Product Guide

McAfee GetSusp

Product version 4.1.0

Contents

Preface

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

Contents

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.

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

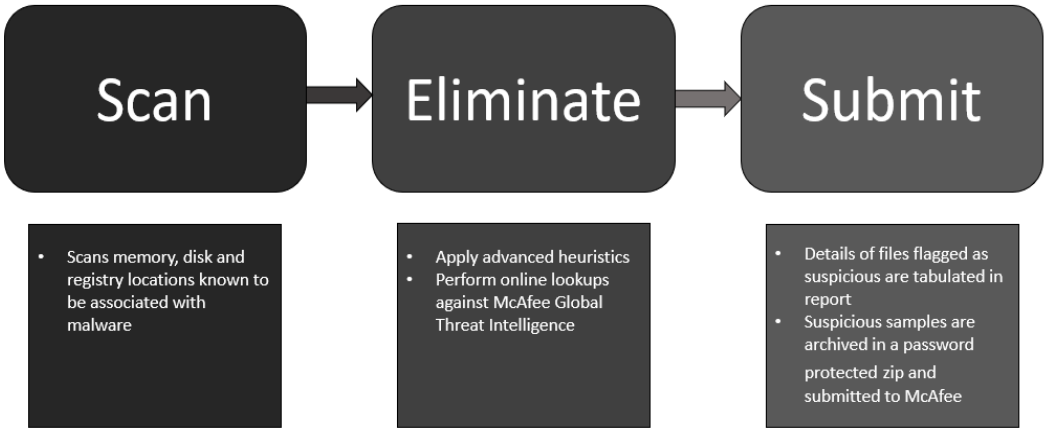
When an undetected piece of malware infects users' systems, they often do not have the technical skills to troubleshoot their infected system. With a plethora of free diagnostic tools available, users have less or no knowledge of these tools to infer their output. The onus is on the infected user to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

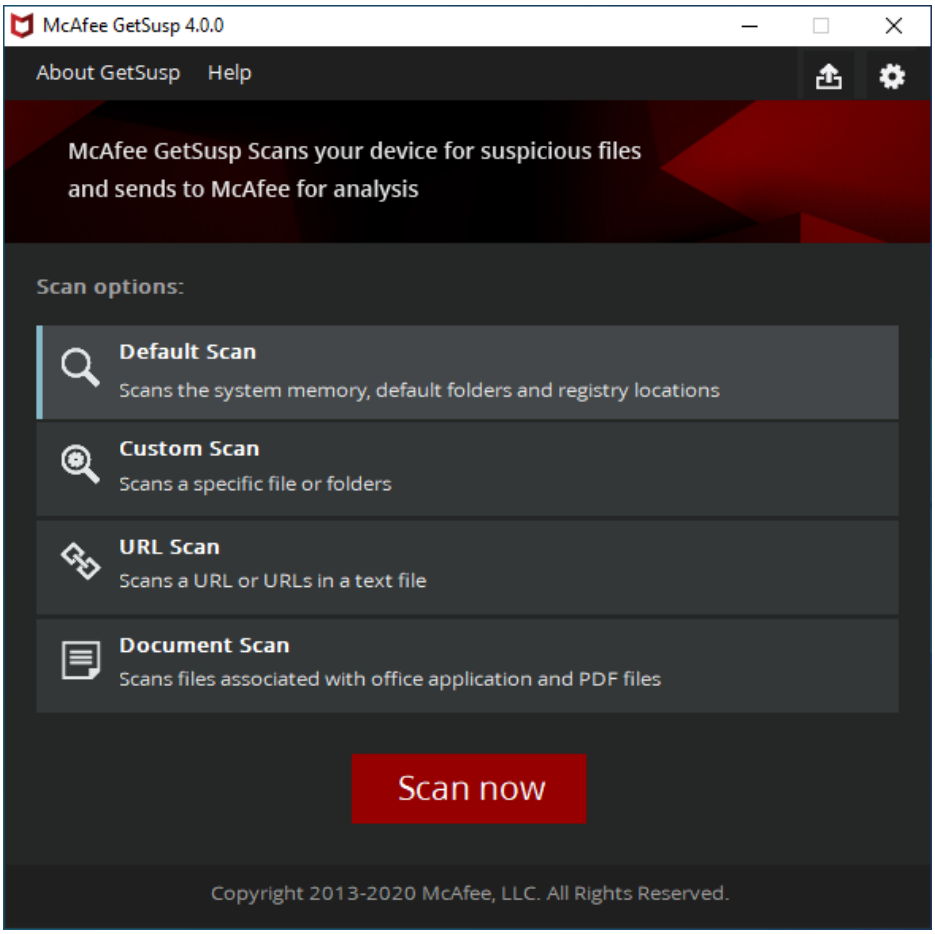
System requirements

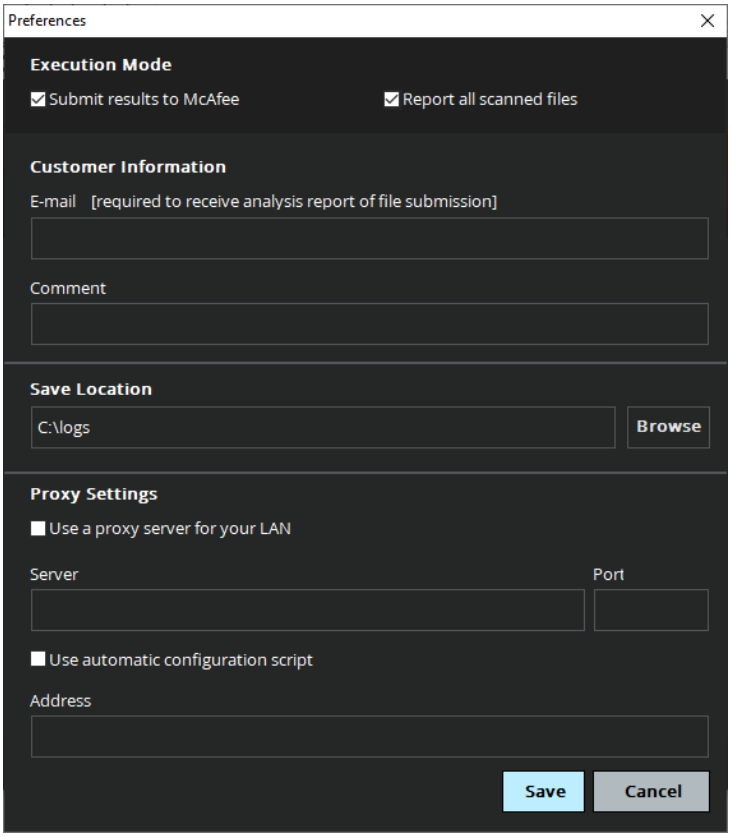
Make sure to check for these requirements to use GetSusp.

Component	Requirements
Operating system	One of the following Microsoft operating systems: • Windows Server 2008 R2 SP1 • Windows Server 2012 • Windows Server 2016,2019 • Windows 7, 8, 8.1 & Win10 (RS1, RS2, RS3, RS4, RS5, RS6),19H1, 20H1, 20H2, 21H1, 21H2
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
ePO	5.3.2, 5.3.0, 5.9, 5.10, Extension reports [5.10]

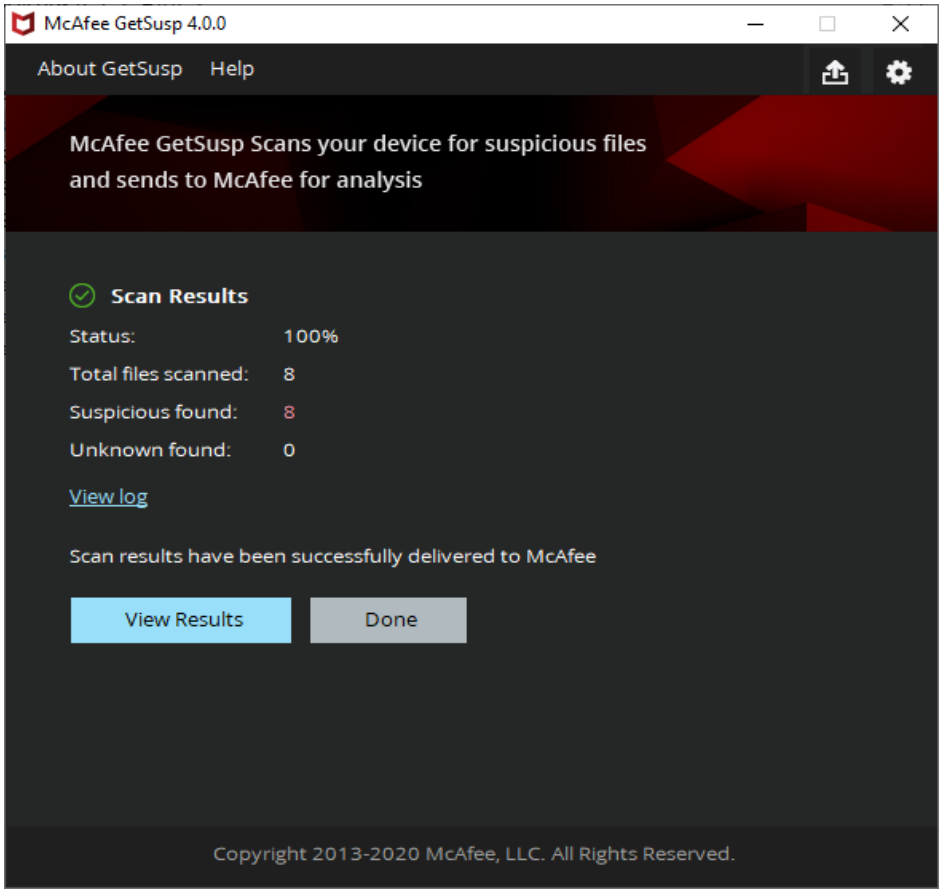
Understanding the GetSusp user interface

The GetSusp user interface is user-friendly and simple.

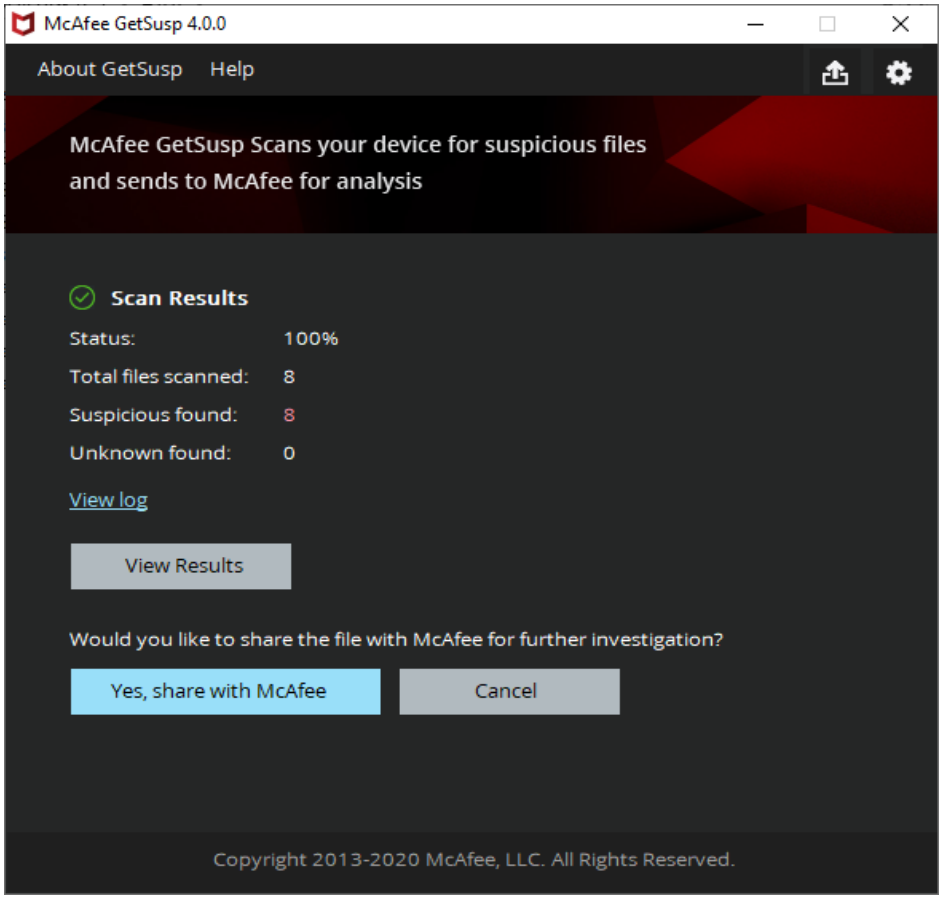

McAfee GetSusp 4.0.0
About GetSusp
Help
McAfee GetSusp Scans your device for suspicious files and sends to McAfee for analysis
Scan options:
Default Scan
Scans the system memory, default folders and registry locations
Custom Scan
Scans a specific file or folders
URL Scan
Scans a URL or URLs in a text file
Document Scan
Scans files associated with office application and PDF files
Scan now
Copyright 2013-2020 McAfee, LLC. All Rights Reserved.

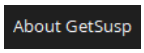
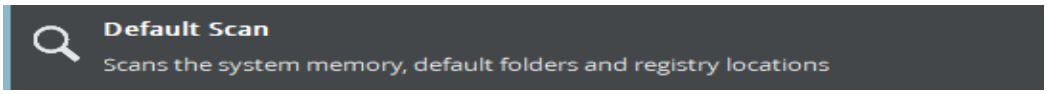
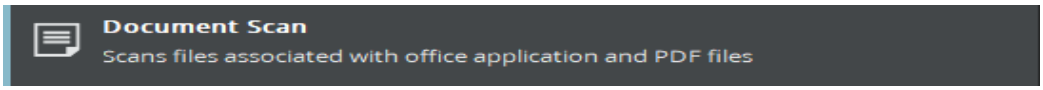
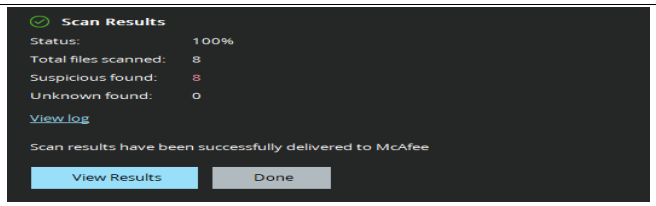
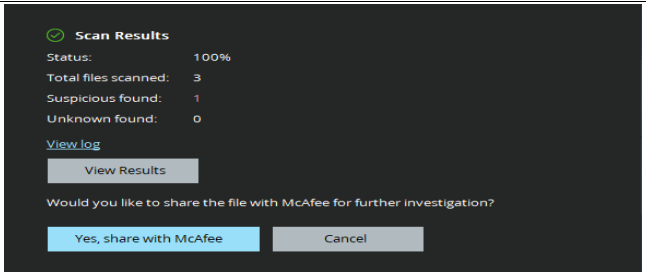

Preferences
Execution Mode
Submit results to McAfee
Report all scanned files
Customer Information
E-mail [required to receive analysis report of file submission]
Comment
Save Location
C:\logs
Browse
Proxy Settings
Use a proxy server for your LAN
Server
Port
Use automatic configuration script
Address
Save
Cancel

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



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



Option	Definition
	**About GetSusp** Specifies GetSusp version details.
	**Help** Provides the list of Command Line options.
	**Send to McAfee** Enables user to send a .zip file to McAfee for analysis by browse, select and upload.
	**Preferences** Specifies customer details and mode of submitting the identified suspicious files. • **Execution Mode** — 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. • **Customer Information** — Specifies details like email address and comments. • **Save Location** — Specifies the location of the result files on the system. • **Proxy Settings** — Specifies server and port details for the proxy server.
Scan Options : Default Scan	
Scan Options : Custom Scan	
Scan Options : URL Scan	
Scan Options : Document Scan	
Scan Results with “Submit results to McAfee” checked in Preferences	 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
Scan Results with “Submit results to McAfee” Unchecked in Preferences	 Yes, share with McAfee – Enables to share the file to McAfee after scan completion

2 How to use GetSusp

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

Contents

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.

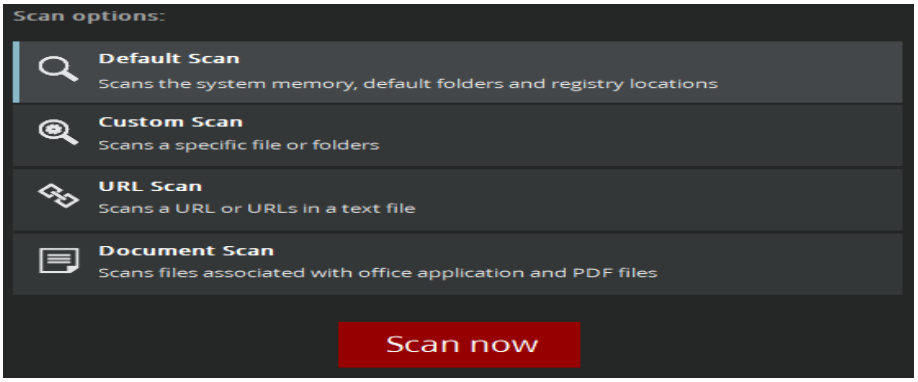
Task

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].

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.

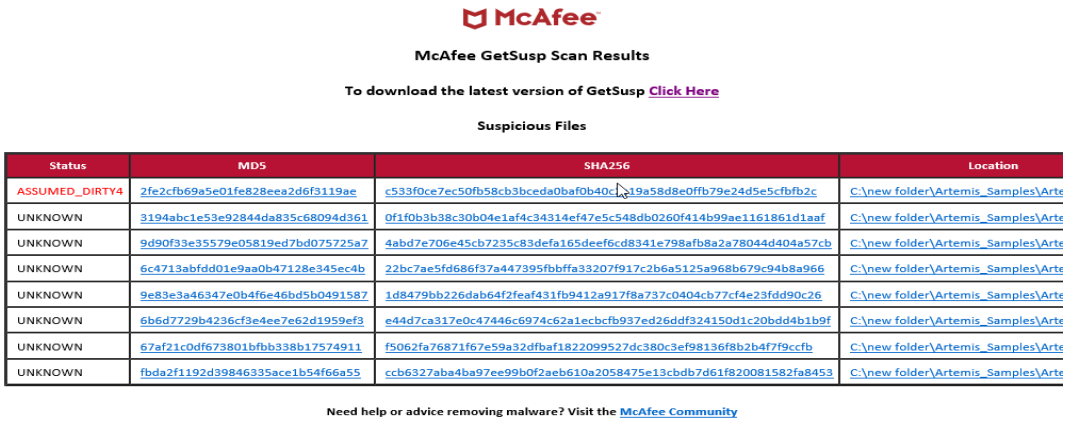
Discarding files before an upload

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

McAfee GetSusp Scan Results

To download the latest version of GetSusp Click Here

Suspicious Files

Status	MD5	SHA256	Location
ASSUMED_DIRTY4	2fe2cfb69a5e01fe828eea2d6f3119ae	c533f0ce7ec50fb58cb3bceda0baf0b40c...19a58d8e0ffb79e24d5e5cfbfb2c	C:\new folder\Artemis_Samples\Arte
UNKNOWN	3194abc1e53e92844da835c68094d361	0f1f0b3b38c30b04e1af4c34314ef47e5c548db0260f414b99ae1161861d1aaf	C:\new folder\Artemis_Samples\Arte
UNKNOWN	9d90f33e35579e05819ed7bd075725a7	4abd7e706e45cb7235c83defa165deef6cd8341e798afb8a2a78044d404a57cb	C:\new folder\Artemis_Samples\Arte
UNKNOWN	6c4713abfdd01e9aa0b47128e345ec4b	22bc7ae5fd686f37a447395fbbffa33207f917c2b6a5125a968b679c94b8a966	C:\new folder\Artemis_Samples\Arte
UNKNOWN	9e83e3a46347e0b4f6e46bd5b0491587	1d8479bb226dab64f2feaf431fb9412a917f8a737c0404cb77cf4e23fdd90c26	C:\new folder\Artemis_Samples\Arte
UNKNOWN	6b6d7729b4236cf3e4ee7e62d1959ef3	e44d7ca317e0c47446c6974c62a1ecbcfb937ed26ddf324150d1c20bdd4b1b9f	C:\new folder\Artemis_Samples\Arte
UNKNOWN	67af21c0df673801bfbb338b17574911	f5062fa76871f67e59a32dfbaf1822099527dc380c3ef98136f8b2b4f7f9ccfb	C:\new folder\Artemis_Samples\Arte
UNKNOWN	fbda2f1192d39846335ace1b54f66a55	ccb6327aba4ba97ee99b0f2aeb610a2058475e13cbdb7d61f820081582fa8453	C:\new folder\Artemis_Samples\Arte

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.

ePolicy Orchestrator Support

To support in ePO environment, ePO deployable and extension reports package are available.

Supported Version: ePO On-Prem 5.10

To add GetSusp deployment package in ePO

1. Log on to the ePO console.
2. Open the Master Repository and check in the GetSusp packages [x86 and x64]:

    a. Click **Menu**, **Software**, **Master Repository**.
    b. Click **Actions**, **Check in Package**.
    c. Click **Browse**, locate the GetSusp package, and click **Next**.
    d. Click **Save**.

3. Verify that GetSusp was checked in successfully.

To add GetSusp extension reports package in ePO

1. Log on to the ePO console.
2. Install the GetSusp extension reports package in Extension:

    a. Click **Menu**, **Extensions.**
    b. Click **Install Extension.**
    c. Click **Browse**, locate the GetSusp extension reports package, and click **Ok**.

3. Verify GetSusp extension shows up under McAfee category in the extensions page with Running state.
4. Verify GetSusp Scan task templates [x86 and x64] added to Product deployment task catalog list.
    a. Click **Menu**, **Client Task Catalog.**
    b. Click **McAfee Agent, Product Deployment.**
    c. Verify **GetSuspx64 Scan Task Template** and **GetSuspx86 Scan Task Template** are displayed.

To Deploy GetSusp scan task via ePO

1. Log on to the ePO console.
2. Open the Master Repository and check in the GetSusp package:

    a. Click **Menu**, **Software**, **Master Repository**.
    b. Click **Actions**, **Check in Package**.
    c. Click **Browse**, locate the GetSusp package, and click **Next**.
    d. Click **Save**.

3. Verify that GetSusp was checked in successfully.
4. Create a Product Deployment task:

    a. Click **System Tree**.
    b. Click the **Client Tasks** tab and click **Actions**, **New Task**.
    c. Provide a name for the task, select **Product Deployment (McAfee Agent)** from the **Type** section, and click **Next**.
    d. In the **Products and components** field, select the **GETSUSP** package entry (x86 or x64), and click Install for the **Action** and **Save**

e. In the **Command-line** field, provide your email ID and the ZIP file path, where the ZIP file created by GetSusp can be placed.
f. Click **Next**.

NOTE: Make sure that the file path where GetSusp is placed has read/write access.

Example
--email=myemail@example.com --zippath=C:\

Additional information:
- The **--SILENT** option is built into the package already. So, you do not have to provide it.
- If you do not provide any additional parameters, the program exits with GetSusp running.

g. In the **Schedule type** field, click Run **immediately**, and click **Next**.
h. Click **Save**.

5. Select the systems that the GetSusp utility is deployed to and send an agent wakeup call:

a. Click **System Tree**.
b. In the **Filter** drop-down list, select **This Group and All Subgroups**.
c. Select the systems that you want to deploy GetSusp utility to.
d. Click **Actions**, **Agent**, **Wake Up Agents**.
e. Keep the default settings and click **OK**.

6. Review the agent status log and verify that GetSusp is successfully installed:

a. In Windows Task Manager, click the **Processes** tab and verify that **GetSusp.exe** is listed.
b. To verify GetSusp was installed successfully, open the McAfee Agent Log. Verify that the product deployment task name created in step 4 completed successfully.
c. To verify GetSusp is running successfully, navigate to the path specified for the log files. The **getsusp.xml** and log files are created in that location.

Using GetSusp Task Template [Built-in with extension package]:

Note:

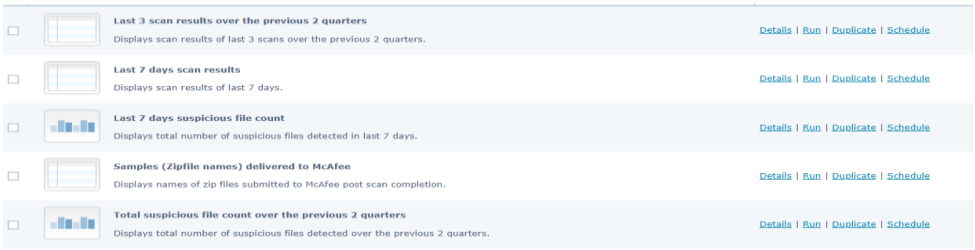
- GetSusp Scan Task Templates are not editable.
- Displayed only when extension reports packaged checked into ePO.

1. Click **Menu**, **Client Task Catalog**
2. Click **McAfee Agent, Product Deployment.**
3. Duplicate the GetSusp Scan Task Template and create a new deployment task
4. Edit the new task created, provide your email ID and the ZIP file path, where the ZIP file created by GetSusp can be placed in the Command-line field.
5. Configure the task to Run immediately and Save.
6. Assign the task to the required systems to deploy.

To View Scan Reports in ePO

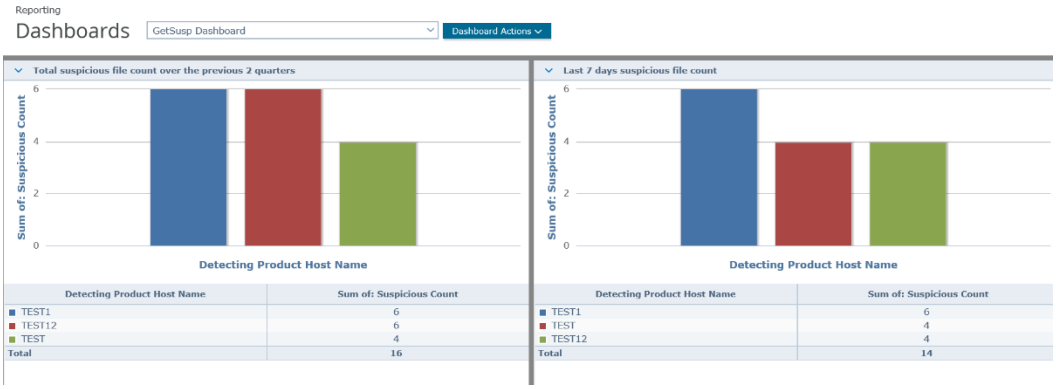
Note: To view scan reports, ePO extension package needs to be checked into ePO before scan task deployment.

1. Click **Queries & Reports**, Expand **McAfee Groups**
2. Click **GetSusp**
3. List of Queries available for GetSusp will be displayed.
    a. Last 3 scan results over the previous 2 quarters.
    b. Last 7 days scan results.
    c. Last 7 days suspicious file count.
    d. Samples (Zipfile names delivered to McAfee).
    e. Total suspicious file count over the previous 2 quarters.



5. To execute a specific query, Click **Run** on Actions.
6. Detailed GetSusp Scan report will be displayed in table and chart format based on query.
7. Click on each system to get more details on the scan task completed on it [Suspicious file count, Unknown file count, Samples delivered]
8. Click on **Go to related Threat Event Log** to get more information on the files list identified by scan.
9. Events generated by GetSusp are tagged with separate even Ids in ePO.
    a. 34500 – GetSusp scan completed. Detected suspicious or unknown files.
    b. 34501 – GetSusp scan completed. No detections found.

10. To View GetSusp Dashboard
    a. Click **Dashboards**, Select **GetSusp Dashboard** from the drop down.
    b. **Total suspicious file count over the previous 2 quarters** and **Last 7 days suspicious file count** query results will be displayed in charts.



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.

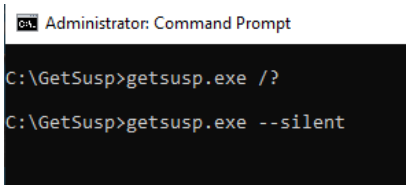
How do I follow up with McAfee for support on a GetSusp submission?

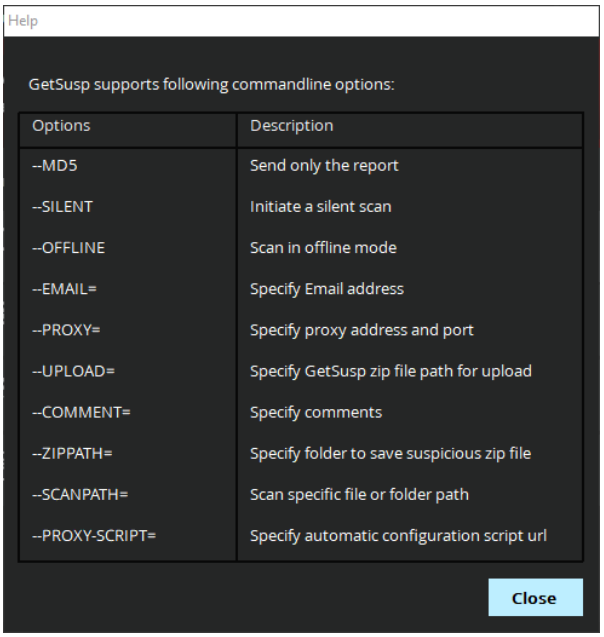
GetSusp submissions with an email address receive an acknowledgement and work item ID from McAfee Workflow systems for tracking purposes. This work item ID can be used to follow up with support team.

Does GetSusp support command line parameters?

Yes, GetSusp supports command line parameters.

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





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.

How to delete GetSusp Scan events in ePO

To delete scan events automatically:

Goto Queries and Reports, and Duplicate Last 7 days scan results query, give it a new name say purge Last 1-month GetSusp events and save it under a group.

Now in the Queries and Reports sidebar, navigate to the group where the duplicated query is saved and click on edit.

Click Next until you reach the filter stage, and now under scan finished change the value to whatever required (above ex uses 1 month) and save the query

Goto Menu, Server Tasks, New task

Provide a task name, set schedule status to enabled, click next

Choose Purge Threat Event log under Actions

Under Purge by query Choose the query which you just saved (Purge last 1-month GetSusp events)

Select an appropriate schedule for the task and save it.

The task will now automatically run according to set schedule and purge GetSusp events returned by the Purge last 1-month GetSusp query.

To delete scan events manually:

Goto Queries and reports, McAfee Groups, Threat Events, execute any query that will display events you want to delete.

For example,

Executing Most Numerous Threat Event Descriptions query will bring up a table as shown below


Reporting

Queries & Reports

Most Numerous Threat Event Descriptions

Event Description	Number of Threat Events
GetSusp scan completed. No detections found	2
GetSusp scan completed. Detected suspicious or unknown files	1
Scan completed. No viruses found.	1
Total	4

Here GetSusp related events can found under either

GetSusp scan completed. Detected suspicious or unknown files OR

GetSusp scan completed. No detections found

Clicking on either of the event descriptions will display all events of that type,

Now choose events you wish to delete by checking the checkboxes on the left

Click on Actions, Delete at the bottom left.

This will delete selected events from both EPOEvents and GetSuspEvents table.

How to allow non-admin ePO users to view GetSusp queries

To allow non admin users to view GetSusp queries, the epo admin should

Create a new permission set

Create a new user and assign the newly created permission set to the user

To create new permission set:

Open Menu, Permission Sets, New Permission set

Provide a name for the perm set(Ex: Test_permission_set) and save. This will create the new perm set

On the permission sets page left pane , click on the newly created permission set(Test_permission_set)

Search for threat event log, click edit, Click view events

Search for system Tree access, click edit, Check the node under which there are machines which the new user will get access to.

Search for queries and reports, click edit, Click Use public groups or any other appropriate permission.

Search for GetSusp query, Click view events

Note: Threat event log, Queries and Reports system tree access are prerequisite permissions for GetSusp query

To create new user with custom permission set:

Open Menu, Users, New User

Provide necessary details like user name,password for the new user

Under Manually assigned permission sets, click on Test_permission_set checkbox

Click Save. This will create a new user with permissions provided in Test_permission_set

Logoff and login as the new user. New user will only be able to perform actions which were assigned in the Test_permission_set

Index