nProtect Online Security

Setting a New Standard in Web Fraud Detection & Prevention

User Manual

Contact Us

3003 N. First Street, Suite #301 San Jose, CA 95134

Website: http://www.nProtect.com

TEL: 408-477-1742 / Toll Free: 855-466-7768 (1-855-GO-NPROT)

Table of Content

1. Overview

1.1. Product Description

nProtect Online Security (hereinafter **NOS**) is a total online security solution that secures online transactions on end-user's system with multi-layered protection such as **Malware Monitoring**, **Network Protection**, **Keystroke Protection**, **Anti-Phishing**, **Anti-Screen Capture**, and **DNS Monitoring**.

1.2. Product Strengths

Some of the key advantages of using NOS is:

- Multi-layered online security solution
- Top of the line kernel level technology
- Detects and repairs various financial malwares such as Zeus and SpyEye w/o cleaning utility
- Approximately 94% lighter file size compared to global anti-virus products and 50% lighter file size than competitor product.
- 24/7 proactive support from Response Center(ISARC)
- Coverage of malwares from all around the globe

1.3. System Specification

[Table 1-1] lists hardware and software specifications needed to operate NOS.

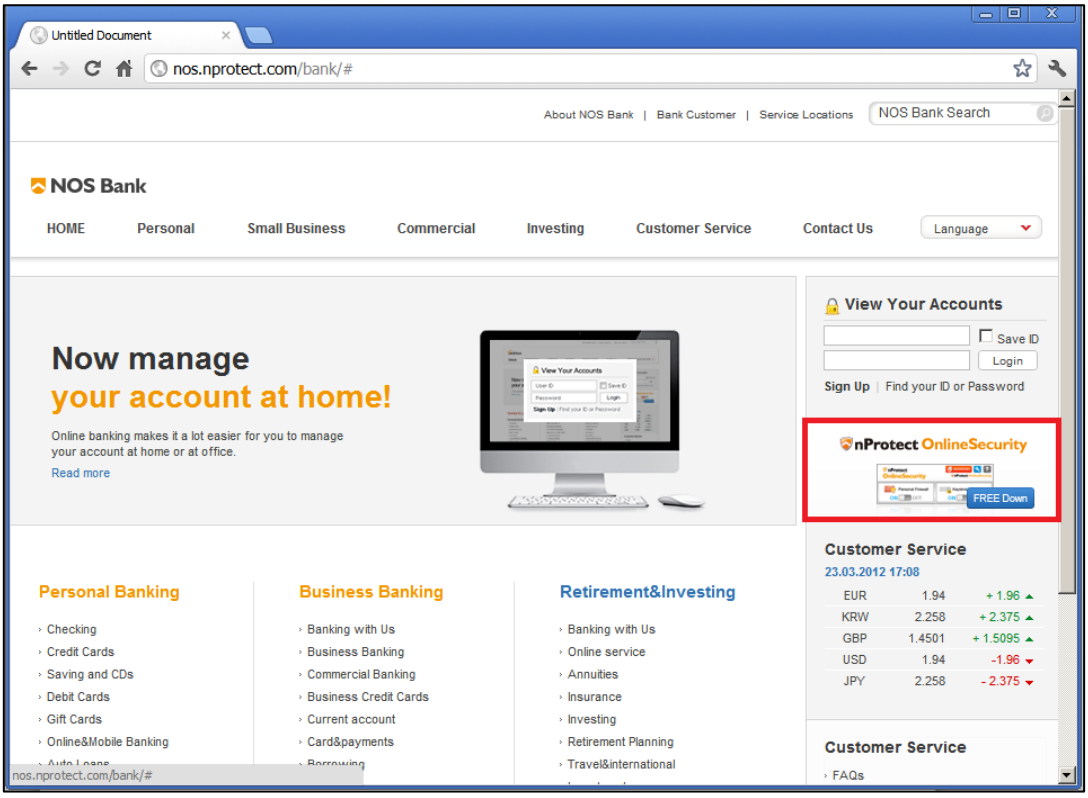
Item	Minimum requirements
Hardware	CPU: Intel Pentium IV 1.0Ghz or higher Memory: RAM 512MB or higher HDD: 150MB free space
OS	Windows XP(x32), VISTA(x32/x64), 7(x32/x64), 8(x32/x64)
Browser	Internet Explorer 8, 9 and 10(Win 8) Firefox 17 and later Chrome 23 and later

[Table 1-1] System Specifications

2. Installation and Uninstallation

2.1. Installation

Download NOS setup file from NOS customer website. Or click the banner on the NOS sample trusted Financial Institute website.



[Image 2-1] Sample Trusted Financial Institute Website

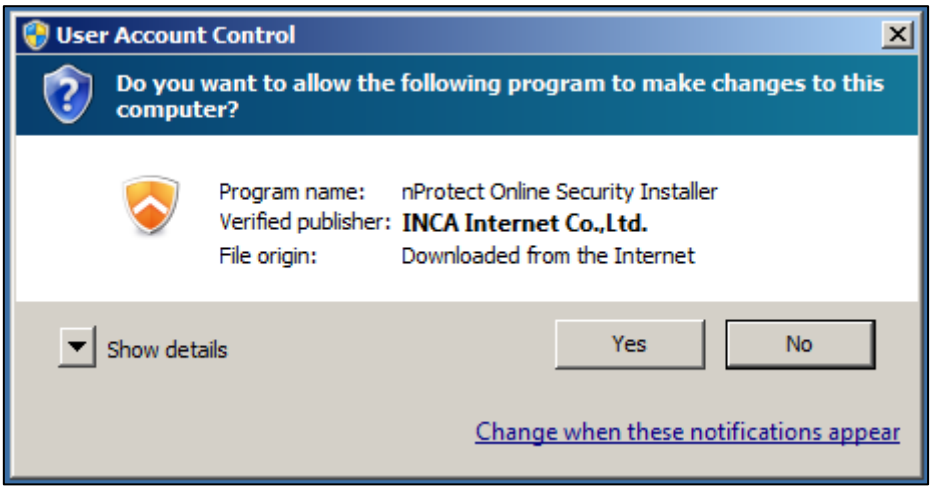
When prompted, click ‘Run’ to begin the NOS installation.

[Image 2-2] Setup File Download

By clicking ‘Save’ or ‘Save As’, nProtectOnlineSecurity.exe file will be saved on the local system.

[Image 2-3] Setup File Icon

Once executed, Windows User Account Control will ask to allow NOS to be installed on the local system. Click ‘Yes’ to begin NOS Setup.



[Image 2-4] Windows User Account Control

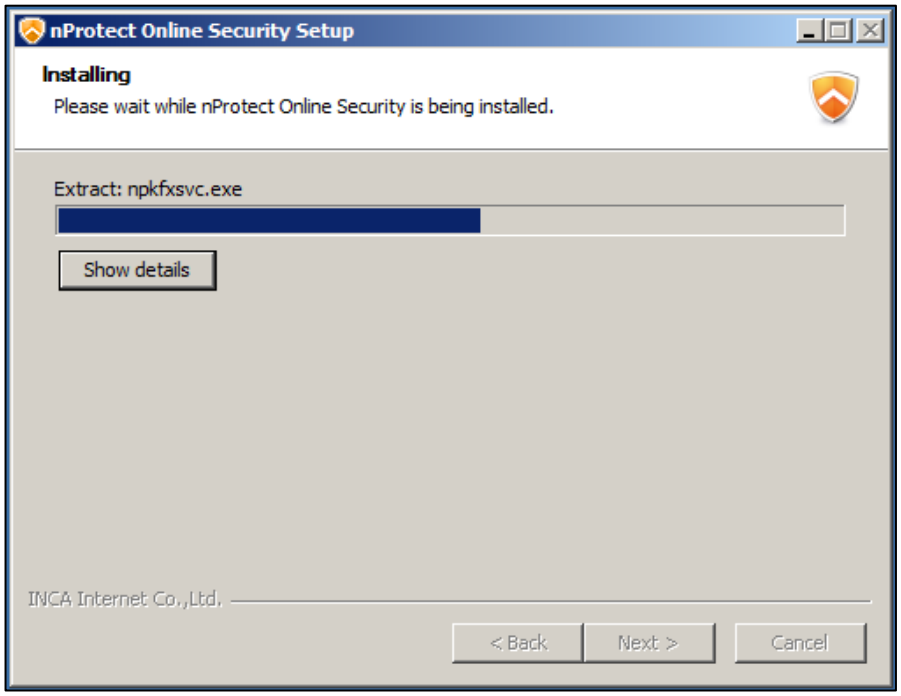
Click ‘Next’ to continue installation

[Image 2-5] nProtect Online Security Setup

Please read the End User License Agreement and click 'I Agree' to continue installation.

[Image 2-6] End User License Agreement

Installation will not take more than few seconds, depending on user's system specifications.



[Image 2-7] Installing nProtect Online Security

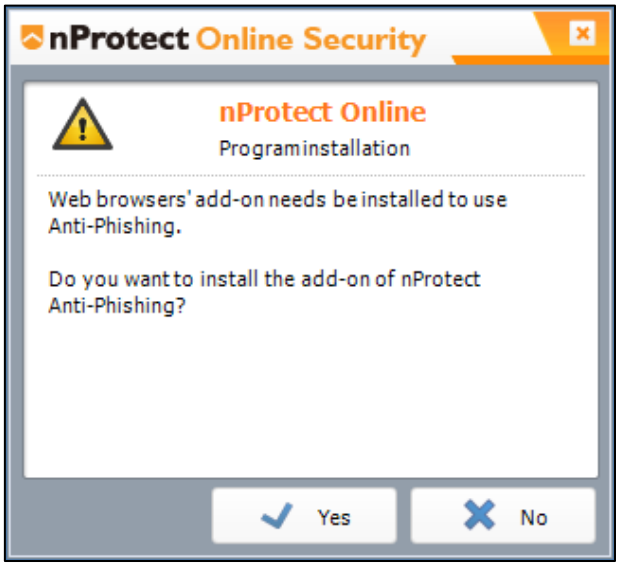
Click ‘Finish’ to complete the installation.

[Image 2-8] Completing nProtect Online Security Installation

When the installation is complete, NOS icon will appear on the system tray as shown below.

[Image 2-9] nProtect Online Security Tray Icon

Once installation is complete, pop-up window ask to install Anti-Phishing add-on. To enable Anti-Phishing function, please click ‘Yes’ and install browser add-on.



[Image 2-10] Browser Add-ons

Once installation is complete, visit a Trusted Website (ex. bank.nProtect.com) and NOS will launch automatically.

The system tray icon will turn green to indicate that NOS is ON and website is secured.**[Image 2-11]**

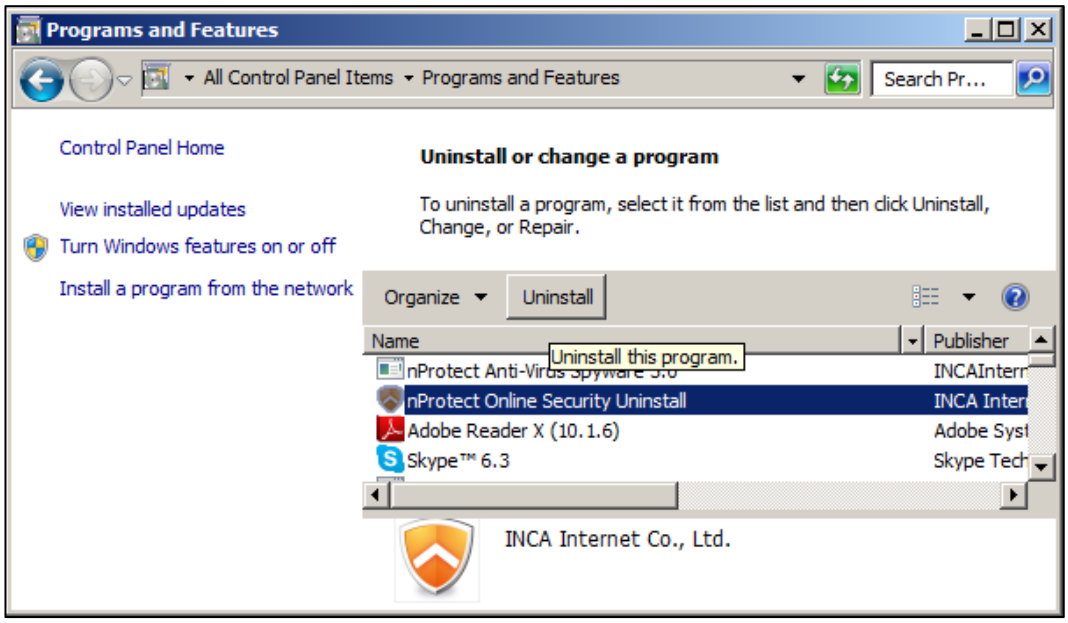
[Image 2-11] Protection Status

Double click on the system tray icon and NOS mini UI will be shown as below.[Image 2-12]

[Image 2-12] nProtect Online Security UI

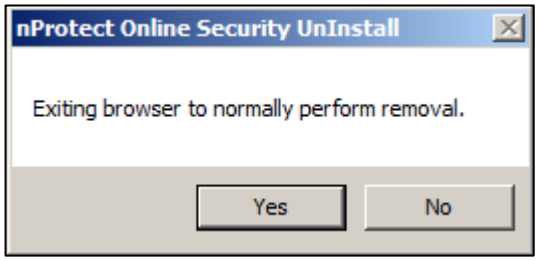
2.2. Uninstallation

Go to ‘Programs and Features’ on the Control Panel. (Start > Control Panel > Programs and Features)



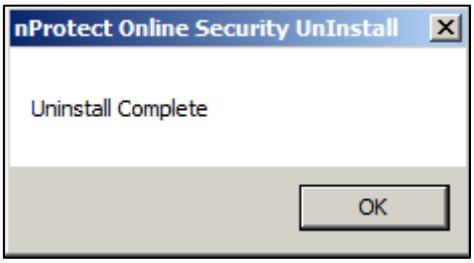
[Image 2-13] Uninstalling nProtect Agent

Select NOS and click ‘Uninstall’ button. If a browser is open, uninstall will ask to close all running browsers. (Internet Explorer, Firefox, Chrome, etc) Click ‘Yes’, to remove NOS from the program list.



[Image 2-14] Alert Message

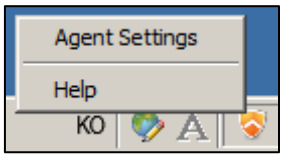
Once uninstallation is complete, ‘Uninstall Complete’ message will be shown as below.



[Image 2-15] Uninstall Complete

3. NOS Agent

Click the right-mouse button on the NOS tray icon and NOS Agent menu will be shown as below.



[Image 3-1] nProtect Online Security Agent Menu UI

The main functions are as follows.

Function	Description
Agent Settings	Move to menu window. User can turn on or turn off main functions of the nProtect Online Security such as Anti-Phishing, Hosts File Protection and Auto-start. User can also view all event logs of the Protect Agent.
Help	Moves to the Help page website.

[Table 3-1] nProtect Online Security Agent Menu Funtions

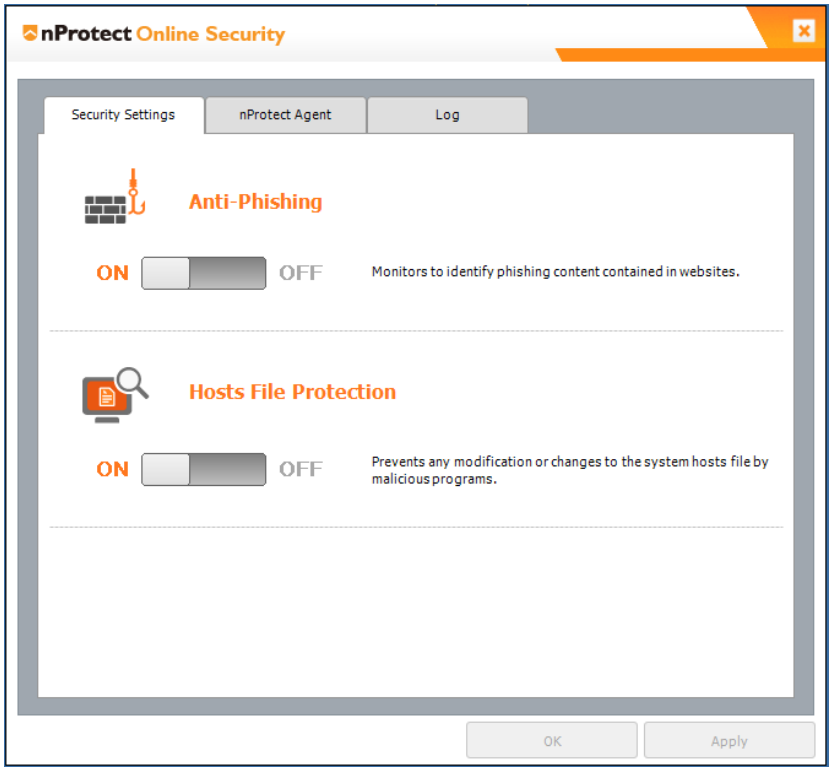
When ‘Agent Settings’ is selected, NOS agent UI will be displayed.**[Image 3-2]**

Function	Description
Security Settings	Anti-Phishing: Monitors the websites you visit and gives a warning upon detection of a phishing site. Hosts File Protection: Prevents any modification or change of Host files in your local system.
nProtect Agent	Auto-start Setting: Using the ON/OFF option, users can decide whether nProtect Online Security is starts automatically when you visit a trusted website.
Log	You can view all event logs of nProtect Agent.

[Table 3-2] nProtect Online Security Agent Funtions

3.1. Anti-Phising

Anti-Phishing function can be turned off by moving the slide to ‘OFF’ and clicking ‘OK’ or ‘Apply’.



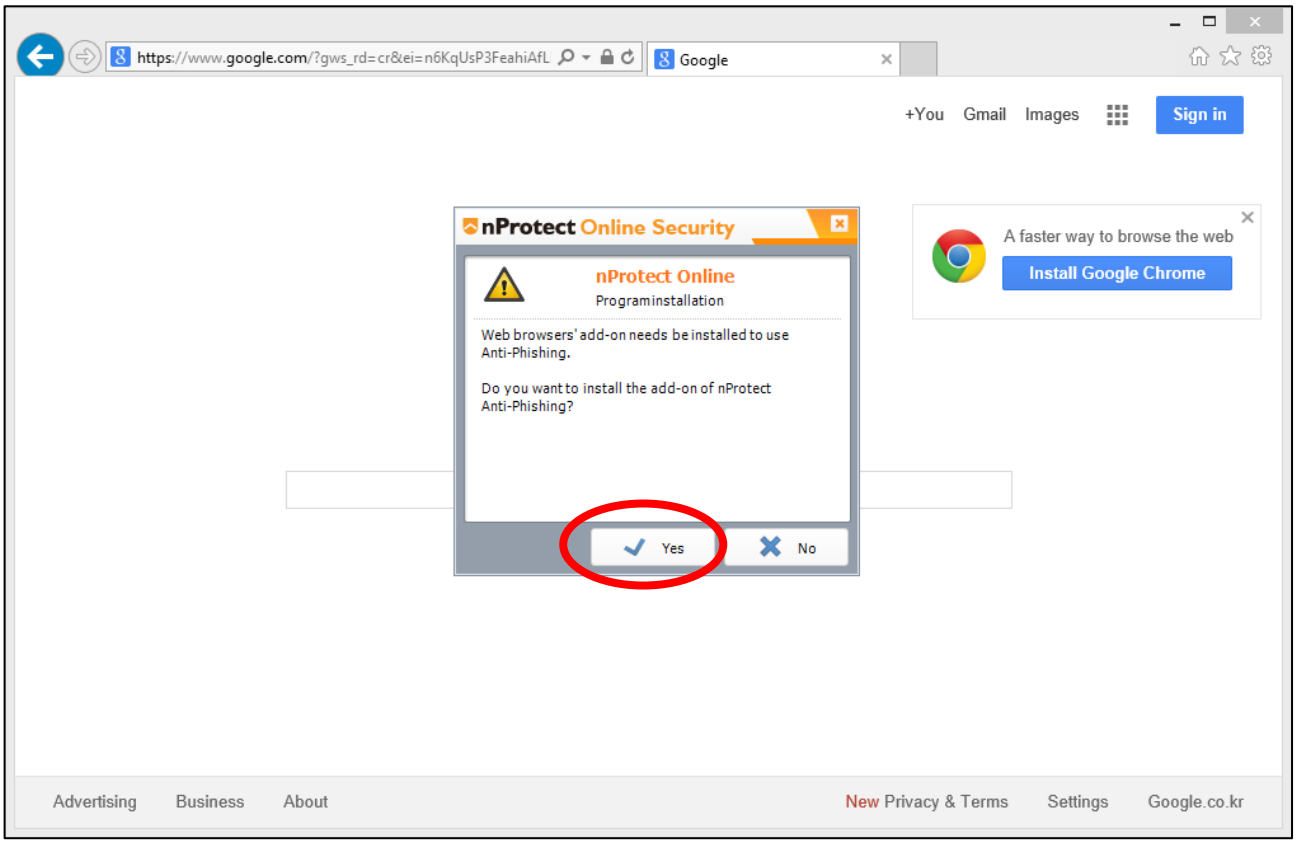
[Image 3-2] Security Setting

When a suspicious website is visited, Anti-Phishing will alert users with the folllowing warning message.

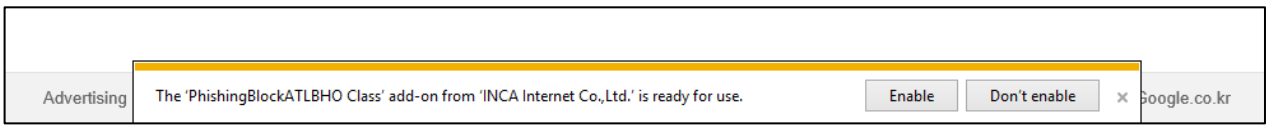
[Image 3-3] Anti-Phishing Warning

- **Internet Explorer**

After installing NOS, open Internet Explorer browser. An NOS pop-up window will show asking to install the Anti-Phishing add-on. Click “Yes” to install the add-on.



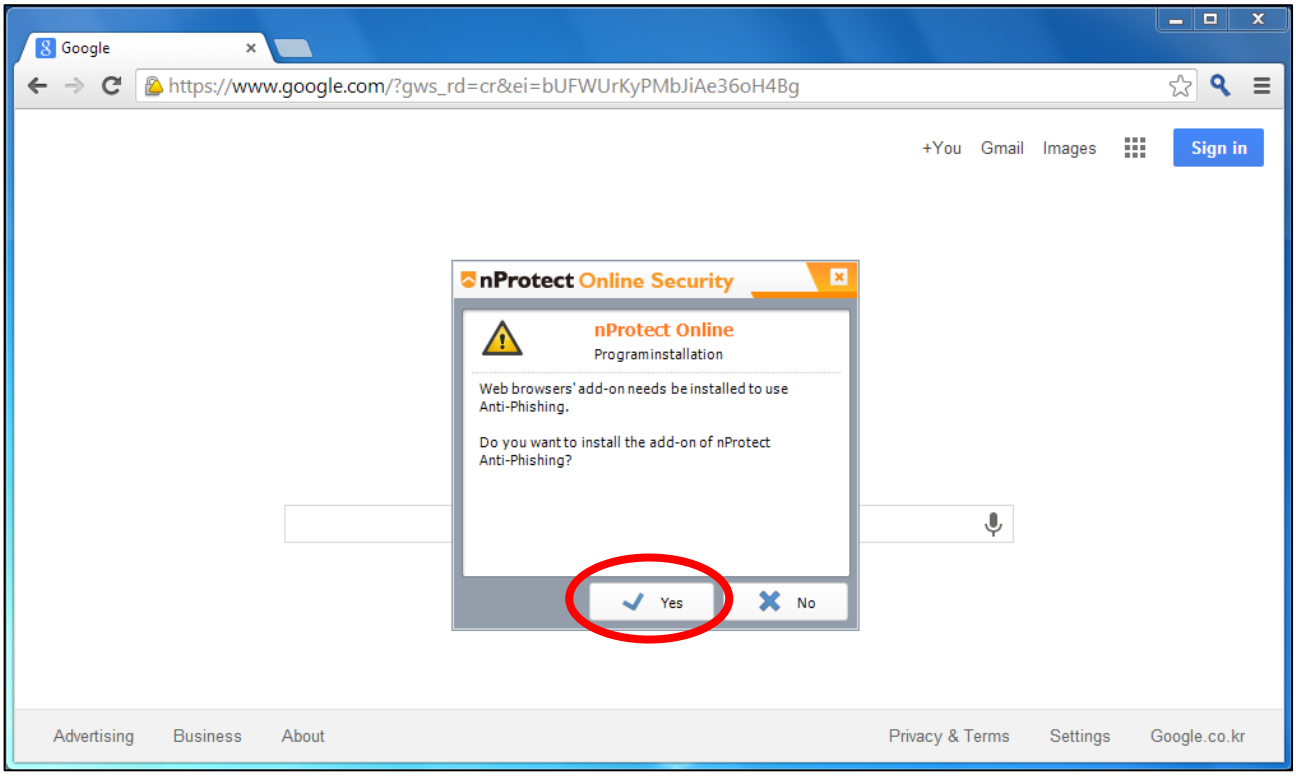
After the installation is complete, restart Internet Explorer. A message will appear on the bottom of the browser to enable ‘PhishingBlockATLBHO Class’. Click Enable.



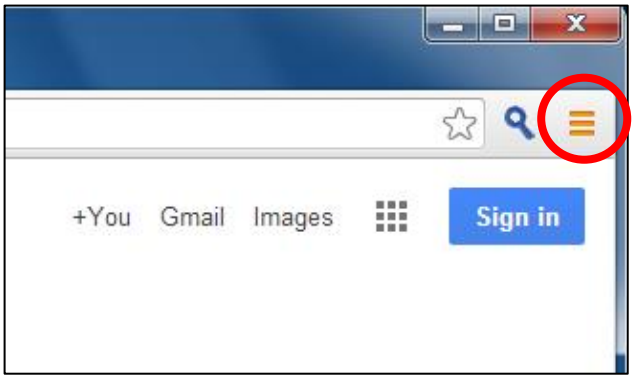
Restart Internet Explorer and visit the sample phishing site (phishingdemo.nprotect.com) to see if Anti-Phishing feature is working properly.

- **Chrome**

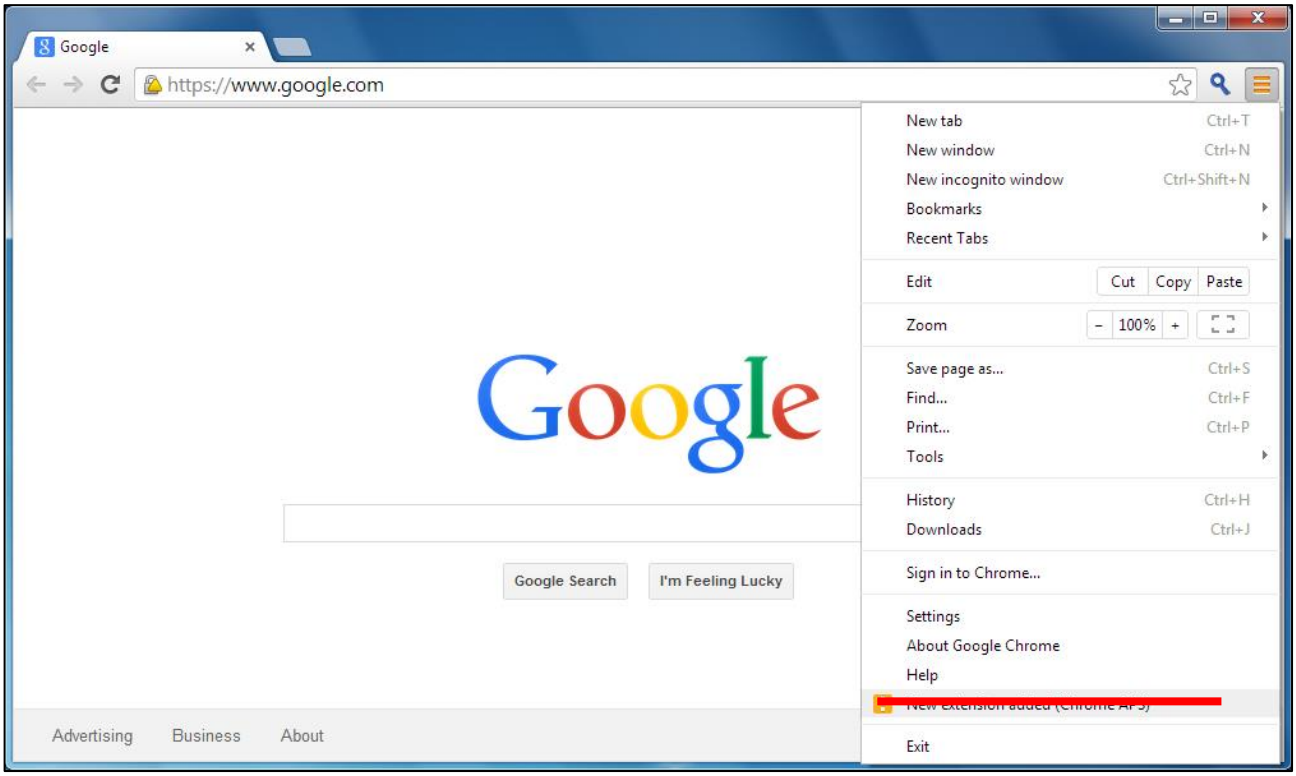
When Chrome browser is first started, NOS pop-up window will show asking to install the Anti-Phishing add-on. Click “Yes” to install the add-on.



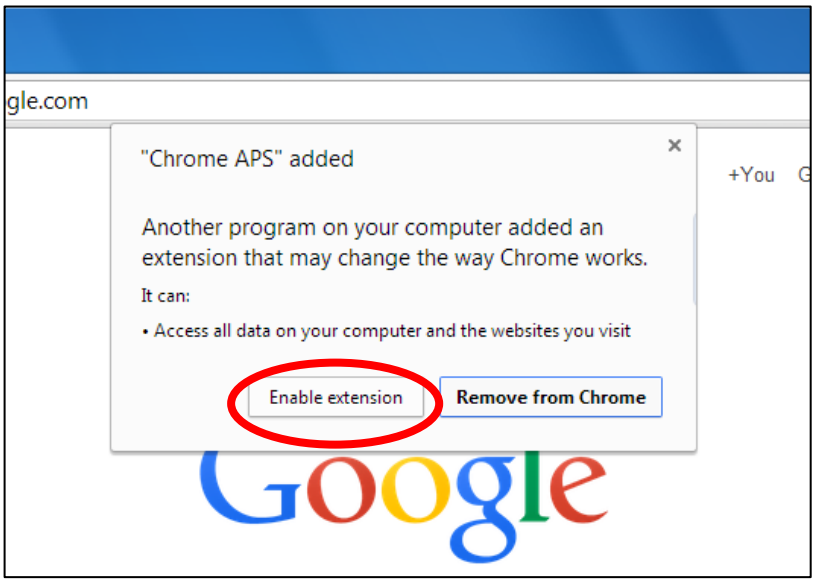
After waiting about 10 seconds for the browser to install the add-on, close the Chrome browser and restart. When the browser is restarted, the menu button wil be highlighted in orange.



Click the menu bar and select “New extension added(Chrome APS)”



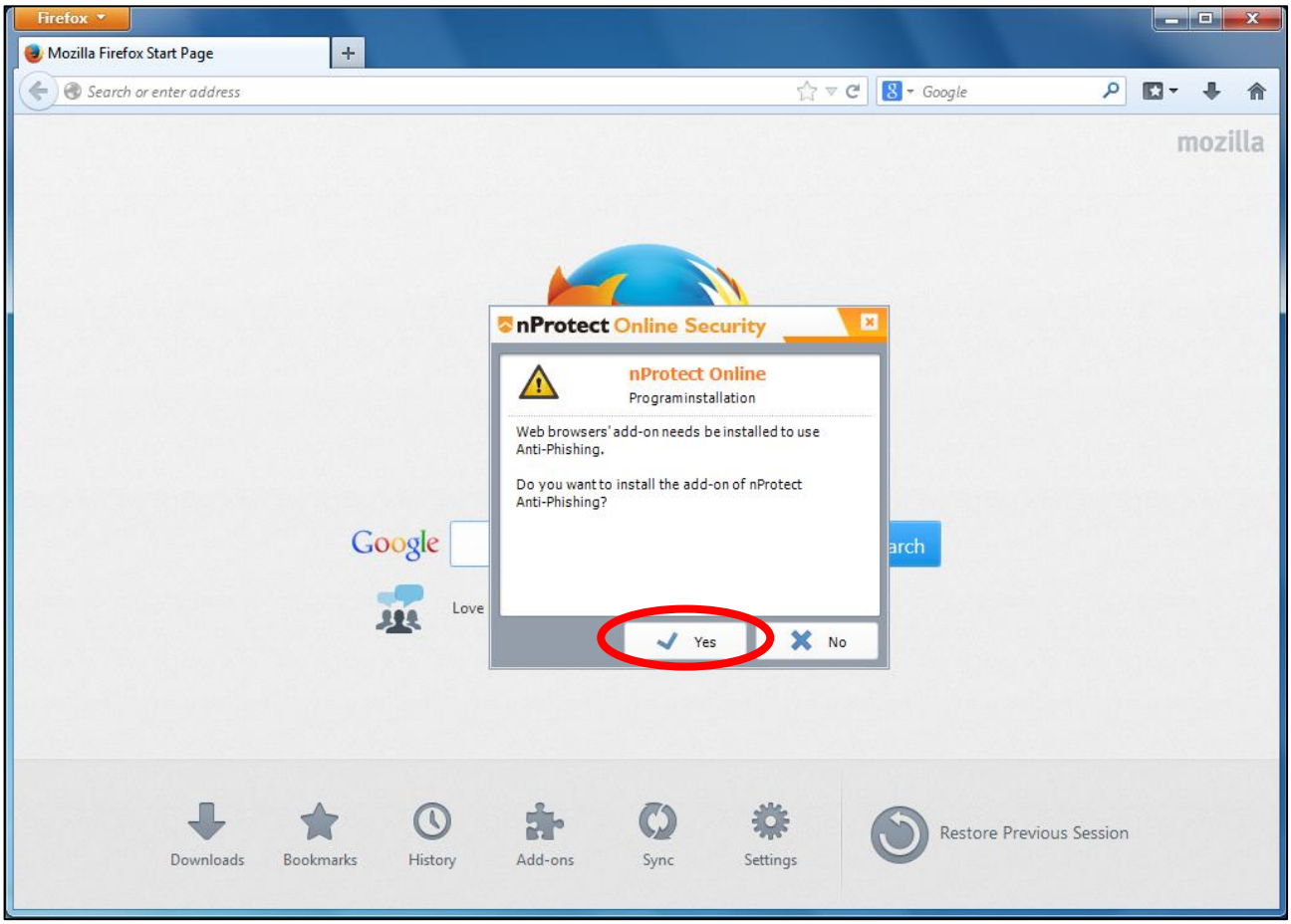
When “New extension added(Chrome APS)” is selected, it will pop-up a message asking to “Enable extension”.



After the installation is complete, visit the sample phishing site(phishingdemo.nprotect.com) to see if Anti-Phishing feature is working properly.

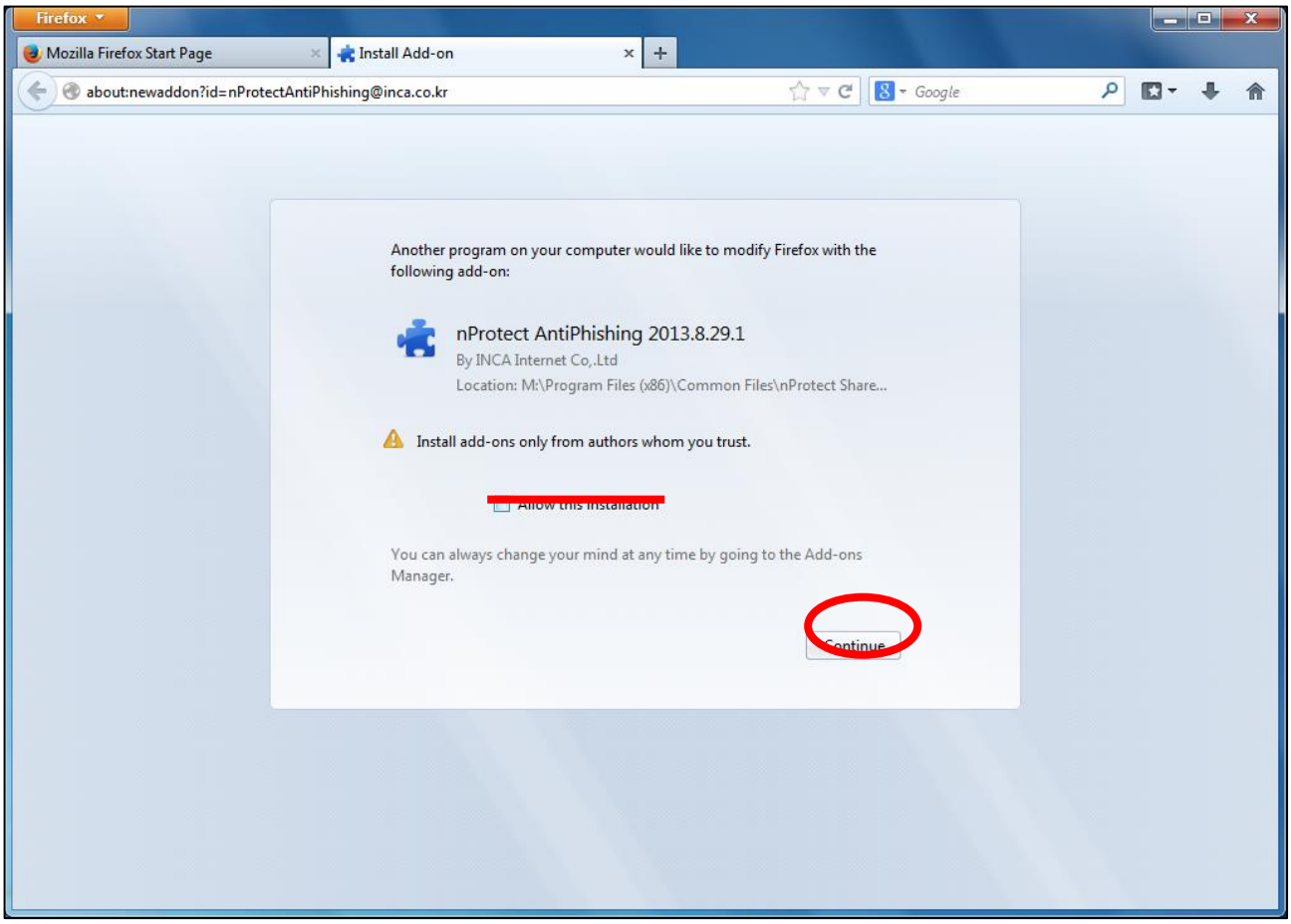
- **Firefox**

When Firefox browser is first started, NOS pop-up window will show asking to install the Anti-Phishing add-on. Click “Yes” to install the add-on.

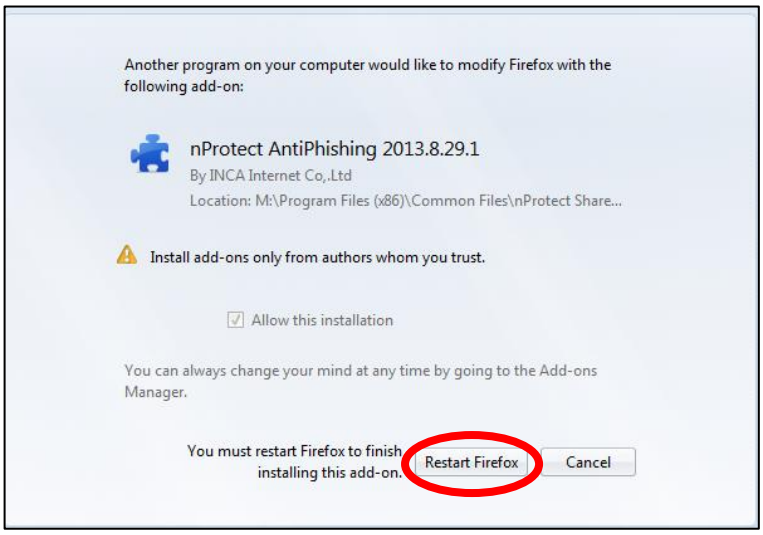


“nProtect Online Security Setup” pop-up will show asking to restart Firefox. Click “OK” to continue.

After restarting Firefox, “Install Add-on” tab will appear. Check “Allow this installation” and click “Continue".



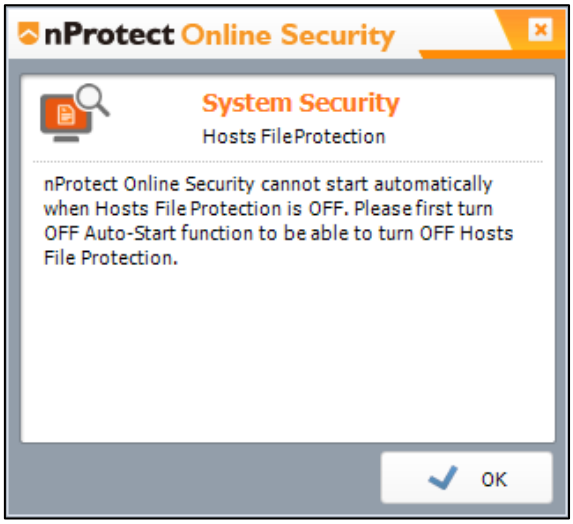
Firefox will ask to restart Firefox to finish installation. Click “Restart Firefox” to finish installation.



After the installation is complete, visit the sample phishing site(phishingdemo.nprotect.com) to see if Anti-Phishing feature is working properly.

3.2. Hosts File Protection

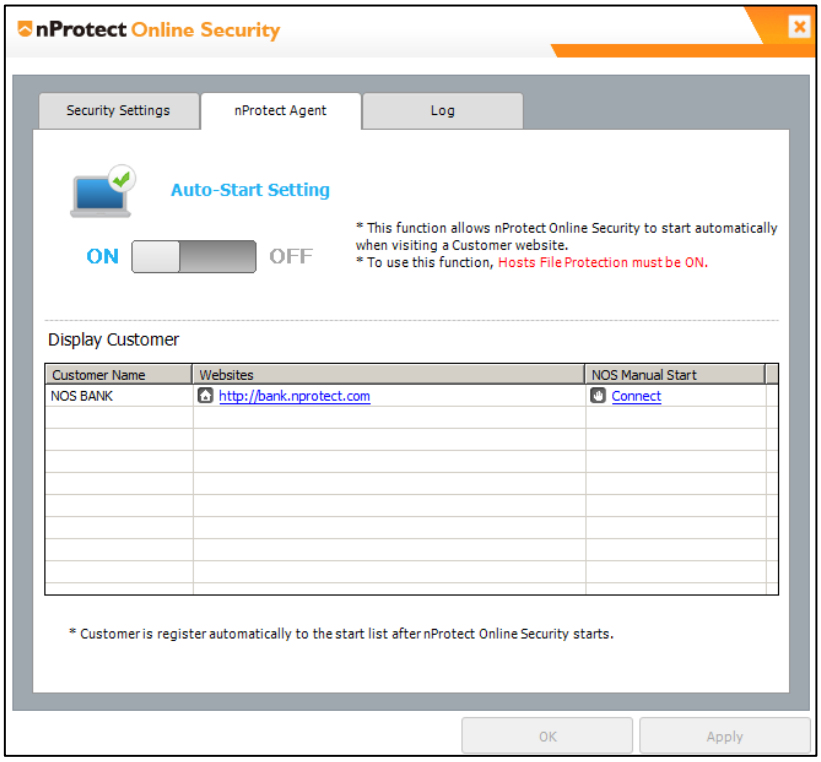
Hosts File Protection can be turned off by moving the slide to ‘OFF’ and clicking ‘OK’ or ‘Apply’.**[Image 3-2]** When Hosts File Protection is turned OFF, an alert message will be shown as below.**[Image 3-4]** Auto-Start function on nProtect Agent tab menu must be first turned OFF to turn OFF Hosts File Protection.



[Image 3-4] Hosts File Protection Alert Message

3.3. Auto-Start Setting

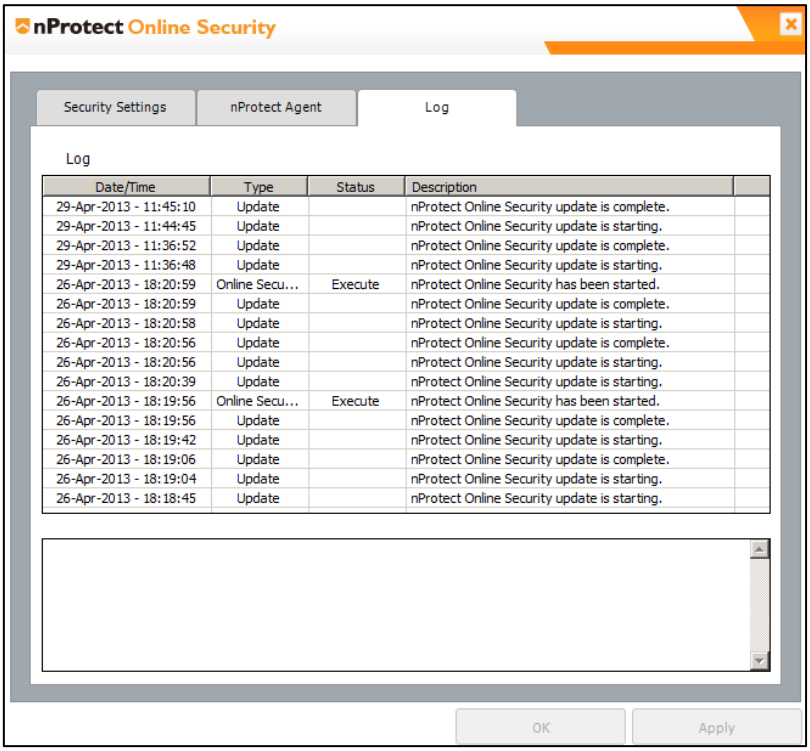
Auto-Start can be turned off by moving the slide to ‘OFF’ and clicking ‘OK’ or ‘Apply’.**[Image 3-5]** When a trusted website is visited, Customer Name and Website URL will be added to the Auto-Start list.



[Image 3-5] Auto-Start Setting

3.4. Log

All event logs for agent update, phishing, hosts file protection can be seen on this tab.



[Image 3-6] nProtect Agent Log

4. nProtect Online Security

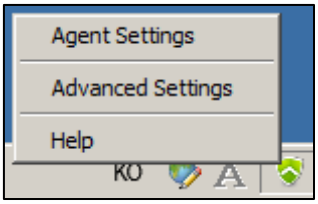
When a user visits a trusted website, NOS will start automatically.

[Image 4-1] nProtect Online Security UI

Function	Mark	Description
Company Logo	nProtect Online Security	On the top left, a company logo can be placed to be recognized where nProtect Online Security is running.
Settings		Click this button to view the main menu UI.
Help		Click this button to open the help page.
Network Protection	Network Protection ON OFF	This quick option allows users to change the Network Protection option without opening the main menu UI.
Keystroke Protection	Keystroke Protection ON OFF	This quick option allows users to change the Keystroke Protection option without opening the main menu UI.
DNS Monitoring	SAFE WARNING	Shows the security status of DNS Monitoring, showing whether URL address matches the IP address.

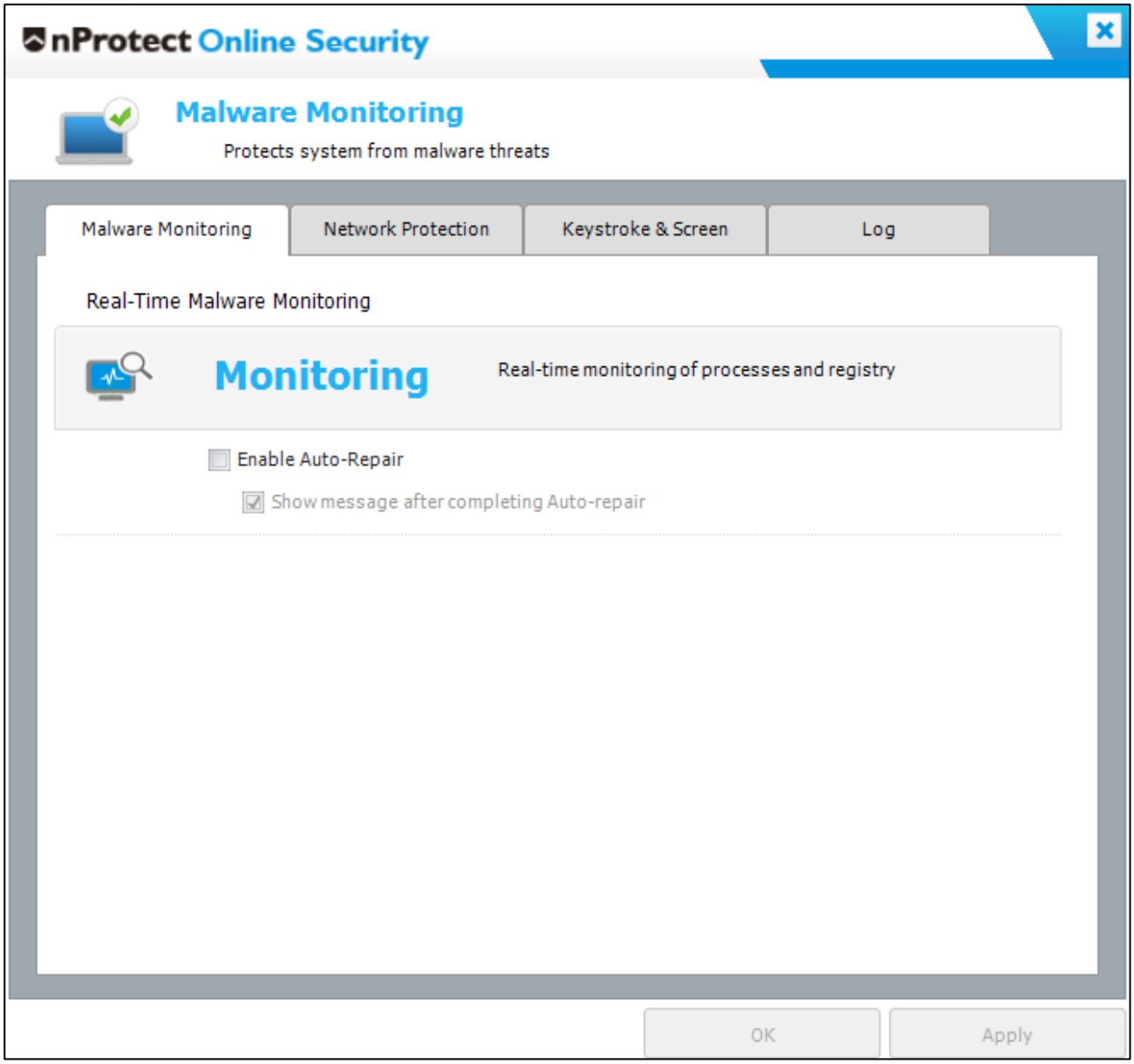
[Table 4-1] nProtect Online Security UI

When NOS tray icon is green, click with the right-mouse button to see that ‘Advanced Settings’ has been added to NOS menu.



[Image 4-2] nProtect Online Security Agent Menu UI

Click ‘Advanced Settings’ or the settings button ( ) in the UI to see the main menu UI.**[Image 4-3]**



[Image 4-3] nProtect Online Security main menu

The features are as follows.

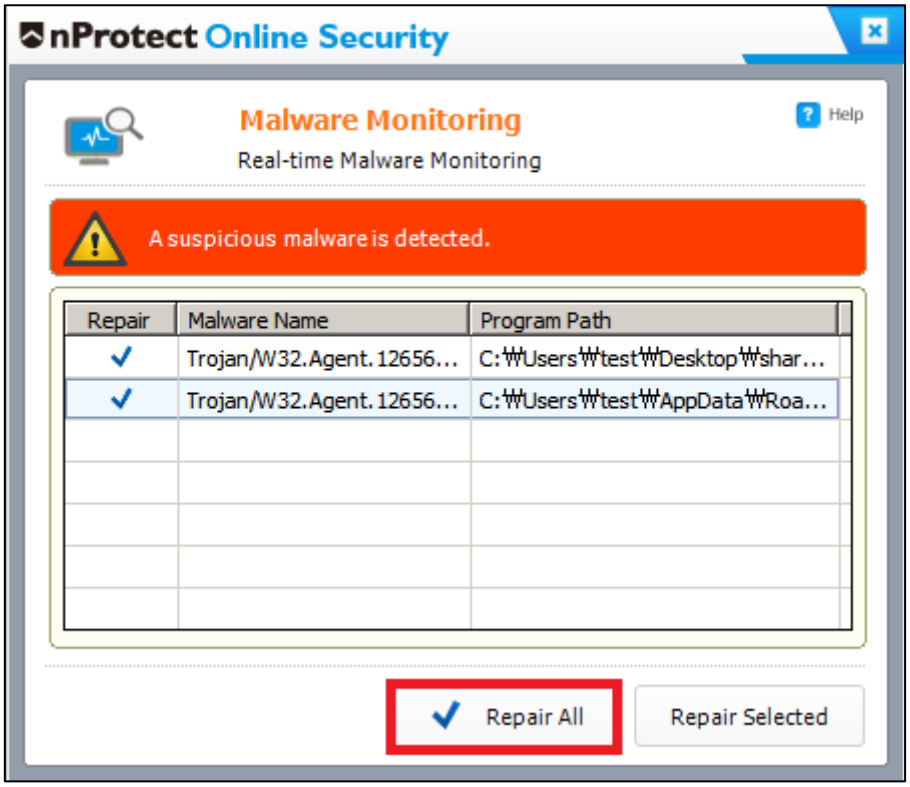
Function	Description
Malware Monitoring	Monitors all running processes and registry in real-time. Can choose to enable Auto-Repair.
Network Protection	Allows or blocks network access based on policies. Users can choose to turn ON and OFF Network Protection function. Also users can add or remove programs to the list.
Keystroke & Screen	Menu to turn ON and OFF Keystroke Protection and Anti-Screen Capture.
Log	Shows all event logs of nProtect Online Security.

[Table 4-2] nProtect Online Security Functions

4.1. Real-Time Malware Monitoring

When users open trusted websites, NOS will launch automatically and start scanning the user's system for malware. If a malware is detected, Real-Time Malware Monitoring will show an alert message as below.

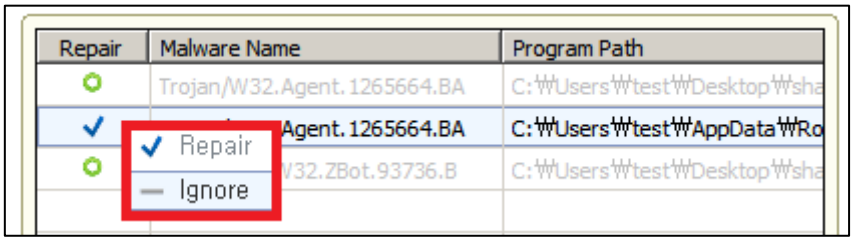
Click 'Repair All' to repair the malwares.



[Image 4-4] Repair All

To repair the malwares selectively, please select a specific malware name in the list and click 'Repair Selected'.

To change the Repair status, click the check mark ( ) in the Repair list and select 'Ignore' or 'Repair'.

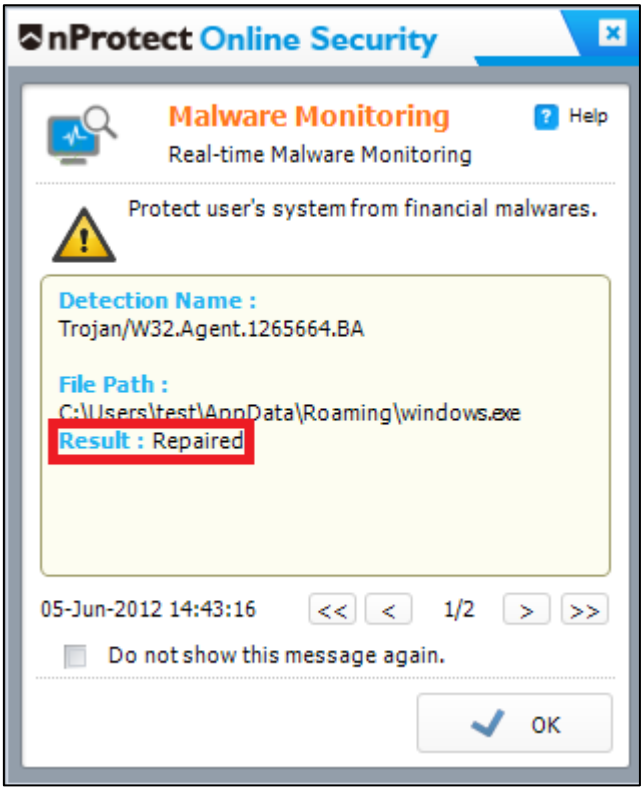


[Image 4-5] Change Repair Status

If the ‘Enable Auto-Repair’ is checked, detected malwares will be repaired automatically without additional consent from the user.

To see the results of Auto-Repair, please check ‘Show message after completing Auto-Repair’.

If a malware is repaired by Auto-Repair, the results will be shown as below.



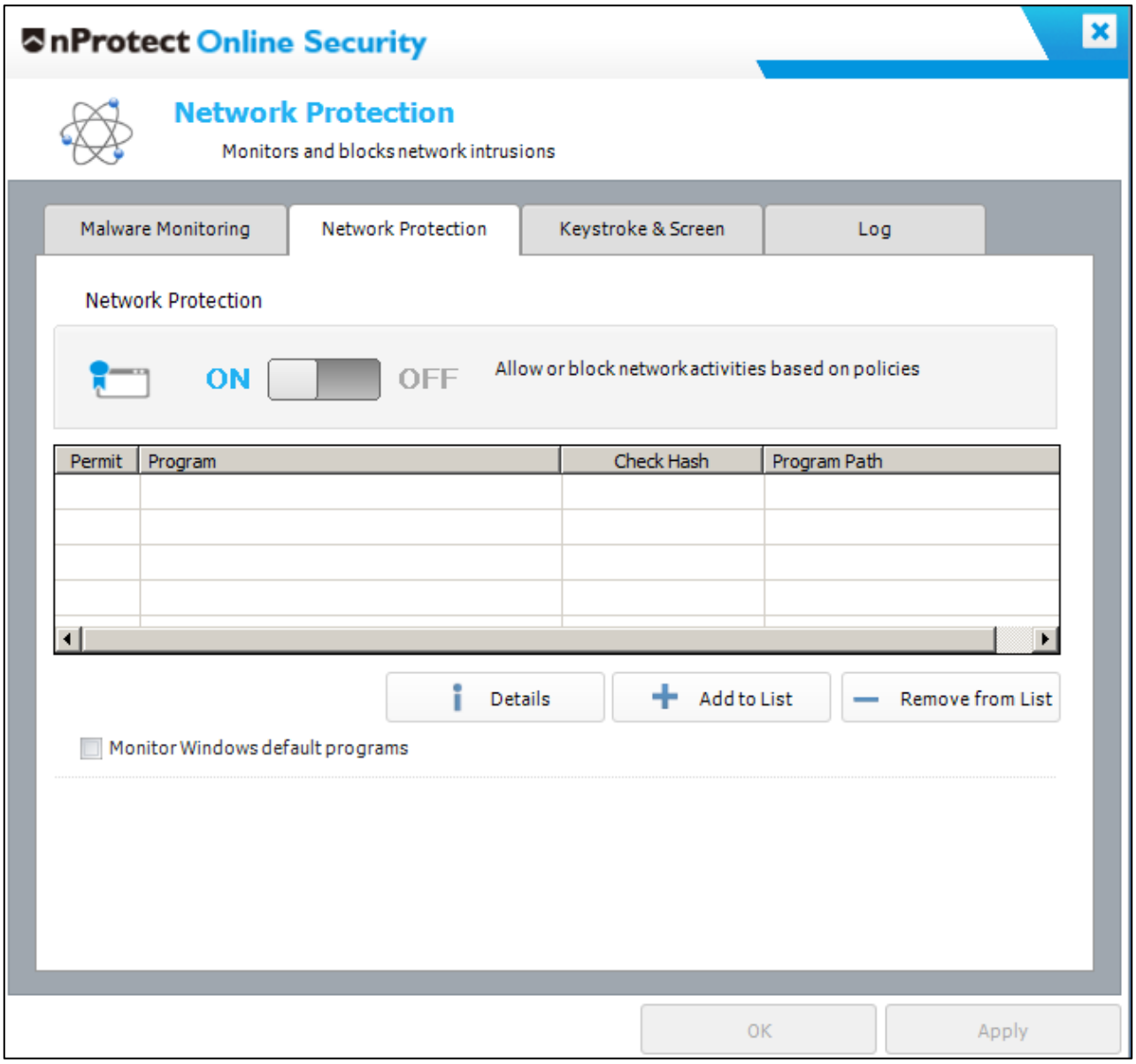
[Image 4-6] Auto-Repair Message

The user can choose to not show this message by checking ‘Do not show this message again’.

4.2. Network Protection

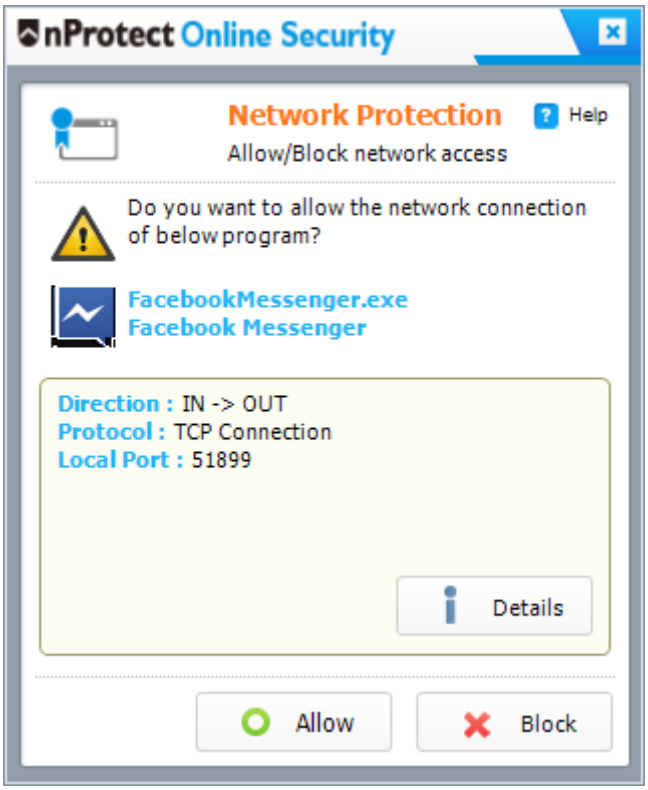
4.2.1. Automatic Process Authentication

Network Protection allows or blocks network access based on policies. The default setting for Network Protection is ON. To disable the Network Protection function, move the slide bar to OFF.



[Image 4-7] Network Protection ON/OFF

When Network Protection is enabled, all applications that access the network will be detected automatically as in **[Image 4-8]**. The user can choose to allow or block by clicking ‘Allow’ or ‘Block’.

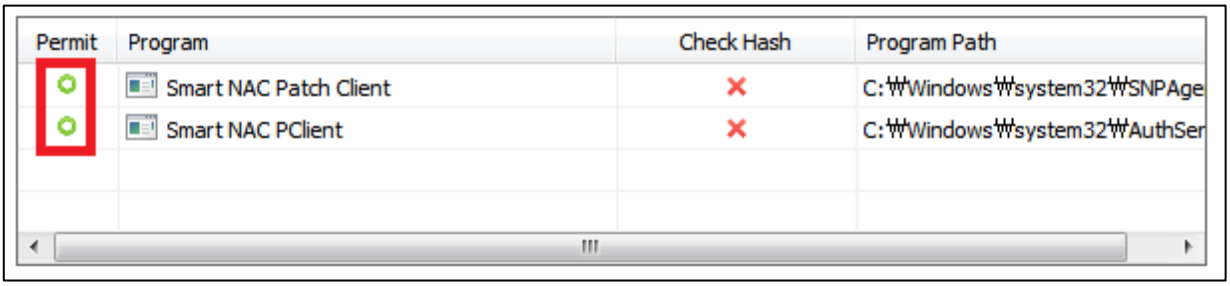


[Image 4-8] Process Authentication

<NOTE>

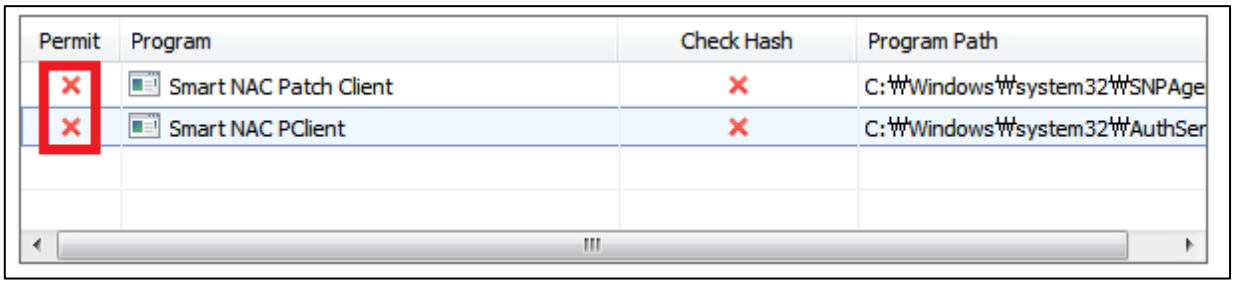
Windows default programs and trusted applications signed by 3rd party authorities(ex.Verisign) will not be blocked by Network Protection to enhance usability.

By clicking ‘Allow’ button in the above message box, the status of Permit will be displayed as “ ”.



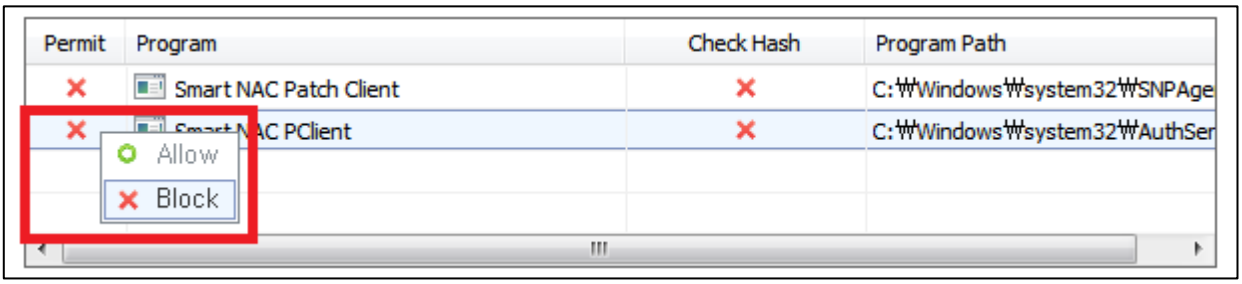
[Image 4-9] ‘Allow’ network access of programs

By clicking ‘Block’ button in the above message box, the status of Permit will be displayed as “ ✕ ”.



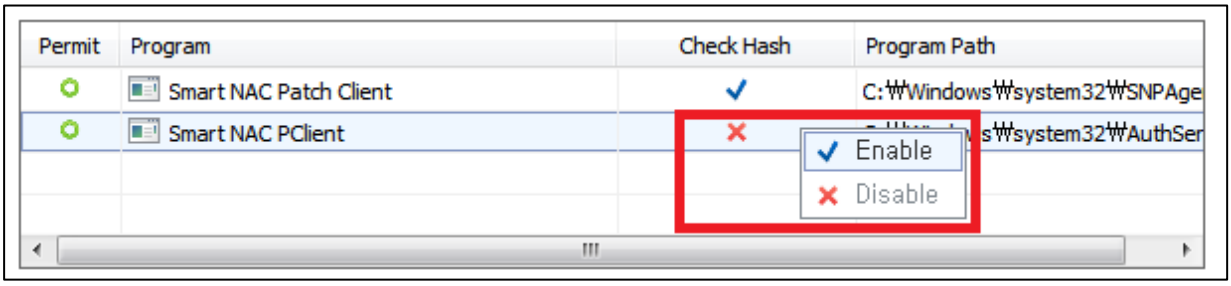
[Image 4-10] ‘Block’ network access of programs

To change the option of ‘Permit’ directly from the main UI, click “ ○ ” or “ ✕ ” from the list and a small menu will be displayed as below.



[Image 4-11] Change of Process Authentication

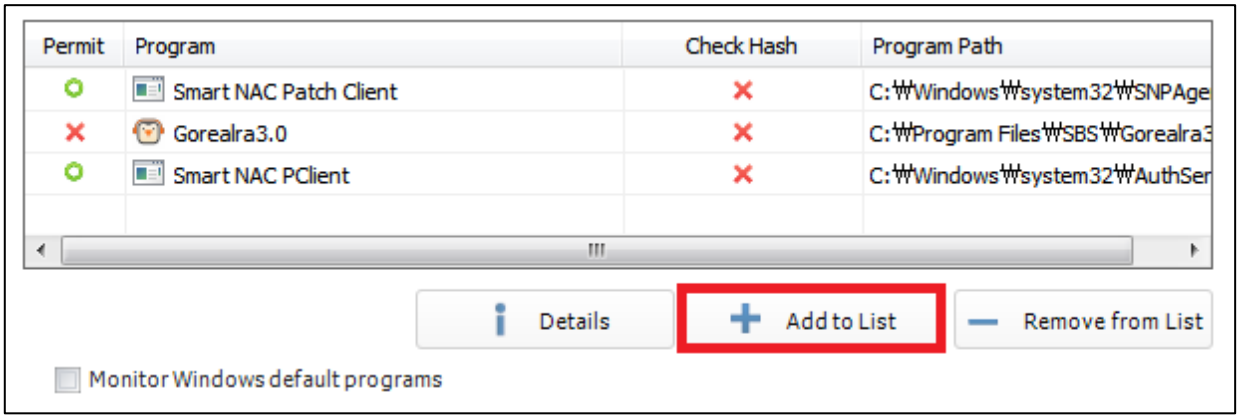
To ensure whether an application is genuine or not, ‘Check Hash’ function can be used. Click “ ✓ ” or “ ✕ ” to change the status as below.



[Image 4-12] Change of the Check Hash

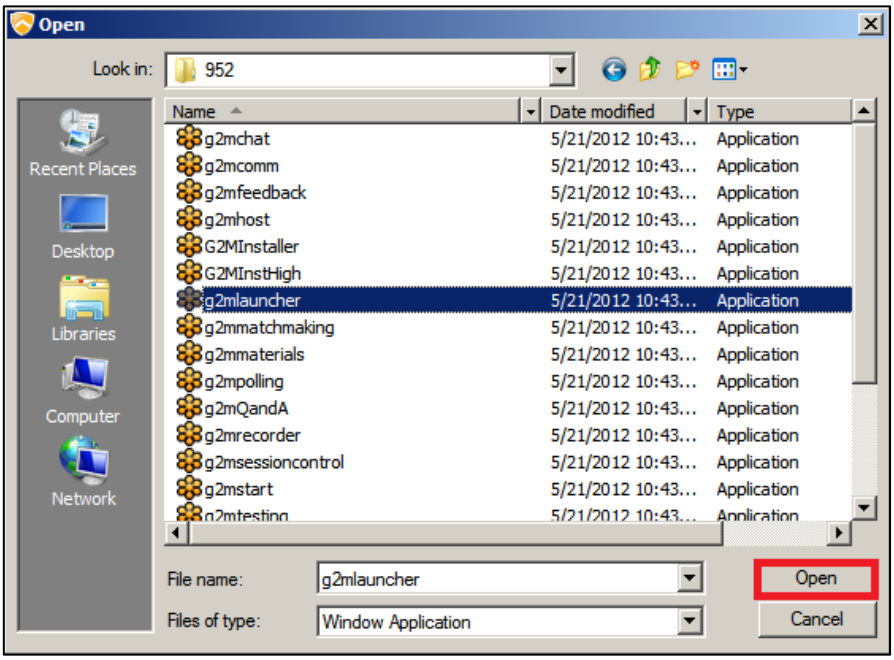
4.2.2. Manual Process Authentication

To manually add programs to the allowed list(‘White list”), click ‘Add to List’ button.



[Image 4-13] Add to List

When a file explorer window is shown as below, select a program and click ‘Open’ to add to the White list.

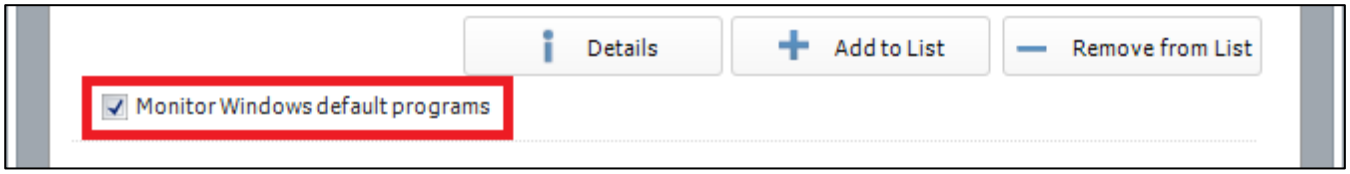


[Image 4-14] Select Application

To remove a program from the list, select the name of the program and click ‘Remove from List’ button and then click ‘Apply’.

4.2.3. Windows Default Programs Monitoring

If the checkbox for 'Monitor Windows default programs' is checked, Network Protection will also check basic programs such as Internet Explorer or Outlook.

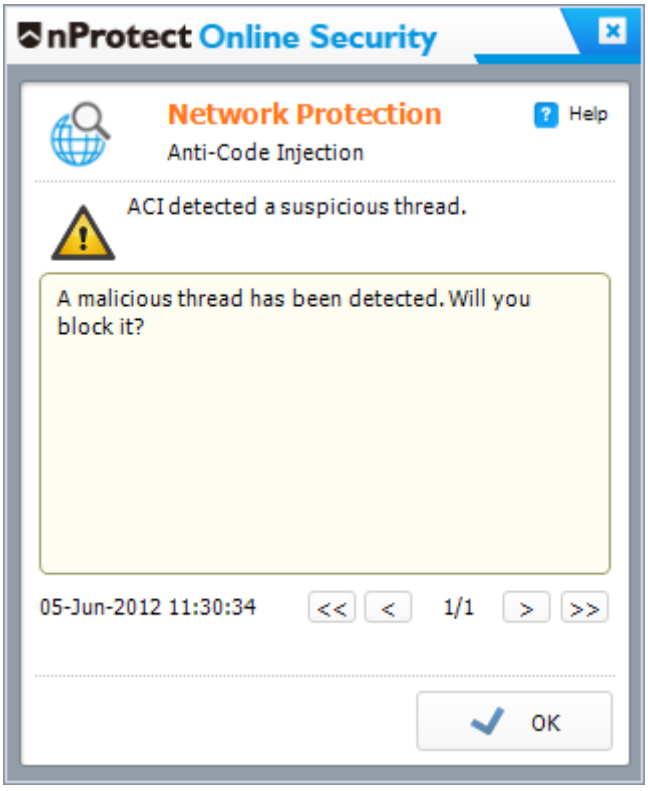


[Image 4-15] Enable to monitor Windows default programs

4.2.4. Anti-Code Injection

Zeus is a Trojan that steals banking information by injecting malicious thread into a running process. Periodically, the injected thread will send stolen personal data through the Internet to the hacker's server.

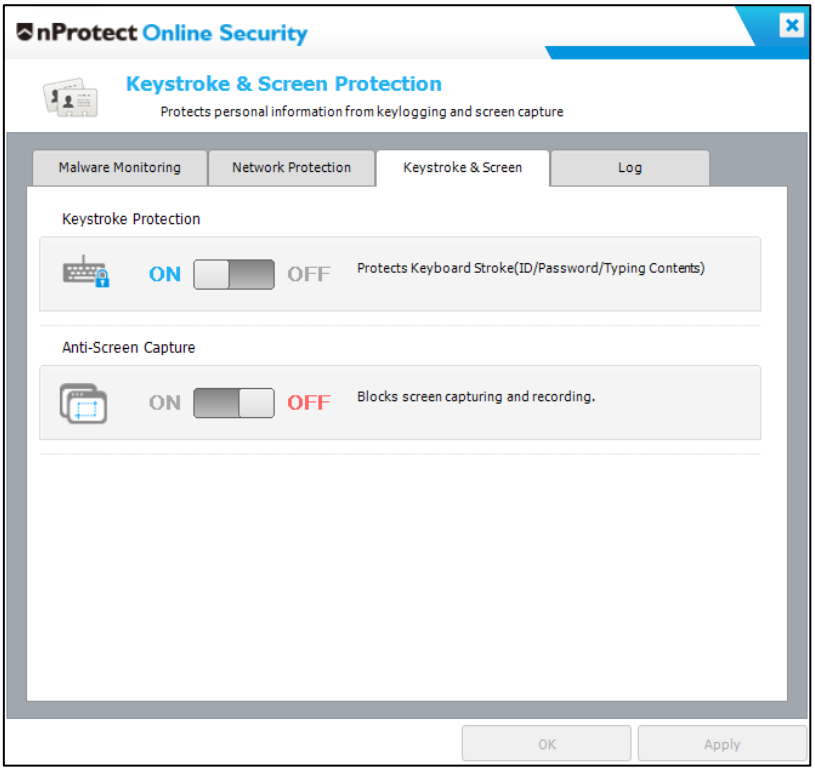
nProtect Online Security provides an Anti-Code Injection(ACI) function under Network Protection. If any suspicious threads are detected by Anti-Code Injection, a warning message is shown as below. By clicking OK, the suspicious thread will be blocked from using the network.



[Image 4-16] Anti-Code Injection

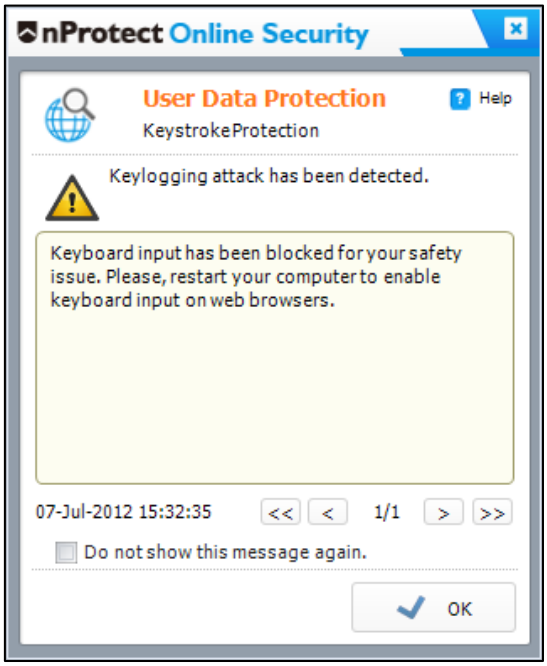
4.3. Keystroke Protection

Keystroke Protection protects user keystrokes from keyloggers. The default setting for Keystroke Protection is ON. To disable Keystroke Protection function, move the slide bar to OFF.



[Image 4-18] Keystroke Protection & Anti-Screen Capture Setting

When a keylogger(i.e. Bus Hound) attempting to steal user's keyboard input data in the kernel/driver level is detected in the system, Keystroke Protection will block all keyboard input.



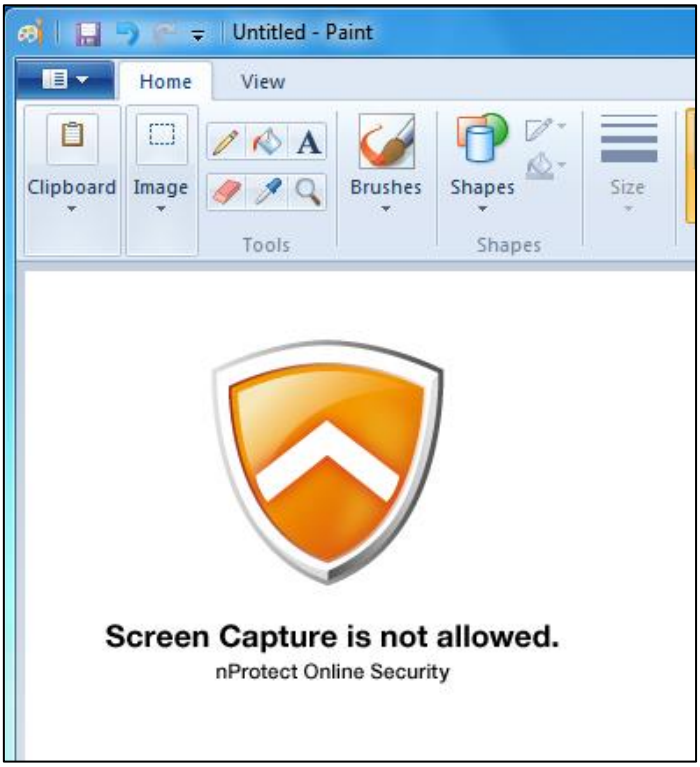
[Image 4-19] Keystroke Protection Alert Message

4.4. Anti-Screen Capture

Anti-Screen Capture blocks all screen capture attempts while user is visiting a trusted website(bank.nProtect.com). The default setting for Anti-Screen Capture is ON. To disable Anti-Screen Capture function, move the slide bar to OFF.**[Image 4-18]**

4.4.1. Screen Capture by PrintScreen Key

Attempts to capture the screen with keyboard printscreen function will be blocked by Anti-Screen Capture. Captured screen image will be shown as an altenative nProtect image as shown below.



[Image 4-20] Protected image

4.4.2. Screen Capture by Screen Capturing Tools

Attempt to use screen capturing tools such as Easy Capture, ScreenshotCaptor, Gadwin PrintScreen, and other free tools to capture the screen will be blocked by Anti-Screen Capture. Captured screen image will be shown as an altenative nProtect image.

4.5. DNS Monitoring

DNS Monitoring prevents DNS hijacking and DNS changer by matching the Name Resolution with URL-IP records. To enable this function, customers need to provide the URL-IP information to nProtect first.

If the URL address and IP match, DNS Monitoring shows a “SAFE” message in green color as shown in the mini UI below.

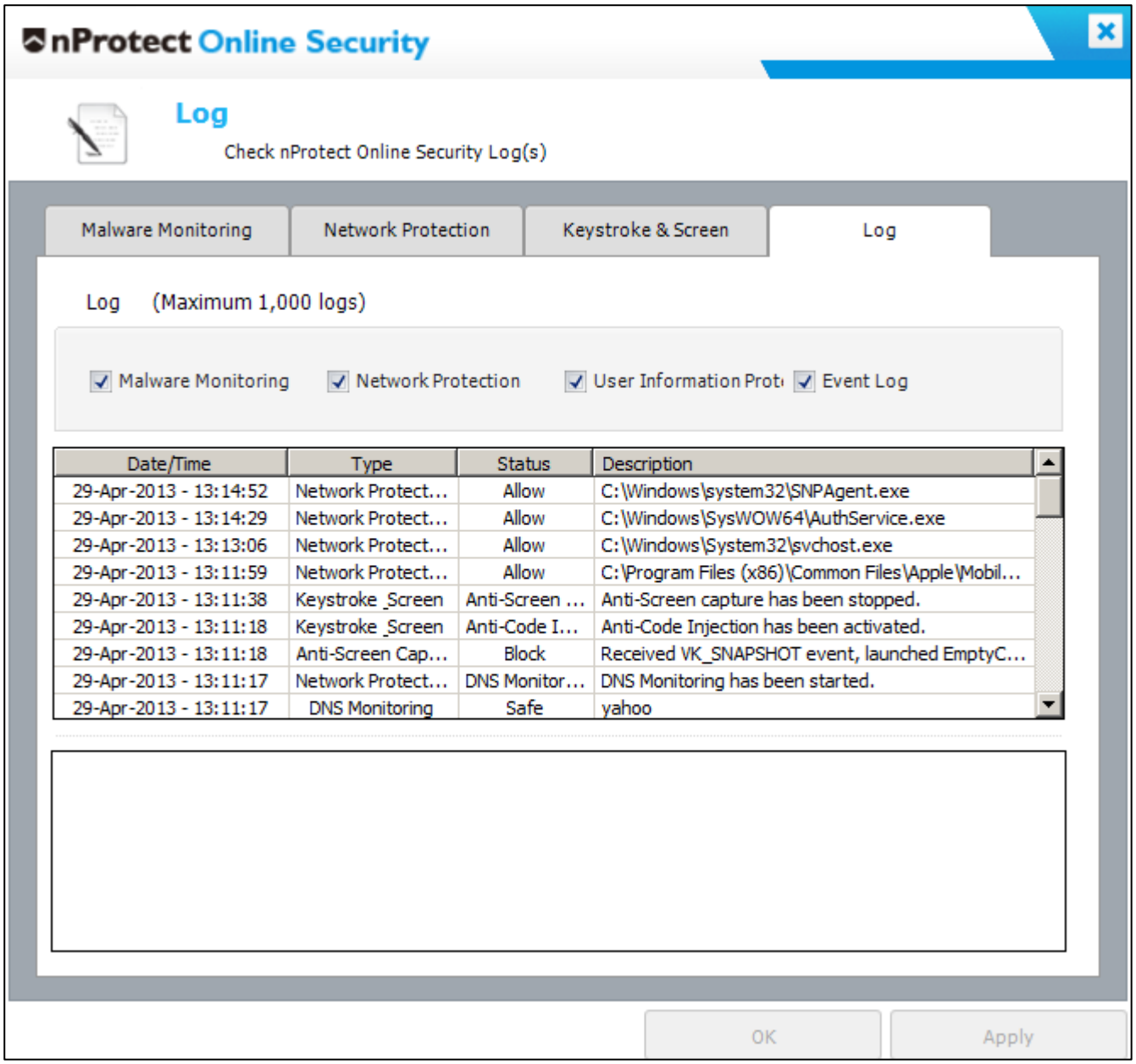
[Image 4-21] DNS Monitoring status - SAFE

If the URL address and IP does not match, DNS Monitoring show a “WARNING” message in red color as shown in the mini UI below.

[Image 4-22] DNS Monitoring status - WARNING

4.6. Log

All NOS event logs can be seen on this tab.



[Image 4-23] nProtect Online Security Log

To view the log according to each event, check or uncheck the checkboxes.

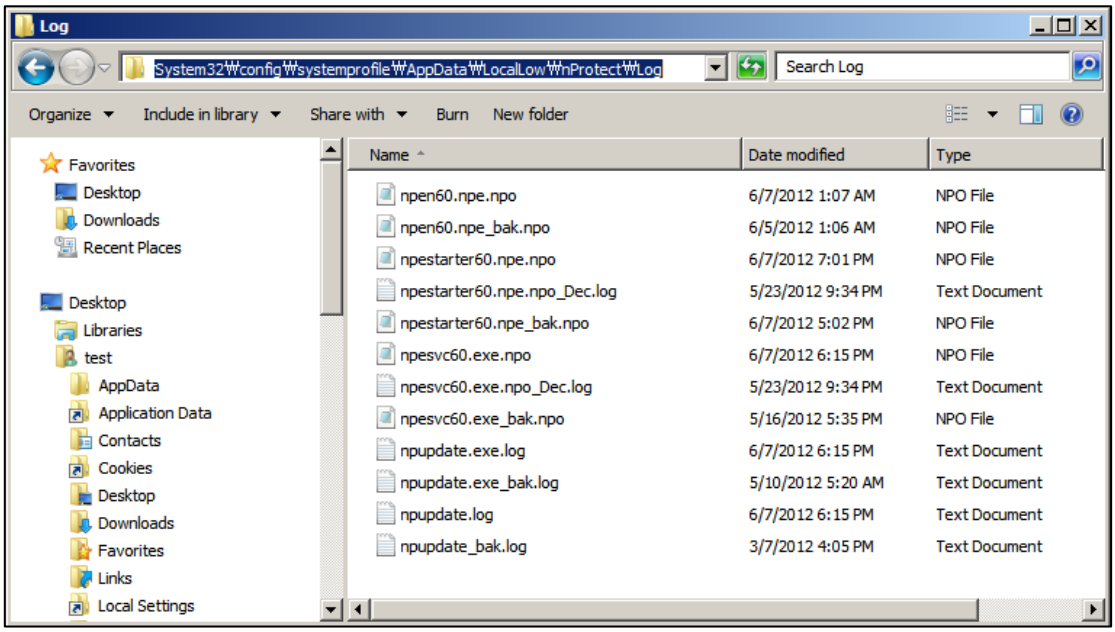
5. Problem Solving

5.1. How to Collect Logs

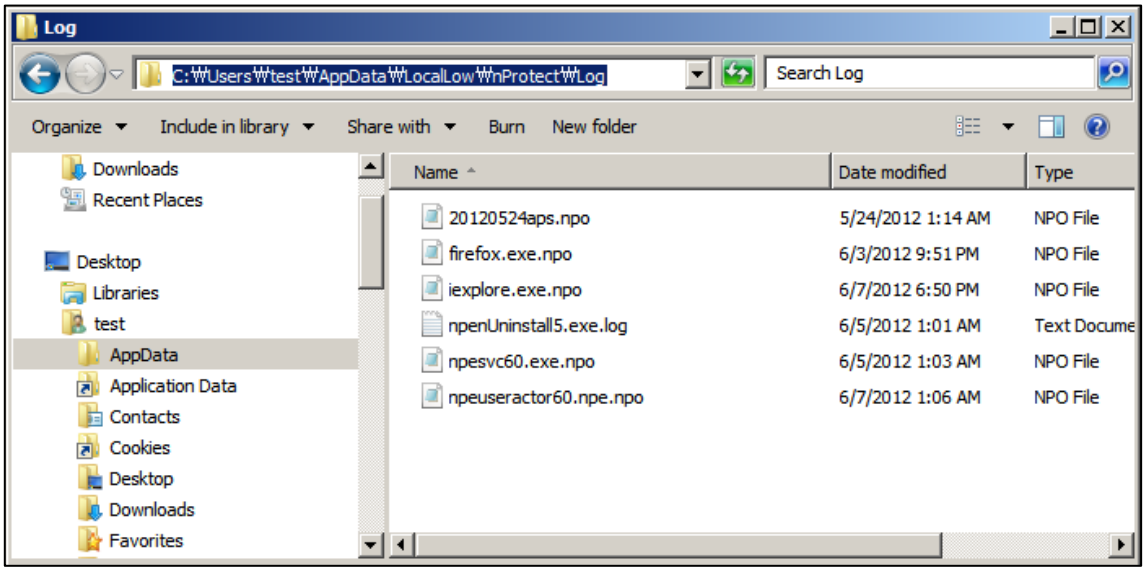
For any program errors or update failures, please send the log files to support@nprotect.com.

The log files of nProtect Online Security can be collected from the following paths:

- C:\Windows\System32\config\systemprofile\AppData\LocalLow\nProtect\Log
- C:\Users\[User Name]\AppData\LocalLow\nProtect\Log



[Image 6-1] C:\Windows\System32\config\systemprofile\AppData\LocalLow\nProtect\Log



[Image 6-2] C:\Users\[User Name]\AppData\LocalLow\nProtect\Log

5.2. Customer Support

nProtect provides customer support for NOS users through website chat, email and telephone. For questions and technical support, please contact:

1) Website Chat

- http://www.nprotect.com

2) E-mail

- Business Inquiries: sales@nProtect.com
- Technical Support: support@nProtect.com

3) Telephone

- Office: 408-477-1742
- Toll Free: 855-466-7768 (1-855-GO-NPROT)