

SMAC 2.0

MAC Address Changer User Guide

Version 2.1

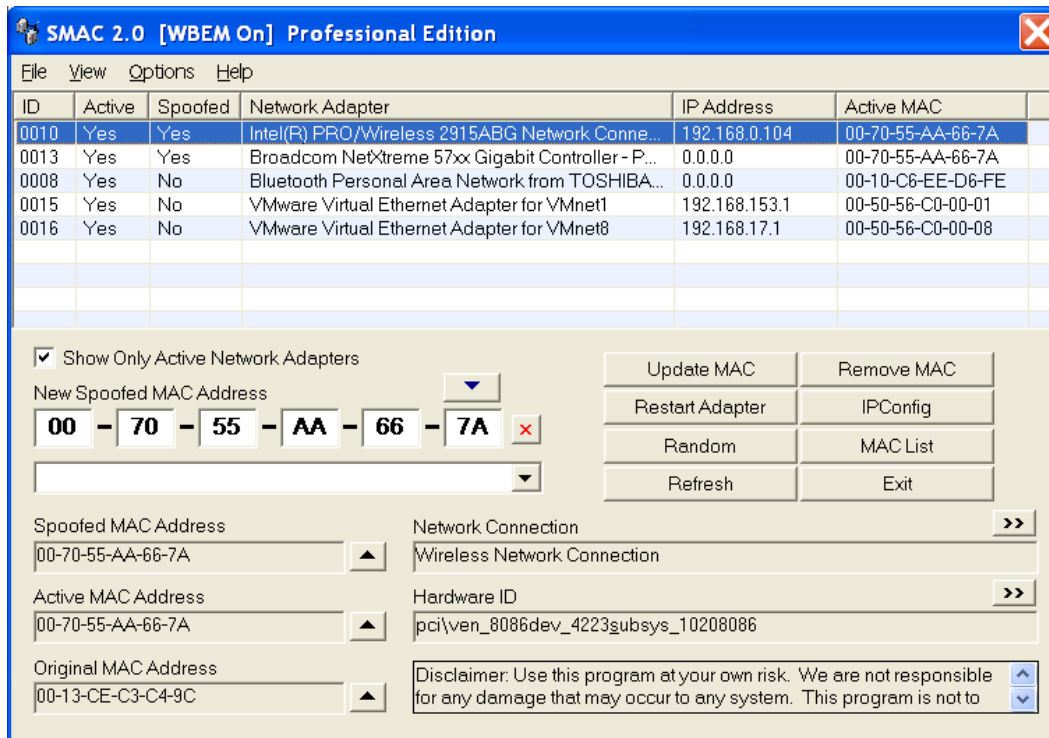
By

KLC Consulting, Inc.

<http://www.klcconsulting.net>
info@klcconsulting.net

Introduction:	3
Features	4
Quick Start Steps	5
Purchase SMAC Software.....	6
System and User Requirements	6
Install SMAC Software	6
Evaluate / Register SMAC Software	6
Updates for SMAC Software	7
Use SMAC Software	8
Data Grid Display.....	8
Show Only Active Network Adapters	9
New Spoofed MAC Address	9
Spoofed MAC Address	10
Active MAC Address.....	10
Most Recently Used (MRU) MAC Addresses	11
Network Connection / Network Adapter.....	11
Hardware ID / Configuration ID.....	12
Update (Change) MAC Address	12
Remove MAC Address	13
Generate a Random MAC Address	14
Restart Adapter	14
Refresh Information Display	15
IPConfig Information	15
Exit Software	16
MAC Address List.....	16
Dropdown Menus	18
Troubleshooting	21
About KLC Consulting, Inc.	22

Introduction:



SMAC is a powerful, yet easy-to-use and intuitive Windows MAC Address Changer (MAC Address spoofer) which allows users to change MAC address for almost any Network Interface Card (NIC) on the Windows 2000, XP, and 2003 Server systems, regardless of whether the manufacturers allow this option or not.

SMAC does not change the hardware burned-in MAC address. SMAC changes the "software based" MAC address on the Windows 2000, XP, and 2003 systems, and the new MAC address will sustain from reboots.

SMAC is the first New Windows MAC Address Spoofer (since 2002). It was developed base on the extensive research of [KLC Consulting, Inc.](#) SMAC is continuously updated with the latest trends in the networking and security, as well as valuable customers' wishes and feedback.

SMAC is created and maintained by Certified Information Systems Security Professionals (**CISSP**), Certified Information Systems Auditors (**CISA**), Microsoft Certified Systems Engineers (**MCSE**), and professional software engineers. With combined efforts, SMAC is a well designed user-friendly tool for both technical and non-technical users. SMAC is used by many Fortune 500 companies and

government agencies. In addition, SMAC has is featured [in news, books, training materials, and several major tool libraries.](#)

[KLC Consulting, Inc.](#) is a proud leader in Windows MAC Address Spoofing Research. We have satisfied users all over the world, and have received tremendous feedback from IT, network, Information Security professionals, and gamers. Yet, we do not just stop here. *We thrive to improve our products and bring the next generation of technology to our customers.*

SMAC is a **MUST-HAVE TOOL** for IT, Security, Networking professionals, online gamers, and everyone who needs a MAC Addresses Changer.

Features

- Easy, user friendly GUI for viewing and changing MAC addresses.
- Change MAC Address with a few simple clicks.
- Displays the following information about a Network Interface Card (NIC)
 - Device ID
 - Active Status
 - NIC description
 - NIC Manufacturer
 - Spoofed status (Yes/No)
 - IP Address
 - Active MAC addresses
 - Spoofed MAC Address
 - NIC Hardware ID
 - NIC Configuration ID
- Generate New Spoof MAC Addresses
- Option to display detailed information for all available adapters, or just active network adapters.
- Display IPConfig information which shows detailed Network and IP configuration.

- Load a MAC Address List and choose a New Spoofed MAC Address from the list. (Professional Edition only)
- Create comprehensive Network Adapter reports (Professional Edition only)
- Built-in logging capability tracks MAC address change activities. (Professional Edition has the option to disable)

Quick Start Steps

To spoof MAC Address on a Network Adapter:

1. Install SMAC software by running “SMAC20_Setup.exe”
2. Select a network adapter from the Network Adapter information grid appears on the top portion of the SMAC window.
3. Enter a “New Spoofed MAC Address” or click on “Random” button to generate one. (Not available in the Evaluation Edition).
4. Go to “Option” menu and select “Automatically Restart Adapter” and make sure the checkmark appears to the left of this menu item.
5. Click on “Update MAC” button.

*Note: The network connection will temporarily disconnect while activating the new Spoofed MAC Address. If you are using DHCP IP Address (Automatically obtaining an IP Address) you may get a new IP address after reconnecting with the new MAC Address.

6. You will see the new MAC Address updated in the Network Adapter Information grid.

To Remove the Spoofed MAC Address on a Network Adapter:

1. Select a network adapter with a spoofed MAC Address.
2. Click on the “Remove MAC” button to remove the spoofed MAC Address and return to the original MAC Address.

*Note: The network connection will temporarily disconnect while activating the original MAC Address. If you are using DHCP IP Address (Automatically obtaining an IP Address) you might get a new IP address after reconnecting with the original MAC Address.

Purchase SMAC Software

There are 2 ways to purchase SMAC Software:

1. Purchase SMAC software from the SMAC website:
<http://www.klcconsulting.net/smac/default.htm#download>
2. From the "Help" menu, choose "Registration", and then click on the "Buy" button to purchase SMAC 2.0.

System and User Requirements

- SMAC 2.0 works on Windows 2000, XP, and 2003 systems
- SMAC works with Network Interface Cards (NIC) that are on the [Microsoft Hardware Compatibility List \(HCL\)](#). Usually a "Designed for Windows 2000," "Designed for Windows XP," or "Designed for Windows 2003" logo is on the Network Interface Card (NIC) package. If your NIC is not on the HCL, please contact your NIC manufacturer to check for Microsoft platform compatibility.
- User must install and run SMAC with an user account that has the administrator right on the computer.
- SMAC is not to be used for any illegal or unethical purposes.

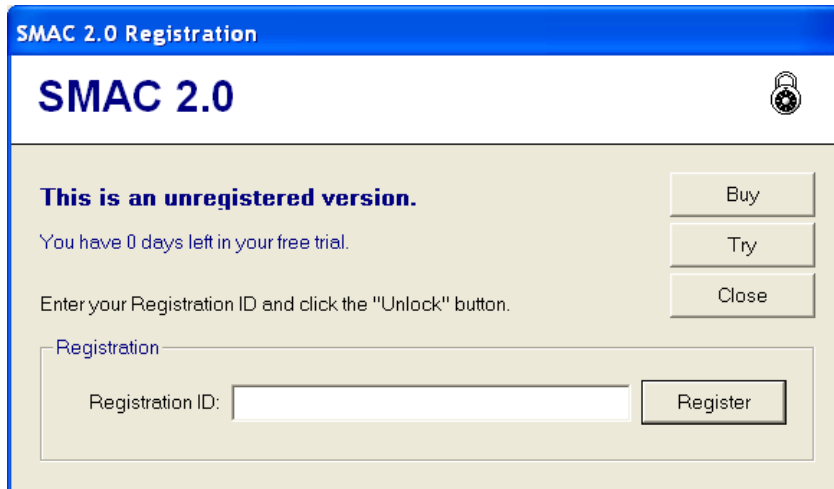
Install SMAC Software

Install SMAC 2.0:

1. If a previous version of SMAC was installed, uninstall the previous version by going to "Control Panel -> Add/Remove Programs."
2. Install SMAC 2.0 by running "SMAC20_Setup.exe"

Evaluate / Register SMAC Software

When you start SMAC 2.0 software the first time, you will see the SMAC 2.0 Registration Window.



Evaluate SMAC Software

If you are evaluating SMAC Software, click on the “Try” button and you will get a 14 day trial period.

Evaluation Edition allows you to change one MAC Address (0C-0C-0C-0C-0C-01) to test if you can change (spoof) the MAC Address on your computer. The following functions are enabled for Evaluation Edition:

- Update MAC (Change MAC Address)
- Remove MAC (Remove MAC Address)
- Restart Adapter
- IPConfig (to view IP configuration information via IPConfig)
- Refresh (To refresh display of Network Adapter, IP and MAC Address information)

Register SMAC Software

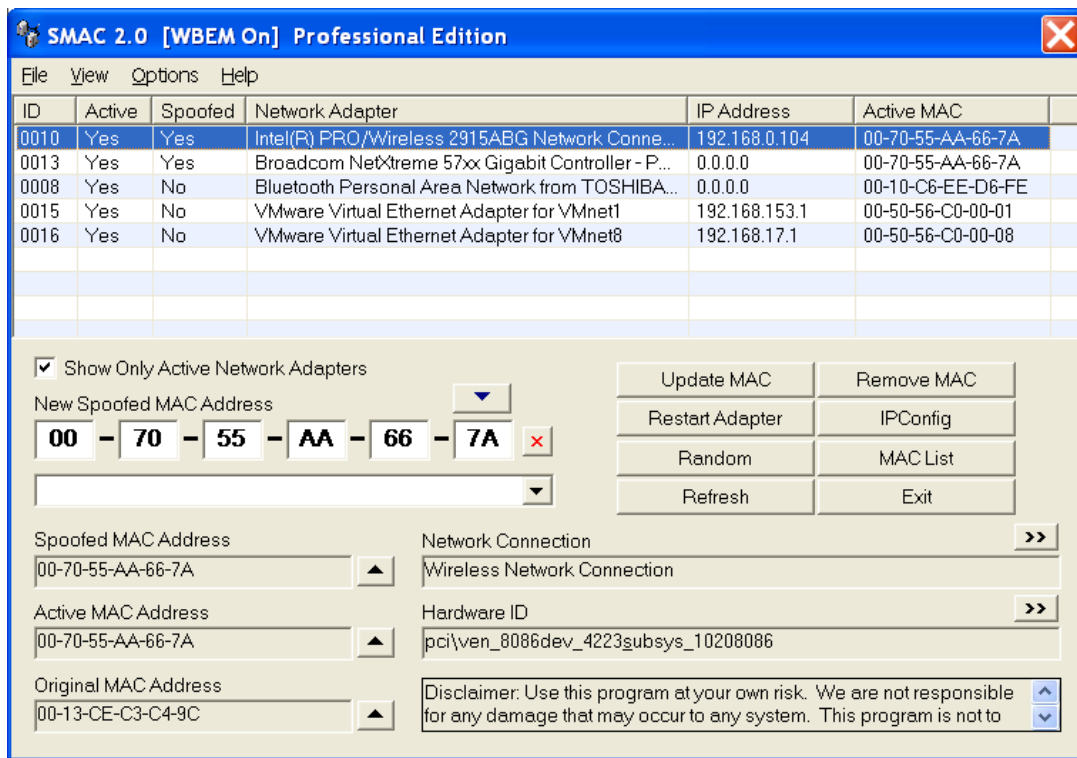
After you purchase SMAC 2.0, you should receive a serial number to register SMAC 2.0.

To register SMAC 2.0, enter the serial number into the registration ID field, then click “Register.”

Updates for SMAC Software

We regularly have new updates for SMAC. To check for updates, go to “Help” menu and click on “Check for Updates.” You can also go to the [SMAC website](http://www.klcconsulting.net/smac) for the update information: <http://www.klcconsulting.net/smac>

Use SMAC Software



Data Grid Display

Column	Description
ID	Network device ID
Active	Indicates whether a network adapter is active and available for use.
Spoofed	Indicates whether a Spoofed MAC Address is set for the Network Adapter.

Network Adapter	Displays the description of the Network Adapter
IP Address	Displays the assigned IP address
Active MAC	Displays the current MAC Address recognized by the Windows system

Show Only Active Network Adapters

Show Only Active Network Adapters


If you have this feature checked, you will see only the active network adapters.

If you have this feature unchecked, you will see both active and inactive network adapters. You can still see if a network adapter is active by its “Active” status in the data grid.

New Spoofed MAC Address





“New Spoofed MAC Address” contains the new MAC Address to be spoofed. You can enter the New Spoofed MAC Address

1. Manually
2. Click on the “Random” button to generate a random MAC Address.
3. Click on the  button to copy the “Spoofed MAC Address” or “Active MAC Address”.

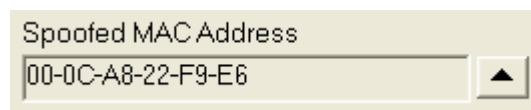
The dropdown box below the “New Spoofed MAC Address” displays the Network Adapter manufacturer associated with the MAC Address. If you assign a MAC

Address that is not associated with any Network Adapter manufacturer, this box is blank.

The button  will clear the “New Spoofed MAC Address.”

The button  will show the last 10 “Most Recently Used” (MRU) MAC Addresses. Please see “Most Recently Used (MRU) Mac Addresses” section for more details.

Spoofed MAC Address

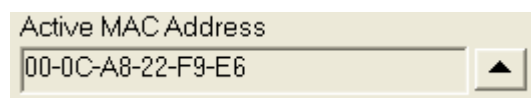


A screenshot of a software interface showing a text input field labeled "Spoofed MAC Address". The field contains the hexadecimal value "00-0C-A8-22-F9-E6". To the right of the text field is a small square button with a black upward-pointing triangle.

This field shows the Spoofed MAC Address stored on the computer. If the Spoofed MAC Address does not match the Active MAC Address, you need to click on “Restart Adapter” button or reboot your system to activate the Spoofed MAC Address.


Click on the  button to copy the Spoofed MAC Address to “New Spoofed MAC Address.”

Active MAC Address

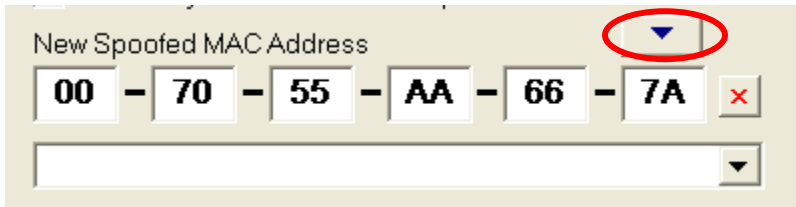


A screenshot of a software interface showing a text input field labeled "Active MAC Address". The field contains the hexadecimal value "00-0C-A8-22-F9-E6". To the right of the text field is a small square button with a black upward-pointing triangle.

Active MAC Address shows the current MAC Address recognized by your computer.

Click on the  button to copy the Active MAC Address to “New Spoofed MAC Address.”

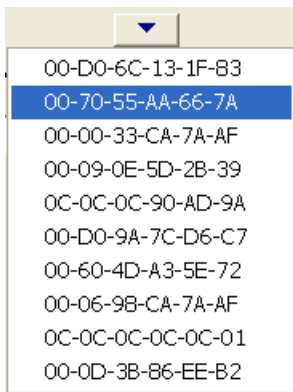
Most Recently Used (MRU) MAC Addresses



The MRU MAC Address button is circled in red in the above figure.

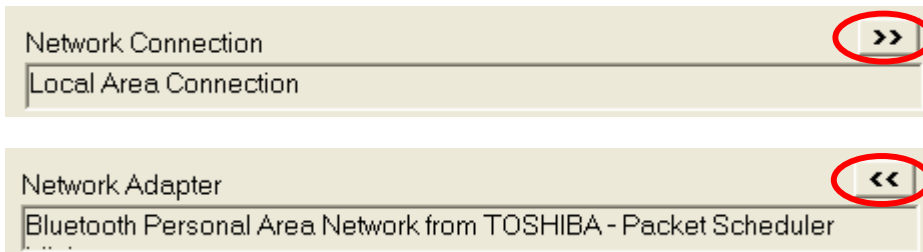
If you click on the MRU MAC Address button, it will show you the last 10 MAC Addresses used. You can select a MAC Address to spoof directly from the MRU MAC Address list.

Here is an example of the MRU MAC Address list.





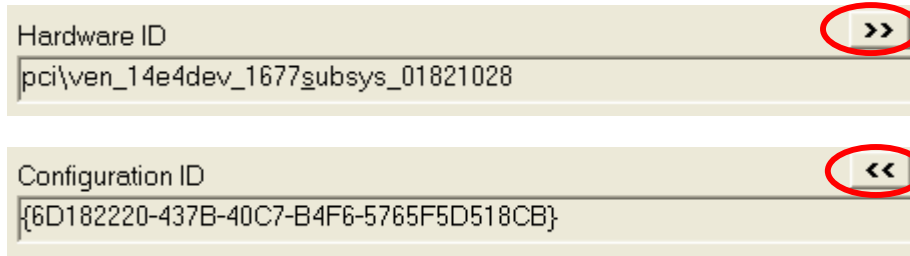
Network Connection / Network Adapter

The “Network Connection” displays the Network Connection name. When you click on **<<** or **>>** button, the display will change to show “Network Adapter” information. This button toggles between Network Connection and Network Adapter information.

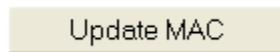


Hardware ID / Configuration ID

The “Hardware ID” displays the Network Adapter’s Hardware ID. When you click on  or  button, the display will change to show “Configuration ID” information. This button toggles between Hardware ID and Configuration ID.



Update (Change) MAC Address



The above button is for updating the new MAC Address to the network adapter.

To update the MAC Address, here are the steps:

1. First you must select a network adapter from the data grid which you want to change the MAC Address
2. Enter a “New Spoofed MAC Address”
3. Click on the “Update MAC” button to update the new MAC Address. Please note that “Update MAC” button stays disabled (grayed out) until a “New Spoofed MAC Address” is entered.
4. Once you click on the “Update MAC” button, if you have checked the option of “Automatically Restart Adapter,” the new spoofed MAC Address will update immediately. Otherwise, click on “Restart Adapter” when you are ready to activate the new spoofed MAC Address. See steps below to select these activation options.

You have 2 options when you activating the new MAC Address after you click the “Update MAC”:

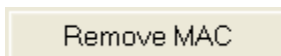
1. Activate the new MAC Address immediately after clicking the “Update MAC” button (this is the default setting.) -- Activation of new MAC Address will cause temporary disconnection of network adapter. The network disconnection is required to activate the new Spoofed MAC Address.
 - To choose this option, go to “Option” menu, check “Automatically Restart Adapter.” A checkmark appears on the left side when this option is selected as shown below.



2. Manually activate the new MAC Address -- This feature allows users to delay the activation of new Spoofed MAC Address. For example, some users may want to configure the new Spoofed MAC Address and other configurations, and then reboot the system so all changes can take effect at the same time.
 - To choose this option, go to “Option” menu, uncheck “Automatically Restart Adapter” as shown below.



Remove MAC Address



To Remove MAC Address, here are the steps:


1. Select a Network Adapter with a spoofed MAC Address. To determine if a Network Adapter is spoofed, check the “Spoofed” status on the data grid.
2. Click on the “Remove MAC” button to remove the existing spoofed MAC Address. If there is no spoofed MAC Address for the selected Network Adapter, the “Remove MAC” button is disabled (grayed out). Activation of new spoofed MAC Address will cause temporary disconnection of network adapter. The network disconnection is required to activate the original MAC Address.

Generate a Random MAC Address

Random

This feature generates a random MAC Address and inputs it into the “New Spoofed MAC Address” to simplify MAC Address spoofing.

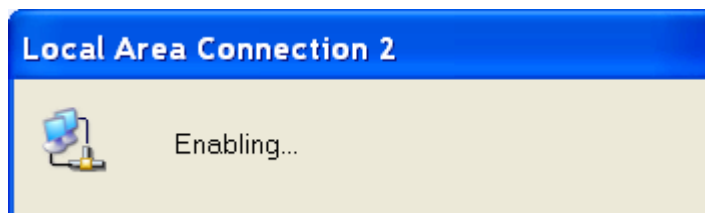
If all 6 octets of the “New Spoofed MAC Address” are not populated, clicking on the “Random” button will generate a completely random MAC Address.

You can also select a network adapter manufacturer from the dropdown list below the “New Spoofed MAC Address”, and SMAC will populate the first 3 octets of the address owned by the manufacturer. Then click the “Random” button to generate a random MAC Address for the selected manufacturer. You will only changes on the last 3 octets of the new Spoofed MAC Address. To create a completely new MAC Address, just click , then the “Random” button.

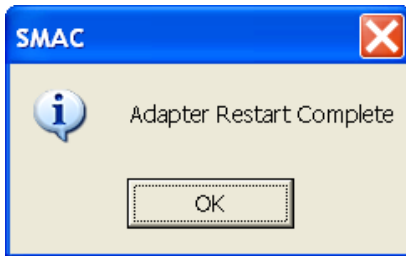
Restart Adapter

Restart Adapter

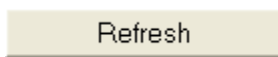
After clicking on the “Restart Adapter” button, the selected Network Adapter will be restarted. Please note that restarting a Network Adapter will cause temporary disconnection of network adapter. You will see a similar window when the network adapter is restarting:



When the network adapter completes the restart process, you will see the following window:



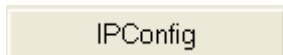
Refresh Information Display



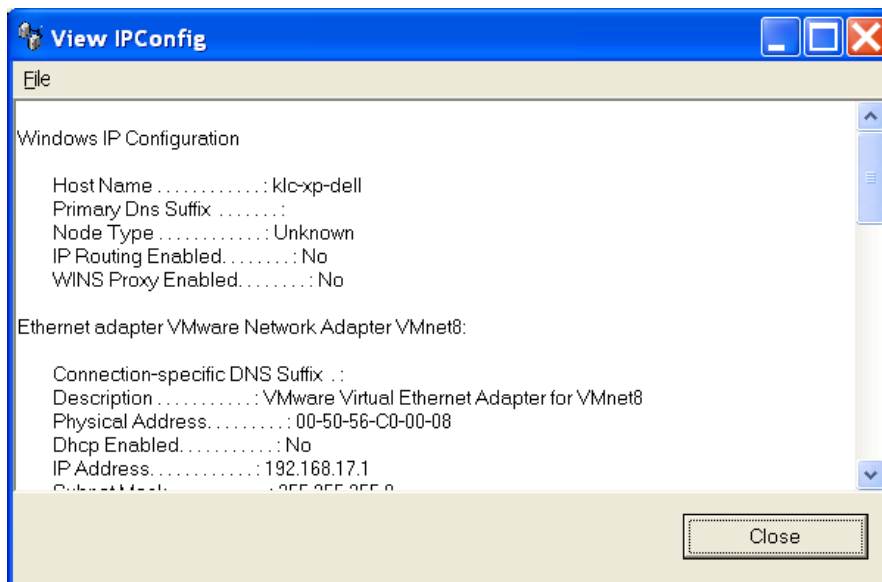
The "Refresh" button will refresh the information displayed on the SMAC Window.

IPConfig Information

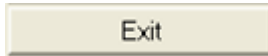
1. Click on the "IPConfig" Button to bring up the IPConfig information window.



2. The IPConfig information will show in the "View IPConfig" Window. You can use the File menu to save or print the IPConfig information.



Exit Software



Click the Exit button to exit SMAC.

MAC Address List

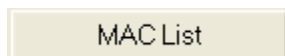
*Note: This feature is only available on the [SMAC 2.0 Professional Edition](#).

You can import the MAC Addresses List into SMAC so you can select the MAC addresses you want to spoof easily.

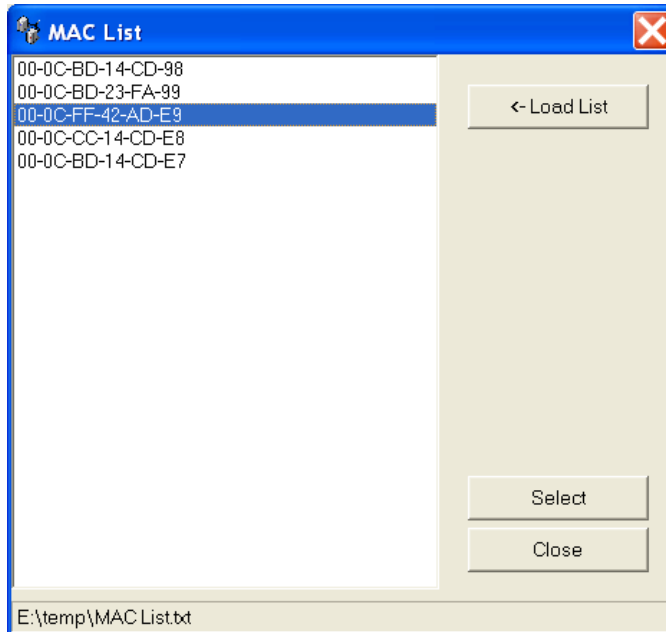
Click the MAC List button to import the MAC Addresses from your MAC Address List file into SMAC.

Steps:

1. Click on the “MAC List” button to go to the MAC List Window.



2. If there is no address in the MAC Address list, then click on the “Load List” to choose a MAC Address List file you have created.



3. Choose a MAC Address, then click the “Select” button or double-click on the desired MAC Address, and the MAC Address will be copied to “New Spoofed MAC Address” in the main SMAC screen.

How to Create a MAC Address List file:

Enter a 12 digits MAC Address followed by a line return for each MAC Address. Separating each 2 digit with “-“ is optional. Partial MAC Addresses can be used.

The sample MAC Address List file “Sample_MAC_Address_List.txt” is included in your installed SMAC program folder.

Sample format of MAC Address List file:

```
0010FEEB4738
00006EAABBCC
00-0C-BD-14-CD-98
00-0C-BD-23-FA-99
00-0C-FF-42-AD-E9
00-00-F8
00097B
```

Dropdown Menus

File Menu



The menu items under the File Menu have the same functionality as their respective buttons.

View Menu



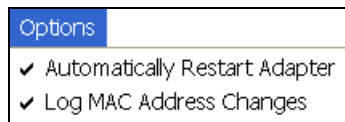
Network Adapter Report

Generate a Network Adapter Report with all network adapters displayed in the data grid in the HTML format.

MAC Address Log

Show the MAC Address change activity log.

Options Menu



Automatically Restart Adapter

Click on this menu item to check or uncheck this option. When this option is checked, a checkmark appear next to this menu item.

When “Automatically Restart Adapter” option is checked, SMAC will restart adapter automatically at the time you click the “Update MAC” button to update MAC Address or the “Remove MAC” button to remove MAC Address.

When “Automatically Restart Adapter” option is not checked, SMAC will NOT restart adapter automatically at the time you click the “Update MAC” or the “Remove MAC” button. You will need to click “Restart Adapter” button to manually restart the selected network adapter.

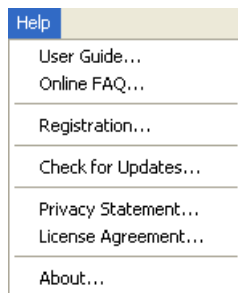
Log MAC Address Changes (only available for Professional Edition)

Click on this menu item to check or uncheck this option. When this option is checked, a checkmark will show next to this menu item.

When “Log MAC Address Changes” option is checked, SMAC will turn on the MAC Address change activity logging.

When “Log MAC Address Changes” option is not checked, SMAC will turn off the MAC Address change activity logging.

File Menu



User Guide

This option will bring up the User Guide.

Online FAQ

This option will bring up the Online Frequently Asked Questions (FAQ).

Registration

This option will bring up the Registration Screen.

- If you have already completed registering SMAC with a valid serial number, Registration Window will display the Registration ID (Serial number) registered.
- If you have not registered SMAC, the Registration Window will display the number of days left for evaluation, and give you an option to enter the Registration ID or to buy SMAC.

Check for Updates

This will go to the KLC Consulting (creator of SMAC) website to check for updates.

Privacy Statement

This will display the KLC Consulting Privacy Statements.

License Agreement

This will display the SMAC User License Agreement.

About

This will display the SMAC version, creator, and copyright information.

Troubleshooting

To avoid problems in your local area network:

- Make sure you assign one unique MAC Address per Network Adapter. DO NOT assign one MAC address to multiple Network Adapters within the local area network (LAN) because you may see some network problems.
- You must assign MAC address according to the [IANA Ethernet-number assignment database](#).
- Make sure you DO NOT assign Multicast MAC addresses unless intended. You can obtain the Multicast MAC addresses at this website: <http://www.iana.org/assignments/ethernet-numbers>.
- **"00-00-00-00-00-00" is NOT a valid MAC address.** If you assigned the new MAC Address to "00-00-00-00-00-00," your network adapter will reject this MAC address and use the original MAC Address.
- If "Restart Adapter" does not work with your computer, you are required to restart your computer to activate the new MAC Address.

About KLC Consulting, Inc.

[KLC Consulting](#)'s mission is to provide a continuous effort to protect the confidentiality, integrity and availability of your corporate resources and data. Through each stage of the information security lifecycle, we help you prevent, detect, react, and resolve your enterprise security issues. We present a full range of Professional Security Services.

[KLC](#) focuses on 4 areas of expertise:

- Information Security –
 - Security Architecture Assessment, Design and Implementation
- IT Audit –
 - COBIT, COSO, ISO 17799/27000, Risk-Based Audit Framework (RBAF)
- Regulatory Compliance –
 - HIPAA, GLBA, FFIEC, SOX, SB 1386
- Security Process Re-Engineering –
 - Process Documentation and Improvement via 6-Sigma approach.

KLC CONSULTING THRIVES TO IMPROVE INFORMATION SECURITY, ONE CLIENT AT A TIME.

Contact KLC Consulting:

KLC Consulting, Inc.
<http://www.klcconsulting.net>

Telephone: 617-314-9721
E-Mail: info@klcconsulting.net

Postal Mail:
KLC Consulting, Inc.
PO Box 395
Holden, MA 01520