

# Track changes in sensitive security in Windows

Attack Surface Analyzer is a tool released by Microsoft that allows users to easily detect sensitive security changes of the Windows operating system.

**Attack Surface Analyzer is a tool released by Microsoft that allows users to easily detect sensitive security changes of the Windows operating system.**



Attack Surface Analyzer as a bodyguard for the system.

More specifically, the *Attack Surface Analyzer* allows you to display any additional files, registry keys, ActiveX controls and show open ports of the server when users feel worried about security. inside my system, especially after installing some software. In addition, it is also responsible for evaluating configuration access privileges for added files.

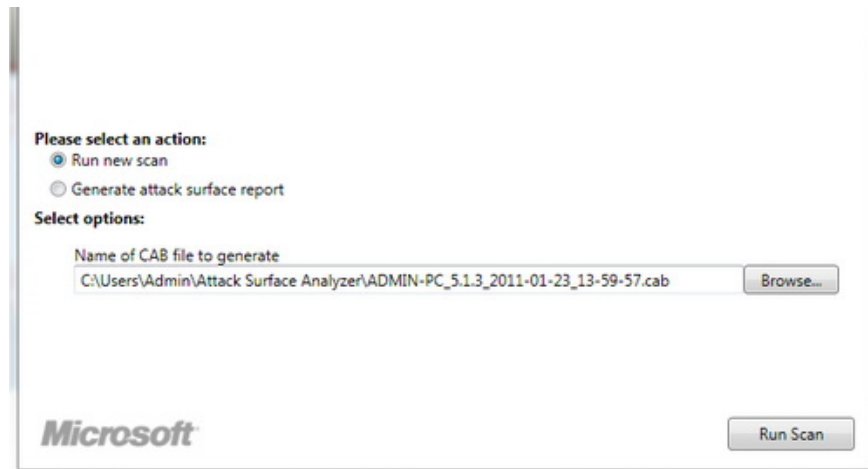
## **Create system image files for comparison**

Users access [here](#) to download the installation version of Attack Surface Analyzer beta 5.1.3 in accordance with their system. This version is compatible with Windows Vista / 7 and requires a pre-installed system for .NET Framework 3.5 or higher.

Basically, *Attack Surface Analyzer* will undergo 2 steps of taking a picture of the system, one is an image file before installing a software and another is a photo file after installation. Based on these two photos, users can identify the changes, thereby making sure that their system has been compromised. The program stores reports in

a compressed file of the \* **.cab** format.

After starting the software, please proceed to create a \* **.cab** file to take a picture of the system before installing a certain software. To do this, click on the option first **Run new scan** in the **Please select an action section** as well as declare the \* **.cab** file location to back up the system image by clicking the **Browse** button of the field *Name of the file CAB to generate* in **Select options** . Then click the **Run Scan** button at the bottom for the program to scan the system.



Make a backup of the system before installing new software

After performing system imaging before installing certain software, users proceed to create a new backup point after installing a software on their system as well as \* **.cab** file.

## Collecting Data

Attack Surface Analyzer is now collecting data from your system to identify potential security issues. This may take several minutes and the total time depends on your system's configuration. Attack Surface Analyzer will then consolidate the information collected into a CAB file once the tasks are complete.

Task	Start Time
Scanning security event log	Complete
Enumerating files	9:00 PM
Enumerating registry keys	9:00 PM
Enumerating memory information	Complete
Enumerating windows	Complete
Enumerating Windows Firewall	Complete
Enumerating GAC assemblies	9:00 PM
Enumerating network shares	Complete
Enumerating logon sessions	Complete
Enumerating ports	Complete
Enumerating named pipes	Complete
Enumerating autorun tasks	Complete
Enumerating RPC endpoints	Complete
Enumerating processes	9:00 PM
Enumerating threads	Pending
Enumerating desktops	Pending
Enumerating handles	Pending
Enumerating Microsoft Internet Information Server	Pending
Enumerating services	Pending
Releasing file database	Pending
Writing security identifiers	Pending

Microsoft

Cancel

The process of scanning all system information into the \* .cab file for comparison

## Make comparison

Now, to compare the two points of the system before and after installing the software, the user should first click on the *Generate Attack Surface Report option* in the **Please select an action section** . At this point, in **Select options** , users click on the **Browse** button of **Baseline Cab** field to point to the file \* .cab containing the system image when stable operation. Then click the **Browse** button in the **Product Cab** field to point to the \* .cab file that contains the system image after installing the software.

### Please select an action:

Run new scan

Generate attack surface report

### Select options:

Baseline Cab in\Attack Surface Analyzer\ADMIN-PC\_5.1.3\_2011-01-23\_13-59-52.cab

Product Cab in\Attack Surface Analyzer\ADMIN-PC\_5.1.3\_2011-01-23\_13-59-52.cab

Report Filename C:\Users\Admin\Attack Surface Analyzer\ADMIN-PC\_5.1.3\_2011-01-23\_13

Microsoft

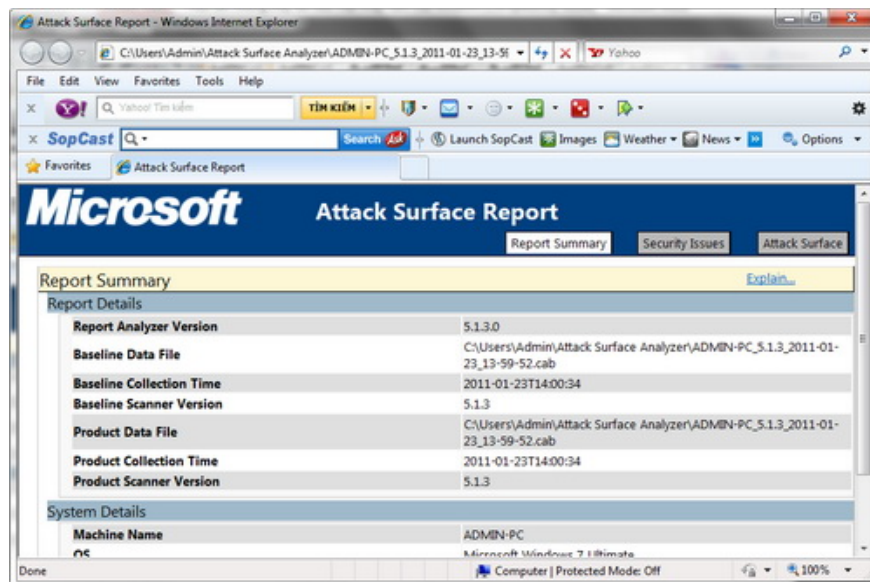
Generate

Declare the \* **.cab** files you want to compare with the Attack Surface Analyzer

When the declaration is completed, the user should click on **Generate** button to proceed with the test program. This information will be exported in the file format \* **.mht** to view with the web browser, the path information will be saved. in the **Report Filename** field, users can change this link by clicking the **Browse** button.

After the scan is completed, the user should open the \* **.mht file** created to see the comparisons. There are 3 columns of information available for users to observe.

- **Report Summary:** provides information about the 2 \* **.cab** files that users compare, along with information about the system's configuration.



Report information changed between two system image files before and after installing the software

- **Security Issues:** provide information related to the security issues of the system, users can rely on it to know if their system can face security risks, risks or not.

- **Attack Surface:** where reports changes related to the system surface, very useful for developers to change the effects of the application to the Windows operating system platform.

**Note:** To view the reports, users need to accept the activation of the ability to read ActiveX files for their web browser.

Overall, *Attack Surface Analyzer* is a very useful application for those who are worried about security issues. The beta version of the limited application is somewhat unimpressive notification file, presented only at a brief level.

You finished reading the article "**Track changes in sensitive security in Windows**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.