



3.0 Trend Micro Portable Security™

Standalone Scanning Tool



Endpoint Security

Trend Micro Incorporated reserves the right to make changes to this document and to the product described herein without notice. Before installing and using the product, review the readme files, release notes, and/or the latest version of the applicable documentation, which are available from the Trend Micro website at:

<http://docs.trendmicro.com/en-us/enterprise/portable-security.aspx>

Trend Micro, the Trend Micro t-ball logo, and Trend Micro Portable Security are trademarks or registered trademarks of Trend Micro Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Copyright © 2019. Trend Micro Incorporated. All rights reserved.

Document Part No.: TP38823/191001

Release Date: October 2019

Protected by U.S. Patent No.: Patents pending.

This documentation introduces the main features of the product and/or provides installation instructions for a production environment. Read through the documentation before installing or using the product.

Detailed information about how to use specific features within the product may be available at the Trend Micro Online Help Center and/or the Trend Micro Knowledge Base.

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please contact us at docs@trendmicro.com.

Evaluate this documentation on the following site:

<http://www.trendmicro.com/download/documentation/rating.asp>

Privacy and Personal Data Collection Disclosure

Certain features available in Trend Micro products collect and send feedback regarding product usage and detection information to Trend Micro. Some of this data is considered personal in certain jurisdictions and under certain regulations. If you do not want Trend Micro to collect personal data, you must ensure that you disable the related features.

The following link outlines the types of data that Trend Micro Portable Security collects and provides detailed instructions on how to disable the specific features that feedback the information.

<https://success.trendmicro.com/data-collection-disclosure>

Data collected by Trend Micro is subject to the conditions stated in the Trend Micro Privacy Notice:

<https://www.trendmicro.com/privacy>

Table of Contents

Chapter 1: Introduction

| | |
|---|-----|
| Trend Micro Portable Security | 1-2 |
| Scanning Tool (USB Device) | 1-2 |
| What's New | 1-4 |
| Older Versions of Trend Micro Portable Security | 1-5 |

Chapter 2: Getting Started

| | |
|---|------|
| Activation | 2-2 |
| Activating a Standalone Scanning Tool | 2-3 |
| Changing the Activation Code | 2-5 |
| Upgrading Using the Support Tool | 2-6 |
| Scanning Tool Agent | 2-9 |
| Installing the Scanning Tool Agent | 2-9 |
| Uninstalling the Scanning Tool Agent | 2-10 |
| Scanning Tool Agent Console | 2-10 |

Chapter 3: Using the Scanning Tool Console

| | |
|---|------|
| Scanning a Windows Endpoint | 3-2 |
| Scan Settings | 3-4 |
| Security Threats Found | 3-10 |
| Restore Tab | 3-12 |
| Logs Tab | 3-13 |
| Status & Update Tab | 3-14 |
| Component Updates | 3-15 |
| Changing the Scanning Tool Settings | 3-16 |

Chapter 4: Scanning Linux Endpoints

| | |
|---------------------------------|-----|
| Linux System Requirements | 4-2 |
|---------------------------------|-----|

| | |
|--|-----|
| Linux Command Line Reference | 4-2 |
| Scanning a Linux Endpoint for Security Risks | 4-3 |
| Restoring Files on a Linux Endpoint | 4-4 |
| Performing Debug Logging on Linux Systems | 4-5 |
| Viewing Linux Scan Logs | 4-6 |

Chapter 5: Additional Tools

| | |
|--|-----|
| Trend Micro Portable Security Diagnostic Toolkit | 5-2 |
| Debug | 5-2 |
| Reset Device | 5-4 |
| Support Updates | 5-6 |
| Trend Micro Rescue Disk | 5-8 |
| Step 1: Preparation | 5-8 |
| Step 2: Using the Rescue Disk | 5-9 |

Chapter 6: Technical Support

| | |
|---|-----|
| Troubleshooting Resources | 6-2 |
| Using the Support Portal | 6-2 |
| Threat Encyclopedia | 6-2 |
| Contacting Trend Micro | 6-3 |
| Speeding Up the Support Call | 6-4 |
| Sending Suspicious Content to Trend Micro | 6-4 |
| Email Reputation Services | 6-4 |
| File Reputation Services | 6-5 |
| Web Reputation Services | 6-5 |
| Other Resources | 6-5 |
| Download Center | 6-5 |
| Documentation Feedback | 6-6 |

Index

| | |
|-------------|------|
| Index | IN-1 |
|-------------|------|

Chapter 1

Introduction

This chapter introduces the Trend Micro Portable Security™ product and features.

Trend Micro Portable Security

Trend Micro Portable Security™ delivers high-performance, cost-effective security services, helping protect companies by finding and removing security threats from computers or devices that do not have security software or an Internet connection.

The Scanning Tool is an antivirus security program in a portable USB device that you can easily use to find and remove security threats from computers or devices without having to install an antivirus program.

Most antivirus programs are installed on each device and need an Internet connection to be able to download the latest components. With Trend Micro Portable Security™, the antivirus software is already in the portable USB device and you can just plug the USB device and then scan the computer or device.

Scanning Tool (USB Device)

The Scanning Tool can check the endpoint for security threats after you plug it in. The Scanning Tool can also fix, quarantine, or just log the threats found. The results of each scan are saved on the Scanning Tool.

**Note**

- If the Scanning Tool does not start, you can open Windows Explorer and double-click `Launcher.exe` from the `TMPS3 SYS` partition.
 - The Scanning Tool console is only available for Windows computers.
-

Each Scanning Tool launches its own console. However, the features seen on the console depends on the mode you choose. You can choose either Standalone Scanning Tool or Management Program.

Refer to *Standalone Scanning Tool on page 1-3*.

**Note**

Make sure you select the correct mode because you can only change the mode after activation if you reset the device.

For more information, see [Reset Device on page 5-4](#).

TABLE 1-1. Scanning Tool Modes

| | MANAGEMENT PROGRAM | STANDALONE SCANNING TOOL |
|---------------|--|--|
| Updates | In addition to downloading specified components from Trend Micro ActiveUpdate server or a specified source, components can be updated from the Management Program. | Downloads all components from Trend Micro ActiveUpdate server or from any endpoint with an Internet connection or from a specified source. |
| Scan settings | Same as the Management Program or configured from the Scanning Tool. | Change the scan settings directly from the Scanning Tool console. |
| Logs | <ul style="list-style-type: none"> Exported to the Management Program Imported from another Scanning Tool | Imported from or exported to a endpoint. |

**Note**

While scanning for security threats, Trend Micro may create temporary files on the endpoint. These files will be deleted after the Scanning Tool stops any running processes. You can also choose to scan endpoints without saving the temporary files.

For more information, refer to [Scan Settings \(Advanced\) on page 3-6](#).

Standalone Scanning Tool

The Standalone Scanning Tool mode uses the Scanning Tool as a standalone device, wherein you can use any endpoint that has Internet connection to update the components, change scan settings, or check the logs.

This setting is for those who want to use the Scanning Tool without having to go to the Management Program for updates or changes to the settings. With this mode, you can make any changes to the Scanning Tool settings from the Scanning Tool console.



Note

Trend Micro recommends regularly updating the components before scanning any device to make sure that the latest threats can be fixed and quarantined.

What's New

Trend Micro Portable Security includes the following new features and enhancements.

| FEATURE | DESCRIPTION |
|------------------------------|--|
| Linux support | <p>Trend Micro Portable Security supports scanning Linux endpoints running the following operating systems:</p> <ul style="list-style-type: none"> • Red Hat Enterprise Linux 6.0 or later • CentOS 6.0 or later |
| Asset information collection | <p>Trend Micro Portable Security can collect basic information about any endpoint the you plug the Scanning Tool into, including system statistics and application lists.</p> <hr/> <p> Note</p> <ul style="list-style-type: none"> • You must install the Management Program to export asset information logs. • Only activated Scanning Tools can collect asset information. After activating a Scanning Tool, unplug and plug the Scanning Tool back into the endpoint to start asset information collection. • Scanning Tools cannot collect asset information on an endpoint with the Management Program installed. |

| FEATURE | DESCRIPTION |
|-----------------|--|
| Windows support | Trend Micro Portable Security extends Windows support to the following operating systems: <ul style="list-style-type: none"><li data-bbox="525 326 901 350">• Windows 10 19H1 case sensitive<li data-bbox="525 370 790 394">• Windows Server 2019 |
| USB enhancement | The Scanning Tool device storage capacity upgraded to 16 GB. |

Older Versions of Trend Micro Portable Security

Older versions of Portable Security are similar to Trend Micro Portable Security 3. However, each version is sold independently and uses different activation code formats.



Tip

Trend Micro recommends keeping older versions of Portable Security on a separate computer to be able to use these versions with the newer Scanning Tools.

Chapter 2

Getting Started

This chapter describes Trend Micro Portable Security™ activation and upgrade procedures.

Activation

After plugging in the Scanning Tool, you must select the operating mode and Activate the device before you can begin scanning endpoints. If you later decide to change operating modes (for example, from **Standalone Scanning Tool** to **Management Program Tool**), you must reset the device to factory default settings.

For more information, see [Resetting the Device on page 5-5](#).



Important

This function is only available on Windows endpoints.

You can view the current activation status of your Scanning Tool by opening the console and going to the **Status and Update** tab.

You can view the current activation status of your Management Program by opening the console and going to the **Overview** tab.

TABLE 2-1. Icons and messages regarding Activation Codes

| ICON | MESSAGE |
|---|---|
|  | This Activation Code is already active and no action is needed. |
|  | <ul style="list-style-type: none"> This Activation Code is going to expire soon and you need to renew your subscription. |
|  | <ul style="list-style-type: none"> This Activation Code has not yet been activated and you need to activate to be able to use the product. This Activation Code has already expired and you need to get a new Activation Code or renew your subscription to continue using the product. |



Tip

Trend Micro recommends getting a new Activation Code before your current license expires to ensure that the Scanning Tool always has the most recent updates.

Activating a Standalone Scanning Tool

Standalone Scanning Tools are independent of the Management Program and you can update the components directly from the Internet.

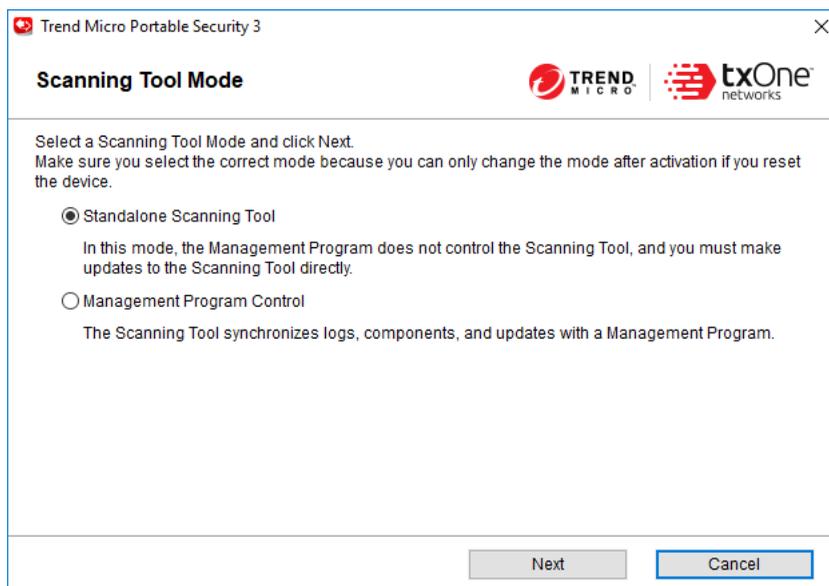


Important

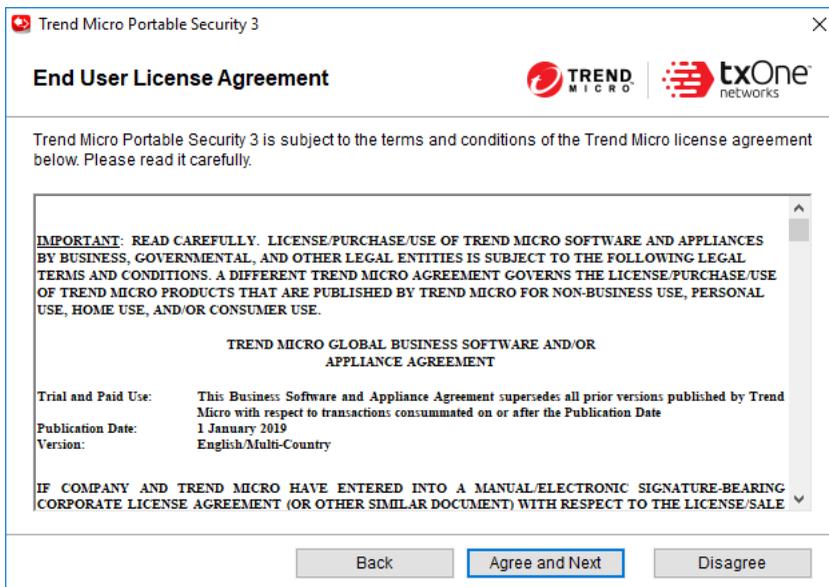
This function is only available on Windows endpoints.

Procedure

1. Plug-in the new Scanning Tool or any Scanning Tool that has not yet been activated to a computer.
2. Open Windows Explorer and double-click `Launcher.exe` from the `TMPS3\SYS` partition to start the program.



3. Select **Standalone Scanning Tool** and click **Next**.



4. When the **End User License Agreement** screen appears, read the agreement and click **Agree and Next**.



The screenshot shows a dialog box titled "Trend Micro Portable Security 3". In the top right corner, there are logos for "TREND MICRO" and "txOne networks". The main text reads: "Enter your Activation Code for Trend Micro Portable Security 3 in the format shown below." Below this is a label "Activation Code:" followed by a text input field. Underneath the input field, it says "(Use this format: XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX)". At the bottom of the dialog, there are three buttons: "Back", "Activate", and "Cancel".

5. Specify your Activation Code and click **Activate**.

The Scanning Tool console opens.



Note

Trend Micro recommends immediately updating all components after activating the license or upgrading the program. Go to the **Status & Update** tab and click **Update Now**.

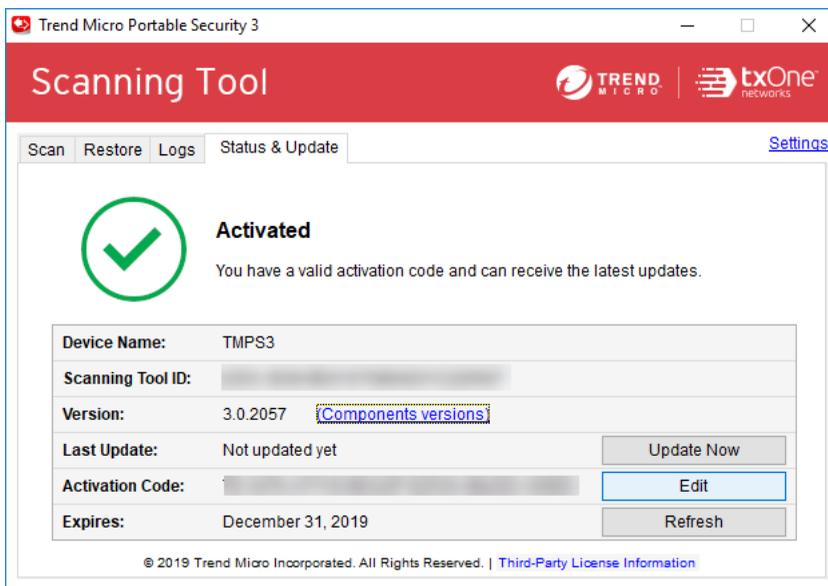
Changing the Activation Code

The date next to Expires shows when you need to get another Activation Code. If you recently provided a new Activation Code, click **Refresh** to get the latest expiration date or click **Edit** to change the Activation Code.

For more information, refer to [Activation on page 2-2](#).

Procedure

1. For a standalone Scanning Tool, open the Scanning Tool console and click the **Status & Update** tab.



2. Click **Edit**.
3. Type the new Activation Code.
4. Click **OK**.

Upgrading Using the Support Tool

Trend Micro releases updates to Trend Micro Portable Security occasionally to provide more features and improve performance.

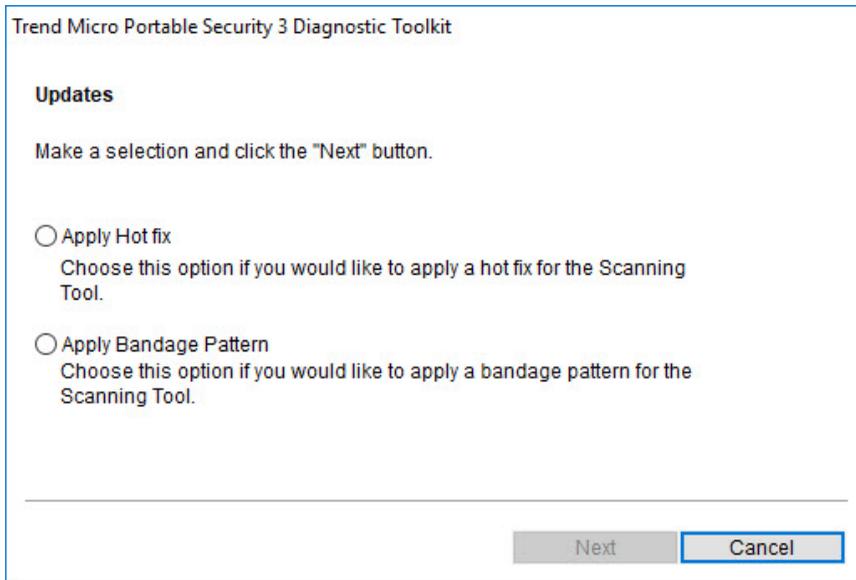
Trend Micro recommends immediately updating all components after activating the license or upgrading the program. Go to the **Status & Update** tab and click **Update Now**.

**Note**

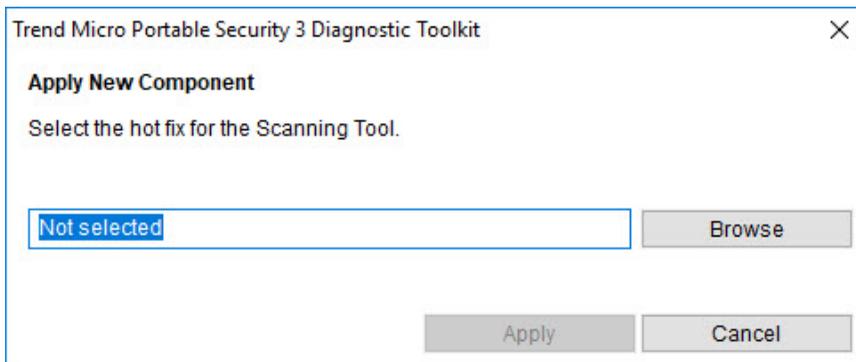
Portable Security does not support upgrading from older versions.

Procedure

1. Close the Scanning Tool console if it is open.
2. Log on to the endpoint using an account with administrator privileges and connect the Scanning Tool.
3. Download the Trend Micro Portable Security service pack.
4. Extract the contents of the service pack to a local folder on the endpoint where you have connected the Scanning Tool.
5. From the `TMPS3 SYS` drive, copy the `SupportTool` folder from the USB device onto your local drive.
6. In the appropriate `Win32` or `x64` folder, double-click the `TMPSuprt.exe` file .
7. Go to the **More Tools** tab.
8. Click the **Use for Updates** button.



9. Select **Apply Hot fix** and click **Next**. The **Apply New Component** screen opens.



10. Click **Browse** and select the .bin file from the service pack provided by Trend Micro.
11. Click **Apply**. A confirmation window opens.

Scanning Tool Agent

The Scanning Tool Agent is a service that is programmed to automatically trigger a scan after inserting the Scanning Tool. The Scanning Tool Agent also provides options to configure the update, scan, and synchronization settings of a Scanning Tool.

The Scanning Tool Agent is recommended for environments that require minimal handling, or endpoints that do not have a screen during normal use.

Installing the Scanning Tool Agent



Important

This function is only available on Windows endpoints.

Procedure

1. Plug in the Scanning Tool USB device to the endpoint where you want to install the Scanning Tool Agent.
2. Open the `TMPSAgent` folder in the `TMPS3 SYS` drive, and double-click the `Setup.exe` file.
3. The Setup program checks the system for Microsoft Visual C++ 2008 Redistributable and prompts you to install the package if necessary.
4. When the **End-User License Agreement** screen appears, read the agreement and click **Agree and Continue**.



Note

You must close the Scanning Tool console before continuing.

5. When the **Specify Destination** screen opens, type or browse for a folder and click **Install**.
6. When the **Installation Complete** screen appears, click **Exit**.

By default, the Scanning Tool Agent console opens. To disable this function, clear the **Open Scanning Tool Agent Console** option.

Uninstalling the Scanning Tool Agent

Uninstall the Scanning Tool Agent using your version of Windows Control Panel.



Note

- Make sure the Scanning Tool is not plugged into the endpoint before continuing.
- Make sure to unlock Trend Micro Safe Lock™ before uninstalling the Scanning Tool Agent.

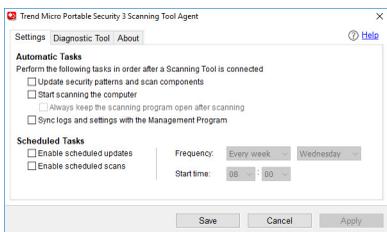
Scanning Tool Agent Console



Important

This function is only available on Windows endpoints.

The Scanning Tool Agent console allows you to perform some basic automated tasks after detecting a plugged in Scanning Tool on the endpoint. You can also use the Scanning Tool Agent to perform diagnostic tasks.



Settings Tab

The following table outlines the options available on the **Settings** tab.

| SECTION | OPTIONS |
|------------------------|--|
| Automatic Tasks | <ul style="list-style-type: none"> • Update security patterns and components: Select to automatically update the Scanning Tool for the latest security patterns and components. • Start scanning the computer: Select to automatically start scanning. To view the result of this scan immediately after it is complete, select Always keep the scanning program open after scanning. <ul style="list-style-type: none"> • Always keep the scanning program open after scanning: Select to ensure that you can view scan logs immediately after a scan completes. This option interrupts the automatic execution of tasks by the Scanning Tool Agent including synchronization or scheduled updates. • Sync logs and settings with the Management Program: Select this option to synchronize logs and settings of the Scanning Tool with the Management Program. <hr/> <p> Note Ensure that there is a working network connection between the Scanning Tool Agent and the Management Program.</p> <hr/> <p> Important Only functional for Scanning Tools operating in Management Program Control mode.</p> |
| Scheduled Tasks | <ul style="list-style-type: none"> • Enable scheduled updates: Select to have the Scanning Tool updated at the defined frequency and start time. • Enable scheduled scans: Select to have the Scanning Tool scan the endpoint at the specified frequency and start time. <hr/> <p> Note If both scheduled updates and scheduled scans are enabled, the Scanning Tool performs the update first. The Scanning Tool console automatically closes when both tasks are complete.</p> |

Diagnostic Tool Tab

Use the Diagnostic Tool to help Trend Micro Technical Support collect useful troubleshooting information. Only use the tool when instructed by Trend Micro Technical Support.

Procedure

1. From the Scanning Tool Agent console, click the **Diagnostic Tool** tab.
2. Click **Start Diagnostic Tool**.
3. Click **Start Diagnostic Logging** to start collecting information.
4. Reproduce the issue you are investigating on the endpoint.
5. Click **Stop Diagnostic Logging** to stop recording system information.

The Diagnostic Tool performs final system checks and saves the collected log data to a ZIP package.

6. Click **Open Folder** to open the folder containing the ZIP package.
 7. Send the collected information to Trend Micro Technical Support for further analysis.
-

Chapter 3

Using the Scanning Tool Console

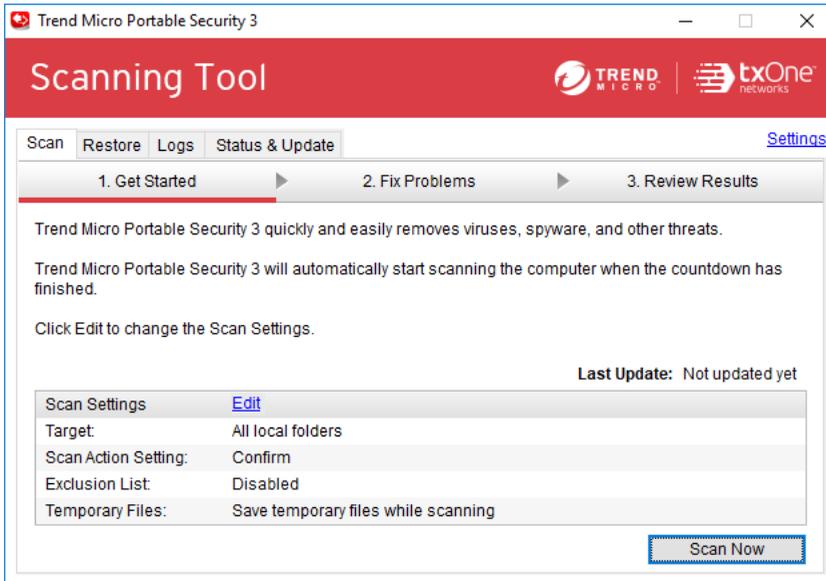
This chapter outlines the features available on the various tabs of the Scanning Tool console.



Important

This function is only available on Windows endpoints.

Scanning a Windows Endpoint



Use the **Scan** tab to manually start scanning an endpoint, monitor scan progress or change scan settings.

Procedure

1. Open the Scanning Tool console.
2. Click the **Scan** tab.
3. Click **Scan Now** to begin scanning the endpoint using the current scan settings.

To change scan settings before starting a scan, click the **Edit** link.

For more information, see *Scan Settings on page 3-4*.

Refer to the LED lights on the Scanning Tool device to determine the scan status.

TABLE 3-1. Scanning Tool indicator lights.

| INDICATOR LIGHTS | DESCRIPTION |
|------------------------------------|--|
| Blue (Blinking) | Information is being written to or retrieved from the Scanning Tool. |
| Blue | The scan completed and Portable Security did not detect any threats. |
| Yellow | The scan completed and Portable Security cleaned all detected threats. |
| Red | The scan completed with detected threats that require further action. |
| Blue, Yellow, and Red (Continuous) | The Scanning Tool is currently scanning the endpoint. |

4. Monitor the scan progress on the **Fix Problems** screen.
 - Click **Stop** if you want to stop scanning the endpoint.
 - Click **Suspend** if you want to suspend the current scan. Use the **Resume** button to resume the suspended scanning immediately after the Scanning Tool is relaunched.

The **Suspend** permission is only available if configured by the scan administrator.

For more information, see *Scan Settings (Basic)* on page 3-4.
 - **Apply Now** (threats detected): Click to apply actions on detected threats.

For more information, see *Security Threats Found* on page 3-10.
 - **Comment:** Type a comment to add to the log entry for the scan

**WARNING!**

Trend Micro does not recommend unplugging the Scanning Tool while the LED is flashing or while the Scanning Tool console is open.

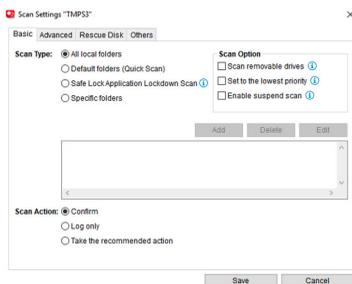
5. The **Review Results** screen displays with the following options after the scan completes.

- **Scan again:** Click to return to the **Get Started** screen and begin a new scan of the endpoint.
- **Comment:** Type a comment to add to the log entry for the scan
- **Close:** Exits the Scanning Tool console.

Scan Settings

To change scan settings, click the **Scan** tab and click **Edit** from the Scanning Tool console.

Scan Settings (Basic)



Change the scan type, scan option, and scan action settings of the Scanning Tool device. You can change the following:

- **Scan Type:** Specify the folder locations to scan, whether to scan only file types vulnerable to malware, or only **Safe Lock Application Lockdown Scan** violations
 - **All local folders:** Scan all folders on the target endpoint
 - **Default folders (Quick Scan):** Scan only the folders most vulnerable to system threats (such as the Windows System folder)
 - **Safe Lock Application Lockdown Scan:** Scan only the files that were quarantined or blocked after the Trend Micro Safe Lock™ Application

Lockdown function was turned on and files that were executed (but not listed on the Approved List)

- **Specific folders:** Limit the scan to the drives and folders you select
- **Scan Option**
 - **Scan removable drives:** Select to scan any removable drives connected to the endpoint
 - **Set to the lowest priority:** Select to reduce any performance impact on the endpoint but extend scanning times
 - **Enable Suspend scan:** Select to display the **Suspend** button during scanning
- **Scan Action:** Specify what action the Scanning Tool takes after detecting a threat.
 - **Confirm:** Prompts user to confirm the action to perform
 - **Log only:** Logs but takes no further action on detected threats
 - **Take the recommended action:** Automatically takes the Trend Micro recommended action per threat type

Scan Settings (Advanced)

To access advanced scan settings of the Scanning Tool device, go to the **Advanced** tab:

Scan Settings "TMP53"

Basic Advanced Rescue Disk Others

Exclusion List: Select files, folders, or extensions to exclude from scans.

Folders: Add Delete Edit

Files: Add Delete Edit

Extension: (Ex: txt, bmp, dat)

Temporary Files: Scan without saving temporary files

Administrator Account: Scan as Administrator

Account: Password:

Number of Compressed Layers to Scan: 2

Save Cancel

- **Exclusion List:** Add files, folders, or file extensions to exclude from scans
Refer to [Changing the Exclusion List Settings on page 3-7](#).
- **Scan without saving temporary files:** Scans without saving files to the target computer



Important

Using this option reduces scanning capability for certain types of malware.

- **Scan as Administrator:** Allows you to specify an administrator user name and password for users without administrative privileges

**Note**

You can use a backslash (\) or the at sign (@) to separate the user name from the domain.

- **Number of Compressed Layers to Scan:** Choose the number of compression layers and skip scanning any excess layers

Changing the Exclusion List Settings

Use this setting to exclude files, folders, or extensions from being scanned.

**Note**

You can exclude up to 100 files and folders and use commas to exclude different extensions.

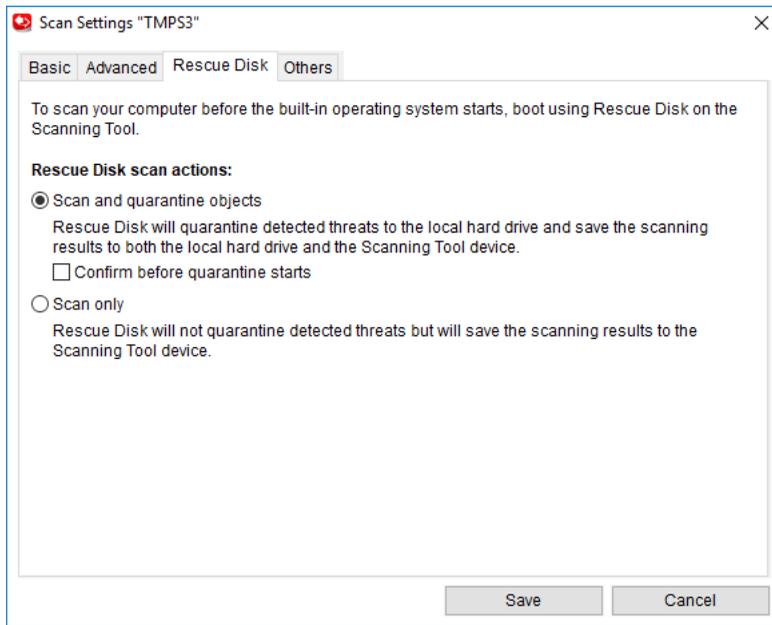
Additionally, you can do the following:

- Add a drive or folder on the list.
 - Delete selected drives or folders from the list.
 - Edit list items.
-

**Tip**

Synchronize the settings to your device after saving the changes you made to the configuration.

Scan Settings (Rescue Disk)



Changes the Rescue Disk settings for scan actions. You can change the following:

- **Scan and quarantine objects:** Select this option to quarantine detected files to the local hard drive while scanning using the Rescue Disk. To be prompt before quarantine starts, select **Confirm before quarantine starts**.
- **Scan only:** Select this option to only scan without quarantining any detected threats.

For details on Rescue Disk, refer to [Trend Micro Rescue Disk on page 5-8](#).

Scan Settings (Others)

Scan Settings "TMPS3"

Basic Advanced Rescue Disk Others

Scanning Tool Name:

Proxy Options:

No proxy server

Use individual proxy server settings

Use proxy server settings from Management Program

Proxy Server:

Import the Internet Explorer proxy settings

Enter the necessary proxy server settings in the following fields

Address: Port:

If your proxy server requires credentials, provide that information below. Otherwise, leave these fields blank.

User name: Password:

Collect logs from Trend Micro Safe Lock™

Save Cancel

Change other settings for the Scanning Tool device. You can change the following:

- **Scanning Tool Name:** Change the name of the Scanning Tool device.
- **Proxy Server:** Enable this option if your computer is required to use a proxy server to connect to the Internet. Then choose one of the following options:
 - **Import the Internet Explorer proxy settings:** Choose this option if you wish to use the same settings as those set for Microsoft™ Internet Explorer™
 - **Enter the necessary proxy server settings in the following fields:** Choose this option to enter the proxy server settings yourself.
- **Collect logs from Trend Micro Safe Lock:** Enable this option to collect logs from computers with Trend Micro Safe Lock™.

Security Threats Found

If the scan finds a threat, review the results before selecting an option.

Fixing Threats

Procedure

1. Check the name of the file and the risk, then select a response from the Action column, or just keep the default response.
 - **Ignore:** Portable Security will not take any action against the threat.
 - **Fix:** Portable Security will respond to the threat by trying to clean or quarantine the file involved.



Tip

The exact response depends on the type of threat detected. Trend Micro periodically reviews and revises the automatic responses to different threats, so they may change after a pattern file or scan engine update.

2. Click **Apply Now**.



Note

You can click **Scan Again** to check for security threats once more.

3. After confirming that no more security threats were found, you can add some notes about the scan in the **Comment** field, and then click **Close**.



Tip

You can type up to 63 characters in the **Comment** field. This information will appear along with the log data in the scan results. The name of the computer is the default value of this field.

Restoring Quarantined Files

You can restore files if Portable Security fixed and quarantined files that you need.



WARNING!

Restoring these files may put your security at risk. You have to be very sure that the files are NOT infected before restoring the files because Trend Micro does not guarantee the safety of your devices if you restore infected files.

Procedure

1. Open the Scanning Tool console.
2. Go to the **Restore** tab.
3. Select the date and time of the scan from the drop-down list next to **Last scan started** and the files that were quarantined during that scan will show.
4. Select the file and click **Restore**.



Note

Restoring files can be only performed on a computer after Portable Security has quarantined a file and the files can only be restored on the same computer.

5. Click **OK** to confirm.



WARNING!

You have to be absolutely sure that the file is essential and that the file is not infected.

6. Click **Close**.
-

Restore Tab



Note

You can store quarantined files in the USB device, instead of on the target computer but you cannot use the Scanning Tool to store other files.

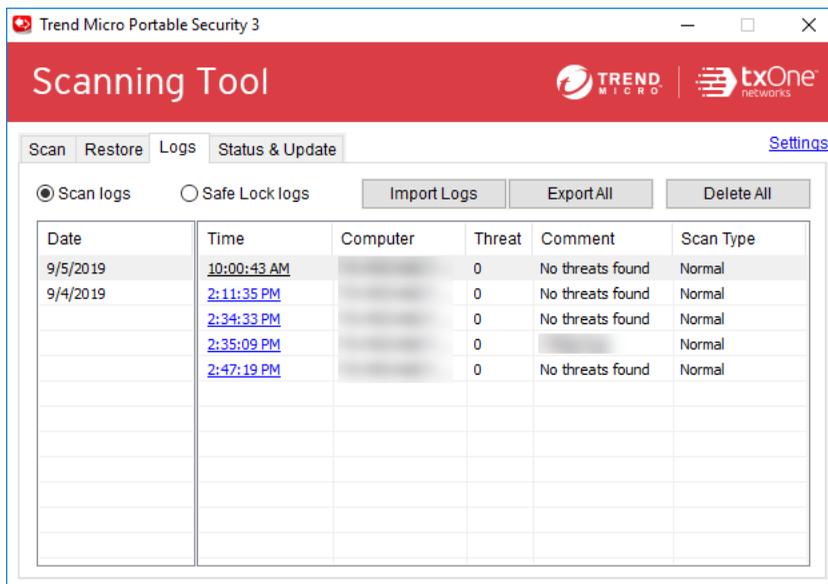
- **Last scan started:** Select the time that the scan was performed to view the logs and actions done at that time.
- **Scan:** This function is enabled for files that are tagged "ignored" or "unable to fix." Selecting **Scan** opens a confirmation message box for users to choose the appropriate scan action to apply for the selected file(s).
- **Restore:** Select a file or files and click this button to put the file back and leave it in its original location. Refer to [Restoring Quarantined Files on page 3-11](#).



WARNING!

Restore files only if you are sure that the file is not infected.

Logs Tab

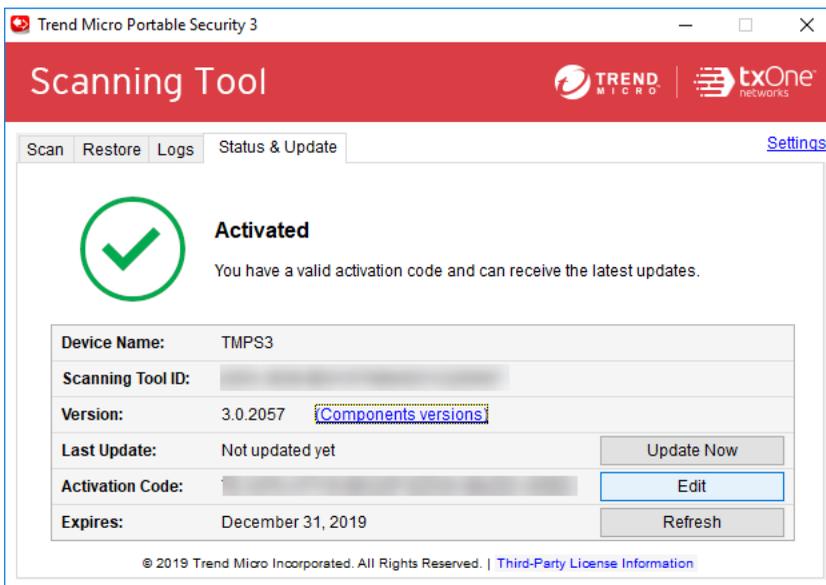


To view results for each scan, select **Scan logs** and click an item from the Time column. To view logs from Trend Micro Safe Lock™, select **Safe Lock logs**.

For more information on Safe Lock log collection, see *Scan Settings (Others)* on page 3-9.

- **Import Logs:** Click this button to import database format logs.
- **Export All:** Click this button to export all the logs into database or csv format.
- **Delete All:** Click this button to delete all log entries.

Status & Update Tab



The **Status & Update** tab shows the device component status.

For more information on the device activation status, refer to [Activation on page 2-2](#).

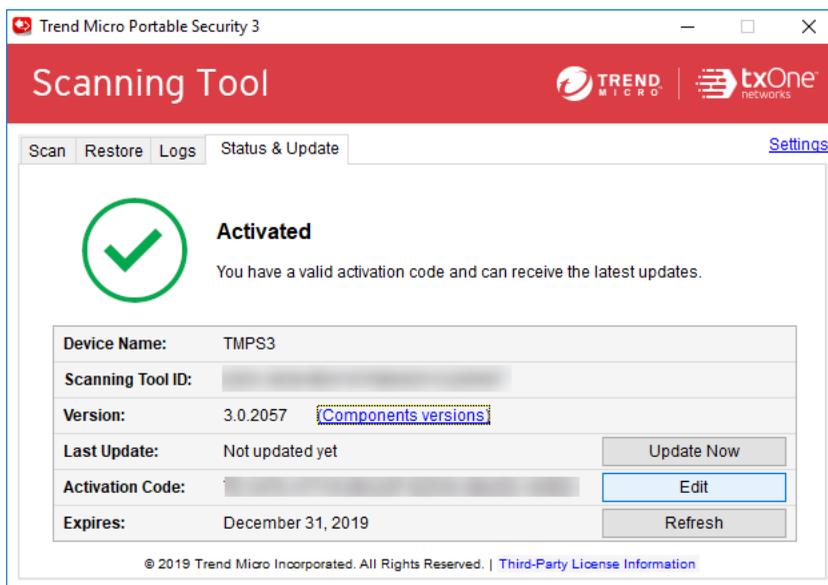
- **Device Name:** This is the name of the Scanning Tool.
- **Scanning Tool ID:** The Scanning Tool ID is a unique identification number given to every Scanning Tool device.
- **Version:** The build number of the Portable Security Scanning Tool appears next to **Version**. Click the **Component versions** link to see the component details and the date of the last update.
- **Last Update:** Shows the update status. Click **Update Now** to manually update the Scanning Tool for the latest components and hot fix.
- **Activation Code:** Click **Edit** to change or update the activation code.

See *Changing the Activation Code on page 2-5*.

- **Expires:** Shows the expire date of the activation code. Click **Refresh** after you have changed the activation code and it still says expired.

Component Updates

Make sure to update your Scanning Tool for the most recent security pattern file or scan engine from Trend Micro. Click the **Components versions** link to check the current version and the date of the last update.



Updating Components On-Demand

Update the Scanning Tool whenever required.

Procedure

1. Plug in the Scanning Tool on a computer with access to the update source.

**Note**

For details on update source settings, refer to *Changing the Scanning Tool Settings on page 3-16*.

2. From the Scanning Tool console, go to the **Status & Update** tab.

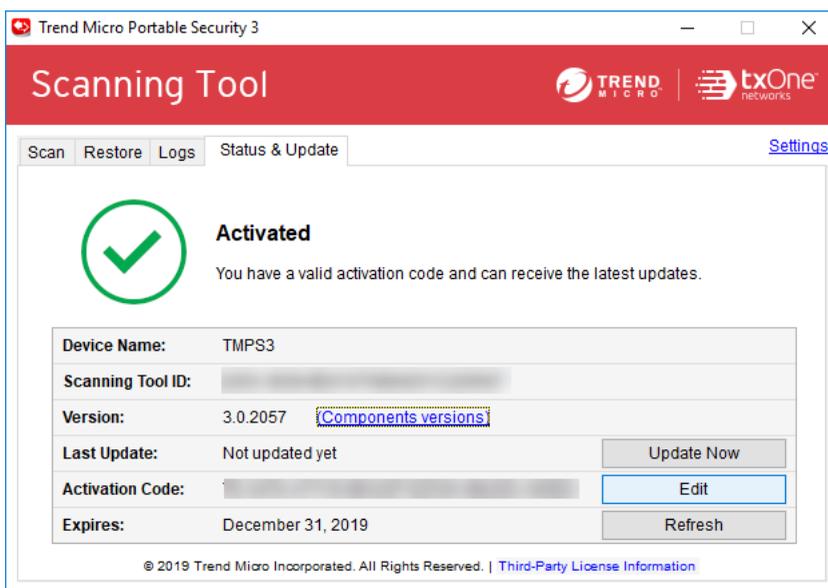


FIGURE 3-1. Standalone device

3. Click **Update Now**.
-

Changing the Scanning Tool Settings

Configure the update source and language setting of your Scanning Tool.

Procedure

1. Open the Scanning Tool console.

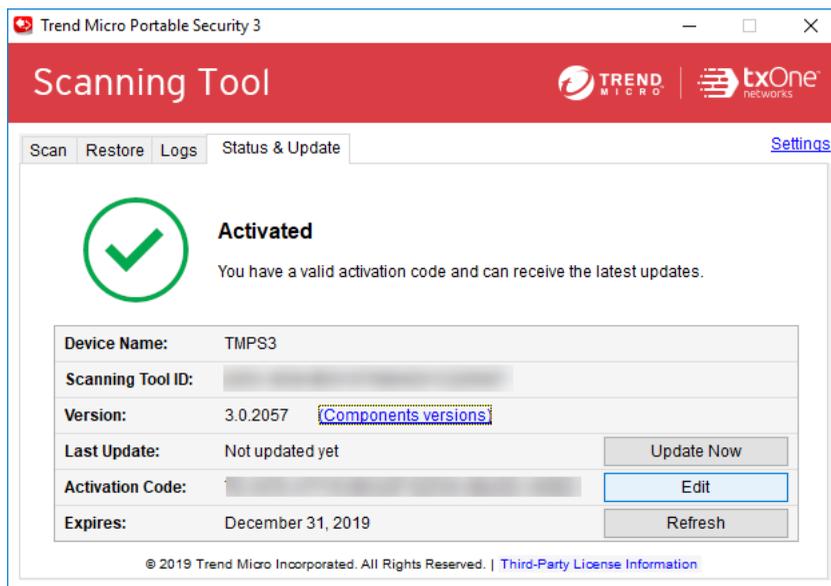
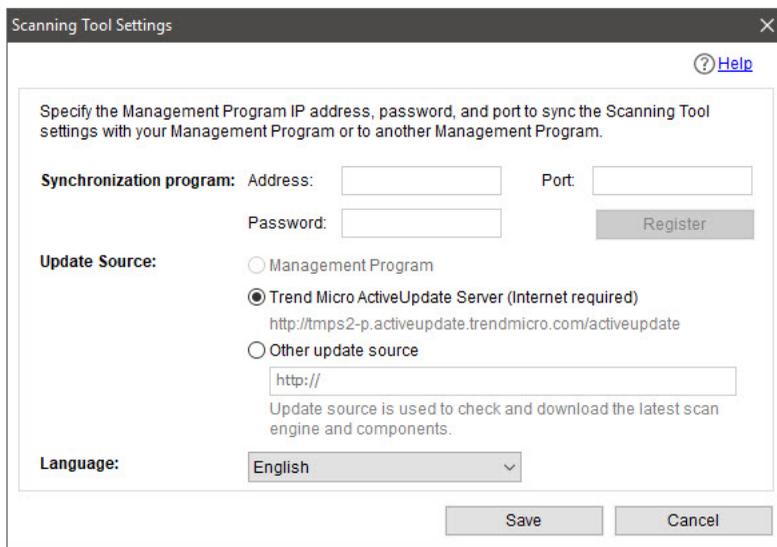


FIGURE 3-2. The Standalone Scanning Tool console

2. Click **Settings**.



The image shows a screenshot of the 'Scanning Tool Settings' dialog box. The title bar reads 'Scanning Tool Settings' with a close button (X) on the right. A help icon and the text '? Help' are in the top right corner. The main content area contains the following sections:

- Specify the Management Program IP address, password, and port to sync the Scanning Tool settings with your Management Program or to another Management Program.**
- Synchronization program:** Address: [text box] Port: [text box] Password: [text box] Register [button]
- Update Source:**
 - Management Program
 - Trend Micro ActiveUpdate Server (Internet required)**
http://tmps2-p.activeupdate.trendmicro.com/activeupdate
 - Other update source**
http:// [text box]
Update source is used to check and download the latest scan engine and components.
- Language:** English [dropdown menu]

At the bottom right, there are 'Save' and 'Cancel' buttons.

**Note**

The Management Program settings are automatically disabled for Standalone Scanning Tool.

3. Specify an update source.
 - **Trend Micro ActiveUpdate Server:** Obtain updates from the Trend Micro ActiveUpdate Server. Internet access is required.
 - **Other update source:** Obtain updates from a specified source which can be located in a closed network.
4. (Optional) Select a language from the drop-down menu to change the Scanning Tool language.
5. Click **Save**.

Chapter 4

Scanning Linux Endpoints

This chapter outlines how to use the Scanning Tool device to scan Linux endpoints.



Important

Before you can use a Scanning Tool on a Linux endpoint, you must activate the Scanning Tool device on a Windows endpoint, in either standalone mode or through the Management Program.

For more information, see [Activation on page 2-2](#).

Linux System Requirements

| ITEM | REQUIREMENTS |
|------------------|---|
| Operating system | <ul style="list-style-type: none"> Red Hat Enterprise Linux 6.0 or later CentOS 6.0 or later |
| Privileges | <p>The logged on account must have one of the following privileges:</p> <ul style="list-style-type: none"> “root” user “sudo” privilege |

Linux Command Line Reference

After mounting the Scanning Tool folders, you must perform all actions using the Linux command line.

Usage:

- `sudo sh ./LauncherLinux.sh -c scan [<scan options>] <scan targets>`
- `sudo sh ./LauncherLinux.sh -c restore`

| COMMAND STRUCTURE | DESCRIPTION |
|-------------------|---|
| Command | <ul style="list-style-type: none"> <code>-c --command <scan restore></code> <code>-h --help</code> <p>Displays the help screen</p> |
| <scan options> | <ul style="list-style-type: none"> <code>-a --action <action></code> <p>Scan action to apply that overrides default configuration settings: <code>log confirm recommended</code></p> |
| <scan targets> | Specify folder location or full file path. Separate multiple targets using the whitespace character. |

Scanning a Linux Endpoint for Security Risks

This task assumes that your Linux environment supports the auto-mounting of USB drives. If your Linux environment does not support auto-mounting, refer to your Linux documentation to learn how to manually mount a USB device.



Important

Before you can use a Scanning Tool on a Linux endpoint, you must activate the Scanning Tool device on a Windows endpoint, in either standalone mode or through the Management Program.

For more information, see [Activation on page 2-2](#).

Procedure

1. Plug the Scanning Tool device into the target Linux endpoint on which you have “root” or “sudo” privilege.

The endpoint auto-mounts the device and the `TMPS3_DAT` and `TMPS3_SYS` drives appear on the screen.

2. Open the `TMPS3_SYS` drive.
3. Right-click anywhere within the folder (but not on a file or folder icon) and click **Open in Terminal**.

The terminal opens pointing to the `TMPS3_SYS` directory.

4. Scan the endpoint through use of the following command structure:

```
sudo sh ./LauncherLinux.sh -c scan [<scan options>] <scan targets>
```

To scan the entire endpoint using the Management Program settings, type the following:

```
sudo sh ./LauncherLinux.sh -c scan /
```

To scan all files in the `/tmp` folder and perform the “recommended” action, type the following:

```
sudo sh ./LauncherLinux.sh -c scan -a recommended /tmp
```

For more information about the available options, see [Linux Command Line Reference on page 4-2](#).

The Scanning Tool begins scanning the endpoint.

5. Allow some time to allow the scan to complete or press CTRL-C to cancel an on-going scan.
 6. If the configured scan action is **Confirm**, Portable Security prompts you for an action after detecting a threat.
 - **f**: Portable Security attempts to clean or quarantine the detected threat
 - **i**: Portable Security takes no action on the detected threat
 - **F**: Portable Security attempts to clean or quarantine all detected threats
 - **I**: Portable Security takes no action on any detected threat
 7. Portable Security displays the scan results and action results, and saves the scan logs to the Scanning Tool device.
-

Restoring Files on a Linux Endpoint

This task assumes that your Linux environment supports the auto-mounting of USB drives. If your Linux environment does not support auto-mounting, refer to your Linux documentation to learn how to manually mount a USB device.

Procedure

1. Plug the Scanning Tool device into the target Linux endpoint on which you have “root” or “sudo” privilege.

The endpoint auto-mounts the device and the `TMPS3 DAT` and `TMPS3 SYS` drives appear on the screen.

2. Open the `TMPS3 SYS` drive.

3. Right-click anywhere within the folder (but not on a file or folder icon) and click **Open in Terminal**.

The terminal opens pointing to the `TMPS3 SYS` directory.

4. Restore files on the endpoint through use of the following command structure:

```
sudo sh ./LauncherLinux.sh -c restore
```

The Scanning Tool displays a list of previous scan logs for the endpoint.

5. Type the scan log **Index** that you want to restore files from.

The Scanning Tool displays a list of quarantined files.

6. Type the quarantined file **Index** that you want to restore.

The Scanning Tool restores the quarantined file to the endpoint.

7. Portable Security displays the action result and saves the logs to the Scanning Tool device.
-

Performing Debug Logging on Linux Systems

If you encounter errors while scanning a Linux endpoint, you can enable debug logging and send the logs to your Trend Micro representative for troubleshooting.

Procedure

1. Plug the Scanning Tool device into the target Linux endpoint on which you have “root” or “sudo” privilege.

The endpoint auto-mounts the device and the `TMPS3 DAT` and `TMPS3 SYS` drives appear on the screen.

2. Open the `TMPS3 SYS` drive.
3. Right-click anywhere within the folder (but not on a file or folder icon) and click **Open in Terminal**.

The terminal opens pointing to the `TMPS3 SYS` directory.

4. Scan the endpoint using the following command:

```
[root@localhost]# sudo sh ./LaucherLinux.sh --debug -c scan  
[target folder] > /tmp/tmps.log 2>&1
```

The Scanning Tool begins scanning the endpoint, records all log data to the `/tmp/tmps.log` file, and displays status messages on the console.

5. After scanning completes, execute the following command to collect additional log information:

```
[root@localhost]# sudo dmesg > /tmp/dmesg.log
```

6. Copy the following log files and send the files to your Trend Micro representative:

- `/tmp/tmps.log`
 - `/tmp/dmesg.log`
 - `/var/log/syslog`
-

Viewing Linux Scan Logs

You cannot directly view the entire scan logs using a Linux endpoint. To view complete scan logs, plug the Scanning Tool into a Windows endpoint or an endpoint with the Management Program installed.

Chapter 5

Additional Tools

This chapter discusses how to use the additional tools provided with Trend Micro Portable Security.

Trend Micro Portable Security Diagnostic Toolkit

Use the Trend Micro Portable Security Diagnostic Toolkit to diagnose and troubleshoot problems. Trend Micro Portable Security automatically includes the toolkit during installation and you can access the toolkit from the Windows Start Menu.

Debug

Use the **Debug** tab to generate debug logs for troubleshooting issues with the product.

Generating Debug Logs for Installation Issues

Follow the steps below to generate debug logs for installation issues of Scanning Tool Agent.

Procedure

1. From the Start menu of the Trend Micro Portable Security endpoint, click **Trend Micro Portable Security 3 > Trend Micro Portable Security 3 Diagnostic Toolkit**.
 - a. Plug-in the Trend Micro Portable Security Scanning Tool to the endpoint.
 - b. Copy the SupportTool folder from the USB device into your local drive.
 - c. Double-click the TMPSSuprt.exe file .
 2. In the **[A] Debug** tab, select **Diagnose installation issues** and click **Start**.
 3. Click **Collect Data**.
 4. Click **Finish**.
 5. Click **Open Folder**.
-

Generating Debug Logs for Scanning Tools

Procedure

1. Plug-in the Trend Micro Portable Security Scanning Tool to the endpoint.
2. On the TMPS3 SYS drive, navigate to the SmallDebugTool folder.
3. Launch SmallDebugTool.exe to collect logs.
 - a. Double-click the SmallDebugTool.exe file ().
 - b. Click **Start Scanning Tool** to start debugging mode.
 - c. Reproduce the problem encountered by Trend Micro Portable Security.
 - d. After the problem has been reproduced, enable **Troubleshooting data has been collected**.
 - e. Click **Stop Debugging Mode**.
 - f. Click **Transfer Data**.

The program starts transferring the logs to the Scanning Tool. It may take a while for the process to complete.
 - g. Click **Close**.
4. Remove the Scanning Tool from the endpoint and plug into an endpoint that has Trend Micro Portable Security installed.
5. Launch the Trend Micro Portable Security 3 Diagnostic Toolkit.

From the Start menu of the Trend Micro Portable Security endpoint, click **Trend Micro Portable Security 3 > Trend Micro Portable Security 3 Diagnostic Toolkit**.

If you are using a different endpoint, you can do the following:

- a. Plug-in the Trend Micro Portable Security Scanning Tool to the endpoint.
- b. Copy the SupportTool folder from the USB device into your local drive.

- c. Double-click the `TMPSSuprt.exe` file .
6. Use the Trend Micro Portable Security 3 Diagnostic Toolkit to export the logs.
 - a. In the **Debug** tab, select **Load logs from the Scanning Tool**, and click **Start**.
 - b. Connect the Scanning Tool to the endpoint and click **Next**.

The Diagnostic Toolkit displays the storage path of the logs.
 - c. Click **Open Folder** to navigate to the path.

Locate and open the zip file to verify that the debug logs have been successfully generated.
-

Reset Device

You can use the Trend Micro Portable Security Diagnostic Toolkit to reset the device to either program or factory settings.

You also need to reset the device if you want to change the current Scanning Tool mode. For example, if the Scanning Tool is currently a Standalone tool, you need to reset the device to be able to change the mode and register to the Management Program.

There are two reset modes:

- **Program Reset:** Select this option if the Scanning Tool is not working because some component might be damaged. This mode keeps the activation code and status.
- **Factory Reset:** Select this option to reset to factory status.



Note

- You can only reset one device at a time.
 - The Trend Micro Portable Security Diagnostic Toolkit does not support resetting any previous versions of Trend Micro Portable Security Scanning Tools.
-

Resetting the Program

Procedure

1. Plug-in the Trend Micro Portable Security 3 Scanning Tool to the endpoint.
2. Copy the SupportTool folder from the USB device into your local drive.
3. Double-click the TMPSSuprt.exe file .
4. Go to the **More Tools** tab.
5. Click the **1. Reset Device** button.
6. Select **Default Program Settings** and click **Next**.
7. Confirm the reset.



Note

Do not unplug the Scanning Tool until the reset process has completed and a popup appears stating “You have successfully reset the device”.

8. Unplug and then plug-in the device again to verify that the Scanning Tool has been reset.
-

Resetting the Device

Procedure

1. Plug the Trend Micro Portable Security 3 Scanning Tool into the endpoint.
2. From the TMPS3 SYS drive, copy the SupportTool folder from the USB device onto your local drive.
3. In the appropriate Win32 or x64 folder, double-click the TMPSSuprt.exe file .
4. Go to the **More Tools** tab.

5. Click **Reset Device**.
6. Select **Default Factory Settings** and click **Next**.
7. Copy the Activation Code, and select the **Finished saving the Activation Code** option.
8. Click **Yes**.



Note

Do not unplug the Scanning Tool until the reset process has completed and a screen appears stating that the reset was successful.

9. Remove and reinsert the device, then execute `Launcher.exe` to verify that the Scanning Tool has been reset.

The **Scanning Tool Mode** screen appears after successfully resetting the Scanning Tool.

Support Updates

Use the **Trend Micro Portable Security Diagnostic Toolkit** to apply hotfixes or bandage patterns to the Scanning Tool, if needed.



Note

These updates can only be applied to one device at a time.



WARNING!

Bandage patterns are a pre-release version of a Trend Micro virus pattern, for emergency antivirus protection. These patterns are not publicly available because these have not been fully tested. Apply **ONLY** those provided by Trend Micro Premium Support and only to the specified devices.

Applying Hot Fixes

Hot fixes are a workaround or solution to customer-reported issues. Trend Micro provides hotfixes to individual customers. Hotfix file names use the `xxx.bin` format.



WARNING!

Hot fixes are not publicly available because these not have been fully tested. Apply **ONLY** those provided by Trend Micro and only to the specified devices.

Procedure

1. Copy the `SupportTool` folder from the USB device into your local drive.
2. Open the Trend Micro Portable Security 3 Diagnostic Toolkit console.
3. Go to the **More Tools** tab.

The **More Tools** tab opens.

4. Click **Use for Updates**.

The **Updates** window opens.

5. Select **Apply Hot fix**, and click **Next**.

The **Apply New Components** window opens.

6. Select the hotfix file provided by Trend Micro.

7. Click **Apply**.

A confirmation window opens.

8. To update another Scanning Tool, click **Yes**.

To finish the update, select **No** and replug the device for the update to take effect.

Trend Micro Rescue Disk

Use the Trend Micro Rescue Disk to examine your endpoint without launching your operating systems. It finds and removes persistent or difficult-to-clean security threats that can lurk deep within your operating system.

Rescue Disk can scan hidden files, system drivers, and the Master Boot Record (MBR) of your endpoint's hard drive without disturbing the operating system. Rescue Disk does not load potentially-infected system files into memory before trying to remove them.



Note

By default, Trend Micro Rescue Disk quarantines any detected threats to the local hard drive. If you wish to scan without writing any information to your local hard drive, change the scan action settings to **Scan only**.

For details, see *Scan Settings (Rescue Disk)* on page 3-8.

Rescue Disk supports the following file systems:

| OPERATING SYSTEM | FILE SYSTEM |
|------------------|---|
| Windows | NTFS and FAT |
| Linux | EXT, EXT2, EXT3, EXT4 and XFS <div data-bbox="381 1040 432 1083" data-label="Image"> </div> <div data-bbox="438 1040 494 1065" data-label="Section-Header"> <h3>Note</h3> </div> <div data-bbox="435 1073 1012 1130" data-label="Text"> <p>Rescue Disk runs on any Linux distribution installed on a supported file system.</p> </div> |

Step 1: Preparation

Procedure

1. Insert the USB device into the endpoint.

2. Restart the endpoint.
3. When the endpoint powers up again, open the BIOS or UEFI Setup Utility.
4. Look for Boot, Boot Order, or Boot Options in the menu and change the First Boot Device to the USB device.
5. Exit the menu.

Trend Micro Rescue Disk automatically opens after restarting.

Step 2: Using the Rescue Disk

Procedure

1. After you have restarted the endpoint, the Trend Micro Rescue Disk console opens automatically.
2. Press ENTER, or wait for a while. The **Confirm Disk Log** window appears.
3. Select **Yes**.

The **Choose Action** window appears.

4. Select **[1] Scan for Security Threats** and then select the type of scan.
 - **[1] Quick Scan:** Scan only the folders most vulnerable to system threats (such as the Windows System folder)
 - **[2] Full Scan:** Scan all folders

The Rescue Disk automatically starts scanning. Wait for the scan to finish.

5. If any threats are detected, the message "Are you sure you want to resolve these objects?" appears.

Select **Yes** to remove threats.



Note

The confirmation message only appears if you have configured the Rescue Disk to:

- Scan and quarantine objects
- Inform users before the quarantine starts

-
6. After scan logs are saved to the Scanning Tool, confirm the removal of the Scanning Tool from the endpoint.
 7. Press ENTER to restart the endpoint.
-

Chapter 6

Technical Support

Learn about the following topics:

- *Troubleshooting Resources on page 6-2*
- *Contacting Trend Micro on page 6-3*
- *Sending Suspicious Content to Trend Micro on page 6-4*
- *Other Resources on page 6-5*

Troubleshooting Resources

Before contacting technical support, consider visiting the following Trend Micro online resources.

Using the Support Portal

The Trend Micro Support Portal is a 24x7 online resource that contains the most up-to-date information about both common and unusual problems.

Procedure

1. Go to <http://esupport.trendmicro.com>.
2. Select from the available products or click the appropriate button to search for solutions.
3. Use the **Search Support** box to search for available solutions.
4. If no solution is found, click **Contact Support** and select the type of support needed.



Tip

To submit a support case online, visit the following URL:

<http://esupport.trendmicro.com/srf/SRFMain.aspx>

A Trend Micro support engineer investigates the case and responds in 24 hours or less.

Threat Encyclopedia

Most malware today consists of blended threats, which combine two or more technologies, to bypass computer security protocols. Trend Micro combats this complex malware with products that create a custom defense strategy. The Threat Encyclopedia

provides a comprehensive list of names and symptoms for various blended threats, including known malware, spam, malicious URLs, and known vulnerabilities.

Go to <http://about-threats.trendmicro.com/us/threatencyclopedia#malware> to learn more about:

- Malware and malicious mobile code currently active or "in the wild"
- Correlated threat information pages to form a complete web attack story
- Internet threat advisories about targeted attacks and security threats
- Web attack and online trend information
- Weekly malware reports

Contacting Trend Micro

In the United States, Trend Micro representatives are available by phone or email:

| | |
|---------------|--|
| Address | Trend Micro, Incorporated 225 E. John Carpenter Freeway, Suite 1500 Irving, Texas 75062 U.S.A. |
| Phone | Phone: +1 (817) 569-8900 Toll-free: (888) 762-8736 |
| Website | http://www.trendmicro.com |
| Email address | support@trendmicro.com |

- Worldwide support offices:
<http://www.trendmicro.com/us/about-us/contact/index.html>
- Trend Micro product documentation:
<http://docs.trendmicro.com>

Speeding Up the Support Call

To improve problem resolution, have the following information available:

- Steps to reproduce the problem
- Appliance or network information
- Computer brand, model, and any additional connected hardware or devices
- Amount of memory and free hard disk space
- Operating system and service pack version
- Version of the installed agent
- Serial number or Activation Code
- Detailed description of install environment
- Exact text of any error message received

Sending Suspicious Content to Trend Micro

Several options are available for sending suspicious content to Trend Micro for further analysis.

Email Reputation Services

Query the reputation of a specific IP address and nominate a message transfer agent for inclusion in the global approved list:

<https://ers.trendmicro.com/>

Refer to the following Knowledge Base entry to send message samples to Trend Micro:

<http://esupport.trendmicro.com/solution/en-US/1112106.aspx>

File Reputation Services

Gather system information and submit suspicious file content to Trend Micro:

<http://esupport.trendmicro.com/solution/en-us/1059565.aspx>

Record the case number for tracking purposes.

Web Reputation Services

Query the safety rating and content type of a URL suspected of being a phishing site, or other so-called "disease vector" (the intentional source of Internet threats such as spyware and malware):

<http://global.sitesafety.trendmicro.com/>

If the assigned rating is incorrect, send a re-classification request to Trend Micro.

Other Resources

In addition to solutions and support, there are many other helpful resources available online to stay up to date, learn about innovations, and be aware of the latest security trends.

Download Center

From time to time, Trend Micro may release a patch for a reported known issue or an upgrade that applies to a specific product or service. To find out whether any patches are available, go to:

<http://www.trendmicro.com/download/>

If a patch has not been applied (patches are dated), open the Readme file to determine whether it is relevant to your environment. The Readme file also contains installation instructions.

Documentation Feedback

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please go to the following site:

<http://www.trendmicro.com/download/documentation/rating.asp>

Index

D

documentation feedback, 6-6

S

support

 resolve issues faster, 6-4



TREND MICRO INCORPORATED

225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.
Phone: +1 (817) 569-8900, Toll-free: (888) 762-8736
Email: support@trendmicro.com

www.trendmicro.com

Item Code: TPEM38823/191001