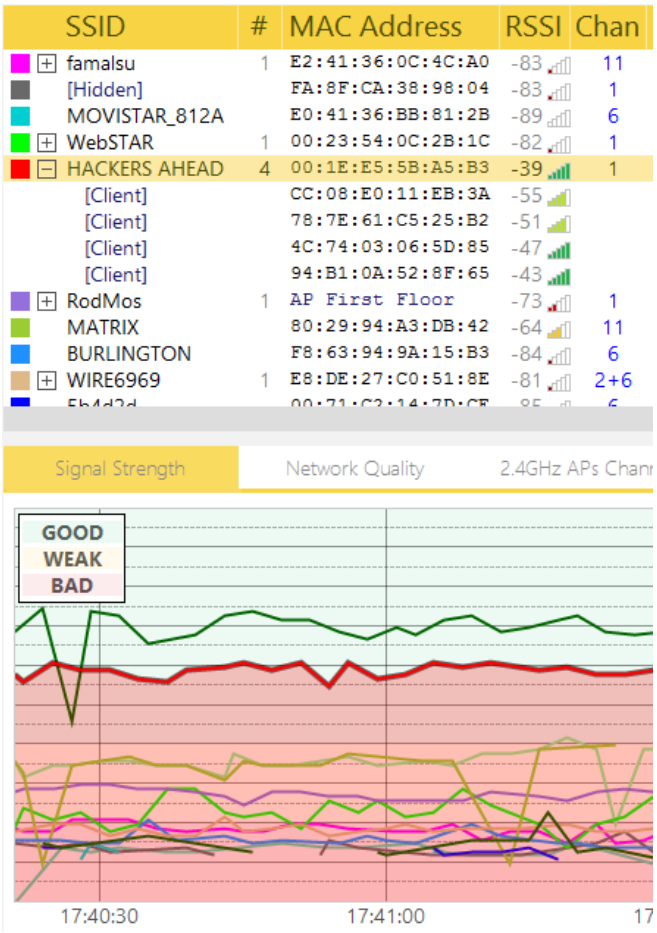
25/04/2016

support@acrylicwifi.com
www.acrylicwifi.com

Content

Access Points

This section displays a general overview of all detected Wi-Fi access points.



Each row represents an access point, and each column includes information such as signal strength, SNR, MAC address, security options, etc.

By using the Monitor Mode (NDIS) or an AirPcap card, you can also visualize all connected client devices to each access point. In case an access point has client devices connected to it, these are listed in the row below that access point. The tree expands when clicking on the '+' sign icon, displaying all the client devices connected to the selected access point.

This window offers helpful information on Wi-Fi device status at a glance.

To hide the access points on the lower views, the colored checkboxes should be unchecked.

Column	Information Provided
SSID	This acronym stands for 'Service Set IDentifier'. In other words, the network's name. A network can hide its name, in which case this field reads the text [Hidden]. This text can be configured from the *Preferences* window that

Column	Information Provided
	appears after clicking on the *Configure* option in the main menu. However, even when a network is not publishing its name, in some cases, the network name can be obtained on Monitor Mode by inspecting and analyzing the Wi-Fi traffic of the devices that are connected to that network. Whenever possible, Acrylic will display this name in red, which means that this is a hidden network and the name has been inferred by the software.
#	This column displays the number of devices connected to that network. If empty, this means that no device has been detected as connected to the network. NOTE: Values are only shown on Monitor Mode (NDIS) or when using an AirPcap card. If the Wi-Fi device is operating on Normal Mode, this field is automatically hidden.
Mac Address	A Media Access Control Address is a unique identifier assigned to network interfaces and used as a network address. This field can display a name instead of the 6-bytes address when the MAC address is previously inventoried.
RSSI	A Received Signal Strength Indication is a dBm value that indicates the wireless signal strength received by the client, and it usually ranges from 0 to -100. The higher the value, the stronger the signal, being 0 the weakest and -100 the strongest.
SNR	The Signal-to-Noise Ratio measured in dB that is used to compare the signal received with the background noise. The higher the value, the better the communication quality. NOTE: These values are only shown if an AirPcap card is used. If the Wi-Fi device is operating on normal or monitor (NDIS) mode, this field is automatically hidden.
Chan	Network operating channel. If the network is operating over more than one channel, all operating channels are displayed here. On the 2.4GHz frequency, access points can operate over either one or two channels. On the 5GHz frequency, they can operate over up to four channels.
Width	Channel bandwidth measured in Mhz. Possible values are 20, 40, 80, and 160. On the 2.4GHz frequency, access points can have a bandwidth of 20 and 40MHz. On the 2.4GHz frequency, access points can have a bandwidth of 20 and 40MHz.
802.11	Access point communication standards. Possible values are a combination of 802.11(a,b,g,n,ac).
Max rate	Maximum transfer rate supported by a network access point measured in Mb/s.

Column	Information Provided
Retries	Percentage of packets that had to be retransmitted due to transmission errors. The total number of retransmitted packets are shown between brackets. It is a percentage, ranging from 0 to 100. Values over 10% are considered to have a negative impact on network performance. NOTE: Values are only shown on Monitor Mode (NDIS) or when using an AirPcap card. If the Wi-Fi device is operating on Normal Mode, this field is automatically hidden.
WEP	Access point WEP security type. If empty, this means that the network does not support WEP security. Possible values are 'SharedKey' and 'Open'.
WPA	Access point WPA security type. If empty, this means that WPA security is not supported by the network. Possible values are 'PSK' (PreShared Key) and 'MGT' (Managed, also known as Enterprise).
WPA2	Access point WPA2 security type. If empty, this means that WPA2 security is not supported by the network. Possible values are 'PSK' (PreShared Key) and 'MGT' (Managed, also known as Enterprise).
WPS	WPS version supported by the access point. If empty, this means that WPS is not supported by the network. WPS authentication is displayed in green if enabled, or otherwise in red.
Password	Some access points provided by ISPs include default passwords. The Scripting section contains scripts that identify those access points and reveal the default password. One or more passwords can be revealed, depending on the device model. In any case, it is possible to use a connectivity module to test a number of passwords on the access point. Please, bear in mind that only a default password can be revealed, so the user should change it for security purposes.
WPS PIN	Some access points provided by ISPs include Pin WPS by default. The Scripting section contains scripts that identify those access points and reveal the WSP PIN. One or more WSP PINs can be revealed, depending on the device model.
Vendor	The manufacturer brand name of the network interface being used by the device
Data	Number of *Data* packets sent by the wireless device. NOTE: Values are only shown on Monitor Mode (NDIS) or when using an AirPcap card. If the Wi-Fi device is operating on Normal Mode, this field is automatically hidden.
Mgt	Number of *Management* packets sent by the wireless device.
First	Time at which a device has been first detected.
Last	Time at which a device has been last detected.
Type	Network type implemented by the access point. Possible values are 'Infrastructure' and 'Adhoc'.

Column	Information Provided
Latitude	GPS latitude of the location where the device has been first detected. NOTE: A GPS device should be connected and a coordinates' capture initiated or otherwise this field will be automatically hidden.
Longitude	GPS longitude of the location where the device has been first detected. NOTE: A GPS device should be connected and a coordinate capture initiated or otherwise this field will be automatically hidden.

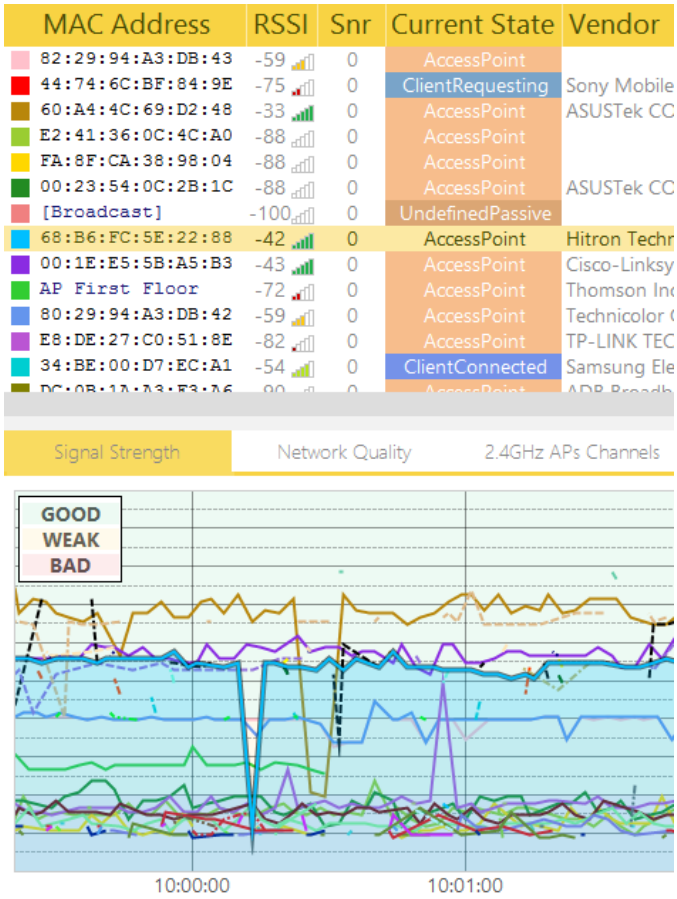
Additional Options

Right-clicking on the *Access Points* window will display the context menu that allows to perform actions on access points and client devices.

Stations

The Stations section displays all the Wi-Fi capable devices.

Generally, a Wi-Fi capable device is called a STATION or STA.



Wi-Fi devices send wireless network packets following the 802.11 protocol while operative. An access point broadcasts a certain wireless network, and devices such as mobile phones, tablets or laptop computers send network packets searching for available networks.

Each device has a unique 6-byte identification address called MAC. Acrylic Wi-Fi Professional gathers each device information and provides transmission metrics that are displayed in the following table:

Column	Information Provided
Mac Address	A Media Access Control Address is a unique identifier assigned to network interfaces and used as a network address. This field can display a name instead of the 6-bytes address when the MAC address is previously inventoried.

<table>
<tr><th>Column</th><th>Information Provided</th></tr>
<tr><td>RSSI</td><td>A Received Signal Strength Indication is a dBm value that indicates the wireless signal strength received by the client, and it usually ranges from 0 to -100.
The higher the value, the stronger the signal, being 0 the weakest and -100 the strongest.</td></tr>
<tr><td>SNR</td><td>Signal-to-Noise Ratio measured in dB that is used to compare the signal received with the background noise. The higher the value, the better the communication quality.
NOTE: These values are only shown if an AirPcap card is used. If the Wi-Fi device is operating in normal or monitor (NDIS) mode, this field is automatically hidden.</td></tr>
<tr><td>Current State</td><td>Acrylic Wi-Fi Professional device categorization according to device current operating mode.</td></tr>
<tr><td></td><td>
<table>
<tr><th>Status</th><th>Description</th></tr>
<tr><td>AccessPoint</td><td>The device operates as an access point.</td></tr>
<tr><td>ClientRequesting</td><td>The device is requesting network access. This is the normal status for smartphones, tablets, laptops, etc.</td></tr>
<tr><td>ClientConnected</td><td>This is a device connected to another Wi-Fi device.</td></tr>
<tr><td>UndefinedActive</td><td>The device is sending wireless network packets, but it still cannot be classified.</td></tr>
<tr><td>UndefinedPassive</td><td>The device is receiving wireless network packets, but it still cannot be classified.</td></tr>
<tr><td>WDS</td><td>The device is operating as a Wireless Distribution System (WDS).</td></tr>
<tr><td>Unknown</td><td>The device cannot be identified.</td></tr>
</table>
</td></tr>
<tr><td>Vendor</td><td>The manufacturer brand name of the network interface being used.</td></tr>
<tr><td>Wps Info</td><td>This indicates whether the device supports WPS and the amount of information it provides.</td></tr>
<tr><td>Retries</td><td>Percentage of packets that had to be retransmitted due to transmission errors. The total number of retransmitted packets is shown between brackets.
It is a percentage, ranging from 0 to 100. Values over 10% are considered to have a negative impact on network performance.
NOTE: These values are only shown on Monitor Mode (NDIS) or when using an AirPcap card. If the Wi-Fi device is operating on normal mode, this field is automatically hidden.</td></tr>
<tr><td>Attempts</td><td>Number of attempts from a wireless device trying to connect to another device.
NOTE: These values are only shown on Monitor Mode (NDIS) or when using an AirPcap card.</td></tr>
<tr><td># Sent</td><td>Number of network packets sent by a wireless device.</td></tr>
<tr><td># Received</td><td>Number of network packets received by a wireless device.</td></tr>
</table>

Column	Information Provided
# BSSID	Number of packets a wireless device acts as an intermediary of.
First	Time at which a device has been first detected.
Last	Time at which a device has been last detected.
Data	Number of *Data* packets sent by a wireless device. **NOTE:** These values are only shown on Monitor Mode (NDIS) or when using an AirPcap card. If the Wi-Fi device is operating on normal mode, this field is automatically hidden.
Mgt	Number of *Management* packets sent by a wireless device.

Additional Options

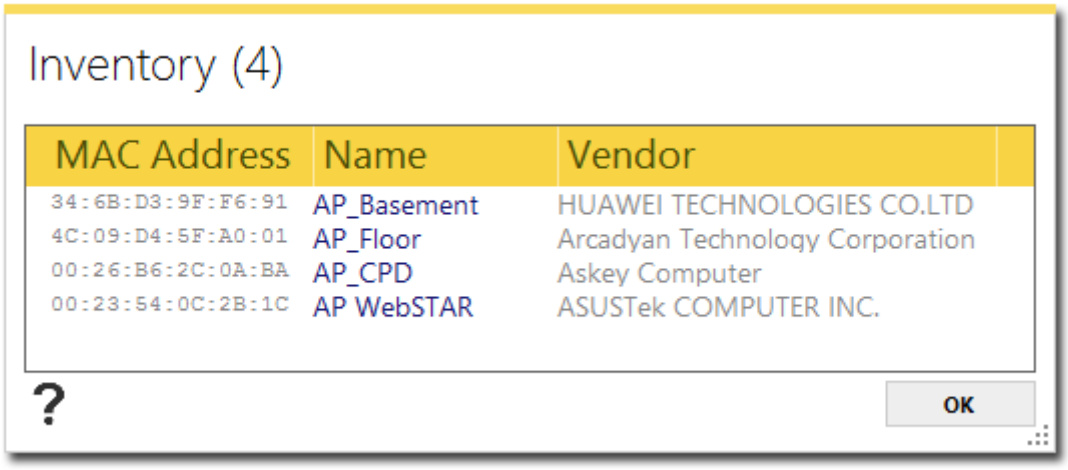
It is possible to interact with the devices shown in this section by using the right-click context menu.

From this context menu, you can interact with all the listed Stations and perform tasks such as generating reports in HTML, TXT or CSV format, tweet device information, or copy to clipboard.

Inventory

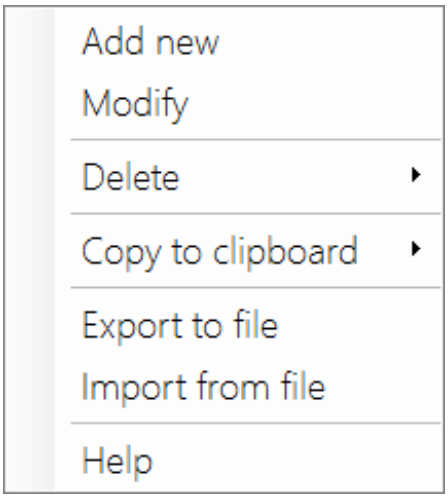
In this section all devices which had been inventoried are listed.

When a device is inventoried, a friendly name is assigned to his MAC Address, so each time you use Acrylic Wi-Fi, this device appears identified with the assigned name instead of the MAC Address.



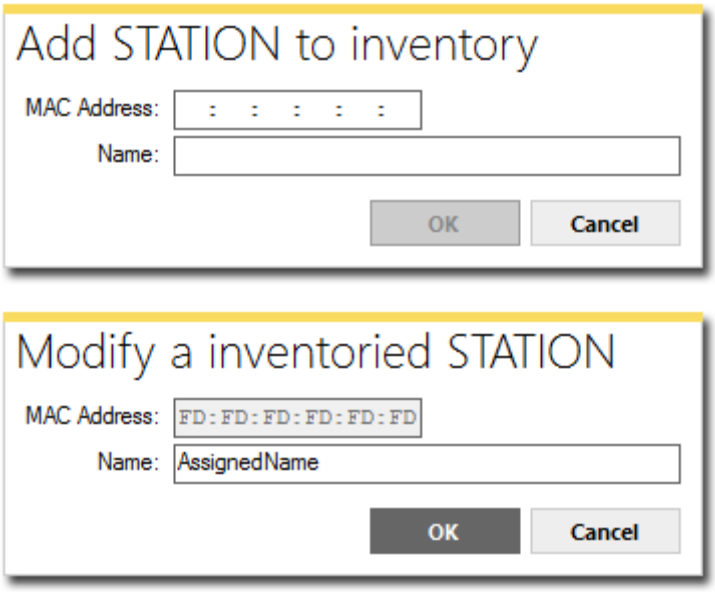
Column	What information gives?
Mac Address	Unique identifier assigned to network interfaces used as a network address (Media Access Control Address)
Name	Friendly name given to this device. This name will be displayed in Acrylic Wi-Fi instead of the MAC Address.
Vendor	Name of the manufacturer of the device. Non editable, is obtained automatically based on the MAC Address

Additional options



Contextual menu only available when pressing the right button on the inventory window

Menu item	Function
Add new	Adds a new entry in the inventory
Modify	Allows to modify the information of an inventoried element
Delete	Removes an inventoried element
Copy to clipboard	Allows to copy inventoried elements information on the clipboard
Export to file	Allows to export inventory content to .csv file
Import from file	Allows to import inventory content from .csv file



The window to add or modify inventory items allows entering device data. In case of modifying, these fields will be filled with the current information to be edited.

Packet viewer

Filters can be applied to receive packets for specific analysis, focusing on certain packets and disregarding others.

These filters can be added from the filter text box, directly if the filter type to be applied is known, or from the packet tree by right-clicking on the tree view to use the selected item as a filter.

As text is entered in the filter text box, the filter is checked for validity. If the filter is valid, the text box background will be displayed in green, or otherwise in red.

Filter examples

Filter	Result
`ieee80211.management.beacon.exists`	Shows all packets containing a 'beacon' field
`ieee80211.management.sa == 00:20:1F:1A:03:F1`	Shows all the packets with the specified origin address
`ieee80211.management.sequencecontrol > 0x3400`	Shows all the packets with a control sequence bigger than 0x3400

Syntax

The packet specifications and fields in the 802.11 protocol have been encapsulated in a tree structure. You can access each one of these items through the field names separated by dots ('.'). The protocol structure is shown by selecting a packet node from the *Packet tree view*.

There are two root nodes to access the packet information:

Root node	Description
`ieee80211`	This is the default root node. All 802.11 protocol wireless network packets start with this node, which allows you to access the whole protocol through its fields. This can be verified by clicking on a packet to see the *Packet tree view* representation. These are some examples of fields that have been accessed through the root node: • `ieee80211.management` • `ieee80211.control` • `ieee80211.data`

Root node	Description
`RadioTapHeader`	This root node allows access to additional data that has been processed by the network card driver for each packet. This data is not part of the transmitted packet, but it provides extra information about it, such as receiving channel, signal strength, etc. Here's an example: `RadioTap.AntennaSignal > -50` <--- Packets that have been received at a signal strength of -50dBm or stronger
`ies`	This is a special node that allows direct access to the *information elements* of each packet when available. This way, it is possible to set up a filter on an *information element* for any type of packet. It would be otherwise required to set up all the possible routes to the *IEs* for each type of packet. Example: `ies.ssid.ssid` <--- Affects beacons and probes.

Valid Operators

Operator	Description
==	Equals Operator. It can be used with numeric and text fields.
!=	Inequality Operator. It can be used with numeric and text fields.
<	Less than.
>	Great than.
<=	Less than or equal.
>=	Great than or equal.
%	Modulo
+	Plus
-	Minus
*	Multiplication
/	Division
and	Logical **AND**. Example: (ies.ssid.ssid == 'HACKERS_AHEAD') **and** (ieee80211.management.sequencecontrol > 0x3400)
or	Logical **OR**. Example: (ies.ssid.ssid == 'HACKERS_AHEAD') **or** (ieee80211.management.sequencecontrol > 0x3400)

Types

Type	Description
Number	Numeric values can be expressed as decimal or hexadecimal (beginning with 0x). Examples:

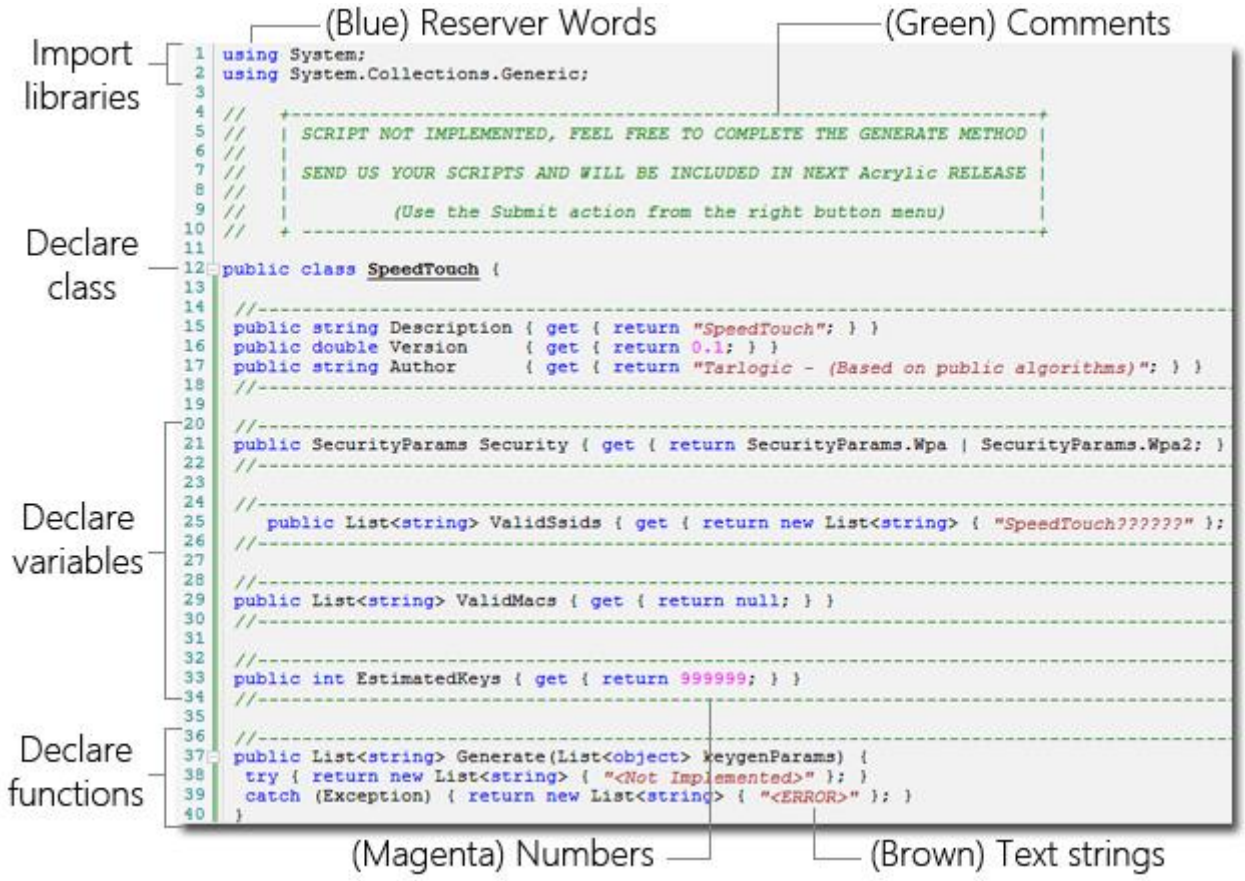
Type	Description
	• Decimal: `ieee80211.management.sequencecontrol > 13312` • Hexadecimal: `ieee80211.management.sequencecontrol > 0x3400`
Text	Text can be expressed between simple quotation marks ('). Example: • `ies.ssid.ssid == '#FBI Surveillance Van #1'`
Bytes	Byte sequences can be expressed by concatenating hexadecimal bytes with colons (:). Examples: • `ieee80211.management.sa == 60:A4:4C:69:D2:48` • `ieee80211.management.beacon.fixed == 85:71:83:07:00:00:00:00:64:00`

Scripts

Script Editor

From this section, you can create and modify existing scripts, and also test them against certain SSIDs/MACs to validate their passwords.

The scripts are programmed in C# language.



The script editor uses syntax highlighting to help the developer.

Scripts can be developed on other IDEs, such as Visual Studio, and they can be added to Acrylic Wi-Fi Professional.

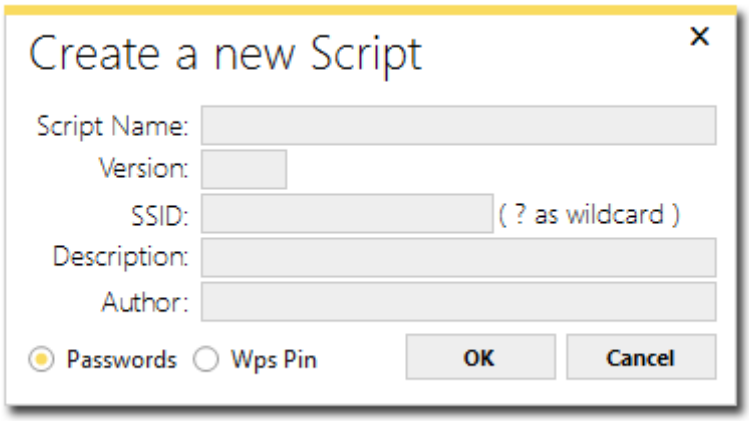
Acrylic also has a script template. You can open the template by selecting *New script* on the right side of the editor.

Acrylic Wi-Fi Professional scripts should always have a main class with the same name as the file. This class should have the following properties:

```
// Script description
public string Description { get { return "DESCRIPTION"; } }
// Script Version.
public double Version { get { return VERSION; } }
// Script Author
public string Author { get { return "AUTHOR"; } }
// Valid SSID's
public List&lt;string&gt; ValidSsids { get { return new List&lt;string&gt; {
"SSIDS" }; } }
// Valid MAC's
public List&lt;string&gt; ValidMacs { get { return null; } }
// Estimated keys
public int EstimatedKeys { get { return 1; } }
// SSID Security type
public SecurityParams Security { get { return SecurityParams.Wpa |
SecurityParams.Wpa2; } }
```

The main class should also have a *Generate* function that is called whenever a password is required.

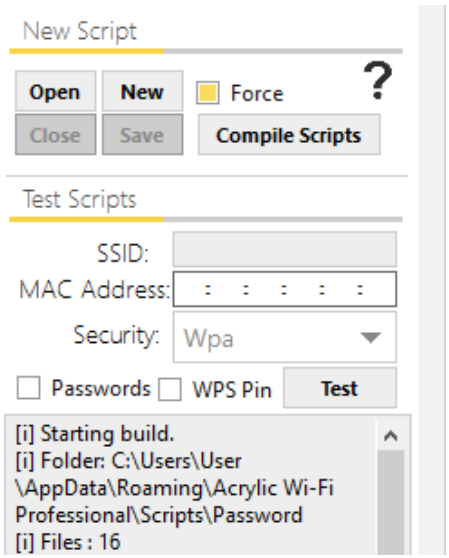
```
public List string Generate(List&lt;object&gt; keygenParams);
```



To make scripting easier, when you create a new script, a window requesting the main details is displayed to help generate a script template, which will be ready to inject code into the Generate function.

You will also be able to access the script editor's context menu by right clicking on the editor.

Editor options



In the script testing section, you can specify the script test parameters to validate they are working correctly. Access point, SSID, MAC and security type fields should be completed in order to run the test. You need to specify whether you are testing passwords or WPS PINs. Finally, you need to click on the Test button to star a new test.

Script list

All available scrips are listed under this section.

The scrips use public algorithms to generate passwords used on commercial Wi-Fi routers.

These scripts are grouped into two different categories; the first one, on top, to generate WPA1/WPA2 security protocol passwords, and the second one, at the bottom, to generate WPS security standard PIN codes.

WPA1/WPA2 Password scripts

Supported SSID	Supported MACs	Supported Security	Posibilities	Version	Descrip
dfs		Wpa - Wpa2	1	34	sdfs
discus--??????		Wpa - Wpa2	1	0.1	Discus
Dlink		Wpa - Wpa2	1	0.1	Dlink
INFINITUM????		Wpa - Wpa2	1	0.1	Infinitum
ONO????	00:01:38 - E0:91:53	Wep - Wpa - Wpa2	8000	0.1	ONOXXXX

Supported SSID	Supported MACs	Posibilities	Version	Description
belkin.???	00:22:75 - 00:1C:DF	1	0.1	Belkin - F9K1104(N900 DB Wireless N+
Belkin_N+_??????	00:22:75	1	0.1	Belkin - F5D8235-4 v 1000
C300BRS4A	00:22:F7	1	0.1	Conceptronic - c300brs4a
FTE-????	04:C0:6F - 20:2B:C1 - 28:	1	0.1	HUAWEI - HG532c

WPS PIN scripts

Column Name	What information gives?
Supported SSID	SSIDs meeting the script's specified criteria.'?' is used as a wild-card character.
Supported MACs	MAC Address meeting the script's specified criteria.
Supported Security	Only required for WPA1 and WPA2 network security protocols. It specifies the security type supported by the script.
Possibilities	Number of passwords generated by the script. In the best case scenario, its value would be 1, but there could be several possibilities.
Version	Script Version (Informative)
Description	Script Description (Informative)
Author	Script Author (Informative)
Filename	Script Filename (Informative)

You can also interact with the listed scripts through the context menu that can be accessed by right clicking on each script.