WSABLogs User Guide

What is WSABLogs?

WSABLogs is a utility written by Webroot's QA department. This utility gathers *Webroot SecureAnywhere Business* software operation information which includes:

- Webroot software operation logs
- Webroot software scan logs
- System and Application Event logs
- Windows MiniDumps
- Network Configuration data
- Registry data pertaining to the operation of the software or common registry locations used to launch malware from
- Webroot program file information
- Key directly listings (using dir function) including directories that are known to house malware
- Scheduled Task data
- The Hosts file
- System MSD

WSABLogs is executed remotely from the Endpoint Protection portal using the Advanced Agent Commands "*Download and Execute a file*" as well as enabling switches using the "*Run Registry Command*" feature, and can be run on multiple systems simultaneously. When WSABLogs is run on a system, it runs silently in the background. WSABLogs gathers the data and compresses it into a 7zip file, which can be automatically uploaded to Webroot Support's secure file repository using PSCP, or can be configured to save a copy locally to a specific location (for example if PSCP is blocked from a corporate firewall perspective) and the file later retrieved by the administrator. WSABLogs can also be configured to gather a Full Windows Dumps if the file is present on the system, or a specified files by absolute path (for example if a screenshot has been saved that needs to be included). WSABLogs typically only takes a minute or less to gather and upload results, but the run time can be extended substantially if a full Windows memory dump is requested to be gathered and returned.

If executed locally from the Command Prompt, WSABLogs can be run with command line switch operations on the desired computer, which will override any WSABLogs settings set in the registry.

Appendix A shows basic format for the registry ADD and DELETE options that can be sent to the endpoint using the Advanced Agent Commands.

Appendix B describes A GUI version of WSABLogs that is also available and is known as WSALogs. This version of the utility is run manually and used locally on the desired computer, and will show the user a progress report on the data gathering, compression, and upload process.

Privacy of data collected

The privacy of our customers is very important to us. All logs are security uploaded to the Webroot server over PSCP and are only accessible to Webroot staff that have been granted access to the repository, no external read capability to this server exists, and the logs on this server are purged regularly. All information gathered is in accordance with Webroot's Privacy Policy and will only be used to expedite the identification and resolution of the issue reported. Webroot's Privacy Policy can be viewed here: www.webroot.com/privacy

WSABLogs quick use guide

The following are the quick steps to run the utility remotely from the Endpoint Protection portal:

1. Navigate to the ***Group Management*** *tab*
2. Select the desired hostname
   Note: If a registry command is being sent, all endpoint hostnames can be selected, to preset the values for the entire group. This avoids the need to send them in the future, especially MyID.
3. Select **Agent Commands** > **Advanced** > "**Run Registry Command**"
4. Type in the registry command "**add HKLM\Software\WSABLogs /v MyID /d *my@email*.com**"
   **replacing my@email.com with your email address*
5. Click the button "**Run Registry Commands**"
6. Select **Agent Commands** > **Advanced** > "**Download and Execute a file**"
7. Type in the URL "**http://download.webroot.com/wsablogs.exe**"
8. Click the button "**Download and Execute**"

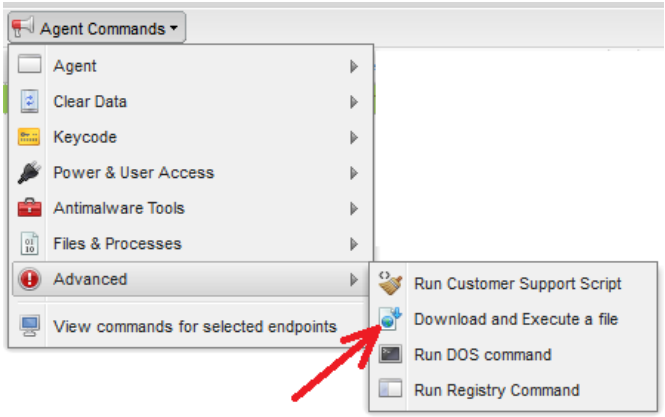
The MyID registry value is added and the WSABLogs utility will be downloaded and run automatically and silently when the agent next refreshes. The agent refreshes when a scan runs, when a Poll occurs (set under Policy > Basic Configuration > Poll Interval), or when a user right-clicks on the Webroot SecureAnywhere tray icon and chooses "Refresh configuration".

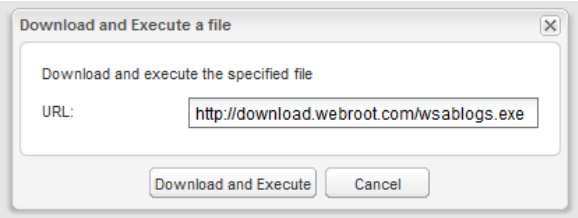
WSABLogs execution and default operations

WSABLogs.exe is available at http://download.webroot.com/wsablogs.exe

To run the utility remotely from the Endpoint Protection portal:

9. Navigate to the ***Group Management*** *tab*
10. Select the desired hostname
11. Select **Agent Commands** > **Advanced** > "**Download and Execute a file**"
12. Type in the URL **http://download.webroot.com/wsablogs.exe**
13. Click the button "**Download and Execute**"





The WSABLogs utility will be downloaded and run automatically and silently when the agent next refreshes. The agent refreshes when a scan runs, when a Poll occurs (set under Policy > Basic Configuration > Poll Interval), or when a user right-clicks on the Webroot SecureAnywhere tray icon and chooses "Refresh configuration".

The WSABLogs utility will attempt to upload and return the logs to Webroot over PSCP twice unless directed not to, via specified *NoSend* registry entry or */ns* command line switches.

The WSABLogs utility output filename by default will be in the format:
wsablog_MyID-MachineName_YYYY-MM-DD-HH.MM.SS.7z

At the end of run operation, WSABLogs will use the same-filename.7z.log to drop extended logs (which include data beyond packaging) into %TEMP%. This will occur even if there is nothing to package.

The following are the default configuration settings used by the utility if no registry overrides are present in *HKLM**Software**WSABLogs*:

Config	Value	Description
`MyID`	NoID	The value “NoID” is used
`Upload`	Yes	Logs are uploaded via PSCP to Webroot
`Grab`	No	No specific files are grabbed
`FullDump`	No	A Full Memory Dump if present on system will not be collected
`LocalDrop`	%TEMP%	The zip file will typically be dropped in *C:**Windows**Temp*, but may revert to local temp if WSABLogs is run manually. Reverts to the location of the exe (Usually %TEMP%) if the defined location cannot be accessed
`Cleanup`	No	Cleanup (deletion) of the WSABLogs registry items will not occur

Registry Key and Values to override defaults granularly

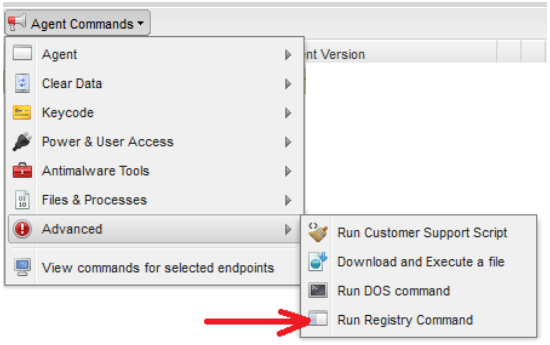
WSABlogs.exe checks for the presence of **HKLM\Software\WSABLogs** registry location for the following overrides:

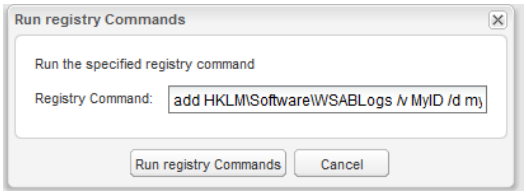
Value	Type	Data	Description
MyID	SZ	ID	Typically the email address of the administrator conversing with support
FGrab	SZ	FilePath	Filename to grab. Include absolute path
NoSend	SZ	1	Do not upload
Cleanup	SZ	1	Delete all WSABLogs registry items except MyID (ONLY can be set in Registry and not via command line switch)
GrabOnly	SZ	1	Grab File Only, do not perform full log gathering, including not *FullDump* even if set. **FGrab* needs to be set as well, otherwise no logs at all are gathered
LocalDrop	SZ	FilePath	Path of location to drop a copy of the results.
MemoryDump	SZ	1	Collect Full (Or Kernel) Crash Dump if present

*Any data in the value above that contains a "1" will trigger the switch, including a "0", since WSABLogs is simply checking for content in the data of the value

To enter these registry entries remotely from the Endpoint Protection Administrator portal:

1. Navigate to the ***Group Management*** *tab*
2. Select the desired hostname
3. Select **Agent Commands** > **Advanced** > "**Run Registry Command**"
4. Type in the registry command, such as "add HKLM\Software\WSABLogs /v MyID /d my@email.com"
   Note: The registry commands use reg.exe format
5. Click the button "**Run Registry Commands**"





The registry key and value will be added when the agent next refreshes. The agent refreshes when a scan runs, when a Poll occurs (set under Policy > Basic Configuration > Poll Interval), or when a user right-clicks on the Webroot SecureAnywhere tray icon and chooses "Refresh configuration".

Examples of registry commands that can be sent:

Value	Registry Command
MyID	add HKLM\Software\WSABLogs /v MyID /d my@email.com
FGrab	add HKLM\Software\WSABLogs /v FGrab /d C:\DOCUME~1\theuser\Desktop\pic.jpg
NoSend	add HKLM\Software\WSABLogs /v NoSend /d 1
Cleanup	add HKLM\Software\WSABLogs /v Cleanup /d 1
GrabOnly	add HKLM\Software\WSABLogs /v GrabOnly /d 1
LocalDrop	add HKLM\Software\WSABLogs /v LocalDrop /d c:\drop
MemoryDump	add HKLM\Software\WSABLogs /v MemoryDump /d 1

Command Line Switches which override defaults and registry granularity

If WSABLogs is run locally on the computer, Command Line Switches can be set to override the defaults as well as what is already set in the registry:

Switch	Description
/id=<id>	MyID
/fg=<file>	File Grab – Include absolute path
/ns	No Send (Do not upload)
/go	Grab Only (Do not gather other logs, including Full Dump if configured)
/ld=<folder>	Local Drop – Path to location to drop a copy of the results.
/md	Memory Dump – Gather a Full (Or Kernel) Crash Dump if present

The following three command line switches can be sent to quickly negate already present registry entries; this is performed by adding "0" to the switch name:

Switch	Description
/ns0	Do send (upload) logs even if NoSend is set is a 1 in the registry
/go0	Grab full logs even if GrabOnly is set to 1 in the registry
/md0	Do not grab a Memory Dump even if MemoryDump is set to 1 in the registry

Appendix A

Below is the basic format for the registry ADD and DELETE options that can be sent to the endpoint using the Advanced Agent Commands “Run Registry Command”.

Registry ADD command:

REG ADD ROOTKEY \Subkey /v ValueName [/t Type] [/s Separator] [/d Data] [/f]

ROOTKEY\SubKey

ROOTKEY [HKLM | HKCU | HKCR | HKU | HKCC]
SubKey The full name of a registry key under the selected ROOTKEY.

/v The value name, under the selected Key, to add.

/t RegKey data types

[REG_SZ | REG_MULTI_SZ | REG_EXPAND_SZ | REG_DWORD | REG_QWORD | REG_BINARY | REG_NONE]

If omitted, REG_SZ is assumed (default data type used by WSABLogs)

/d The data to assign to the registry ValueName being added.

Examples: add HKLM\Software\WSABLogs /v LocalDrop /d c:\drop

Adds a WSABLogs key if it does not exist, and a value (name: LocalDrop, type: REG_SZ, data: c:\drop)

Registry DELETE command:

DELETE ROOTKEY\SubKey [/v ValueName

ROOTKEY\SubKey

ROOTKEY [HKLM | HKCU | HKCR | HKU | HKCC]
SubKey The full name of a registry key under the selected ROOTKEY.

ValueName The value name, under the selected Key, to delete.

When omitted, all subkeys and values under the Key are deleted.

Examples: delete HKLM\Software\WSABLogs /v LocalDrop

Deletes the registry value LocalDrop under the key HKLM\Software\WSABLogs

Appendix B

The GUI version of WSABLogs is named WSALogs. It is available at
http://download.webroot.com/wsalogs.exe

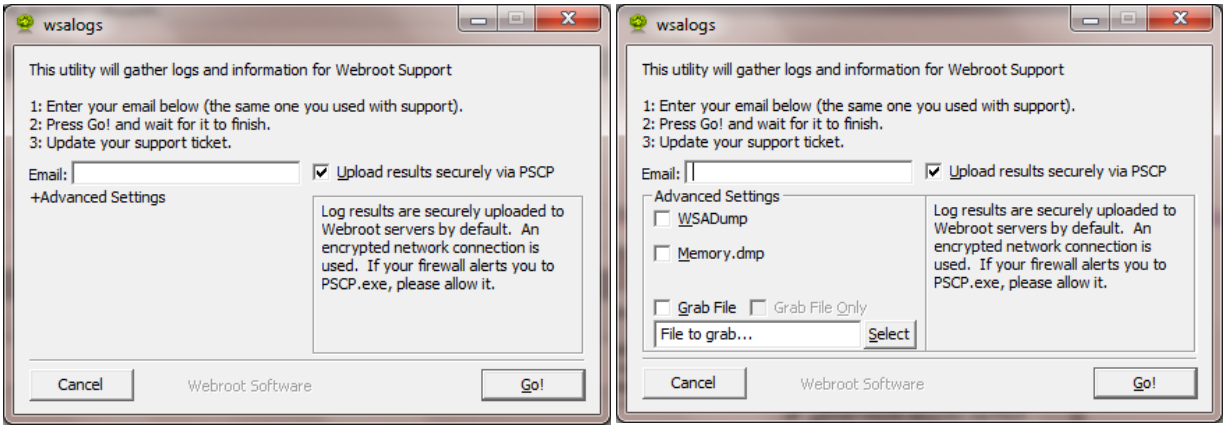
WSALogs.exe is designed to be run directly from the desired computer and requires direct user interaction, and not sent to the endpoint using the portal Agent Commands. The user will need to enter an Email address or any other identifying information in the "Email" field, and can click the "Go!" button. The utility will run and display progress information for both data gathering and compression status, as well as time to complete upload results via PSCP (useful when a large memory dump is being uploaded and you want to know the time for it to complete).

The logs collected by WSALogs are uploaded to Webroot via PSCP, unchecking the box "Upload results securely via PSCP" will disable that feature. A copy of the logs is always saved to the Desktop of the user account the logs are run from. The WSALogs utility output filename will be in the format:
wsalogs_EmailAddr_MM-DD-YYYY-HH.MM.7z

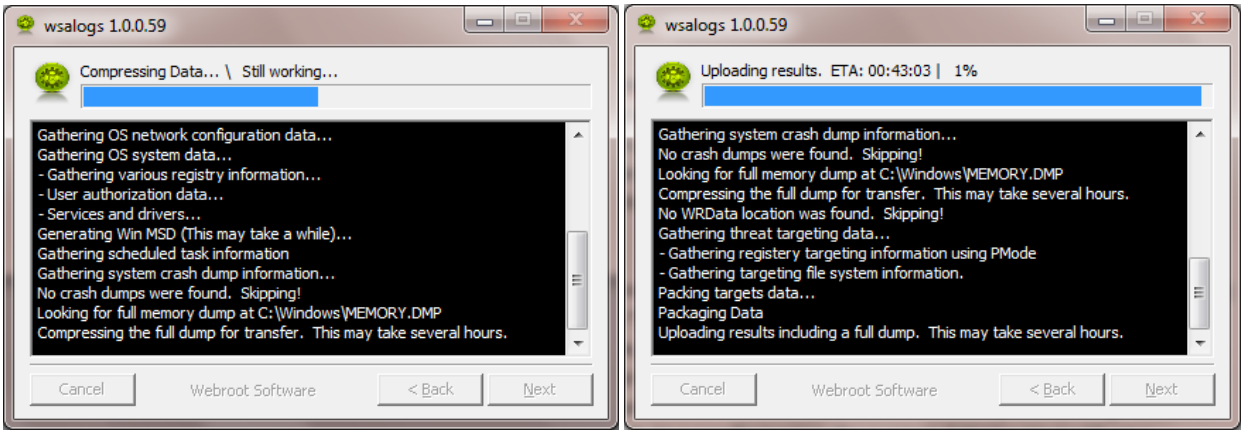
Advanced Settings can be accessed by clicking on "+Advanced Settings", which reveals the following options:

Option	Description
`WSADump`	Dumps the current state of the Webroot WRSA.exe processes from memory *Note:* This feature is only available in WSALogs and not WSABLogs. It is designed to capture the current operation of the Webroot product where an issue with the product at that exact moment is occurring, such as a scan that is not completing or the operation of the program is causing a system conflict.
`Memory.dmp`	Collects a Full (Or Kernel) Crash Dump if present
`Grab File`	Use in order to select a specific file to send to Webroot from the computer. Click the Select button to choose a file.
`Grab File Only`	Only the file grabbed using File Grab will be packaged. No other logs or system data will be collected. Use this to send a single file.

The WSALogs.exe initial screen, and the expanded "+Advanced Settings" options:



Progress screens – Compression operation and Upload ETA are shown:



When the utility completes, the user clicks Finish in the final window to close the program. If the check box “Go to the support page when I click Finish” is not cleared, then the Webroot support page opens. Note that the results of the PSCP upload are displayed on the final screen as well with the line “Automatic log upload Successful” if the upload process was successful, otherwise an “Automatic log upload Failed” message is displayed: