Product Guide

McAfee GetSusp

Version 3.x

Contents

Preface **5**
About this guide 5
Audience 5
Conventions 5
Find product documentation 6

Introducing GetSusp **7**
How GetSusp works 7
Benefits 8
Features 8
System requirements 8
Understanding the GetSusp user interface 9
How to use GetSusp 11
Get ready to participate 11
Download GetSusp 11
Scan and submit suspicious files 12
Interpreting scan results 12
Review scan results and upload suspicious files 14

Frequently asked questions **15**

Preface

This guide provides the information you need to configure, use, and maintain your McAfee GetSusp.

About this guide

This information describes the guide's target audience, the typographical conventions and icons used in this guide, and how the guide is organized.

Audience

McAfee documentation is carefully researched and written for the target audience.

The information in this guide is intended primarily for:

- **Customers and Partners** — People who use our product.
- **Security Officers** — People who determine sensitive and confidential data, and define the corporate policy that protects the company's intellectual property.
- **Reviewers** — People who evaluate the product.

Conventions

This guide uses the following typographical conventions and icons.

Book title or *Emphasis*	Title of a book, chapter, or topic; introduction of a new term; emphasis.
Bold	Text that is strongly emphasized.
`User input, Path,` or `Code`	Commands and other text that the user types; the path of a folder or program; a code sample.
Hypertext	A live link to a topic or to a website.
Note:	Additional information, like an alternate method of accessing an option.
Tip:	Suggestions and recommendations.
Important/Caution:	Valuable advice to protect your computer system, software installation, network, business, or data.
Warning/Danger:	Critical advice to prevent bodily harm when using a hardware product.

Find product documentation

McAfee provides the information you need during each phase of product implementation, from installation to daily use and troubleshooting. After a product is released, information about the product is entered into the McAfee online KnowledgeBase.

1 Go to the McAfee Technical Support ServicePortal at http://mysupport.mcafee.com.

2 Under **Self Service**, access the type of information you need:

To access...	Do this...
User documentation	**1** Click **Product Documentation**. **2** Select a **Product**, then select a **Version**. **3** Select a product document.
KnowledgeBase	▪ Click **Search the KnowledgeBase** for answers to your product questions. ▪ Click **Browse the KnowledgeBase** for articles listed by product and version.

Introducing GetSusp

When an undetected piece of malware infects users' systems, they often do not have the technical skills to troubleshoot their infected system. With a plethora of free diagnostic tools available, users have less or no knowledge of these tools to infer their output. The onus is on the infected user to isolate a suspect sample and figure out the method of submission of the files to the AV vendor.

McAfee® GetSusp is a tool that identifies suspicious files on a given system. While competitive tools provide information about system state and are dependent on user's technical skills, McAfee GetSusp is the first tool to be able to collect suspect samples with reasonable accuracy.

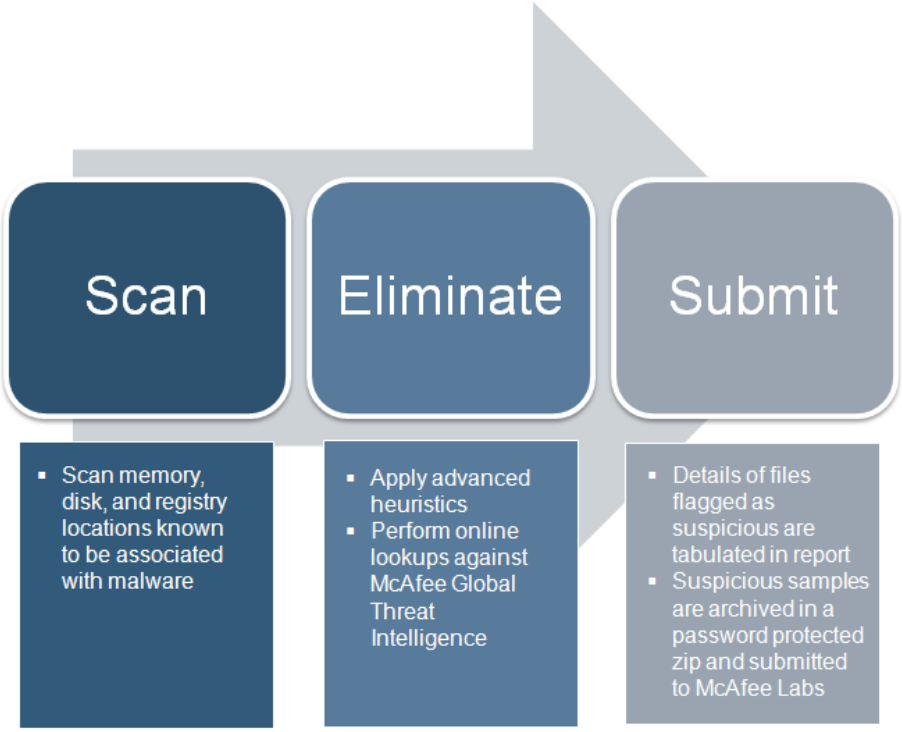
Contents

- *How GetSusp works*
- *How to use GetSusp*
- *Frequently asked questions*

How GetSusp works

GetSusp uses a combination of clever heuristics and queries McAfee Global Threat Intelligence to gather suspicious files on the affected system. GetSusp eliminates the need for deep technical knowledge of systems to isolate undetected malware and we recommend it as a tool of first choice when analyzing a suspect system.

GetSusp performs these actions and submits the suspicious zip file to McAfee.



Benefits

For consumers and enterprise users infected with undetected malware - a user only needs to download GetSusp and run it on their system. With click of a single button, GetSusp scans the system in less than 3 minutes, gathers suspect files, password protects files into a zip archive, and automatically submits files to McAfee Labs for analysis.

Features

GetSusp brings to you these features:

- Available as a single executable file with no installation required
- Option to run in different modes – GUI and command line
- Allows submission of samples or only a MD5 list of the files to McAfee Labs
- Checks each file against McAfee Global Threat Intelligence to determine if the sample is clean or suspicious
- Records system and installed McAfee product information like date of execution, environment variables, and details of suspected files

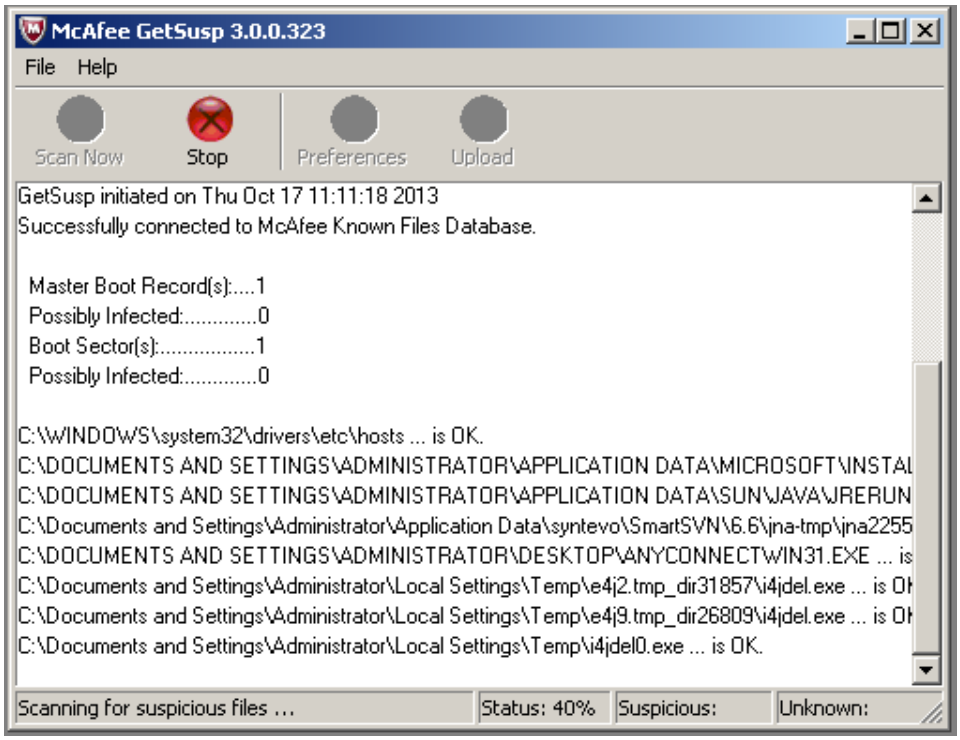
System requirements

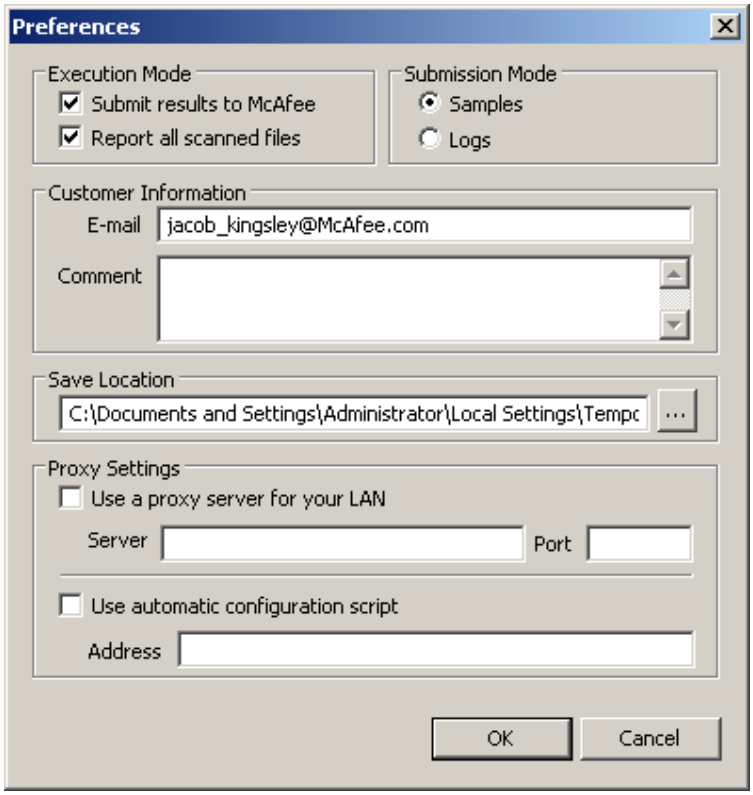
Make sure to check for these requirements to use GetSusp.

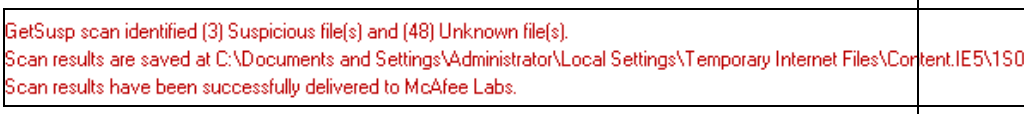
Component	Requirements
Operating system	One of the following Microsoft operating systems: ▪ Windows XP SP2 ▪ Windows 2003 SP2 ▪ Windows Vista SP1 ▪ Windows 2008 SP1 ▪ Windows 7 and 8
Web Browser	One of the following: ▪ Microsoft Internet Explorer, version 6 or later ▪ Mozilla Firefox, version 1.0 or later
Hardware	▪ System memory — 1 GB for scanning operations ▪ At least 100MB of available disk space ▪ At least 100MB of hard disk space for temporary files ▪ Network card

Understanding the GetSusp user interface

The GetSusp user interface is user-friendly and simple.





Option	Definition
File	Enables you to save a report or close GetSusp ▪ **Save report to file —** Saves the scan report as a .txt to a system location. ▪ **Close —** Closes the GetSusp tool.
Help	Provides help to use GetSusp ▪ **Command Line Help —** Provides cli commands that can be used to perform various tasks. ▪ **Check Latest Version —** Allows you to download the latest version of GetSusp from the McAfee downloadcenter site. ▪ **About GetSusp —** Specifies GetSusp version details.
 **Scan Now**	Scans the system memory, disk, and registry locations known to be associated with malware
 **Stop**	Stops the current scan process for suspicious files
 **Preferences**	Specifies customer details and mode of submitting the suspicious files ▪ **Execution Mode —** Specifies whether the .zip file is submitted online to McAfee. By default, the **Submit results to McAfee** and **Report all scanned files** checkboxes are selected. ▪ **Submission Mode —** Specifies if you wish to submit the complete samples or only logs to McAfee. ▪ **Customer Information —** Specifies details like email address and comments. ▪ **Save Location —** Specifies the location of the suspicious file on the system. The file is saved in .zip format. ▪ **Proxy Settings —** Specifies server and port details for the proxy server.
 **Upload**	Enables you to browse to the zip location and submit the suspicious file to McAfee.
Scanning window	Displays the scan in progress and results. During the scan, you can view the file reputation as **OK**, **Suspicious**, or **Unknown**. The **OK** status depicts that these files are known to the McAfee database.  The scan results are saved as a zip file on the system and the submitted files become a part of the McAfee Labs test environment.

How to use GetSusp

You can scan systems, review scan reports, and submit suspicious files to McAfee.

Contents

- *Get ready to participate*
- *Download GetSusp*
- *Scan and submit suspicious files*
- *Interpret scan results*
- *Review scan results and upload suspicious files*

Get ready to participate

Make sure to follow these guidelines prior to using GetSusp.

- GetSusp is free and open to everyone.
- GetSusp requires an internet connection to perform optimally. Outbound UDP port 53 and TCP port 80 must be allowed for McAfee GTI File Reputation and GTI lookups to happen.
- GetSusp identifies suspicious executable files. Scanning of documents, scripts, media and other file formats are unsupported.
- Malware must be actively running on the system or have an associated registry startup entry for GetSusp to identify it.
- Suspicious zip file must be under 10MB for submission to McAfee Labs.
- Rootkit scanning is unsupported and is planned for future releases.

Download GetSusp

Download GetSusp from the McAfee site.

Task

1 Go to McAfee Downloads and download the GetSusp.exe file.

2 Extract the files, navigate to the folder, and view the files.

Scan and submit suspicious files

Make sure to set the preferences for the scan and locations for the scan reports. The scan report is submitted to McAfee Labs.

1 Navigate to the location and double-click the **getsusp** icon.

2 The McAfee GetSusp window is displayed.

3 Click **Preferences** to select the options for execution and sample submission mode. By default, files are submitted to McAfee Labs in online mode. Click **OK**.

4 Click **Scan Now** to begin scanning the system for suspicious files.

5 On the License Agreement window, accept the license agreement. Click **OK**.

6 The Scanning window displays the scan initiation, progress, and scan results.

The scan report files are zipped and uploaded to McAfee Labs via HTTPS whenever GetSusp scans in online mode.

Note The default password for the zip file is **infected**.

Interpreting scan results

The scan results display suspicious and unknown files. When the scan is in progress, the known files are displayed as **OK**.

Additional information on network statistics and installed McAfee products is provided in the logs. Visit the McAfee malware community site or contact technical support for further help in troubleshooting your machine or removing malware.

Discarding files before an upload

You can review the scan results and decide on the files to upload to McAfee. Navigate to the scanned result zip file on your system, use WinRAR or 7Zip to open the zip file, and remove files from the archive. Upload the updated archive to McAfee.

Scan logs

If a scan stops or gets interrupted before completion, you can view the logs that are stored in the same location from where GetSusp is launched. The scan details are displayed.

McAfee GetSusp Scan Results

To download the tool, visit the McAfee Labs Tools website

Suspicious Files

Status	MD5	Location	File Name	Attribute	Company	Description	Product Version	File Version	File Size	Creation Date	Modification Date	Type
TROJAN	14c0219e88bfcd82984a0f1873d78456	C:\Windows\Temp	cvasds0.dll	HRS					78,336	10/15/2009 16:36	06/21/2010 17:19	Module
TROJAN	4db35b0509644b3acd1bf45a9bc79615	C:\Windows\Temp	dsoqq.exe	HRS					116,736	05/24/2010 14:46	06/21/2010 17:04	Run-Key
ASSUMED_DIRTY	f9467725075c79740ddc1a60bf070a42	C:\Windows\Temp	herss.exe	HRS					115,200	10/15/2009 16:36	03/04/2010 15:17	Run-Key
ASSUMED_DIRTY	3333e8f22023aaf4c9d8551b00bae036	C:\Windows\Temp	nodqq.exe	HRS					128,512	04/20/2010 20:54	04/20/2010 20:54	Run-Key
UNKNOWN	32c26310eb2166dc88bfddb05c671c11	C:	autorun.inf	HRS					51	10/15/2009 16:36	06/21/2010 17:37	

Need help or advice removing malware? Visit the McAfee Community

Review scan results and upload suspicious files

You can scan the systems, review the scan results, and then decide to upload suspicious files. In case you are offline, you can choose to upload the files manually at a later point of time.

1 Navigate to the GetSusp folder and double-click the **getsusp** icon.

2 The McAfee GetSusp window is displayed.

3 Click **Preferences** and select the options for execution and submission mode for samples or logs. Deselect the **Submit results to McAfee** checkbox. Click **OK**.

Note

If you deselect the **Report all scanned files**, only the **Unknown** and **Suspicious** files are displayed in the scan results.

4 Click **Scan Now** to begin scanning the system for unknown files.

5 On the License Agreement window, accept the license agreement. Click **OK**.

6 The Scanning window displays the scan initiation, progress, and results for the scanned system.

7 Navigate to the location of the scan report and review the files to be submitted.

8 Click **Upload** and browse to the zip file. Click **Open** and then click **OK**.

Frequently asked questions

This section provides you with answers to a few frequently asked questions about GetSusp.

What user or system details are collected?

Email address, machine name, IP address, operating system and service pack, file location, and information about installed McAfee products are collected. Users who do not want to transmit samples, system data or share their email address with McAfee can choose the option within the GetSusp tool to not submit results to McAfee.

Your email address will enable McAfee to communicate with you regarding the results of the scan.

How does GetSusp complete a system scan in three to five minutes?

Targeted scanning of running processes, registry, and file locations utilized by malware to start up ensures that GetSusp completes a system scan in three to five minutes irrespective of the size of the hard disk.

Note

Malware must be actively running on the system or have an associated registry startup entry for GetSusp to identify it.

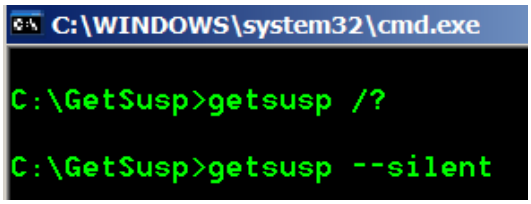
How do I follow up with McAfee for support on a GetSusp submission?

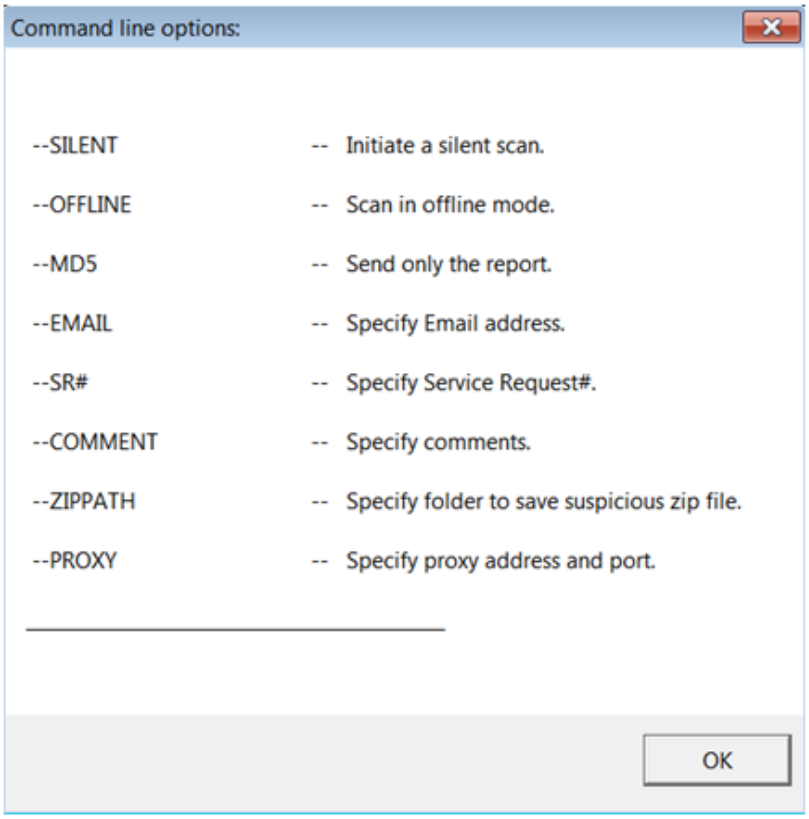
GetSusp submissions with an email address receive an acknowledgement and work item ID from McAfee Workflow systems for tracking purposes. This work item ID can be used to follow up with support team.

Does GetSusp support command line parameters?

Yes, GetSusp supports command line parameters.

At the command prompt, type **/?** The command line help options are displayed.

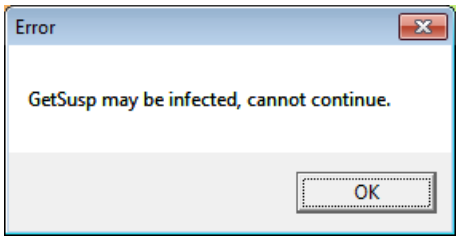




Example:

```
Getsusp.exe --silent --email=john_doe@mcafee.com --zippath="C:\GetSusp"
```

When I run GetSusp on a system infected with a file infector such as W32/Sality or W32/Virut, GetSusp is infected. It does not execute and pops a message *GetSusp may be infected, cannot continue*.



GetSusp.exe is digitally signed and prior to execution performs integrity checks. To execute GetSusp on a system infected with a file infector, run it using the `getsusp.exe --nc` switch. This hidden switch disables integrity check.