Autoruns for Windows v14.09

Article • 02/16/2022 • 3 minutes to read

By Mark Russinovich

Published: February 16, 2022

 Download Autoruns and Autorunsc (3.7 MB)
Run now from Sysinternals Live.

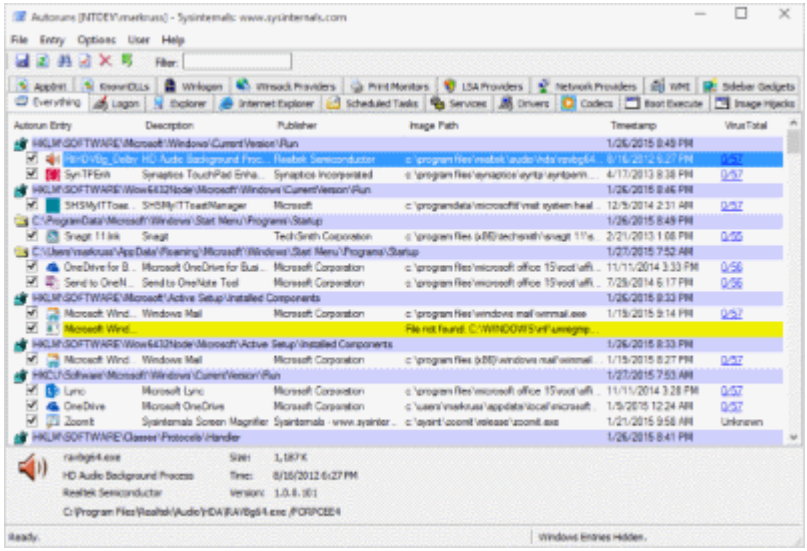
Introduction

This utility, which has the most comprehensive knowledge of auto-starting locations of any startup monitor, shows you what programs are configured to run during system bootup or login, and when you start various built-in Windows applications like Internet Explorer, Explorer and media players. These programs and drivers include ones in your startup folder, Run, RunOnce, and other Registry keys. *Autoruns* reports Explorer shell extensions, toolbars, browser helper objects, Winlogon notifications, auto-start services, and much more. *Autoruns* goes way beyond other autostart utilities.

Autoruns' **Hide Signed Microsoft Entries** option helps you to zoom in on third-party auto-starting images that have been added to your system and it has support for looking at the auto-starting images configured for other accounts configured on a system. Also included in the download package is a command-line equivalent that can output in CSV format, Autorunsc.

You'll probably be surprised at how many executables are launched automatically!

Screenshot



Usage

Simply run *Autoruns* and it shows you the currently configured auto-start applications as well as the full list of Registry and file system locations available for auto-start configuration. Autostart locations displayed by Autoruns include logon entries, Explorer add-ons, Internet Explorer add-ons including Browser Helper Objects (BHOs), Appinit DLLs, image hijacks, boot execute images, Winlogon notification DLLs, Windows Services and Winsock Layered Service Providers, media codecs, and more. Switch tabs to view autostarts from different categories.

To view the properties of an executable configured to run automatically, select it and use the **Properties** menu item or toolbar button. If Process Explorer is running and there is an active process executing the selected executable then the **Process Explorer** menu item in the **Entry** menu will open the process properties dialog box for the process executing the selected image.

Navigate to the Registry or file system location displayed or the configuration of an auto-start item by selecting the item and using the **Jump to Entry** menu item or toolbar button, and navigate to the location of an autostart image.

To disable an auto-start entry uncheck its check box. To delete an auto-start configuration entry use the **Delete** menu item or toolbar button.

The Options menu includes several display filtering options, such as only showing non-Windows entries, as well as access to a scan options dialog from where you can enable signature verification and Virus Total hash and file submission.

Select entries in the **User** menu to view auto-starting images for different user accounts.

More information on display options and additional information is available in the on-line help.

Autorunsc Usage

Autorunsc is the command-line version of Autoruns. Its usage syntax is:

Usage: autorunsc [-a <*|bdeghiklmoprsw>] [-c|-ct] [-h] [-m] [-s] [-u] [-vt] [[-z] | [user]]]

Parameter	Description
-a	Autostart entry selection:
*****	All.
b	Boot execute.
d	Appinit DLLs.
e	Explorer addons.
g	Sidebar gadgets (Vista and higher)
h	Image hijacks.
i	Internet Explorer addons.
k	Known DLLs.
l	Logon startups (this is the default).
m	WMI entries.
n	Winsock protocol and network providers.
o	Codecs.
p	Printer monitor DLLs.
r	LSA security providers.
s	Autostart services and non-disabled drivers.
t	Scheduled tasks.
w	Winlogon entries.
-c	Print output as CSV.
-ct	Print output as tab-delimited values.
-h	Show file hashes.
-m	Hide Microsoft entries (signed entries if used with -v).

Parameter	Description
-s	Verify digital signatures.
-t	Show timestamps in normalized UTC (YYYYMMDD-hhmmss).
-u	If VirusTotal check is enabled, show files that are unknown by VirusTotal or have non-zero detection, otherwise show only unsigned files.
-x	Print output as XML.
-v[rs]	Query VirusTotal for malware based on file hash. Add 'r' to open reports for files with non-zero detection. Files reported as not previously scanned will be uploaded to VirusTotal if the 's' option is specified. Note scan results may not be available for five or more minutes.
-vt	Before using VirusTotal features, you must accept the VirusTotal terms of service. If you haven't accepted the terms and you omit this option, you will be interactively prompted.
-z	Specifies the offline Windows system to scan.
user	Specifies the name of the user account for which autorun items will be shown. Specify '*' to scan all user profiles.

Related Links

- **Windows Internals Book** The official updates and errata page for the definitive book on Windows internals, by Mark Russinovich and David Solomon.
- **Windows Sysinternals Administrator's Reference** The official guide to the Sysinternals utilities by Mark Russinovich and Aaron Margosis, including descriptions of all the tools, their features, how to use them for troubleshooting, and example real-world cases of their use.

Download

 **Download Autoruns and Autorunsc (3.7 MB)**

Run now from Sysinternals Live.