



Product Guide

# McAfee GetSusp

Product version 4.0.0

**COPYRIGHT LICENSE INFORMATION**

Copyright © 2013-2020 McAfee, LLC. YOUR RIGHTS TO COPY AND RUN THIS TOOL ARE DEFINED BY THE MCAFEE SOFTWARE ROYALTY-FREE LICENSE FOUND ON MCAFEE.COM WEBSITE. IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH BY THAT AGREEMENT, THEN DO NOT INSTALL THE SOFTWARE OR STOP ALL USE AND UNINSTALL THE SOFTWARE.

**TRADEMARK ATTRIBUTIONS**

McAfee and the McAfee logo are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the United States and other countries. Other names and brands may be claimed as the property of others.

# Contents

	<b>Preface</b>	<b>4</b>
	About this guide .....	4
	Conventions .....	4
	Find product documentation .....	5
<b>1</b>	<b>Introducing GetSusp</b>	<b>6</b>
	How GetSusp works .....	6
	Benefits.....	6
	Features.....	7
	System requirements.....	7
	Understanding the GetSusp user interface .....	7
<b>2</b>	<b>How to use GetSusp</b>	<b>11</b>
	Get ready to participate.....	11
	Download GetSusp.....	11
	Scan and submit suspicious files .....	11
	Interpreting scan results .....	13
	Discarding files before an upload.....	13
	Scan logs.....	13
	Review scan results and upload suspicious files.....	15
<b>3</b>	<b>Frequently asked questions</b>	<b>16</b>
	<b>Index</b>	<b>18</b>

# Preface

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

## Contents

- ▶ *About this guide*
- ▶ *Find product documentation*





---

## 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.

## Conventions

This guide uses these typographical conventions and icons.

<i>Italic</i>	Title of a book, chapter, or topic; a new term; emphasis
<b>Bold</b>	Text that is emphasized
Monospace	Commands and other text that the user types; a code sample; a displayed message
<b>Narrow Bold</b>	Words from the product interface like options, menus, buttons, and dialog boxes
Hypertext blue	A link to a topic or to an external website
	<b>Note:</b> Extra information to emphasize a point, remind the reader of something, or provide an alternative method
	<b>Tip:</b> Best practice information
	<b>Caution:</b> Important advice to protect your computer system, software installation, network, business, or data
	<b>Warning:</b> Critical advice to prevent bodily harm when using a hardware product

---

## Find product documentation

Release Notes : Refer [KB91065](#)

FAQs : Refer [KB69385](#)

Product Guide : Refer [KB91941](#)

# 1

## 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.

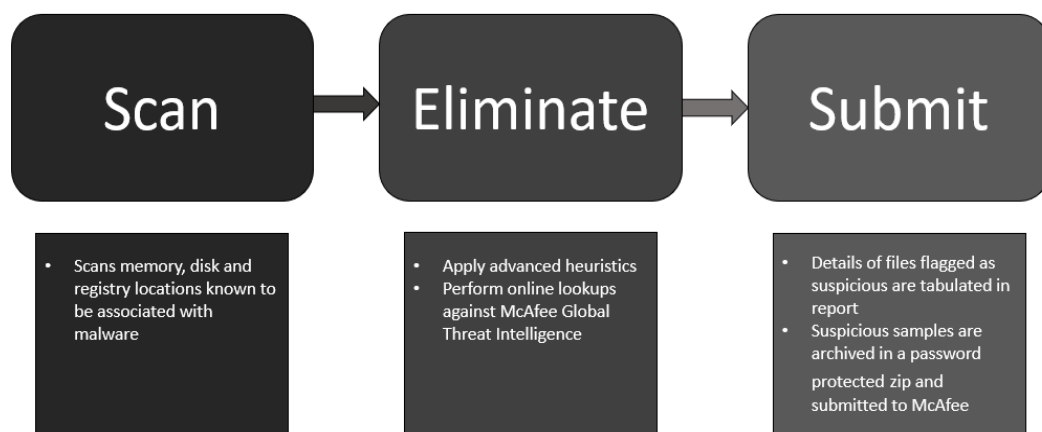
McAfee® GetSusp is a tool that identifies suspicious files on a given system. While competitive tools provide information about system state and are dependent on user's technical skills, McAfee GetSusp is the first tool to be able to collect suspect samples with reasonable accuracy.

---

### 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 for analysis.

## Features

GetSusp brings to you these features:

- Available as a single executable file [32bit and 64bit] with no installation required
- Option to run in different modes – GUI, command line and in ePO
- Scans a URL or URLs in text file to identify suspicious and unknown URL(s) in GUI mode
- Scans files associated with Office applications and PDF files in GUI mode
- Allows submission of samples or only a MD5 list of the files to McAfee
- Checks each file against McAfee Global Threat Intelligence to determine if the sample is clean or suspicious
- Option to select files from the identified suspicious list before sending to McAfee in GUI mode for Default, Custom and Document Scan Options when Submit results to McAfee is checked in Preferences.
- Records system and installed McAfee product information like date of execution, environment variables, and details of suspected files

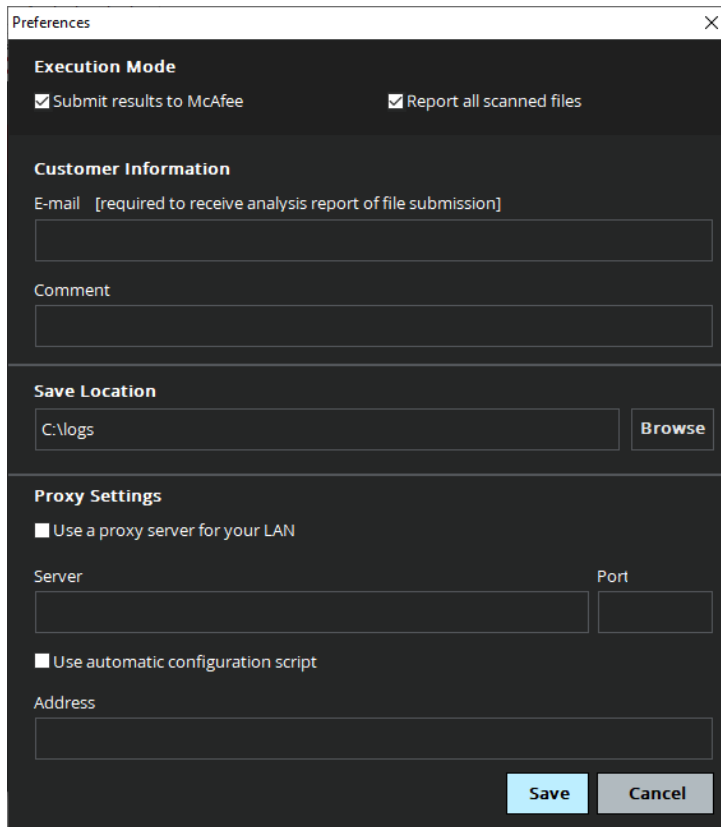
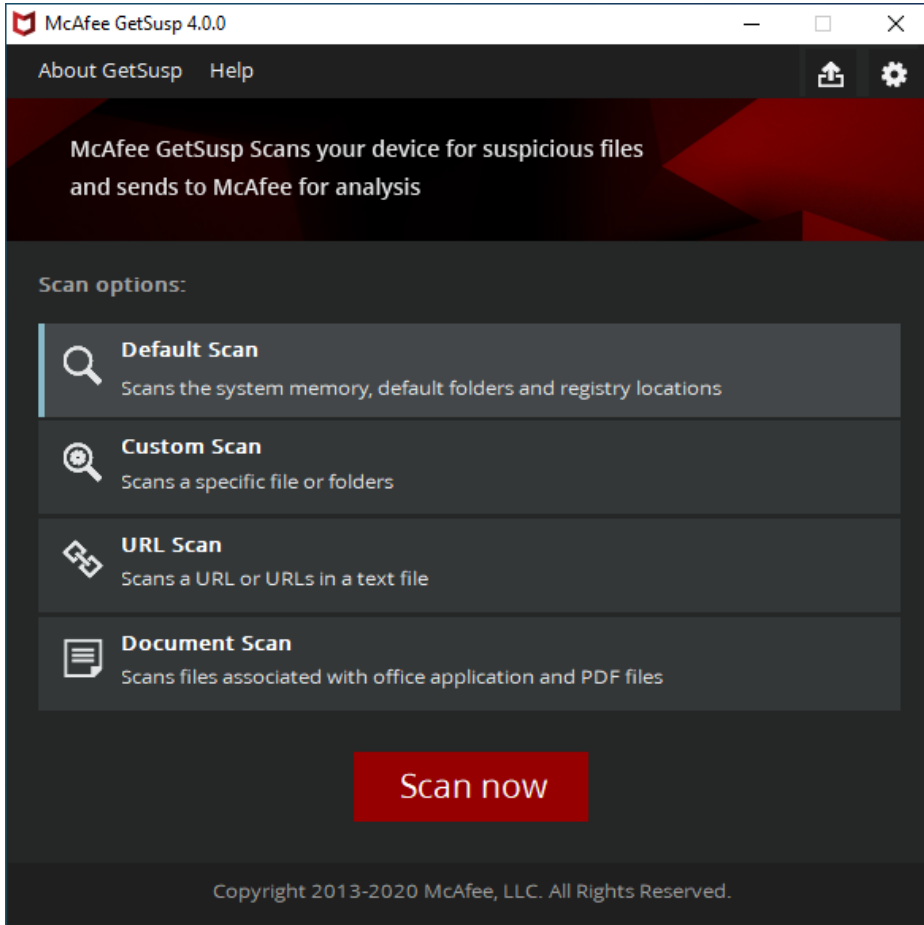
## System requirements

Make sure to check for these requirements to use GetSusp.

Component	Requirements
Operating system	One of the following Microsoft operating systems: <ul style="list-style-type: none"> <li>• Windows Server 2008 R2 SP1</li> <li>• Windows Server 2012</li> <li>• Windows Server 2016</li> <li>• Windows 7, 8, 8.1 &amp; Win10 (RS1, RS2, RS3, RS4, RS5, RS6),19H1</li> </ul>
Web browser	One of the following: <ul style="list-style-type: none"> <li>• Microsoft Internet Explorer, version 6 or later</li> <li>• Mozilla Firefox, version 1.0 or later</li> </ul>
Hardware	<ul style="list-style-type: none"> <li>• System memory — 1 GB for scanning operations</li> <li>• At least 100MB of available disk space</li> <li>• At least 100MB of hard disk space for temporary files</li> <li>• Network card</li> </ul>
ePO	5.3.2, 5.3.0, 5.9, 5.10

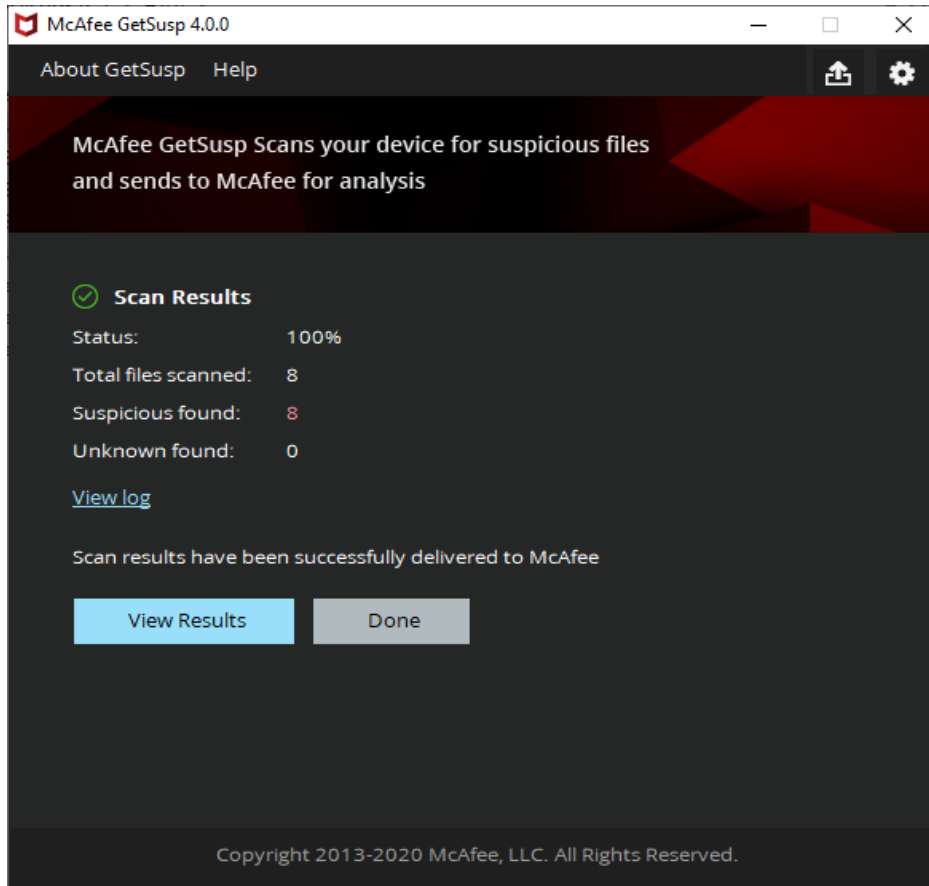
## Understanding the GetSusp user interface

The GetSusp user interface is user-friendly and simple.

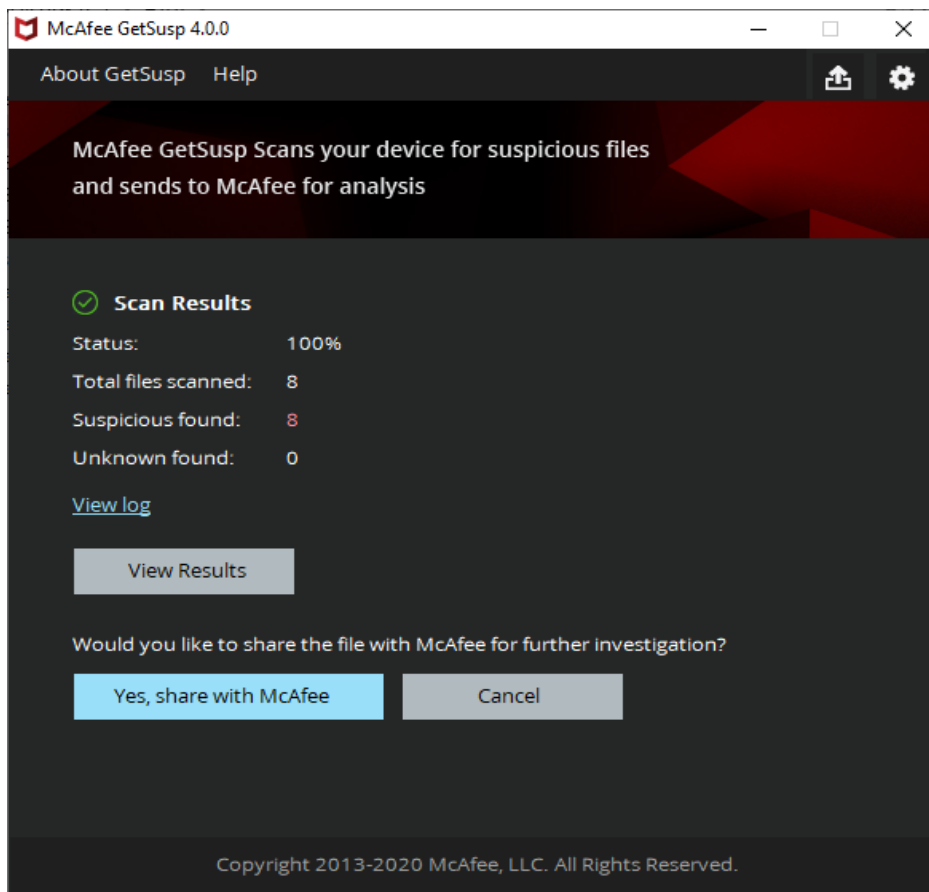


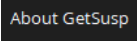



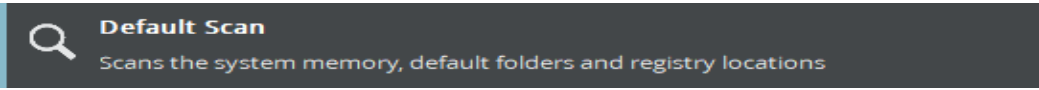


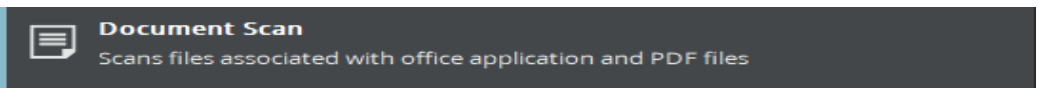

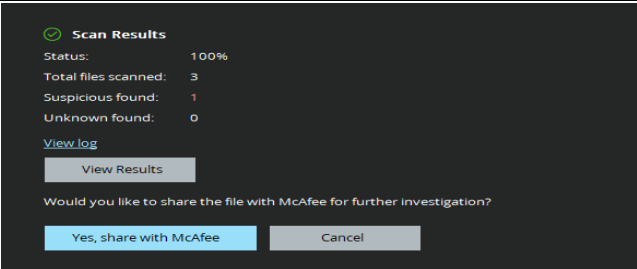


## Scan Results with “Submit results to McAfee” checked in Preferences



## Scan Results with “Submit results to McAfee” Unchecked in Preferences



Option	Definition
	<p><b>About GetSusp</b> Specifies GetSusp version details.</p>
	<p><b>Help</b> Provides the list of Command Line options.</p>
	<p><b>Send to McAfee</b> Enables user to send a .zip file to McAfee for analysis by browse, select and upload.</p>
	<p><b>Preferences</b> Specifies customer details and mode of submitting the identified suspicious files.</p> <ul style="list-style-type: none"> <li>• <b>Execution Mode</b> — Specifies whether the identified suspicious file is submitted online to McAfee. By default, the Submit results to McAfee and Report all scanned files checkboxes are selected.</li> <li>• <b>Customer Information</b> — Specifies details like email address and comments.</li> <li>• <b>Save Location</b> — Specifies the location of the result files on the system.</li> <li>• <b>Proxy Settings</b> — Specifies server and port details for the proxy server.</li> </ul>
<p>Scan Options : Default Scan</p>	
<p>Scan Options : Custom Scan</p>	
<p>Scan Options : URL Scan</p>	
<p>Scan Options : Document Scan</p>	
<p>Scan Results with “Submit results to McAfee” checked in Preferences</p>	 <p>Displays Scan results with Total files scanned, suspicious found and Unknown found. View log – Link to Open log file from results folder View Results – Opens Results folder</p>
<p>Scan Results with “Submit results to McAfee” Unchecked in Preferences</p>	 <p>Yes, share with McAfee – Enables to share the file to McAfee after scan completion</p>

# 2

## 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*
- ▶ *Interpreting scan results*
- ▶ *Review scan results and upload suspicious files*

---

## Get ready to participate

### Before you begin

- 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, URLs and document files. Scanning of 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 50MB for submission to McAfee.
- Rootkit scanning is unsupported.

---

## Download GetSusp

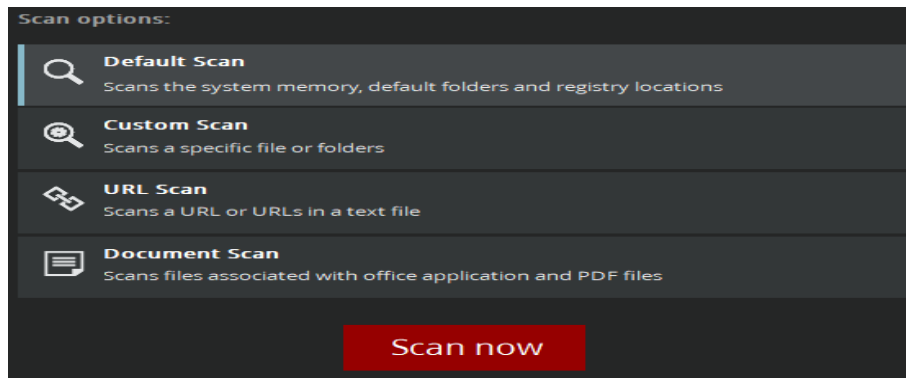
Download GetSusp from the McAfee site.

### 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.



### Scan Options - Default Scan

- 1 Navigate to the location and double-click the **getsusp** icon.
- 2 The McAfee GetSusp window is displayed.
- 3 Select **Default Scan** from **Scan Options** to scan the system memory, default folders and registry locations associated with suspicious files.
- 4 Click **Scan now** to start scanning
- 5 On the License Agreement window, accept the license agreement. Click **OK**.
- 6 The Scanning window displays the scan initiation, progress, and scan results.
- 7 After scan completion, GetSusp ZipFilter popup provides an option to include/exclude identified suspicious files in the process of zip creation. [ZipFilter popup displayed only when "Submit results to McAfee" is checked in Preferences screen].  
The scan report files are zipped and uploaded to McAfee via HTTPS whenever GetSusp scans in online mode ["Submit results to McAfee" is checked in Preferences screen].

### Scan Options - Custom Scan

- 1 Navigate to the location and double-click the **getsusp** icon.
- 2 The McAfee GetSusp window is displayed.
- 3 Select **Custom Scan** from **Scan Options** to scan a file or to select folders to scan.
- 4 Click **Scan now** to provide a specific file or select folders for scanning.
- 5 On the License Agreement window, accept the license agreement. Click **OK**.
- 6 The Scanning window displays the scan initiation, progress, and scan results.
- 7 After scan completion, GetSusp ZipFilter popup provides an option to include/exclude identified suspicious files in the process of zip creation. [ZipFilter popup displayed only when "Submit results to McAfee" is checked in Preferences screen].  
The scan report files are zipped and uploaded to McAfee via HTTPS whenever GetSusp scans in online mode ["Submit results to McAfee" is checked in Preferences screen].

### Scan Options - URL Scan

- 1 Navigate to the location and double-click the **getsusp** icon.
- 2 The McAfee GetSusp window is displayed.

- 3 Select **URL Scan** from **Scan Options** to scan a URL or URLs in a text file.
- 4 Click **Scan now** to provide a specific URL or select a text file with list of multiple URLs [one URL in each line] for scanning and click **Scan**
- 5 On the License Agreement window, accept the license agreement. Click **OK**.
- 6 The Scanning window displays the scan initiation, progress, and scan results.  
Identified unknown URLs list if any, are uploaded to McAfee via HTTPS whenever GetSusp scans in online mode ["Submit results to McAfee" is checked in Preferences screen].



URL scan will work only with internet connection available.

Analysis report will not be sent by mail for unknown URL submission.

If unknown URL(s) fails to deliver to McAfee, user needs to retry scanning to upload again.

### Scan Options - Document Scan

- 1 Navigate to the location and double-click the **getsusp** icon.
- 2 The McAfee GetSusp window is displayed.
- 3 Select **Document Scan** from **Scan Options** to scan files associated with Office application and PDF files.
- 4 Click **Scan now** to provide a specific file or select folders for scanning.
- 5 On the License Agreement window, accept the license agreement. Click **OK**.
- 6 The Scanning window displays the scan initiation, progress, and scan results.
- 7 After scan completion, GetSusp ZipFilter popup provides an option to include/exclude identified suspicious files in the process of zip creation. [ZipFilter popup displayed only when "Submit results to McAfee" is checked in Preferences screen].

The scan report files are zipped and uploaded to McAfee via HTTPS whenever GetSusp scans in online mode ["Submit results to McAfee" is checked in Preferences screen].

### Deployment using ePO

Refer [KB70405](#) for deployment instructions using ePolicy Orchestrator.

---

## 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

Default password for zip file is **infected**.

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 latest version of GetSusp [Click Here](#)

#### Suspicious Files

Status	MD5	SHA256	Location
ASSUMED_DIRTY4	<a href="#">2fe2cfb69a5e01fe828eea2d6f3119ae</a>	<a href="#">c533f0ce7ec50fb58cb3bcda0baf0b40c19a58d8e0ffb79e24d5e5cfbf2c</a>	<a href="#">C:\new folder\Artemis_Samples\Arte</a>
UNKNOWN	<a href="#">3194abc1e53e92844da835c68094d361</a>	<a href="#">0f1f0b3b38c30b04e1af4c34314ef47e5c548db0260f414b99ae1161861d1aaf</a>	<a href="#">C:\new folder\Artemis_Samples\Arte</a>
UNKNOWN	<a href="#">9d90f33e35579e05819ed7bd075725a7</a>	<a href="#">4abd7e706e45cb7235c83defa165deef6cd8341e798afb8a2a78044d404a57cb</a>	<a href="#">C:\new folder\Artemis_Samples\Arte</a>
UNKNOWN	<a href="#">6c4713abfdd01e9aa0b47128e345ec4b</a>	<a href="#">22bc7ae5fd686f37a447395fbbffa33207f917c2b6a5125a968b679c94b8a966</a>	<a href="#">C:\new folder\Artemis_Samples\Arte</a>
UNKNOWN	<a href="#">9e83e3a46347e0b4f6e46bd5b0491587</a>	<a href="#">1d8479bb226dab64f2feaf431fb9412a917f8a737c0404cb77cf4e23fdd90c26</a>	<a href="#">C:\new folder\Artemis_Samples\Arte</a>
UNKNOWN	<a href="#">6b6d7729b4236cf3e4ee7e62d1959ef3</a>	<a href="#">e44d7ca317e0c47446c6974c62a1ecbcfb937ed26ddf324150d1c20bdd4b1b9f</a>	<a href="#">C:\new folder\Artemis_Samples\Arte</a>
UNKNOWN	<a href="#">67af21c0df673801bfb338b17574911</a>	<a href="#">f5062fa76871f67e59a32dfbaf1822099527dc380c3ef98136f8b2b4f7f9ccfb</a>	<a href="#">C:\new folder\Artemis_Samples\Arte</a>
UNKNOWN	<a href="#">fbda2f1192d39846335ace1b54f66a55</a>	<a href="#">ccb6327aba4ba97ee99b0f2aeb610a2058475e13cbdb7d61f820081582fa8453</a>	<a href="#">C:\new folder\Artemis_Samples\Arte</a>

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 [“Submit results to McAfee” is unchecked in Preferences screen] , you can choose to upload the files manually at a later point of time.

### Task

- 1 Navigate to the GetSusp folder and double-click the **getsusp** icon.
- 2 The McAfee GetSusp window is displayed.
- 3 Select the respective Scan Options and Click **Scan Now** to begin scanning the system for unknown files.



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

- 4 On the License Agreement window accept the license agreement. Click **OK**.
- 5 The Scanning window displays the scan initiation, progress, and results for the scanned system.
- 6 Navigate to the location of the scan report and review the files to be submitted.
- 7 Click on  **Send to McAfee**. Click browse to select and upload a zip file.

# 3

## Frequently asked questions

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

### What user or system details are collected?

Machine name, IP address, operating system and service pack, and information about installed McAfee products are collected. No user data, tracking or personal information are captured. Users who do not want to transmit samples or system data to McAfee can choose to run the scan in offline mode. The trade-off is degraded results as no online lookups to the whitelist database occur.

### 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.



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.

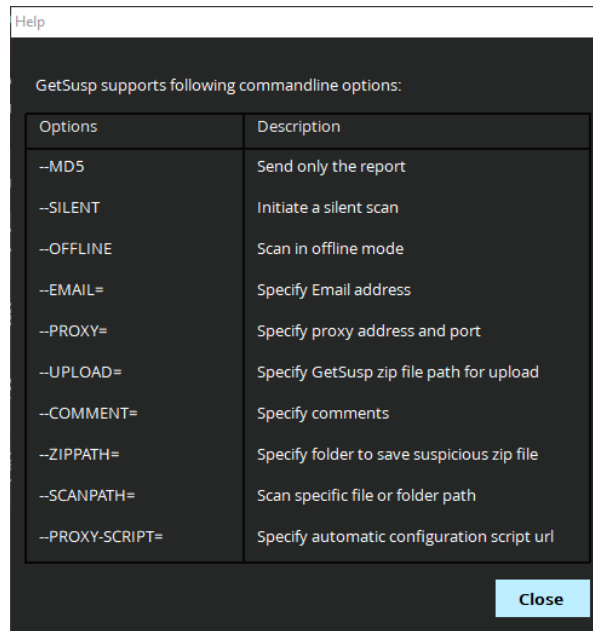
### Does GetSusp support command line parameters?

Yes, GetSusp supports command line parameters.

At the command prompt, type Help. The command line help is displayed.

```
Administrator: Command Prompt
C:\GetSusp>getsusp.exe /?
C:\GetSusp>getsusp.exe --silent
```





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.



# Index

## A

about this guide [4](#)

## C

conventions and icons used in this guide [4](#)

## D

documentation

product-specific, finding [6](#)

typographical conventions and icons [4](#)

## M

McAfee ServicePortal, accessing [5](#)

## S

ServicePortal, finding product documentation [5](#)

## T

technical support, finding product information [5](#)

