# TREND MICRO™

## 3.0

# Trend Micro
# Portable Security™ 3 Pro
## User's Guide

Malware Scanning and Cleanup Tool with Secure File Transfer for
Air-Gapped Systems and Standalone PCs

for Windows™, LINUX™

**Endpoint Security**

# Trend Micro Portable Security™ 3 Pro User's Guide

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 3 Pro 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 4: Using the Scanning Tool Console

## Chapter 5: Scanning Linux Endpoints

## Chapter 6: Using the Secure Storage Console

## Chapter 7: Additional Tools

## Chapter 8: Technical Support

## Index

# Chapter 1

## Introduction

This chapter introduces the Trend Micro Portable Security™ 3 Pro product and features.

# Trend Micro Portable Security

Trend Micro Portable Security™ 3 Pro 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. You can also use the Management Program to manage all updates, scan settings, and the logs generated by the Scanning Tool.

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™ 3 Pro, 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.

Meanwhile, TMPS3 Pro offers a more secure way to transfer files. It monitors data put into secure storage in real time, and only files identified as clean can be placed in secure storage.

Trend Micro Portable Security™ 3 Pro has two main components, both with a console:

- **Management Program**: This program can manage several Scanning Tool devices. Refer to **Trend Micro Portable Security User's Guide**.

- **Scanning Tool**: You can register the Scanning Tool device to the Management Program or you can also use the Scanning Tool as a standalone tool. This means you will not have to install anything on any device.

## Management Program

The Management Program can perform actions including configuring scan settings and importing log data from multiple Scanning Tools.

You can use the Management Program to perform these tasks:

- Update and deploy security pattern files and scan engine components to registered Scanning Tools

- Change the scan settings and synchronize them with registered Scanning Tools

- Exclude files, folders, and extensions from scanning

- Import and manage log data generated by scans

- Specify an administrator account and password to enable scanning endpoints without administrator privileges

## 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 *Management Program Mode on page 1-4*.

> **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 7-4*.

**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 | • Exported to the Management Program<br><br>• Imported from another Scanning Tool | Imported from or exported to a endpoint. |

---

**Note**

TXOne Networks recommends installing OfficeScan™ on the endpoints with the Management Program installed.

While scanning for security threats, TXOne Networks 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.

---

## Management Program Mode

The Management Program Control mode registers the Scanning Tool to the Management Program, which manages all the registered Scanning Tools. All

the Scanning Tool devices can get the updates and scan settings from the Management Program and you can also upload all the logs from each device.



In this mode, there are two ways you can connect the Scanning Tool, by connecting the Scanning Tool directly to the Management Program computer or by connecting the Scanning Tool to a computer with Internet connection, and then remotely connecting to the Management Program computer.

- Direct connection

You can plug in the Scanning Tool device directly to the Management Program computer to get the updates, settings, or to transfer logs.

This setting is applicable for environments wherein all the computers are in one location and the Management Program computer is accessible. Here are some sample scenarios.
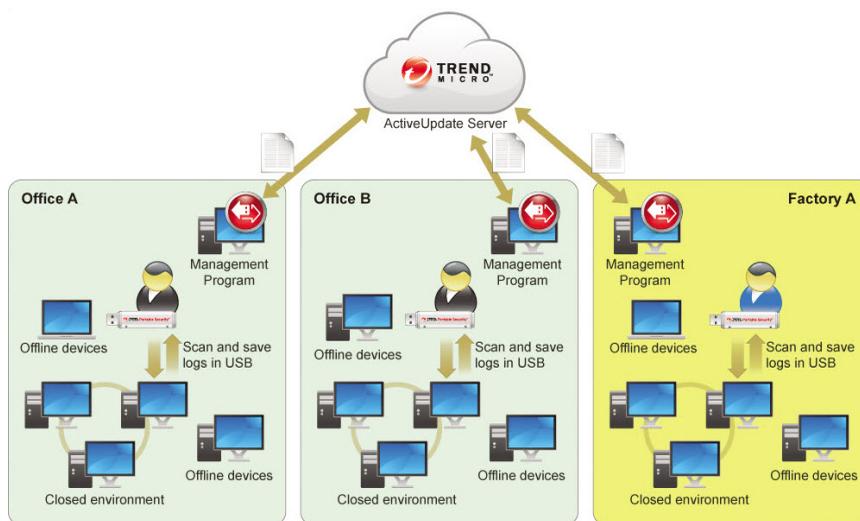


- Remote connection

    You can plug in the device from any computer with an Internet connection and then connect to the Management Program online to get the updates, settings, or to transfer logs.

---

**Note**

There might be communication issues if a firewall is between Management Program and the Scanning Tool. If this is the case, accept and give permission to the `C:\Program Files\Trend Micro\Portable Security 3\SfSrvCom.exe` process.

---
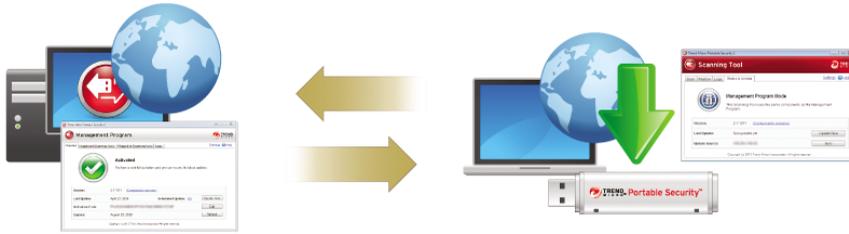
This setting is applicable if you have several locations. In each location, you can have just one computer with an Internet or network connection and use that to regularly connect to the Management Program. Here are some sample scenarios.
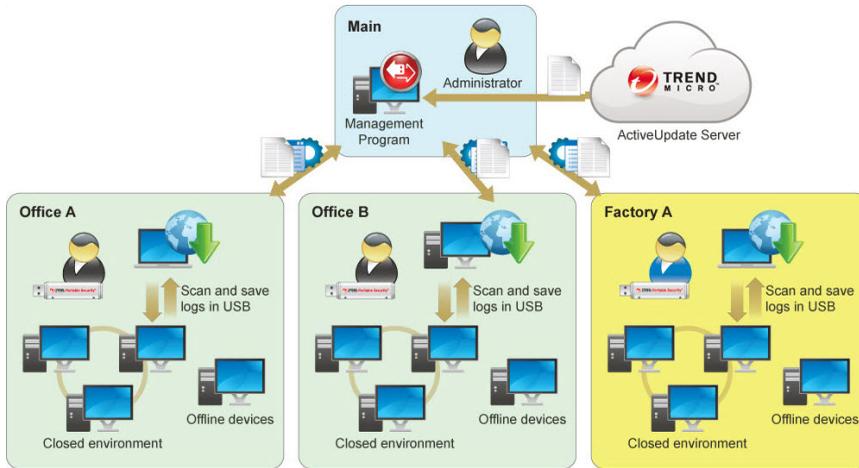


## Standalone Scanning Tool

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 |
| --- | --- |
| Secure storage | Trend Micro Portable Security 3 Pro supports storage with automatic malware scanning prior to transferring the files into the Scanning Tool. For the latest list of supported operating systems, please refer to the system requirements here:<br><br>https://success.trendmicro.com/solution/000245560-Portable-Security-3-0-System-Requirements |
| USB enhancement | 1. The Scanning Tool device's storage capacity has been upgraded to 128 GB. 64GB of this is taken up by secure storage.<br><br>2. Hardware encryption is supported with AES-256 for Secure Storage. Please refer to *Using the Secure Storage Console on page 6-1* for initialization.<br><br>3. The Pro edition of TMPS3 has been given a brand-new design. |

## Older Versions of Trend Micro Portable Security

Older versions of Portable Security are similar to Trend Micro Portable Security 3 Pro. 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

## Setting Up

Before you can use the Trend Micro Portable Security 3 Pro Scanning Tool, remember the following:

> **Important**
>
> You must activate the Scanning Tool before using it. Refer to *Activating a Managed Scanning Tool on page 2-7* for more information.

- If the user account has administrator privileges, you can use Trend Micro Portable Security 3 Pro to scan the computer.

- If the user account does not have administrator privileges, you can enable the **Scan as administrator** option then open Windows Explorer and double-click Launcher.exe from the TMPS3 SYS partition.

- Portable Security saves the scan result logs in the Scanning Tool after scanning a device.

Portable Security saves the scan result logs in the Scanning Tool after scanning a device.

# Installing the Management Program

The Management Program is the central console for the components, settings, and logs of all the Scanning Tool devices. Each managed Scanning Tool can be used in a separate location but can upload and sync with the Management Program locally or remotely.

💡 **Tip**

Trend Micro does not recommend installing the Management Program on an endpoint that has an older version of the Management Program already installed. Install the Management Program on a different endpoint to ensure that your older Scanning Tools can continue to sync logs.

**TABLE 2-1. System Requirements**

| ITEM | REQUIREMENT |
|------|-------------|
| Disk space | Trend Micro recommends dedicating a minimum of 2 GB of disk space on the Management Program endpoint<br><br>• 700 MB for the Management Program<br><br>• 1.3 GB for log files |
| Privileges | You must have Administrator privilege on the endpoint |

**Procedure**

1. Plug-in the Scanning Tool to the target computer.

2. Open Windows Explorer and double-click MP_Install.exe from the TMPS3 SYS\MP directory to start the program.

3. When the **End User License Agreement** screen appears, read the agreement and click **Agree and Install**.
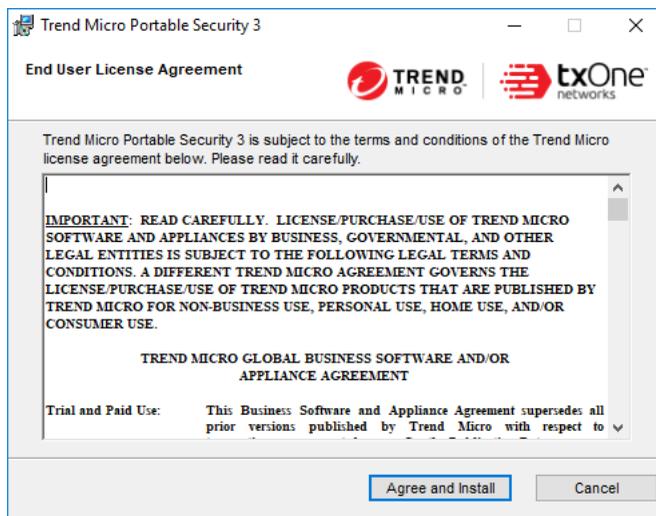
4. When the **Installation Destination** screen appears, type or browse for a folder and click **Next**.
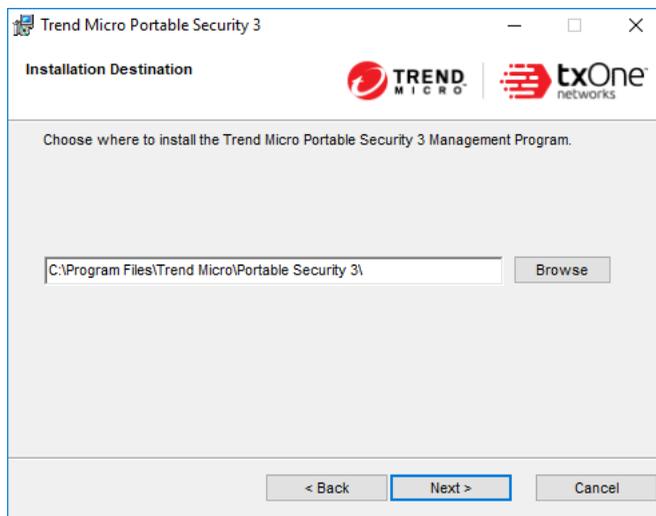
5. When the **Activation Code** screen appears, specify your Activation Code and click **Next**.
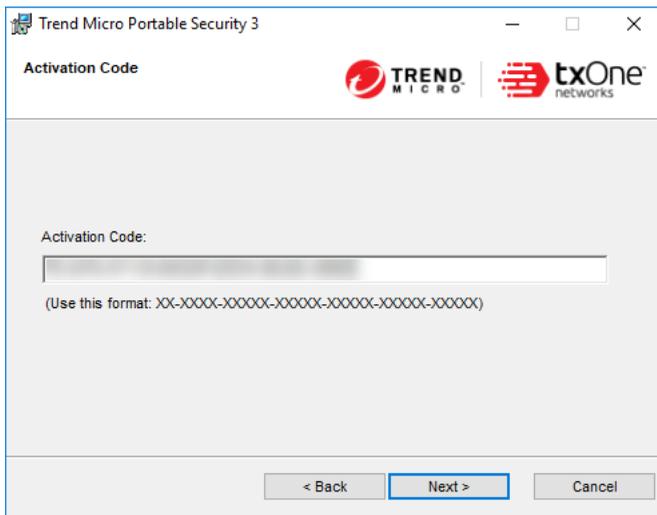


> **Note**
>
> You're able to manage a license for **Portable Security 3** and a license for **Portable Security 3 Pro** here. You can add another license later in the **Overview** tab after installation.

6. When the **Communication Port and Password** screen appears, specify the IP address, port number on the endpoint, and create a password.

7. Click **Next**.

8. When the **Installation Done** screen appears, click **Close**.
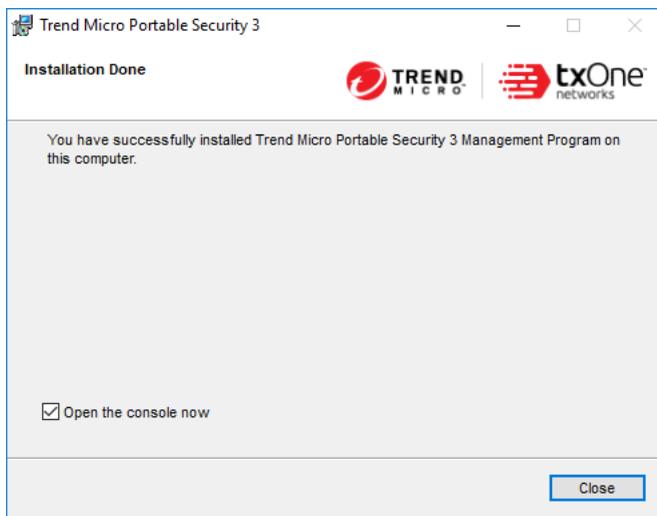
## Activation

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 7-6*.

> **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 2-2. Icons and messages regarding Activation Codes**

| ICON | MESSAGE |
|------|---------|
| ✓ | This Activation Code is already active and no action is needed. |
| ! | • This Activation Code is going to expire soon and you need to renew your subscription. |
| ✕ | • This Activation Code has not yet been activated and you need to activate to be able to use the product.<br>• 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 Managed Scanning Tool

Managed Scanning Tool devices are registered to the Management Program. Each Scanning Tool can synchronize device settings and download the latest updates from the Management Program. Each Scanning Tool device can also upload files to the Management Program.

**Procedure**

• Option 1: Simple Activation

1. Install the Management Program.

2. Plug-in the new Scanning Tool or any Scanning Tool that has not yet been activated to the same computer. The Scanning Tool should automatically activate and register to the Management Program.

- Option 2: Alternative Activation Procedure

  1. Plug the new Scanning Tool or any Scanning Tool that has not yet been activated into a computer running Management Program .

     > **Note**
     >
     > If there is a firewall between the Management Program and the Scanning Tool, accept and give permission to the `C:\Program Files\Trend Micro\Portable Security 3\SfSrvCom.exe` process to continue.

     Open Windows Explorer and double-click `Launcher.exe` in the `TMPS3_SYS` partition to start the program.

     The **Scanning Tool Mode** screen opens.

     Select **Management Program Control** and click **Next**.

     The **Management Program and Proxy Settings** screen opens.

  2. Specify the following:

     - Scanning Tool name

     - Management Program address, port, and password

     - (Optional) Proxy settings

  3. Click **Activate**.

  4. (Optional) Go to the **Status & Update** tab and click **Update Now** to get the latest components.

## 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` or `SecureStorage.exe` from the `TMPS3 SYS` partition to start the program.
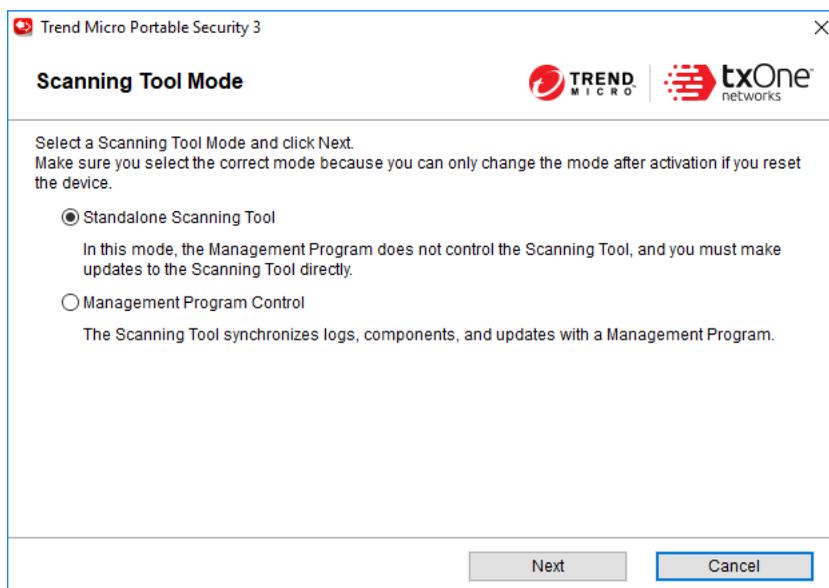


3.  Select **Standalone Scanning Tool** and click **Next**.
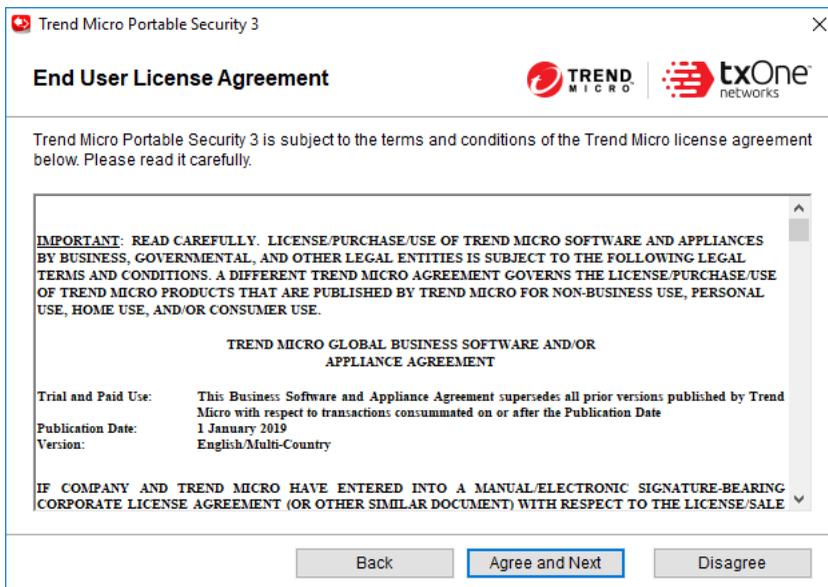
4. When the **End User License Agreement** screen appears, read the agreement and click **Agree and Next**.

**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 2-6*.

**Procedure**

**1.** Access the correct screen for the Scanning Tool type.

a. For a managed Scanning Tool device, open the Management Program.
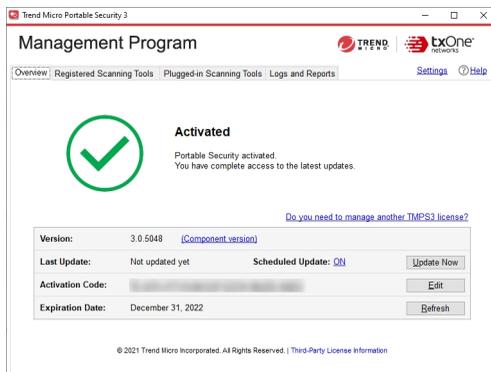


b. For a standalone Scanning Tool, open the Scanning Tool console and click the **Status & Update** tab.
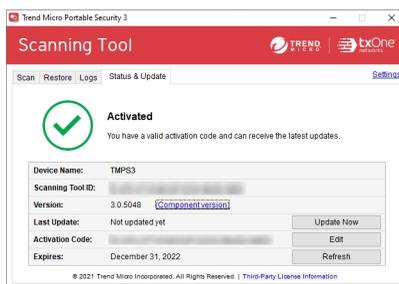


**2.** Click **Edit**.

**3.** Type the new Activation Code.

**4.** Click **OK**.

# Upgrades

Trend Micro releases updates to Trend Micro Portable Security 3 Pro occasionally to provide more features and improve performance.

> **Note**
>
> Portable Security does not support upgrading from older versions.
>
> For more information, see *Older Versions of Trend Micro Portable Security on page 1-9*.

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**.

## Upgrading the Management Program

Trend Micro releases updates to Trend Micro Portable Security 3 Pro occasionally to provide more features and improve performance.

> **Note**
>
> • Portable Security does not support upgrades from older versions of Trend Micro Portable Security.
>
>   For more information, see *Older Versions of Trend Micro Portable Security on page 1-9*.
>
> • Make sure you have at least 2.3 GB of free space on the Management Program endpoint for temporary usage during the upgrade.

**Procedure**

1. Download and double-click the setup package. The **End User License Agreement** page appears.

2. Read the Trend Micro License Agreement and select **Agree and Install**.

**3.** Click **Close** when the upgrade is complete.

## Upgrading the Scanning Tool

Trend Micro releases updates to Trend Micro Portable Security 3 Pro 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**

- Upgrade by Synchronizing with the Management Program

  a. Upgrade the Management Program.

  b. Plug in the Scanning Tool to the Management Program endpoint or connect it remotely through the Internet.

  c. Select the Scanning Tool from the list shown in the Management Program and click **Sync Components and Settings**.

- Upgrade Using the Support Tool

  a. Close the Scanning Tool console if it is open.

  b. Log on to the endpoint using an account with administrator privileges and connect the Scanning Tool.

  c. Download the Trend Micro Portable Security 3 Pro service pack.

  d. Extract the contents of the service pack to a local folder on the endpoint where you have connected the Scanning Tool.

  e. From the `TMPS3 SYS` drive, copy the `SupportTool` folder from the USB device onto your local drive.

f.  In the appropriate Win32 or x64 folder, double-click the TMPSSuprt.exe file ().

g.  Go to the **More Tools** tab.

h.  Click the **Use for Updates** button.

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

j.  Click **Browse** and select the .bin file from the service pack provided by Trend Micro.

k.  Click **Apply**. A confirmation window opens.

# Chapter 3

## Using the Management Program

This chapter describes how to use and configure the Trend Micro Portable Security 3 Pro Management Program.

# Understanding the Management Program Console

The Management Program console consists of tabbed screens and links to configure Scanning Tools, collect and view logs, and administer the console.

**TABLE 3-1. Console Controls**

| CONTROL | DESCRIPTION |
| --- | --- |
| **Overview** | Check the status of the components and perform an update, if needed |
| | For more information, see *Overview Tab on page 3-2*. |
| **Registered Scanning Tools** | Configure the scan settings of all registered Scanning Tools managed by this Management Program |
| | For more information, see *Registered Scanning Tools on page 3-7*. |
| **Plugged-in Scanning Tools** | Check the status of the Scanning Tool devices currently plugged into the Management Program computer |
| | For more information, see *Plugged-in Scanning Tools on page 3-13*. |
| **Logs and Reports** | Check the results of earlier scans performed by the Scanning Tool |
| | For more information, see *Logs and Reports Tab on page 3-15*. |
| **Settings** | Check or change the Management Program settings |
| | For more information, see *Management Program Settings on page 3-16*. |
| **Help** | Open the help and find more information about how to use the console |

# Overview Tab

The **Overview** tab shows the Management Program status and enables changes to program settings.

| Item | Description |
|------|-------------|
| **Version** | The build number of the Trend Micro Portable Security 3 Pro Management Program<br><br>Click the **Component versions** link to see the component details and the date of the last update.<br><br>For more information, see *Checking the Latest Components on page 3-4*. |
| **Last Update** | The date of the last component update<br><br>•   **Scheduled Update**: Enable to automatically update the Management Program components on the configured schedule<br><br>    For more information, see *Scheduled Update on page 3-6*.<br><br>•   **Update Now**: Click to manually update the Management Program components |
| **Activation Code** | The Activation Code currently used by the Management Program and Scanning Tools<br><br>•   **Edit**: Click to change or update the Activation Code<br><br>•   **Refresh**: Click this button when you have changed the Activation Code and it still says expired<br><br>•   **Do you need to manage another TMPS3 license?**: Click here to add a license for managing different versions of the Scanning Tool. |
| **Expiration Date** | The last day that the current Activation Code permits you to receive support or component updates |

## Checking the Latest Components

To check the component version currently used and the date of the last update, click the **Component versions** link on the **Overview** tab.
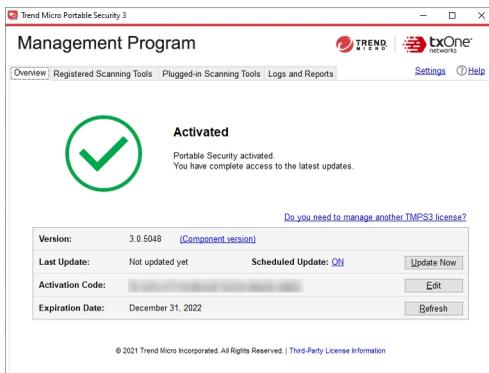


Trend Micro Portable Security uses the following components.

To select the components to download, see *Scan Settings (Others) on page 3-12*.

**TABLE 3-2. Trend Micro Portable Security 3 Pro Components**

| COMPONENT | DESCRIPTION |
| --- | --- |
| Virus Scan Engine (32-bit/64-bit) | At the heart of all Trend Micro products lies the scan engine, which was originally developed in response to early file-based computer viruses. The scan engine today is exceptionally sophisticated and capable of detecting different types of viruses and malware. The scan engine also detects controlled viruses that are developed and used for research. |
| | Rather than scanning every byte of every file, the engine and pattern file work together to identify the following: |
| | •     Tell-tale characteristics of the virus code |
| | •     the precise location within a file where the virus resides |

| Component | Description |
|---|---|
| Advanced Threat Scan Engine (32-bit/64-bit) | The Advanced Threat Scan Engine uses a combination of signature file-based scanning and heuristic rule-based scanning to detect and document exploits and other threats used in targeted attacks.<br><br>Major features include the following:<br><br>1.   Detection of zero-day threats<br><br>2.   Detection of embedded exploit code<br><br>3.   Detection rules for known vulnerabilities<br><br>4.   Enhanced parsers for handling file deformities |
| Behavior Monitoring Core Driver (32-bit/64-bit) | Prevents Trend Micro Portable Security 2 from being affected by rootkits which hide drivers, processes, and registry entries from tools that use common system application programming interfaces (APIs). |
| Scanner (32-bit/64-bit) | This engine scans, cleans, and restores tasks. |
| Damage Cleanup Engine (32-bit/64-bit) | Scans for and removes Trojans and Trojan processes. |
| Virus Pattern | Contains information that helps Security Agents identify the latest virus/malware and mixed threat attacks.<br><br>Trend Micro creates and releases new versions of the Virus Pattern several times a week, and any time after the discovery of a particularly damaging virus/malware. |
| Damage Cleanup Template | Used by the Virus Cleanup Engine to identify Trojan files and processes so the engine can eliminate them. |
| Spyware/Grayware Pattern | Identifies spyware/grayware in files and programs, modules in memory, Windows registry, and URL shortcuts. |
| Digital Signature Pattern | A list of approved programs that are regarded safe and will be excluded for scans. |

| COMPONENT | DESCRIPTION |
|---|---|
| Program Inspection Pattern | The pattern was designed to have the rule set for program inspection. The rule types include CLSID, file path, product name, company name, shortcut, and related registry. It also contains the fake AV detection rules. Currently it is used for fake AV detection for most of cases, so it would also be the fake AV pattern. |

## Scheduled Update

Enable Scheduled Update to automatically download the most recent components at the scheduled times.

**Procedure**

1. From the **Overview** tab, click the link beside **Scheduled Update**.

   **Note**

   The link may show ON or OFF, depending on the current status of the update setting. If the link shows as **ON**, you have enabled scheduled updates. If the link shows as **OFF**, you have not enabled scheduled updates and will only get updates if you manually click the **Update Now** button.

2. Enable the **Use Scheduled Update** option.

3. Select the update frequency and the start time.

4. Click **Save**.

   After making changes, the link in the **Overview** tab should change, depending on whether the scheduled update option has been enabled or disabled.

# Registered Scanning Tools

The **Registered Scanning Tools** tab displays a list of all registered Scanning Tools managed by this Management Program and provides the ability to change scan settings.

| Section | Description |
| --- | --- |
| Standard Scanning Tool Setting | Displays a limited selection of settings currently applied to "Standard" Scanning Tools |
| | **Edit**: Click to view or modify the scan settings for "Standard" Scanning Tool devices registered to the Management Program |
| Scanning Tools List | Displays information about all the Scanning Tools registered to the Management Program |
| | • **Scanning Tool**: Click the Scanning Tool name to view logs on the scans, synchronizations, and updates that the Scanning Tool has performed |
| | • **Scanning Tool ID**: The unique ID of the Scanning Tool device |
| | • **Last Sync**: The last time that the Scanning Tool synchronized data and settings with the Management Program |
| | • **Last Update**: The last time that the Scanning Tool updated components |
| | • **Device Settings**: Click to change between **Standard** (if the Scanning Tool uses the **Standard Scanning Tool Setting**) or **Custom** (to modify existing settings) |
| | • **Lock**: Click to lock or unlock the Scanning Tool user's ability to change settings directly 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

  - **Enable CVE detection**: Select to detect files exploiting known vulnerabilities in commercially available products based on the Common Vulnerabilities and Exposures (CVE) system.

- **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 recommend action**: Automatically takes the Trend Micro recommended action per threat type

---

📝 **Note**

Restart the Scanning Tool program for the changes to take effect.

---

## Scan Type

Use the followings setting to identify which drives and folders you want to scan:

---

💡 **Tip**

Synchronize the settings to your device after making the changes in the Management Program.

---

- **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

  - Click **Add** to put a drive or folder on the list.

  - Click **Delete** to take selected drives or folders off the list.

  - Click **Edit** to make changes to the selected item.

## Scan Option

You can select additional options regarding scan priority and whether to scan removable drives.

- **Scan removable drives**: The Scanning Tool scans any removable storage connected to the endpoint

- **Set to lowest priority**: The scanning process is set to the lowest priority to reduce system resource usage

> **✎ Note**
>
> This may increase the scanning time.

- **Enable Suspend scan**: Displays the **Suspend** button during a scan, which allows users to pause the endpoint scan and resume the scan at a later time

> **✎ Note**
>
> This affects the scanning time and stores temporary files on the endpoint.

- **Enable CVE detection**: Select to detect files exploiting known vulnerabilities in commercially available products based on the Common Vulnerabilities and Exposures (CVE) system.

## Scan Action

The scan action setting determines what the scan will do.

- **Confirm**: The scan will identify security threats and then ask what action to perform.

- **Log only**: The scan will only identify security threats, without taking any action against them.

- **Take the recommended action**: The scan will automatically respond to security threats according to the recommendations of Trend Micro experts.

> **💡 Tip**
>
> Whether the scan will remove the security threat, place the file in quarantine, or skip over it depends on the type of threat. Trend Micro reviews and revises the automatic responses periodically, so they may change after an update.

## Scan Settings (Advanced)

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

- **Exclusion List**: Add files, folders, or file extensions to exclude from scans

  Refer to *Changing the Exclusion List Settings on page 3-11*.

- **Scan without saving temporary files**: Scans without saving files to the target computer

  > **Important**
  >
  > This function is not applicable for scanning a Management Program computer.

- **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.

- **Compressed Layer**: 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 threats 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 more information, see *Trend Micro Rescue Disk on page 7-8*.

## Scan Settings (Others)

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

- **Scanning Tool Name**: Change the name of the Scanning Tool device.

  > 📝 **Note**
  >
  > Only available when modifying **Custom** Scanning Tool settings.

- **Use Proxy Server**: Enable this option if your computer is required to use a proxy server to connect to the Management Program. 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™ on the Management Program computer.

  - **Enter the necessary proxy server settings in the following fields**: Choose this option to enter the proxy server settings yourself.

- **Program Components**: Click the **Settings** button to specify which components to download.

  For more information, see *Checking the Latest Components on page 3-4*.

- **Asset Info**: Allow the collection of endpoint information after launching a Scanning Tool. Select to automatically begin collecting data about the current state of the endpoint after plugging in the Scanning Tool

- **Collect logs from Trend Micro Safe Lock**: Enable this option to collect logs from computers with Trend Micro Safe Lock™.

## Plugged-in Scanning Tools

The **Plugged-in Scanning Tools** tab allows you to view and manage any Scanning Tools currently plugged into the Management Program endpoint.

| Item | Description |
|---|---|
| **Change Name** | Changes the name of the Scanning Tool |
| **Transfer Logs** | Transfers logs from the Scanning Tool device to the Management Program |
| | Trend Micro recommends selecting the confirmation dialog option, **After transferring, delete the log file from the Scanning Tool**, to keep the Scanning Tool disk space available. |
| **Sync Components and Settings** | Downloads components and settings from the Management Program to the Scanning Tool |
| Scanning Tool list | Select a Scanning Tool to view synchronization and component update information |

## Updating Components through a Scanning Tool

You can update the Management Program by importing components from a Scanning Tool which contains the latest components. This update method is suitable for scenarios that satisfy the following conditions:

- The Management Program is established in a closed network and does not have connectivity to the Trend Micro ActiveUpdate Server.

- The Scanning Tool has access to and contains the latest components.

**Procedure**

1. Plug in the Scanning Tool device to the Management Program computer. The Management Program console opens automatically.

2. Click the **Plugged-in Scanning Tools** tab.

3. Select a Scanning Tool. When there are newer components on this device, these components will be indicated as 'newer', and the **Update Now** button will be accessible.

4. Click the **Update Now** button to start the update.

# Logs and Reports Tab

The **Logs and Reports** tab allows you import, export, and manage log data.

| Item | Description |
| --- | --- |
| **Import Logs** | Imports database format logs that you exported from another Management Program |
| **Export Logs** | Export all scan logs to a database or CSV format <br><br> ⚠️ **Important** <br> You must select **Back up all scan data and logs (DB)** if you want to import scan logs to another Management Program. |
| **Delete Logs** | Deletes specified scan logs <br><br> 📝 **Note** <br> Trend Micro recommends exporting logs before performing the delete action. |
| **Export Asset Info** | Exports any asset information collected by the Scanning Tools in CSV format <br><br> • System and hardware information <br><br> • Update information (Microsoft applications only) <br><br> • Installed application list |
| Filter list results | • **Computers**: Lists scan logs based on computer name <br><br> • **Scanning Tools**: Lists scan logs based on Scanning Tool name <br><br> • **Calendar**: Filters scan log entries based on specified time frame |
| View scan logs by **Computer** name | • Click the **Computer** name to view a list of all scan logs performed on that endpoint <br><br> • Click **Last Scan** time to view the scan results for the last available scan data on the endpoint |

| ITEM | DESCRIPTION |
|---|---|
| View scan logs by **Scanning Tools** name | • Click the **Scanning Tool** name to pop up a summary screen about the Scanning Tool device<br><br>  • **Overview**: Display general information about Scan, Sync, and Update actions performed by the Scanning Tool<br><br>  • **Scan**: Lists all scan logs performed by the Scanning Tool<br><br>  • **Sync**: Lists information about log transfers and component updates on the Scanning Tool<br><br>  • **Update**: Lists information about the components updated on the Scanning Tool<br><br>  • **Device Info**: Displays the current component versions on the Scanning Tool<br><br>• Click **Last Scan** time to view the scan results for the last available scan data transferred by the Scanning Tool |

# Management Program Settings

- Click **Settings** > **Management Program Settings...** to make changes to how the Management Console connects to the Internet and Scanning Tools, and the source of component updates.

- Click **Settings** > **Import / Export Settings** to restore or back up Management Program settings.

## General Settings

The **General** tab allows you to control Management Program settings including proxy, external communication authentication, and console language.

---

> **Important**
>
> You must **Save** all changes before navigating to another screen or tab.

---

- **Use Proxy Server**: Enable this option if your computer is required to use a proxy server to connect to the Management Program. 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™ on the Management Program computer.

  - **Enter the necessary proxy server settings in the following fields**: Choose this option to enter the proxy server settings yourself.

- **Listening Settings**: Specify the Password and Port that the Management Program uses for communication with Scanning Tools attempting to connect remotely.

- **Language**: Changes the display language on the Management Program

## Update Settings

The **Update** tab allows you to change the source from which the Management Program receives component updates.

> **Important**
>
> You must **Save** all changes before navigating to another screen or tab.

- **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.

## Backing Up and Restoring Management Program Settings

Trend Micro recommends backing up your Management Program settings in case when you need to migrate or restore the Management Program environment.

An export will include the following Management Program settings:

- Basic configurations

- A list of registered Scanning Tools

- Scanning Tool settings

---

**Note**

The following settings are not included for export:

- Activation Code

- Security patterns and components

- Diagnostic Toolkit settings

- Management Program password and connection port

---

## Exporting and Importing Management Program Settings

To access the settings, click **Settings** from the Management Program console, and click **Export Settings** or **Import Settings**.

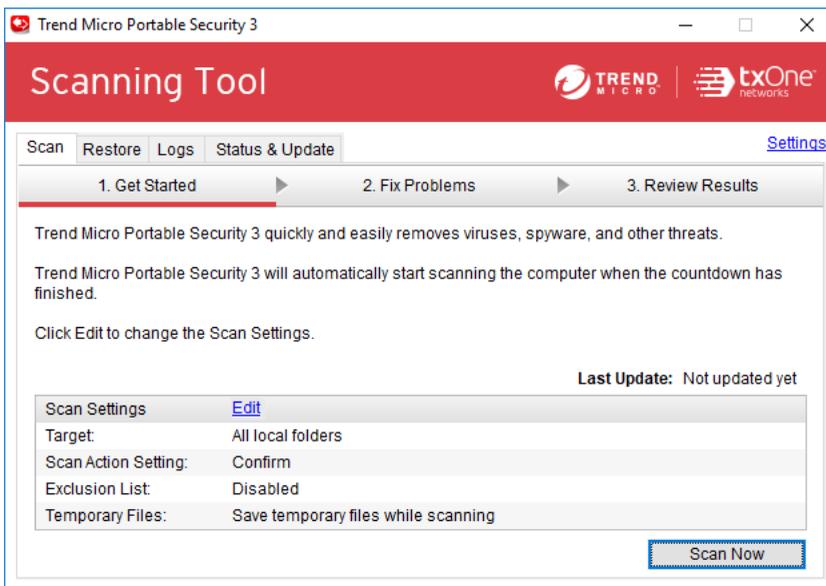# Chapter 4

## 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 4-4*.

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

**TABLE 4-1. 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 4-5*.

- **Apply Now** (threats detected): Click to apply actions on detected threats.

  For more information, see *Security Threats Found on page 4-9*.

- **Comment**: Type a comment to add to the log entry for the scan
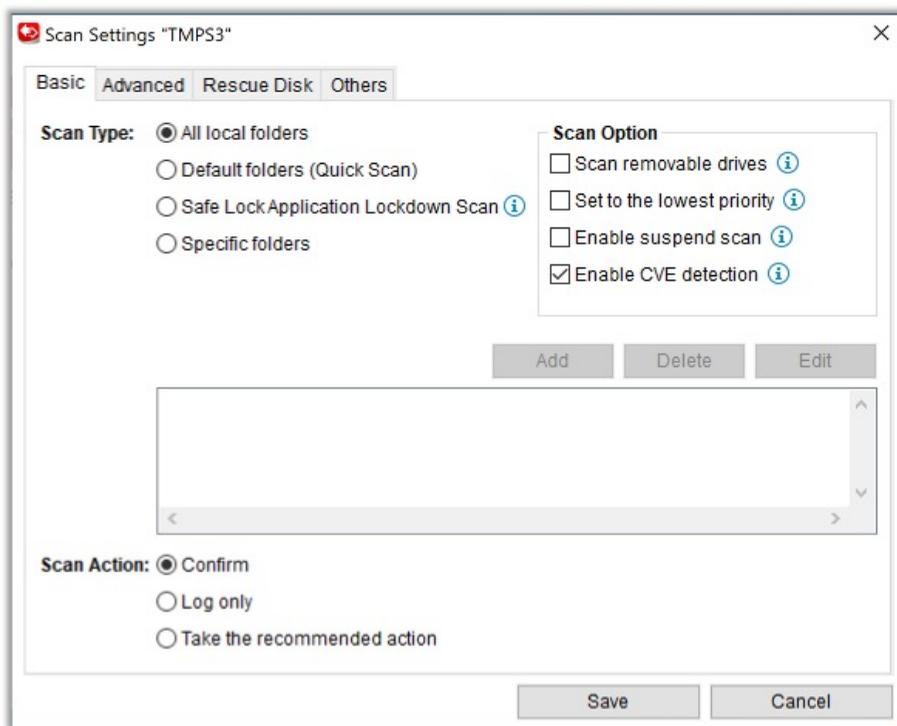
> ⚠️ **WARNING!**
>
> Trend Micro does not recommend unplugging the Scanning Tool while the LED is flashing or while the Scanning Tool console is open.

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:

- **Exclusion List**: Add files, folders, or file extensions to exclude from scans

  Refer to *Changing the Exclusion List Settings on page 3-11*.

- **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.
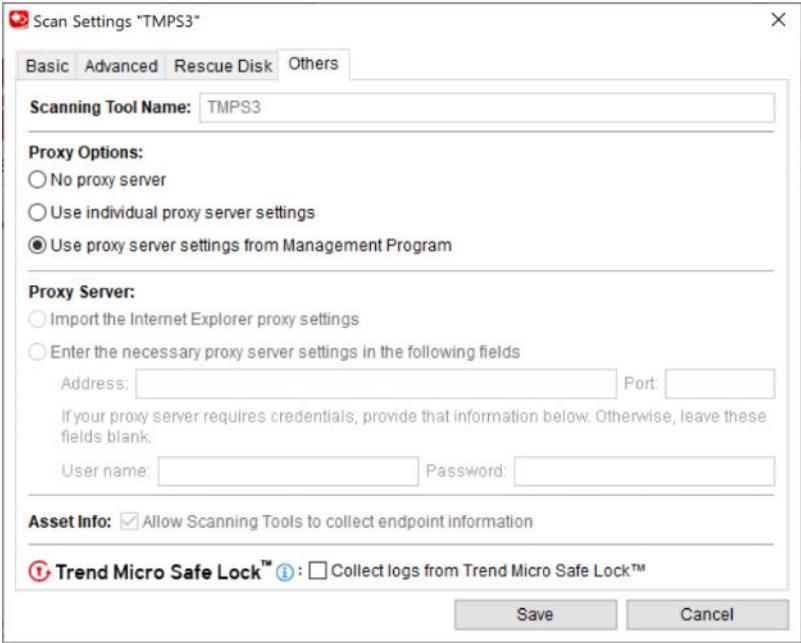
## Scan Settings (Rescue Disk)

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

- **Scan and quarantine objects**: Select this option to quarantine detected threats 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 7-8*.

## Scan Settings (Others)

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.

- **Asset Info**: Allow collection of endpoint information after launching a Scanning Tool.

- **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 4-10*.

---

⚠️ **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 4-8*.

- **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
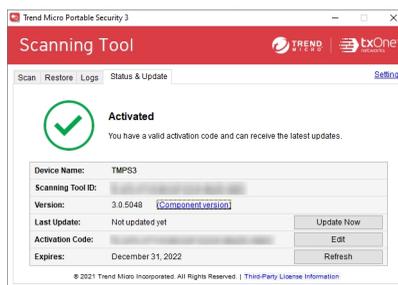


The **Status & Update** tab shows the device component status.

For more information on the device activation status, refer to *Activation on page 2-6*.

- **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.

   For more information, see *Changing the Activation Code on page 2-11*.

- **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.
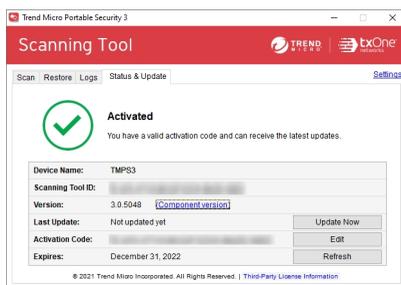


### Updating Components On-Demand

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 4-15*.

2.  From the Scanning Tool console, go to the **Status & Update** tab.
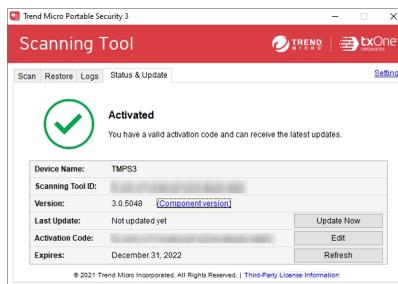
**FIGURE 4-1. Standalone device**

**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.
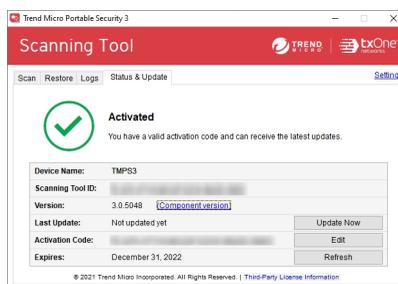


**FIGURE 4-2. The Standalone Scanning Tool console**

**2.** Click **Settings**.

> **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 5

## 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 2-6*.

---

# Linux System Requirements

| ITEM | REQUIREMENTS |
|---|---|
| Operating system | • Red Hat Enterprise Linux 6.0 or later<br>• CentOS 6.0 or later |
| Privileges | The logged on account must have one of the following privileges:<br>• "root" user<br>• "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 | • `-c \| --command <scan \| restore>`<br>• `-h \| --help`<br>Displays the help screen |
| <scan options> | • `-a \| --action <action>`<br>Scan action to apply that overrides default configuration settings:<br>`log \| confirm \| recommended` |
| <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 2-6*.

**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 5-2*.

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 ./LauncherLinux.sh --debug –c scan <scan targets> > /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 6

## Using the Secure Storage Console

This chapter outlines the features available in the Secure Storage console.

> ⚠️ **Important**
>
> This function is only available on Windows endpoints.

# To Transfer Files

Secure Storage is designed to keep malware out and only carry files which that have been scanned by Portable Security prior to being transferred into storage.
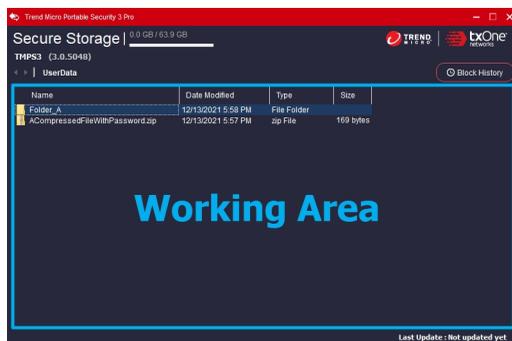


- **Last Update:** Shows the last time that the pattern has been updated.

> **Tip**
>
> The pattern and update settings are shared between the Scanning Tool console and Secure Storage console, which means any pattern update or setting changes made in one console will affect the other.

- **Block History**: Check the history of malware discovered during file transfers.

Use the working area to transfer your files in or out of Secure Storage.

> **Note**
>
> When you launch Secure Storage for the first time, you will be asked to set up a password for Secure Storage.

**Procedure**

**1.** Open the Secure Storage console by double clicking SecureStorage.exe in the TMPS3_SYS folder.

When you launch Secure Storage for the first time, you will be asked to set up a password.
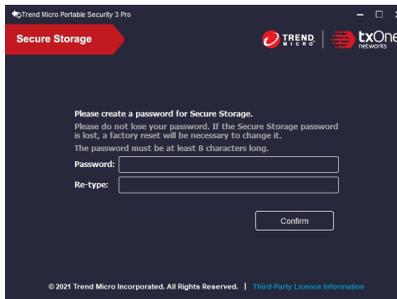


**2.** Click and drag file from where it is on your machine to the working area of Secure Storage, as marked in blue. Portable Security will begin to scan the file before transferring it to the device. Refer to the LED lights on the Portable Security device to determine the scan status.

**TABLE 6-1. Portable Security indicator lights**

| INDICATOR LIGHTS | DESCRIPTION |
|---|---|
| Blue (Blinking) | Launching or closing Secure Storage. |
| Blue (Continuous) | Files were transferred to Secure Storage and no threats were found. |
| Red (Continuous) | Threats were blocked by Secure Storage. |
| Blue, Yellow, and Red (Continuous) | Secure Storage is currently transferring files. |

# Block History
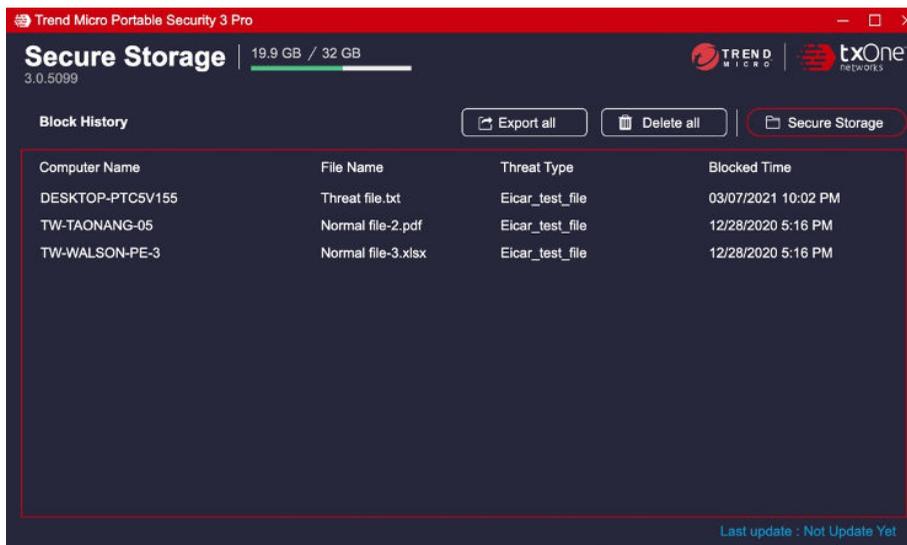


| ITEM | DESCRIPTION |
|---|---|
| **Export all** | Export all malware event logs to a database or CSV format<br><br>⚠️ **Important**<br>You must select **Backup all scan data and logs (DB)** if you want to import scan logs to another Management Program. |

| Item | Description |
|------|-------------|
| **Delete all** | Deletes all event logs |
| | **Note** |
| | Trend Micro recommends exporting logs to back them up before deleting them. |

## Change Password

Please find this function under the password authentication page.
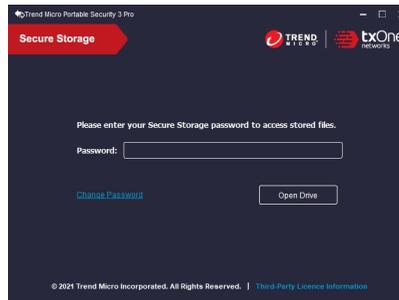


## Resetting Secure Storage

**Reset Device** affects both Scanning Tool and Secure Storage, so please make sure data you want to preserve is backed up before resetting the device.

Please refer to *Reset Device on page 7-4* for more details.

## Lost Password

If you lose your password, Secure Storage will be locked until Portable Security has been reset.

Please refer to *Reset Device on page 7-4* for more details.

## Maximum Number of Password Attempts Exceeded

If you exceed the maximum number of password attempts, Secure Storage will be locked until Portable Security has been reset.

Please refer to *Reset Device on page 7-4* for more details.

# Chapter 7

## Additional Tools

This chapter discusses how to use the additional tools provided with Trend Micro Portable Security 3 Pro.

# Trend Micro Portable Security Diagnostic Toolkit

Use the Trend Micro Portable Security Diagnostic Toolkit to diagnose and troubleshoot problems. Trend Micro Portable Security 3 Pro 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 3 Pro endpoint, click **Trend Micro Portable Security 3** > **Trend Micro Portable Security 3 Diagnostic Toolkit**.

    a.  Plug-in the Trend Micro Portable Security 3 Pro 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 Portable Security Devices

**Procedure**

**1.** Plug-in the Trend Micro Portable Security 3 Pro 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. According to your situation, choose **Scanning Tool** or **Secure Storage** and click **Start**.

    c. Reproduce the problem encountered by Trend Micro Portable Security 3 Pro.

    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 3 Pro installed.

**5.** Launch the Trend Micro Portable Security 3 Diagnostic Toolkit.

From the Start menu of the Trend Micro Portable Security 3 Pro 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 3 Pro 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.

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 more information, see *Scan Settings (Rescue Disk) on page 3-12*.

---

Rescue Disk supports the following file systems:

| OPERATING SYSTEM | FILE SYSTEM |
| --- | --- |
| Windows | NTFS and FAT |

| Operating System | File System |
|---|---|
| Linux | EXT2, EXT3, EXT4 and XFS |
| | **Note** |
| | Rescue Disk runs on any Linux distribution installed on a supported file system. |

## 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.

## Scanning Tool Agent

The Scanning Tool Agent is a service by which the plugged-in Scanning Tool's actions can be initiated. This includes scanning computers, updating components, and configuring as well as synchronizing settings with the Management Program. Actions can be started when a Scanning Tool is plugged in or scheduled to start periodically from a plugged-in Scanning

Tool. Scheduled actions will be conducted according to the configuration in the Scanning Tool Agent. If there is more than one Scanning Tool plugged into an endpoint with Scanning Tool Agent installed, the actions will be executed one by one. That is, there can't be more than one Scanning Tool active at the same time.

Actions that Scanning Tool Agent triggers includes:

- Automatically activating a Scanning Tool into Management Program mode

- Automatically updating components

- Auto scan

- Automatically synchronizing logs and settings

- Periodically scanning

- Periodically updating components

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

With the configuration generator (STAgentConfigGen.exe), users can create a customized configuration to save inside the installer before installation. When users need to auto-activate, they can use this configuration generator.

---

⚠ **Important**

    This function is only available on Windows endpoints.

---

## Installing the Scanning Tool Agent

The folder `TMPSAgent` under `TMPS3 SYS` in the Scanning Tool USB is the installation package. If you want to customize the Scanning Tool Agent configuration before installation, please follow the later section "Customizing the Configuration Before Installation".

Two modes of installation are available: installing with GUI and installing using the command line.

> **Note**
>
> Upgrading an existing Scanning Tool Agent won't change the existing configuration.

## Uninstalling the Scanning Tool Agent

There are also two ways to uninstall the Scanning Tool Agent: uninstalling with GUI and uninstalling using the command line.

> **Note**
>
> • Make sure the Scanning Tool is not plugged into the endpoint before continuing.
>
>   Make sure to unlock Trend Micro Safe LockTM 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.
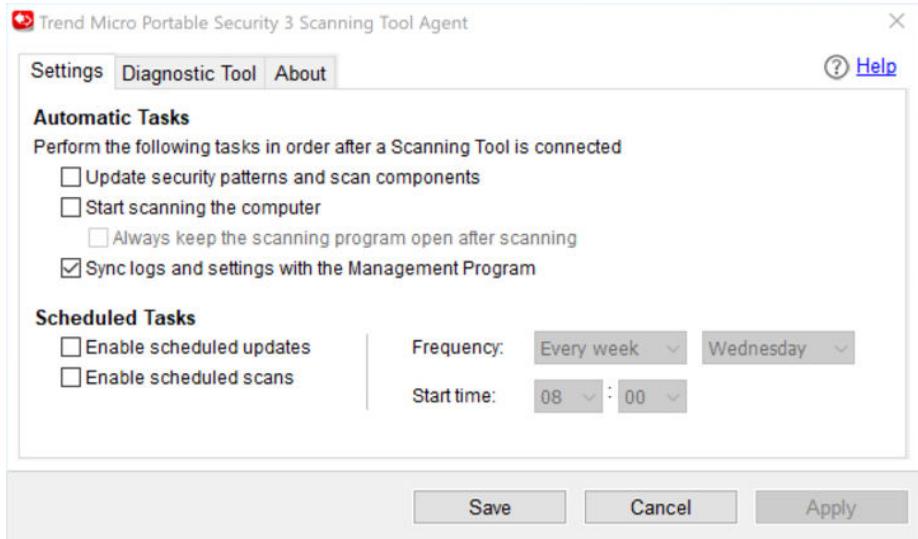
## Settings Tab

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

| Section | Options |
|---|---|
| **Automatic Tasks** | • **Update security patterns and components**: Select to automatically update the Scanning Tool for the latest security patterns and components. <br><br> • **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**. <br><br>    • **Always keep the scanning program open after scanning**: Select to ensure that you can view scan logs immediately after a scan completes. <br><br>     ⚠ **Important** <br>     • This option interrupts all automatic tasks by the Scanning Tool Agent including synchronization and scheduled updates. <br><br> • **Sync logs and settings with the Management Program**: Select this option to synchronize logs and settings of the Scanning Tool with the Management Program. <br><br>    📝 **Note** <br>    Ensure that there is a working network connection between the Scanning Tool Agent and the Management Program. <br><br>    ⚠ **Important** <br>    This feature is only functional for Scanning Tools operating in Management Program Control mode. |

| SECTION | OPTIONS |
|---|---|
| **Scheduled Tasks** | • **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. |
| | **Note** <br> 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. |

## 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 8

## Technical Support

Learn about the following topics:

# 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, 8-6

**S**
secure storage, 1-9
support
    resolve issues faster, 8-4

**T**
TMPS3 Pro, 1-2