



TREND MICRO™
Portable Security 2™
Service Pack 4
User's Guide



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/trend-micro-portable-security-2.aspx>

Trend Micro, the Trend Micro t-ball logo, and Trend Micro Portable Security 2 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 © 2017. Trend Micro Incorporated. All rights reserved.

Document Part No.: TPPEM28077_171019

Release Date: November 2017

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>

Table of Contents

Chapter 1: Introduction

Trend Micro Portable Security 2	1-2
What is Trend Micro Portable Security 2?	1-2
New in Trend Micro Portable Security 2 SP4	1-11
Trend Micro Portable Security 1.5 and Older Versions	1-12

Chapter 2: Setting Up

Installing the Management Program	2-3
Activation	2-8
Activation Status	2-8
Activating Managed Scanning Tool Devices	2-9
Activating a Standalone Scanning Tool	2-12
Changing the Activation Code	2-14
Upgrades	2-17
Upgrading the Management Program	2-17
Upgrading the Scanning Tool	2-19

Chapter 3: Using the Management Program

Understanding the Management Program Console	3-2
Overview Tab	3-5
Registered Scanning Tools	3-6
Plugged-in Scanning Tools	3-8
Logs and Reports Tab	3-9
Scan Settings	3-10
Scan Setting Category	3-10
Scan Settings (Basic)	3-16
Scan Settings (Advanced)	3-19
Rescue Disk	3-22
Scan Settings (Others)	3-23

Component Updates	3-28
Checking the Latest Components	3-28
Updating Components On-Demand	3-30
Scheduled Update	3-31
Updating Components through a Scanning Tool	3-32
Changing the Update Source	3-33
Logs and Reports	3-35
Viewing Logs and Reports	3-35
Importing or Exporting Logs from the Management Program ...	3-41
Transferring Logs from the Scanning Tool	3-46
Collecting Logs from Trend Micro Safe Lock	3-48
Backing Up and Restoring Management Program Settings	3-51
Exporting and Importing Management Program Settings	3-52
Other Settings	3-52
Changing the Management Program Settings	3-52

Chapter 4: Using the Scanning Tool

Understanding the Scanning Tool Device Console	4-2
Scan Tab	4-6
Restore Tab	4-7
Logs Tab	4-8
Status & Update tab	4-10
Component Updates	4-12
Updating Components On-Demand	4-13
Synchronizing Component Updates	4-15
Performing a Scan	4-16
Checking the Scan Results	4-18
Changing the Scanning Tool Settings	4-23
Scanning Tool Name Setting	4-26
Scan Settings	4-29
Synchronizing Logs and Settings	4-31
Removing the Scanning Tool	4-32
For Windows 10	4-33
For Windows 8	4-36

For Windows 7	4-39
For Windows Vista or Windows XP	4-39
Using the Scanning Tool Agent	4-40
Installing the Scanning Tool Agent	4-40
Uninstalling the Scanning Tool Agent	4-43
Settings Tab	4-44
Diagnostic Tool for the Scanning Tool Agent	4-46

Chapter 5: Additional Tools

Trend Micro Portable Security 2 Diagnostic Toolkit	5-2
Debug	5-2
Reset Device	5-15
Support Updates	5-21
Converting Logs	5-24
Trend Micro Rescue Disk	5-25
Step 1: Preparation	5-26
Step 2: Using the Rescue Disk	5-28
Step 3: Viewing the Logs	5-31
Scanning Tool Agent	5-32

Chapter 6: Uninstallation

Option A: From the Windows Start Menu	6-2
Option B: From the Control Panel	6-3
Option C: Use the Trend Micro Portable Security 2 Diagnostic Toolkit	6-4

Chapter 7: Getting Help

Frequently Asked Questions (FAQs)	7-2
Using the Support Portal	7-2
Speeding Up the Support Call	7-3
Threat Encyclopedia	7-3
Data Transmissions to Trend Micro	7-4
Export Controls	7-5

Multi-year Contracts 7-6

Chapter 8: Technical Support

Troubleshooting Resources 8-2

- Using the Support Portal 8-2
- Threat Encyclopedia 8-2

Contacting Trend Micro 8-3

- Speeding Up the Support Call 8-4

Sending Suspicious Content to Trend Micro 8-4

- Email Reputation Services 8-4
- File Reputation Services 8-5
- Web Reputation Services 8-5

Other Resources 8-5

- Download Center 8-5
- Documentation Feedback 8-6

Index

Index IN-1

Chapter 1

Introduction

This chapter introduces the Trend Micro Portable Security 2™ product and features.

Topics in this chapter:

- *Trend Micro Portable Security 2 on page 1-2*
- *New in Trend Micro Portable Security 2 SP4 on page 1-11*
- *Trend Micro Portable Security 1.5 and Older Versions on page 1-12*

Trend Micro Portable Security 2

Trend Micro Portable Security 2™ 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.

What is Trend Micro Portable Security 2?

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 2, 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.

Trend Micro Portable Security 2 has two main components, both with a console:

- **Management Program:** This program can manage several Scanning Tool devices. Refer to **Trend Micro Portable Security 2 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:

- Download security pattern file and scan engine components
- Change the scan settings and synchronize them with the Scanning Tool
- Exclude files, folders, and extensions from scanning

- Import and manage log data generated by scans
- Specify an administrator account and password to enable scanning computers without administrator privileges

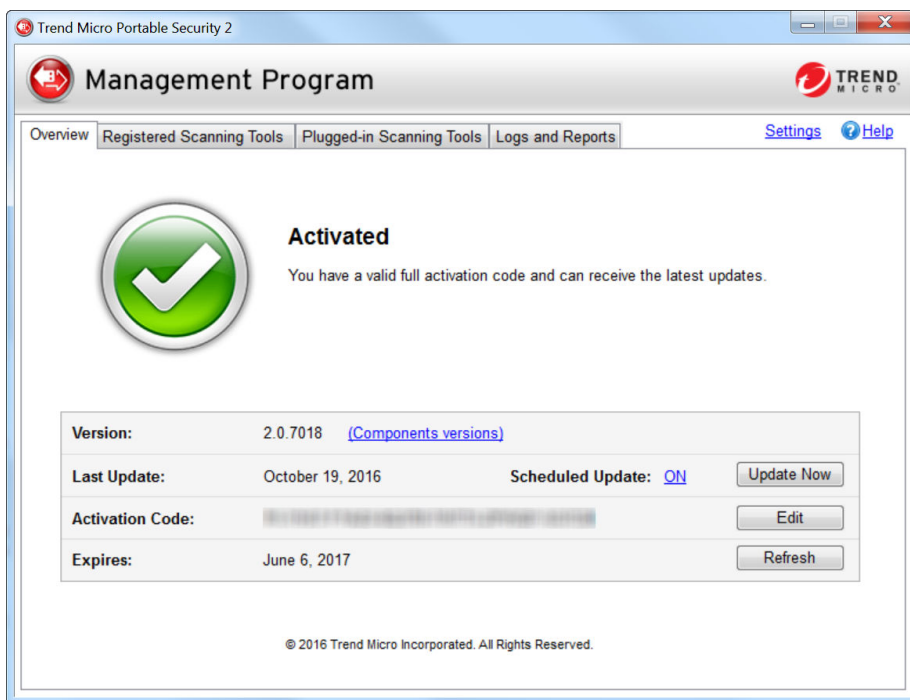


FIGURE 1-1. Main screen of the Management Program

Scanning Tool (USB Device)

The Scanning Tool can check the computer 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.



FIGURE 1-2. The Scanning Tool screen



Note

If the Scanning Tool does not start, you can open Windows Explorer and double-click `Launcher.exe` from the `TMPS2_SYS` partition.

Each Scanning Tool has its own console. However, the features seen on the console will depend on the mode you chose. You can choose either Standalone Scanning Tool or Management Program Control.

Refer to *Management Program Control on page 1-6* or *Standalone Scanning Tool on page 1-10*.

**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 the device on page 5-15](#).

TABLE 1-1. Main differences between Management Program Control and Standalone Scanning Tool

	MANAGEMENT PROGRAM CONTROL	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 computer 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 computer.

**Note**

Trend Micro recommends installing Trend Micro™ OfficeScan™ on the computers with the Management Program installed.

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

For more information, refer to [Scan Settings \(Advanced\) on page 3-19](#).

Management Program Control

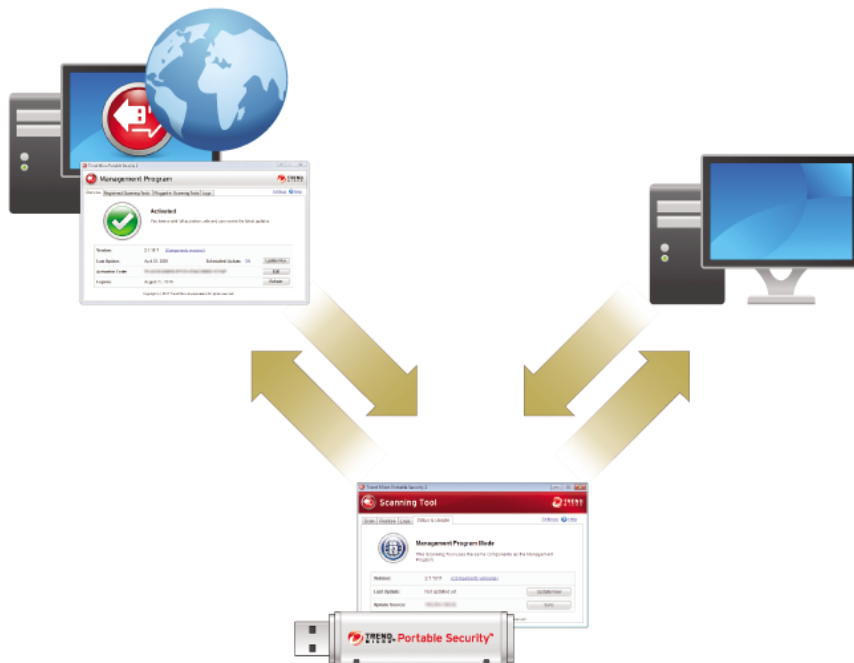
The Management Program Control mode registers the Scanning Tool to the Management Program, which manages all the registered Scanning Tools. All the Scanning Tool devices can get the updates and scan settings from the Management Program and you can also upload all the logs from each device.



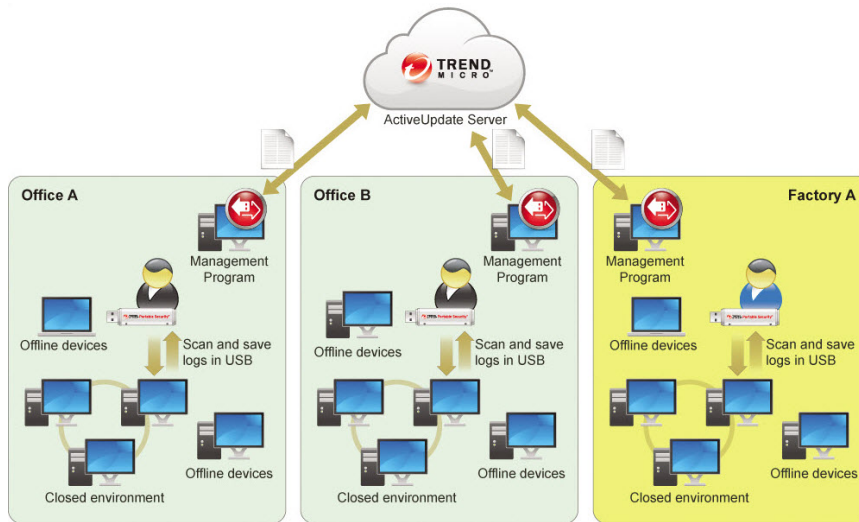
In this mode, there are two ways you can connect the Scanning Tool, by connecting the Scanning Tool directly to the Management Program computer or by connecting the Scanning Tool to a computer with Internet connection, and then remotely connecting to the Management Program computer.

- 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.

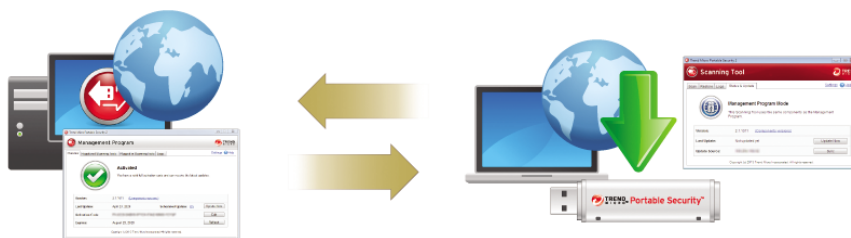


- Remote connection

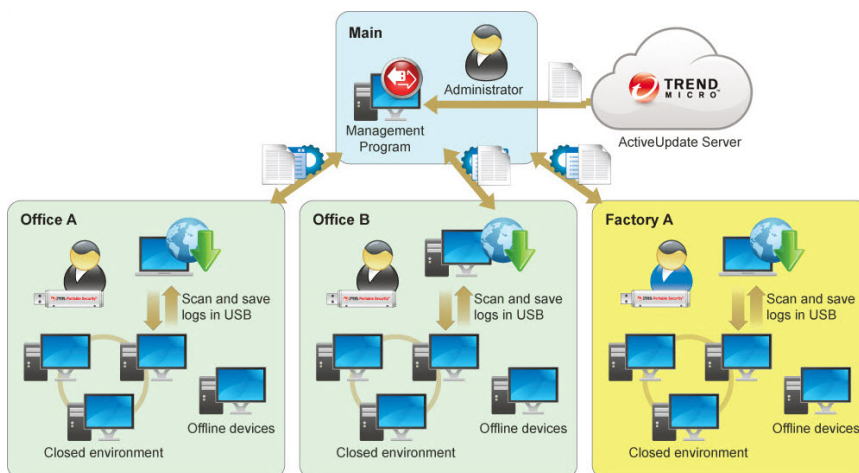
You can plug in the device from any computer with an Internet connection and then connect to the Management Program online to get the updates, settings, or to transfer logs.

 **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 2\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 computer that has Internet connection to update the components, change scan settings, or check the logs.



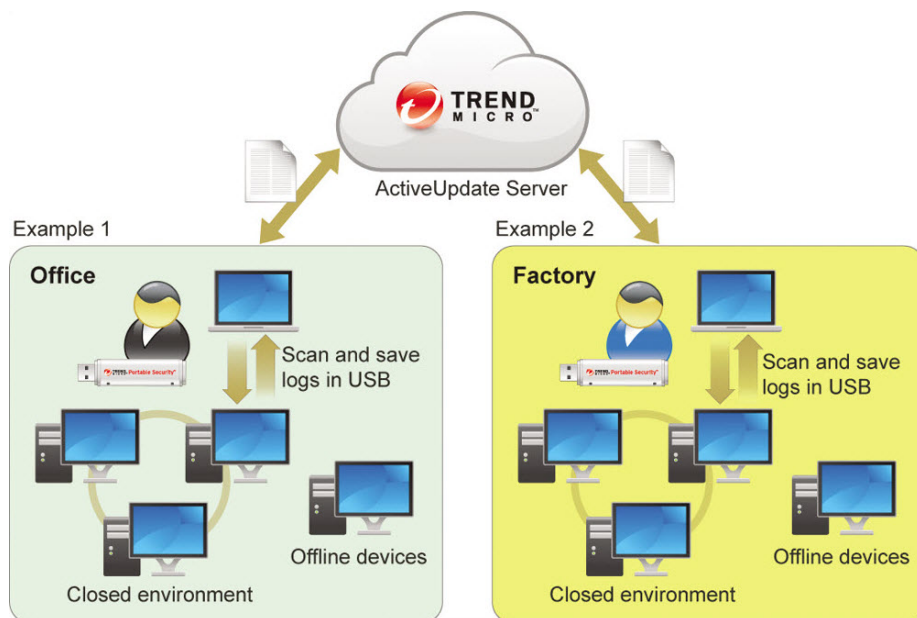
This setting is for those who want to use the Scanning Tool without having to go to the Management Program for updates or changes to the settings. With this mode, you can make any changes to the Scanning Tool settings from the Scanning Tool console.



Note

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

Here are some sample scenarios.



New in Trend Micro Portable Security 2 SP4

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

TABLE 1-2. New Features

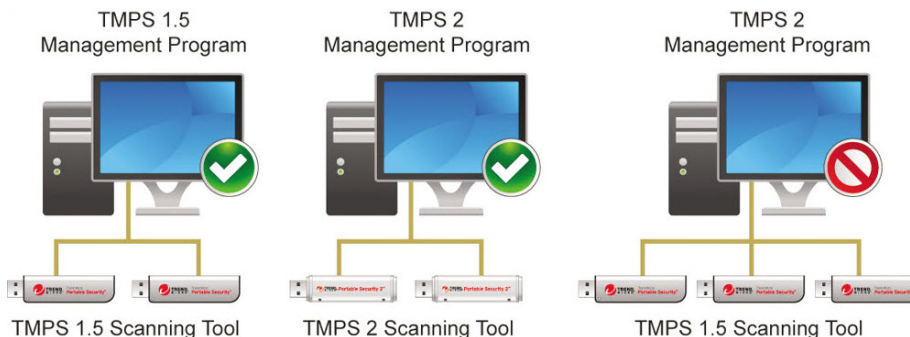
FEATURE	DESCRIPTION
Suspend a running scan	Users now have the option to suspend a scan in progress and resume scanning immediately after the Scanning Tool is launched. See Scan Settings on page 4-29

TABLE 1-3. Enhanced Features

FEATURE	DESCRIPTION
Manual rescan of files containing unresolved threats	You can use the Restore tab on the Scanning Tool console to perform additional scanning of files that still contain security threats. Click Scan to attempt to fix unresolved threats. See Restore Tab on page 4-7 .
Enhanced logs from Rescue Disk scan	Rescue Disk logs have been enhanced with additional scan information. See Step 3: Viewing the Logs on page 5-31 .
Platform support enhancements	<ul style="list-style-type: none"> Windows 10 Creators Update (Red Stone 2) 32/64-bit Windows Server 2016 64-bit

Trend Micro Portable Security 1.5 and Older Versions

Trend Micro Portable Security 1.5 is similar to Trend Micro Portable Security 2 but both products will be sold independently and will have different activation code formats.





Tip

Trend Micro recommends keeping Trend Micro Portable Security 1.5 and older on a separate computer to be able to use Trend Micro Portable Security 1.5 and Trend Micro Portable Security 2 Scanning Tools.

Chapter 2

Setting Up

Before you can use the Trend Micro Portable Security 2 Scanning Tool, remember the following:



Important

You must activate the Scanning Tool before using it. Refer to [Activating Managed Scanning Tool Devices on page 2-9](#) or [Activating a Standalone Scanning Tool on page 2-12](#) for more information.

- If the user account has administrator privileges, you can use Trend Micro Portable Security 2 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 `TMPS2_SYS` partition.
- Trend Micro Portable Security 2 saves the scan result logs in the Scanning Tool after scanning a device.
- To open the Scanning Tool console on an endpoint installed with Management Program, make sure the Management Program console is closed.

Trend Micro Portable Security 2 saves the scan result logs in the Scanning Tool after scanning a device.

Topics in this chapter:

- *Installing the Management Program on page 2-3*
- *Activation on page 2-8*
- *Upgrades on page 2-17*

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 the Management Program locally or remotely.



Note

Make sure you have Administrator privileges and at least 2 GB of free space on this computer for installation. Management Program will occupy 700 MB of space when it is installed.

Procedure

1. Connect the Scanning Tool USB device to the computer where you want to install the Management Program.



Tip

If you have the Trend Micro Portable Security 1.5 Management Program, install the Trend Micro Portable Security 2 Management Program on a separate computer. This is to ensure that you can still use your older Scanning Tools with the Trend Micro Portable Security 1.5 Management Program.

2. When a window opens, click **Open folder to view files**.





Tip

Alternatively, you can double-click the **My Computer** icon and open the TMPS2_SYS drive.

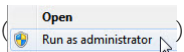
3. Open the MP folder in the TMPS2_SYS drive, and double-click the MP_Install.exe file ().



Note

For some operating systems, you have to make sure you right-click the file and select

Run as administrator



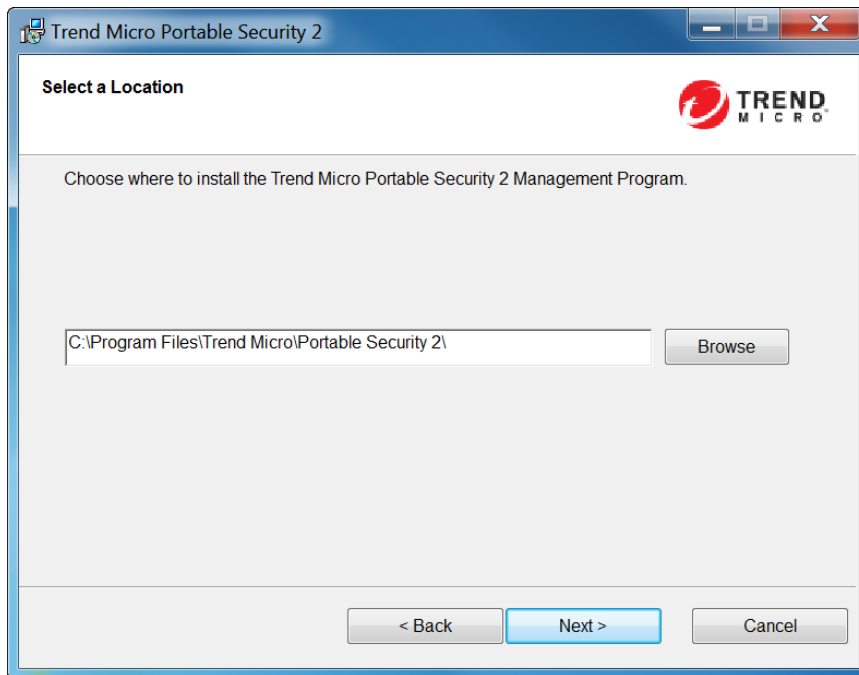
4. When the **End User License Agreement** window appears, read the agreement and click **Agree and Install**.



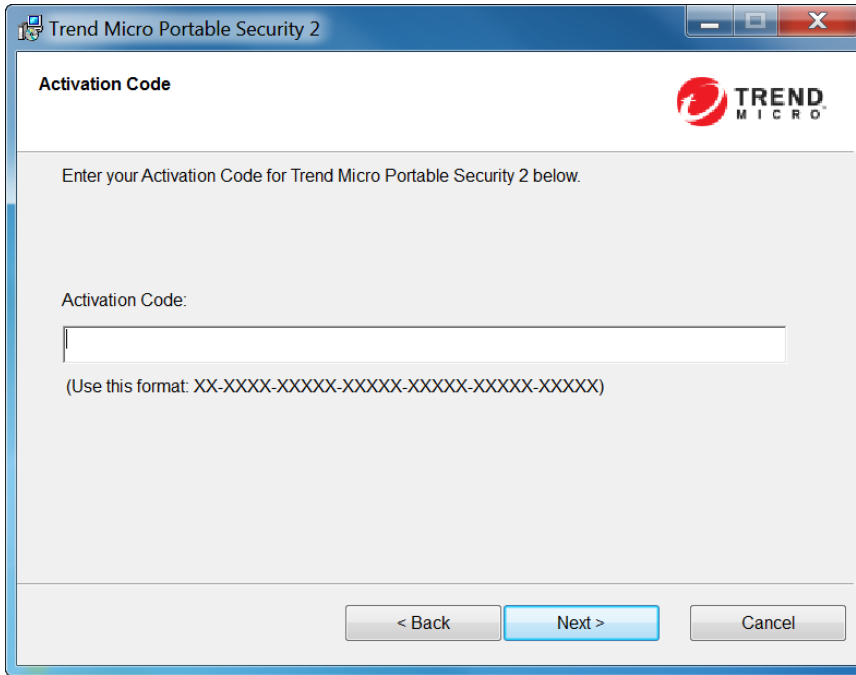
5. When the **Select Location** window opens, you can select a different folder, or click **Next**.

**Note**

To install the program in a different location, click **Browse** and select a folder.



6. When the **Activation Code** window appears, type your activation code, and then click **Next**.



7. When the **Management Port and Password** window appears, specify the port number and the password twice.

Trend Micro Portable Security 2

Management Port and Password

Specify the port number and password that the Management Program will use to establish a connection with the Scanning Tool.

Port:

Password:

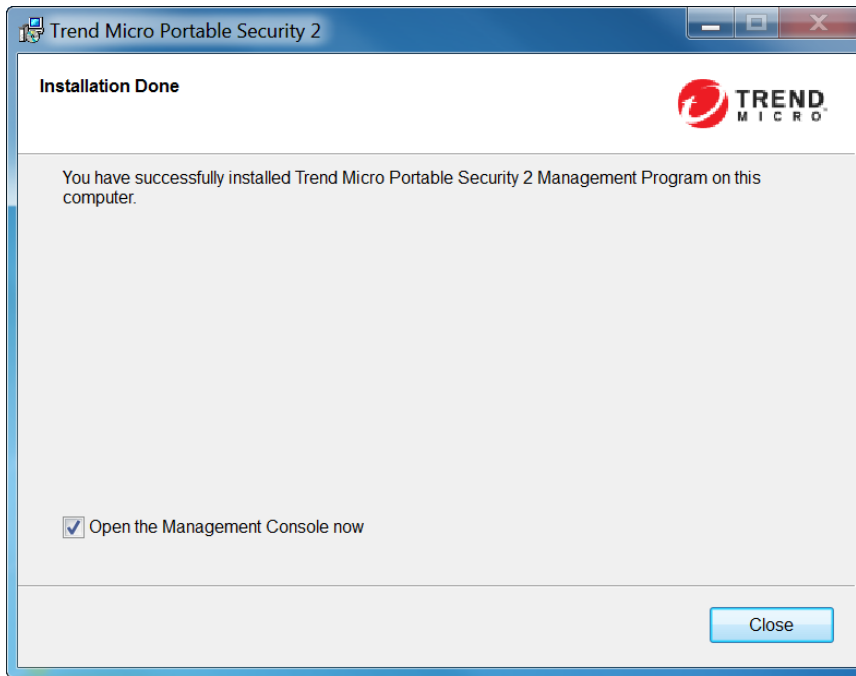
Confirm Password:

< Back Next > Cancel

**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 2\SfSrvCom.exe process to continue.

8. Click **Next**.
9. When the **Installation Done** window appears, click **Close**.



If you marked the **Open the Management Console now** option, the Management Program will open so that you can make changes to your settings.

Activation




Activate the device before you can use the Scanning Tool device. However, make sure you select the correct mode, either Management Program Control or Standalone Scanning Tool, before activating the device. This is because you can only change the mode after activation if you [reset the device on page 5-18](#).

Activation Status

When looking at the **Status and Update** tab of the Scanning Tool console and the **Overview** tab of the Management Program, different messages appear at the bottom of

the window depending on the number of days remaining before your activation code expires.

TABLE 2-1. 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.
	<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 one expires to ensure that the Scanning Tool always has the most recent updates.

Activating Managed Scanning Tool Devices

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

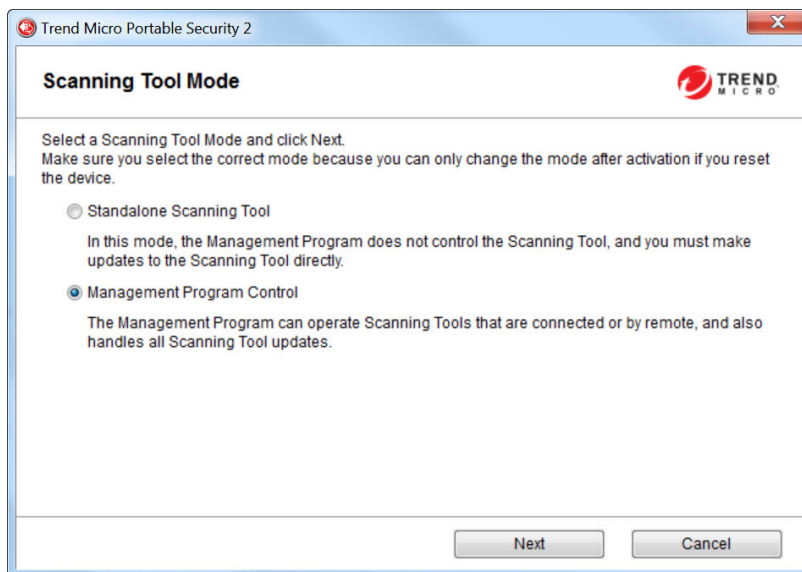
- Option 1: Simple Activation
 1. Install the Management Program.

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-in the new Scanning Tool or any Scanning Tool that has not yet been activated on a Management Program computer.

**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 2\SfSrvCom.exe process to continue.

The **Scanning Tool Mode** screen opens.



**Note**

If the window does not open, your security software or computer may have blocked the autorun process. Open Windows Explorer and double-click `Launcher.exe` from the `TMPS2_SYS` partition to start the program.

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

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

Trend Micro Portable Security 2

Management Program and Proxy Settings

You can edit the setting below.

Scanning Tool Name:

Management Program: Address: Port:
Password:

Proxy Server: Use 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:

Back Activate Cancel

3. Specify the following:
 - Scanning Tool name
 - Management Program address, port, and password
 - (Optional) Proxy settings
4. Click **Activate**.
5. (Optional) Go to the **Status & Update** tab and click **Update Now** to get the latest components.

Activating a Standalone Scanning Tool

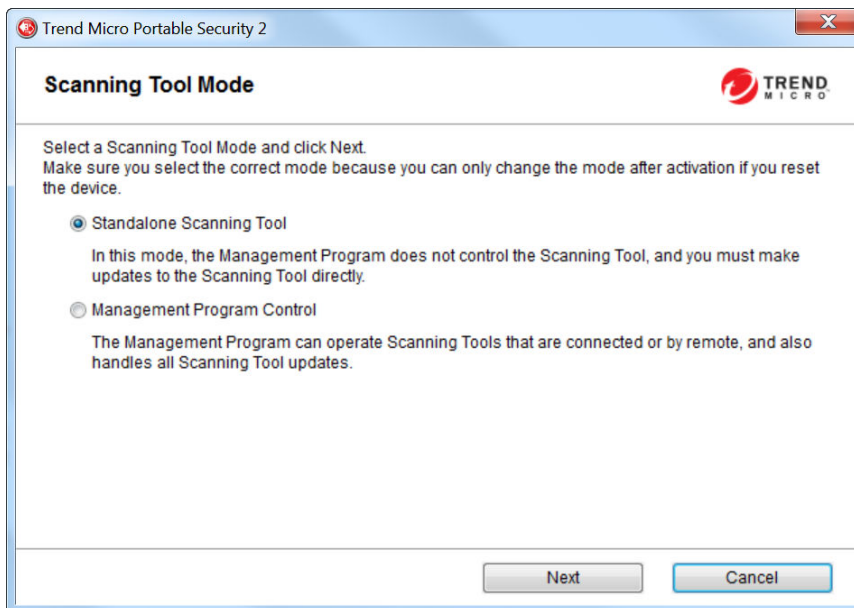
Standalone Scanning Tools are independent of the Management Program and you can update the components directly from the Internet.

**Note**

To activate a managed device, refer to *Activating Managed Scanning Tool Devices on page 2-9*

Procedure

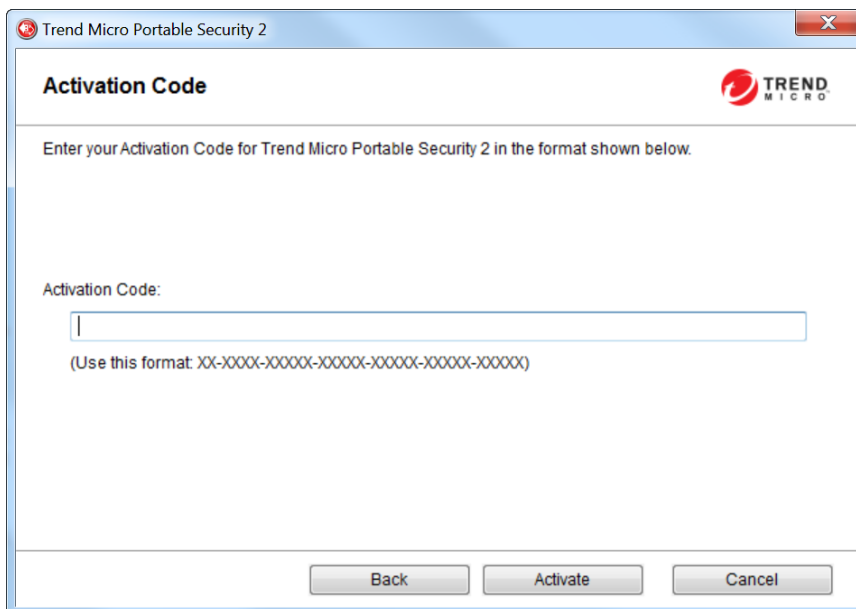
1. Plug-in the new Scanning Tool or any Scanning Tool that has not yet been activated to a computer.
2. Open Windows Explorer and double-click `Launcher.exe` from the `TMPS2_SYS` partition to start the program.



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



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



5. Specify your activation code and click **Activate**.
6. Open the **Status & Update** tab of the Scanning Tool console and click **Activate** to start downloading the latest components.

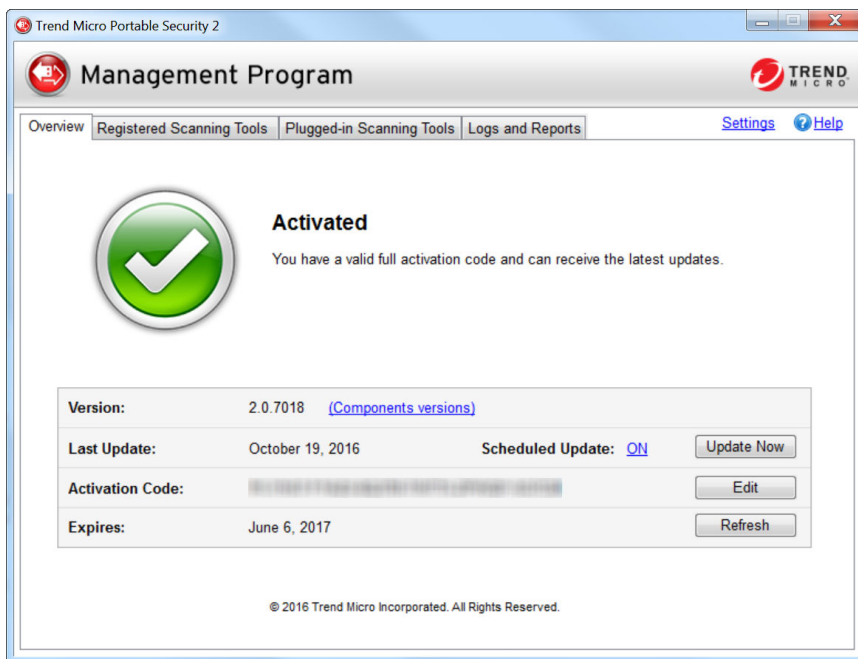
Changing the Activation Code

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

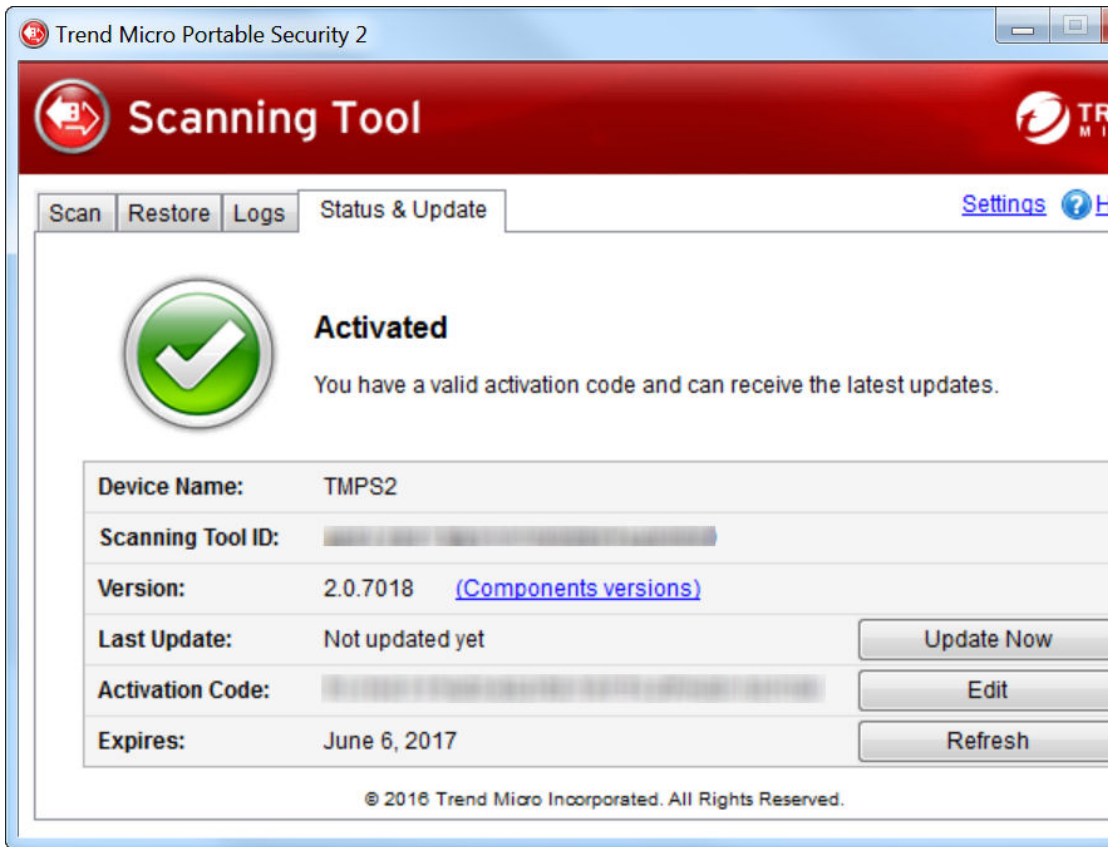
For more information, refer to [Activation Status on page 2-8](#).

Procedure

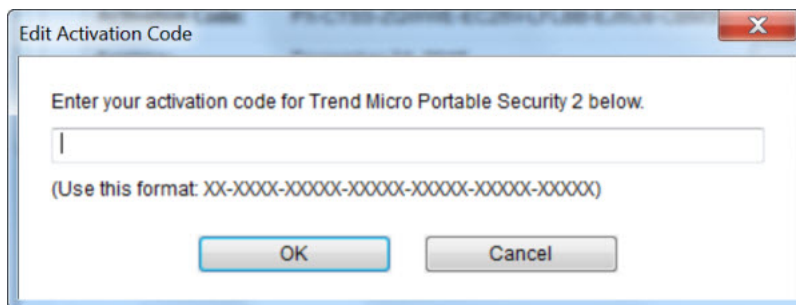
1. For a managed Scanning Tool device, open the Management Program console.



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



3. Click **Edit**.



4. Type in the new activation code.
 5. Click **OK**.
-

Upgrades

Trend Micro will release updates to the Trend Micro Portable Security 2 occasionally to provide more features and improve performance.



Note

Trend Micro Portable Security 2 does not support upgrades from Trend Micro Portable Security 1.5. For more information, refer to [Trend Micro Portable Security 1.5 and Older Versions on page 1-12](#).

Upgrading the Management Program



Note

1. Trend Micro Portable Security 2 does not support upgrades from Trend Micro Portable Security 1.5. For more information, refer to [Trend Micro Portable Security 1.5 and Older Versions on page 1-12](#).
 2. Make sure you have at least 2.3 GB of free space on the Management Program computer 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**. Otherwise, click **Cancel**.
 3. Click **Close** when the upgrade is complete.
-

Upgrading the Scanning Tool

**Note**

Trend Micro Portable Security 2 does not support upgrades from Trend Micro Portable Security 1.5.

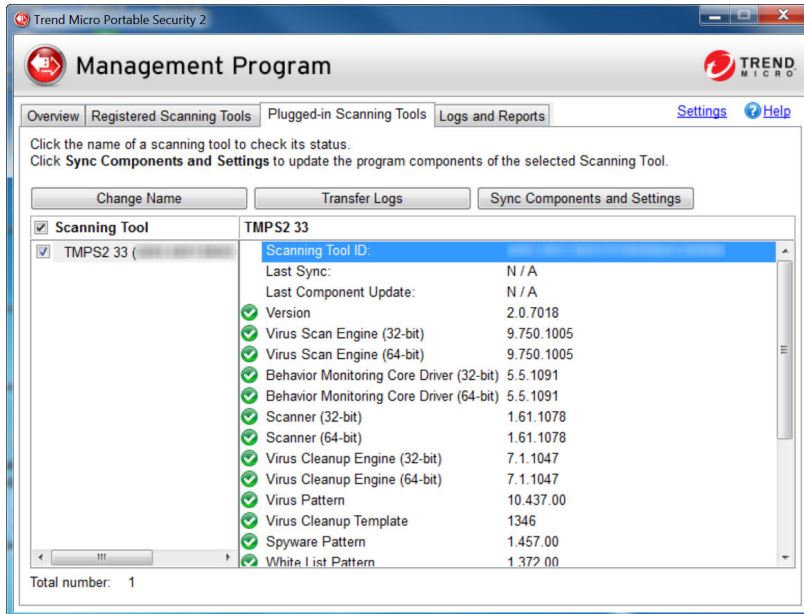
For more information, refer to *Trend Micro Portable Security 1.5 and Older Versions on page 1-12*.

Procedure

- Upgrade by Synchronizing with the Management Program
 - a. Upgrade the Management Program.
 - b. Plug in the Scanning Tool to the Management Program computer or connect it remotely through the Internet.

**Note**


To remotely connect the Scanning Tool to Management Program computer, make sure you are using Trend Micro Portable Security 2 SP2.



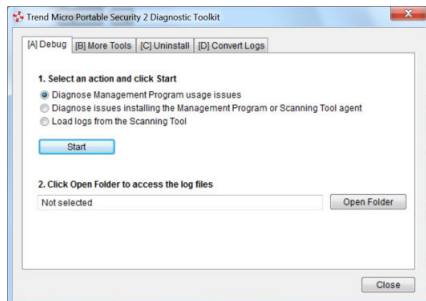
- c. Select the Scanning Tool from the list shown in the Management Program and click **Sync Components and Settings**.
- Upgrade Using the Support Tool
 - a. Close the Scanning Tool console if it is open.
 - b. Log on to the computer using an account with administrator privileges and connect the Scanning Tool.
 - c. Download the Trend Micro Portable Security 2 service pack.
 - d. Extract the contents of the service pack to a local folder on the computer where you have connected the Scanning Tool.

From the Management Program computer Windows Start Menu, select **All Programs > Trend Micro Portable Security 2 > Trend Micro Portable Security 2 Diagnostic Toolkit**.

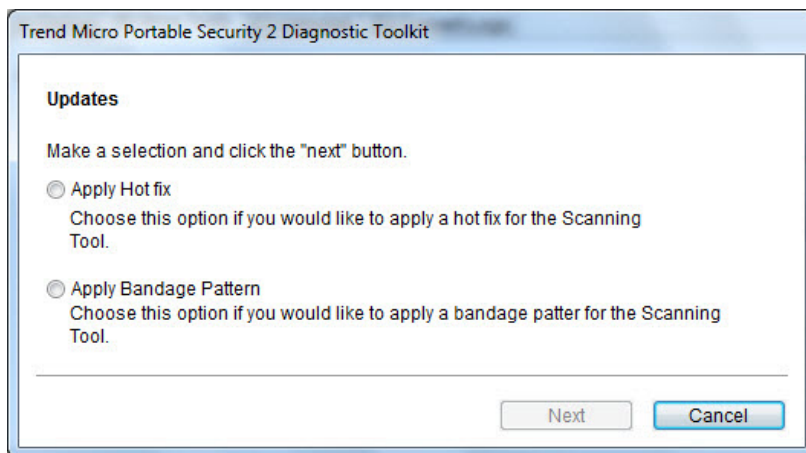
For the Scanning Tool:

- Copy the SupportTool folder from the USB device into your local drive.
- Double-click the TMPSSuprt.exe file .

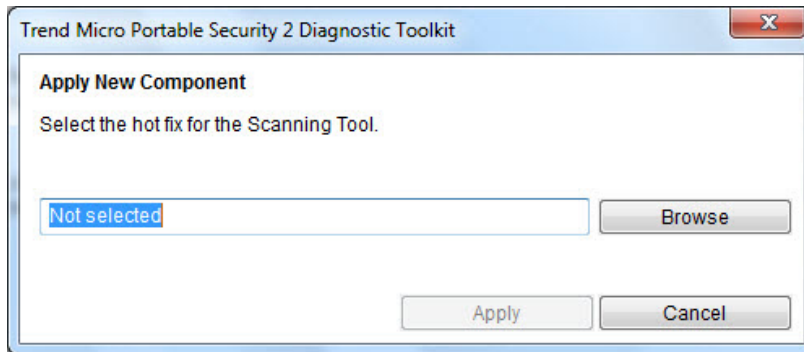
The Trend Micro Portable Security 2 Diagnostic Toolkit console opens.



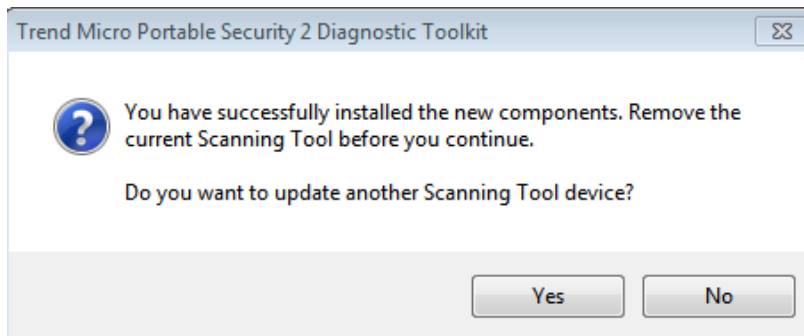
- Go to the **More Tools** tab. The **More Tools** tab opens.
- Click the **Use for Updates** button. The **Updates** window opens.



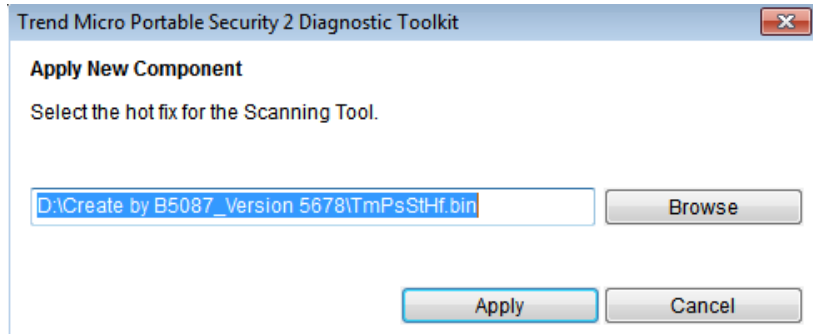
- Select **Apply Hot fix** and click **Next**. The **Apply New Components** window opens.



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



- j. To update another Scanning Tool, click **Yes** and browse for the hot fix file in the pop-up **Apply New Component** window or click **No** to finish the update.



Chapter 3

Using the Management Program

This chapter describes how to use and configure the Trend Micro Portable Security 2™ Management Program.

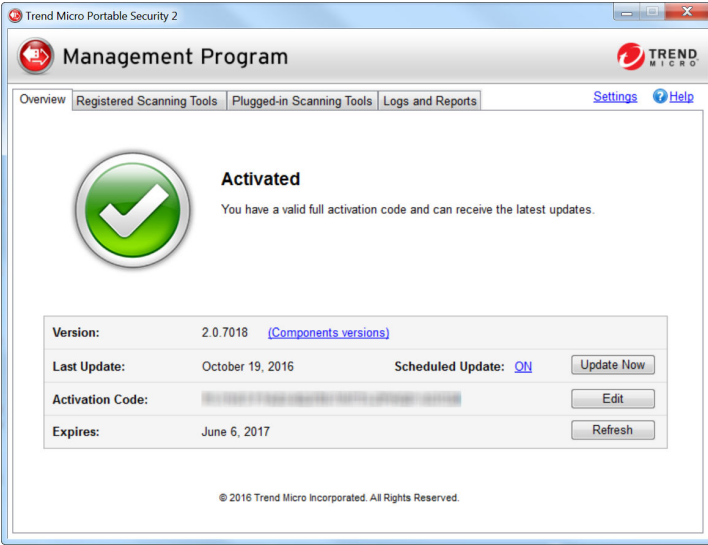
Topics in this chapter:

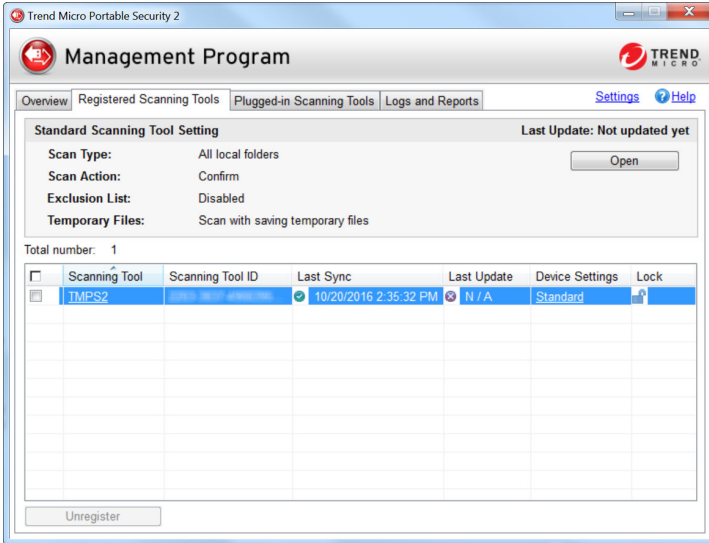
- *Understanding the Management Program Console on page 3-2*
- *Scan Settings on page 3-10*
- *Component Updates on page 3-28*
- *Logs and Reports on page 3-35*
- *Other Settings on page 3-52*

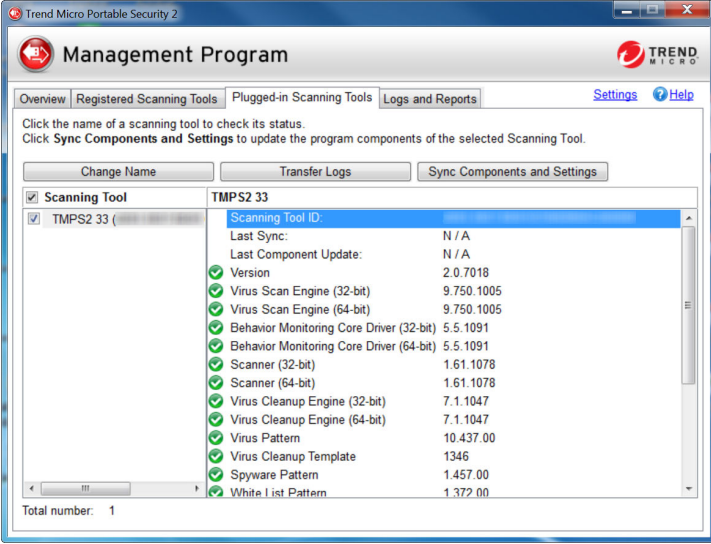
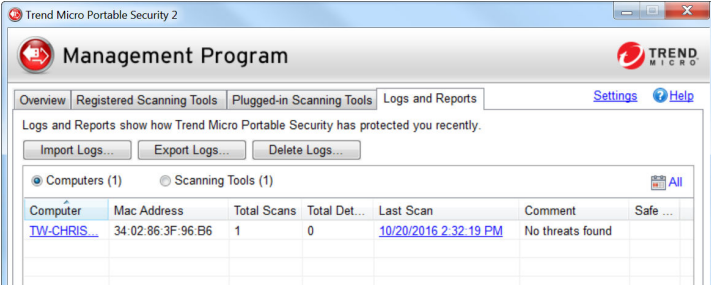
Understanding the Management Program Console

This is a short guide on how to use the Management Program console.

TABLE 3-1. How to use the console

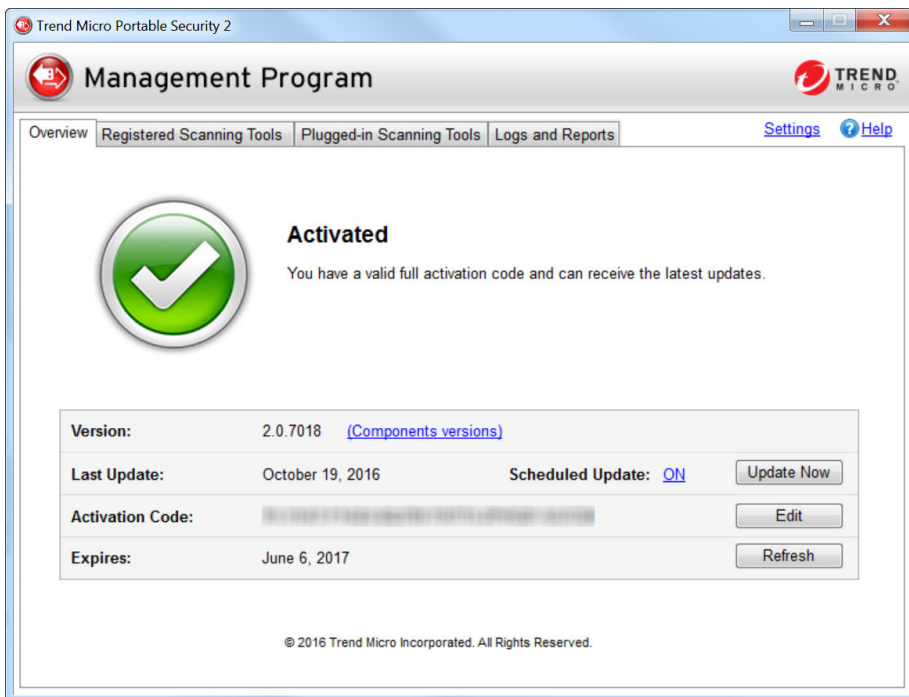
TAB OR BUTTON	DESCRIPTION
Settings	Click this link to check or change the Management Program settings. Refer to Changing the Management Program Settings on page 3-52 .
Help	Click this link to open the help file and to find more information about how to use this console.
Overview tab	 <p>Check the status of the components and perform an update, if needed. Refer to Overview Tab on page 3-5.</p>

TAB OR BUTTON	DESCRIPTION
<p>Registered Scanning Tools tab</p>	 <p>Configure the scan settings of all registered Scanning Tools managed by this Management Program.</p> <p>Refer to Registered Scanning Tools on page 3-6.</p>

TAB OR BUTTON	DESCRIPTION
<p>Plugged-in Scanning Tools tab</p>	 <p>Check the status of the Scanning Tool devices that are currently plugged into the Management Program computer.</p> <p>Refer to Plugged-in Scanning Tools on page 3-8.</p>
<p>Logs and Reports tab</p>	 <p>Check the results of earlier scans performed by the Scanning Tool.</p> <p>Refer to Logs and Reports Tab on page 3-9</p>

Overview Tab

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

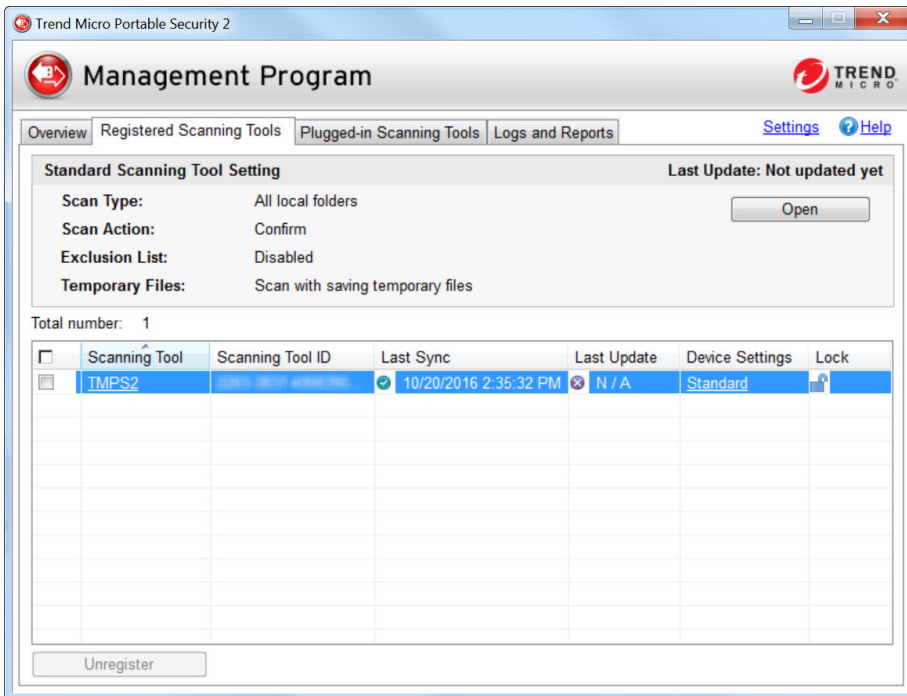


- **Version:** The build number of the Trend Micro Portable Security 2 Management Program appears next to Version. Click the **Component versions** link to see the component details and the date of the last update.
- **Scheduled Update:** Click ON or OFF to enable or disable scheduled update or change the specified time. Refer to *Scheduled Update on page 3-31*.
- **Update Now:** Click this button to manually start updating the components.
- **Edit:** Click this button to change or update the activation code.

- **Refresh:** Click this button when you have changed the activation code and it still says expired.



Registered Scanning Tools

Configure the scan settings of all registered Scanning Tools managed by this Management Program.



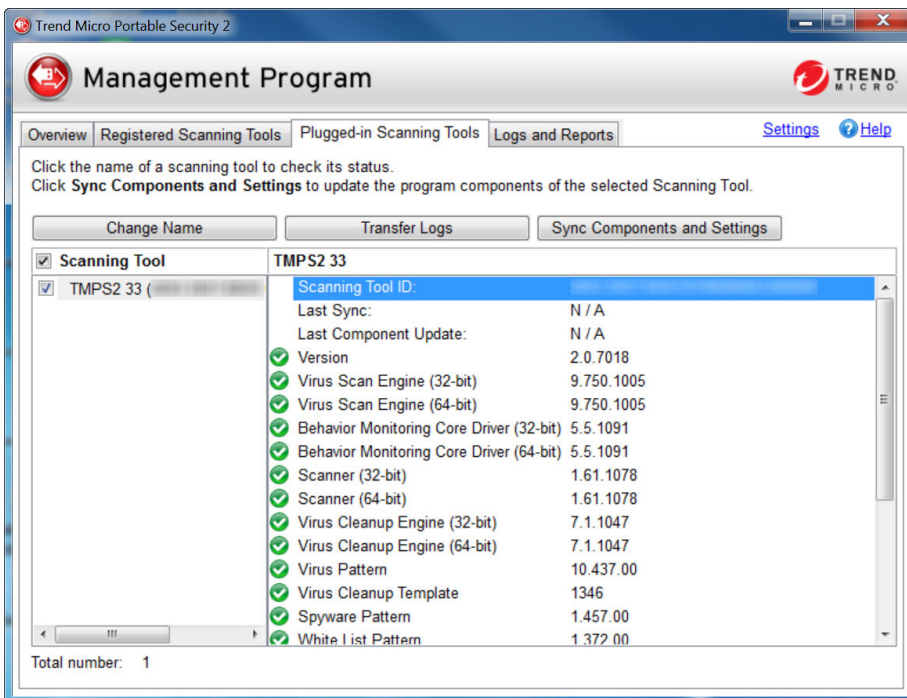
- **Open:** Click to open the standard scan setting for all Scanning Tool devices registered to the Management Program.

For details on scan settings, refer to *Scan Settings on page 3-10*.

- **Standard/Custom:** This link under Device Settings shows whether the device uses the standard scan setting or if the scan setting for this device is specific to this device.
- **Lock/Unlock:** Click the padlock icon to lock or unlock the scan settings for this device.
 - : This indicates that the user will be able to make changes to the scan settings of this device.
 - : This indicates that the Scanning Tool is using the Management Program scan settings and the user will not be able to change the scan settings from the Scanning Tool console.
- **Scanning Tool:** Click an item under the Scanning Tool column to view logs on the scan, synchronization, and update that the Scanning Tool has performed and its components versions.

Plugged-in Scanning Tools

Check the status of the Scanning Tool devices that are currently plugged into the Management Program computer.

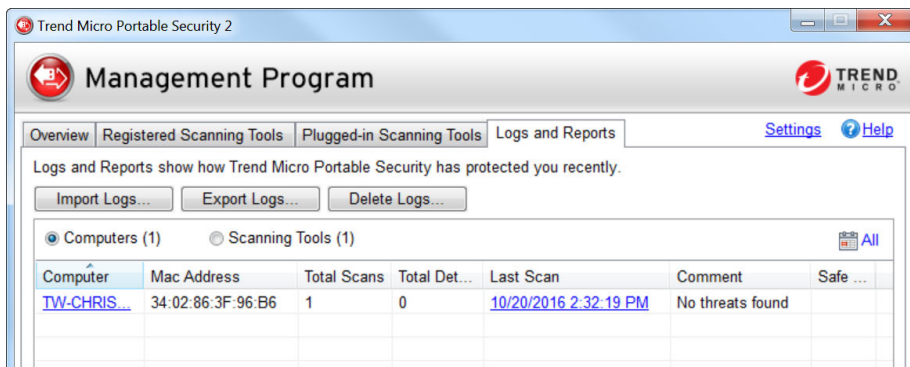


- **Change Name:** Click this button to change the name of the Scanning Tool.
See *Changing the Name of the Scanning Tool* on page 3-25.
- **Transfer Logs:** Click this button to transfer logs from the Scanning Tool device to the Management Program.
See *Transferring Logs from the Scanning Tool* on page 3-46.

- **Sync Components and Settings:** Click this button to download components and settings from the Management Program to the Scanning Tool.

Logs and Reports Tab

Check the results of earlier scans performed by the Scanning Tool. You can display the results by computers or by Scanning Tools.



- **Computers:** Select this option to access scan logs listed by computers.
See *Viewing Logs and Reports on page 3-35*.
- **Scanning Tools:** Select this option to access scan logs listed by Scanning Tools.
See *Viewing Logs and Reports on page 3-35*.
- **Import Logs:** Click this button to import database format logs.
See *Importing Logs on page 3-41*.
- **Export Logs:** Click this button to export all the logs into database or csv format.
See *Exporting Logs on page 3-43*.
- **Delete Logs:** Click this button to delete scan logs or TMSL logs during a specified time frame.



Trend Micro recommends exporting logs before deleting them.

- **Calendar:** Click the calendar icon to display log entries within the specified time frame.

Scan Settings

You can change the scan settings from the Management Program or the Scanning Tool console.

- From the Management Program console, click the **Registered Scanning Tools** tab and click **Open**.
- From the Scanning Tool console, click the **Scan** tab and click **Edit**.



Tip

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

Scan Setting Category

You can use Standard or Custom scan settings for each Scanning Tool device:



Whatever option you chose, after making the changes to the Management Program scan settings, make sure to synchronize the settings to the Scanning Tool devices.

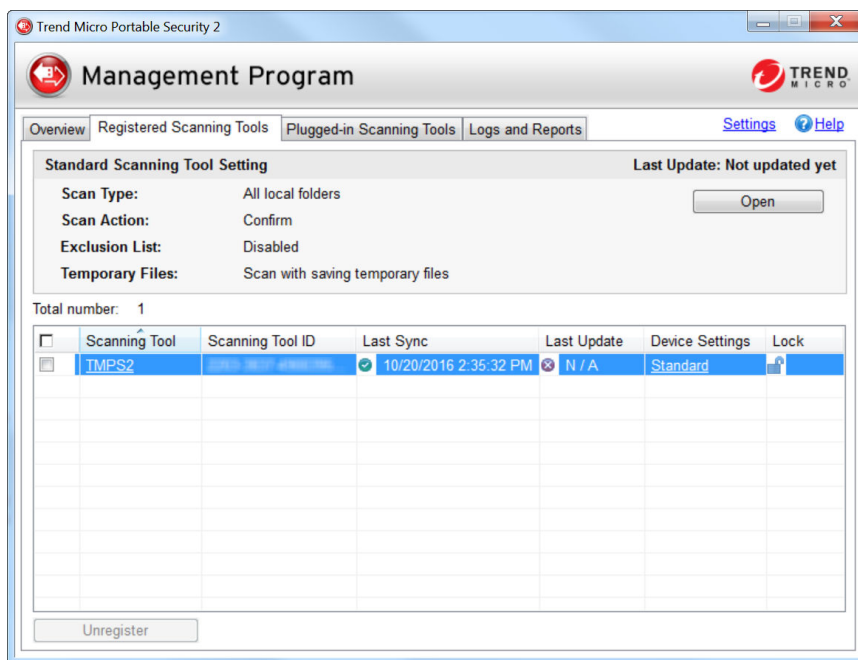
- **Standard:** The Scanning Tool uses the Management Program scan settings for registered devices.
- **Custom:** The scan setting is specific to this device. This can be changed from the Scanning Tool or Management Program console.

Applying Standard Scan Settings

Apply the same scan settings to multiple Scanning Tool devices. After making the changes to the scan settings, the administrator has to synchronize settings to apply the change to the Scanning Tool.

Procedure

1. Open the Trend Micro Portable Security 2 Management Program.
2. Click the **Registered Scanning Tools** tab.



3. Click **Open**.
4. Change the following settings:
 - *Scan Settings (Basic) on page 3-16*

- *Scan Settings (Advanced) on page 3-19*
 - *Rescue Disk on page 3-22*
 - *Scan Settings (Others) on page 3-23*
5. Click **Save**.
 6. Go to the Scanning Tool console and click the **Status & Update** tab.



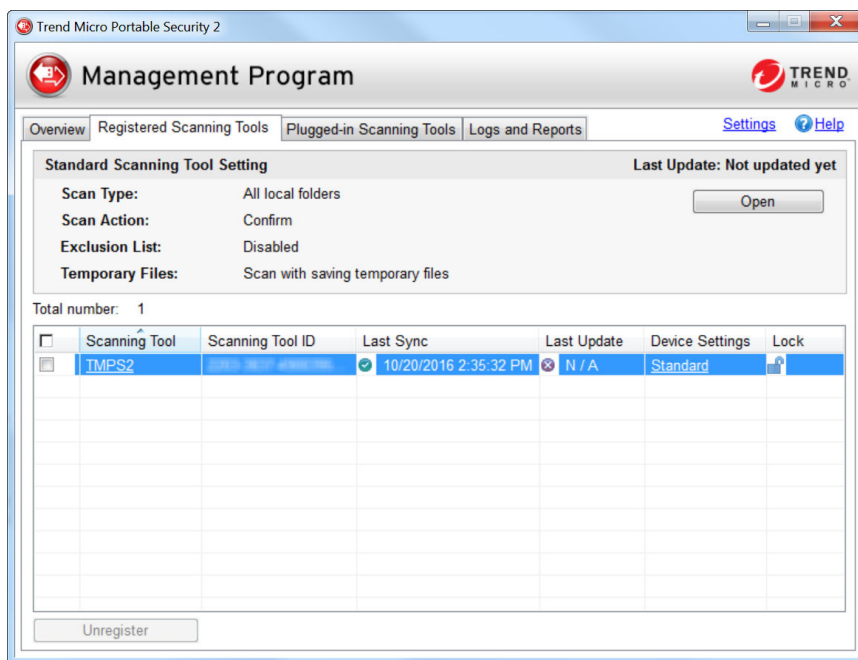
7. Click **Sync Logs and Settings**.

Applying Custom Scan Settings

Apply the scan setting to one device.

Procedure

1. Open the Trend Micro Portable Security 2 Management Program.
2. Click the **Registered Scanning Tools** tab.



3. Under the Device Settings column, click the **Custom** or **Standard** link for the selected Scanning Tool.
4. Change the following settings:
 - *Scan Settings (Basic) on page 3-16*
 - *Scan Settings (Advanced) on page 3-19*
 - *Rescue Disk on page 3-22*
 - *Scan Settings (Others) on page 3-23*

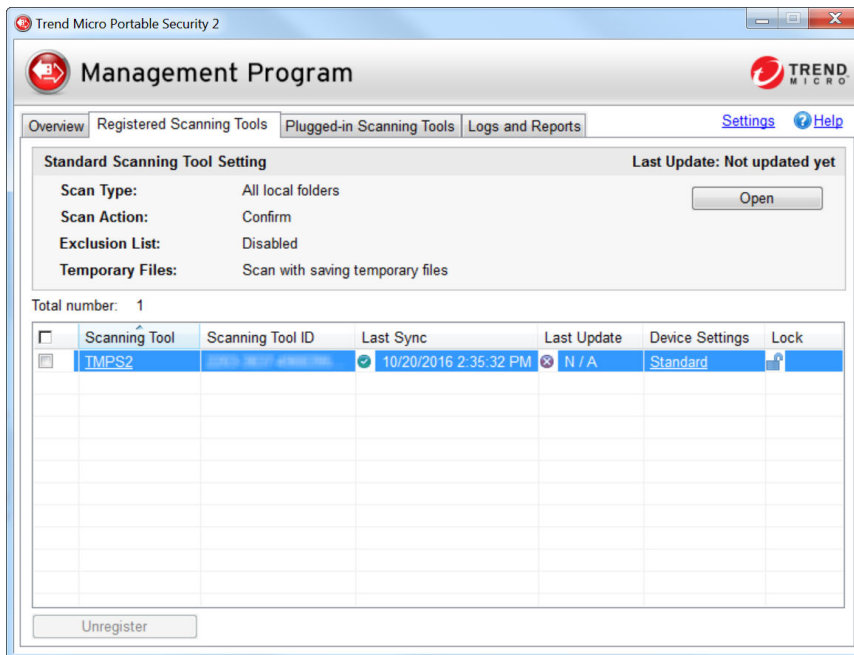
5. Click **Save**.
6. Go to the Scanning Tool console and click the **Status & Update** tab.
7. Click **Sync Logs and Settings**.

Configuring the Scanning Tool Proxy Server

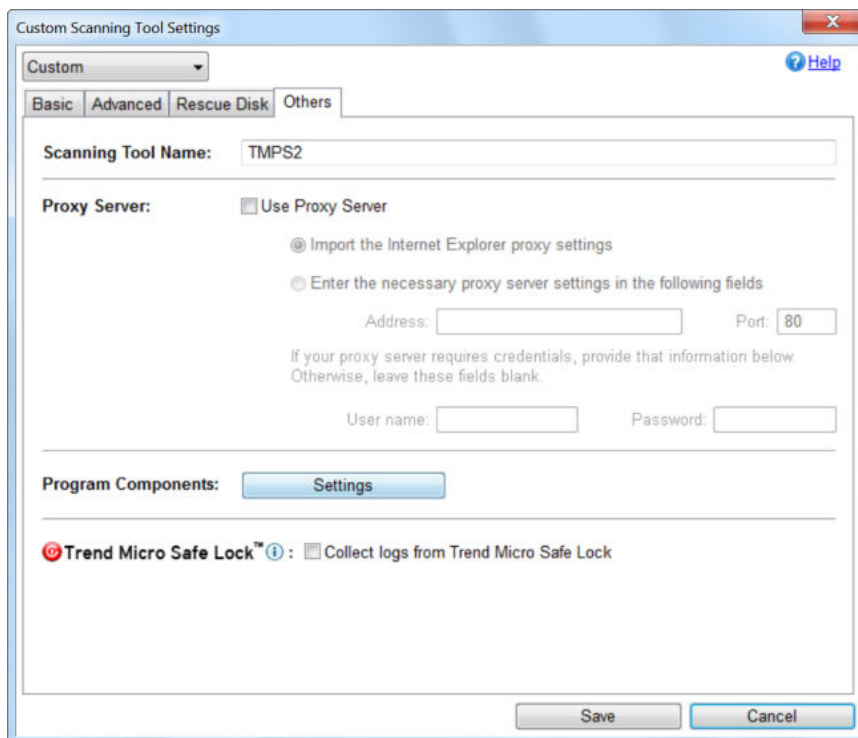
If the computer where you installed the Management Program connects to the Internet through a proxy server, use the **Other** tab to ensure that you can receive the latest components.

Procedure

1. Open the Trend Micro Portable Security 2 Management Program.
2. Click the **Registered Scanning Tools** tab.



3. Choose one of the following:
 - To change the setting of all registered scanning tools, click **Open** in the Standard Scanning Tools section.
 - To change the setting of one Scanning Tool device, click the **Standard** or **Custom** link under the Device Settings column for that device.
4. Go to the **Others** tab.



Custom Scanning Tool Settings

Custom

Basic Advanced Rescue Disk **Others** Help

Scanning Tool Name:

Proxy Server: Use 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:

Program Components:

 Trend Micro Safe Lock™  : Collect logs from Trend Micro Safe Lock

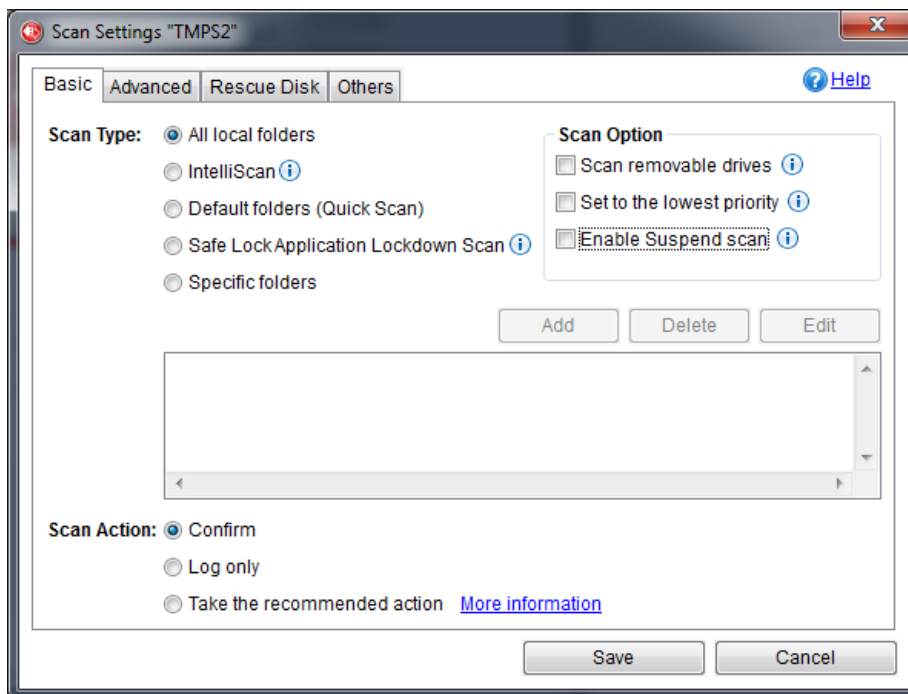
5. Mark the **Use a proxy server** option if your computer is required to use a proxy server to connect to the Management Program. Then choose one of the following options:

- **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.

6. Click **Save**.

Scan Settings (Basic)

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



- **Settings:** Select if you want the device to use the same scan setting as the Management Program or use scan settings specific to this device.

For details, see *Scan setting on page 3-10*.

- **Scan Type:** This determines the type of scan the tool will perform.

For details, see *Scan Type on page 3-17*.

- **Scan Option:** Additional features regarding scan priority and whether to also scan removable drives.

For details, see *Scan Option on page 3-18*.

- **Scan Action:** This specifies what action the Scanning Tool will perform when it detects a threat.

For details, see *Scan Action on page 3-18*.



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 computer.
- **IntelliScan:** Identifies the true file type and determines whether the file is a type that Trend Micro Portable Security 2 should scan.
- **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 on the list below it.
 - 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:** Enabling this option makes the scan check removable drives, as well.
- **Set to lowest priority:** Enable this option to set the scan to the lowest priority and reduce the system resources used.



This may increase the scanning time.

- **Enable Suspend scan:** Enabling this option displays the Suspend button during a scan.



This affects the scanning time and will store temporary files.

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:

The screenshot shows the 'Scan Settings "TMPS2"' dialog box with the 'Advanced' tab selected. The dialog has four tabs: 'Basic', 'Advanced', 'Rescue Disk', and 'Others'. A 'Help' button is located in the top right corner. The 'Exclusion List' section contains the instruction 'Select files, folders, or extensions to exclude from scans.' and two lists: 'Folders:' and 'Files:', each with 'Add', 'Delete', and 'Edit' buttons. Below these is an 'Extension:' field with a text input and '(Ex: txt,bmp,dat)' to its right. The 'Temporary Files:' section has a checkbox labeled 'Scan without saving temporary files'. The 'Administrator Account:' section has a checkbox labeled 'Scan as Administrator' and two text input fields for 'Account:' and 'Password:'. At the bottom, there is a 'Number of Compressed Layers to Scan:' dropdown menu set to '2'. 'Save' and 'Cancel' buttons are at the bottom right.

- **Exclusion List:** Add files or folders that you do not want to be scanned.

Refer to *Changing the Exclusion List Settings on page 3-20*.

- **Scan without saving temporary files:** Scans without saving files to the target computer. Using this option reduces scanning capability for certain types of malware.



Important

- Files may still be saved to the target computer for operations other than scanning.
- This function prevents update for Scanning Tool program and application of hot fix.
- This function is not applicable for scanning a Management Program computer.

-
- **Scan as Administrator:** Selecting this option means you can 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.

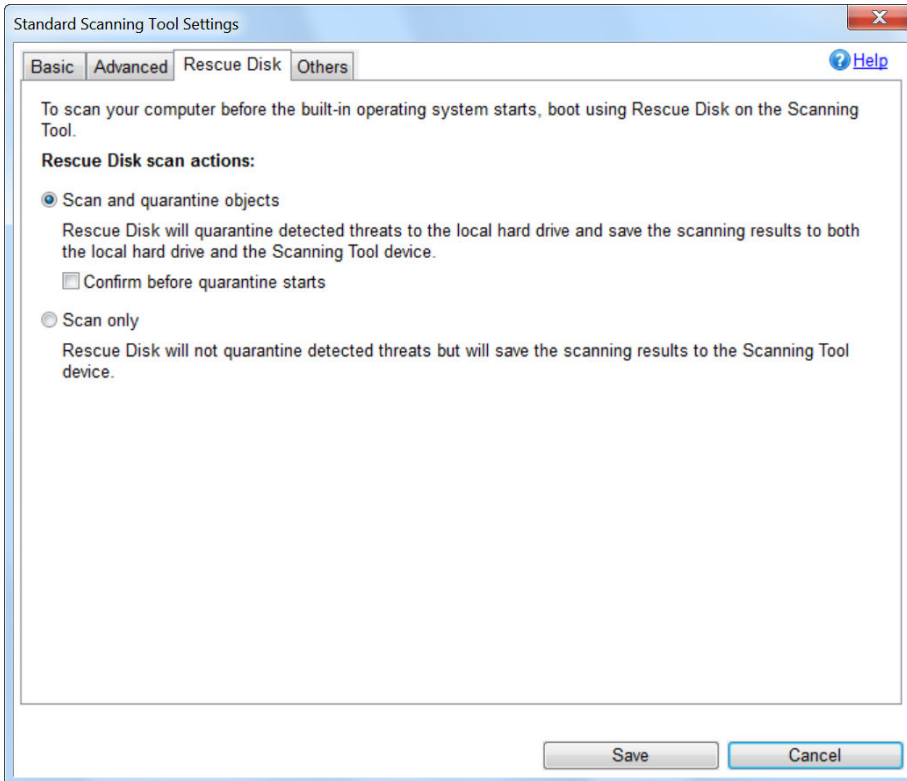


Tip

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

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 5-25*.

Scan Settings (Others)

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

The screenshot shows a dialog box titled "Custom Scanning Tool Settings" with a "Custom" dropdown menu and a "Help" icon. The "Others" tab is selected, showing the following settings:

- Scanning Tool Name:** TMPS2
- Proxy Server:**
 - Use 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:
- Program Components:**
- Trend Micro Safe Lock™** Collect logs from Trend Micro Safe Lock

Buttons for "Save" and "Cancel" are located at the bottom right of the dialog.

FIGURE 3-1. Scan settings for a managed Scanning Tool

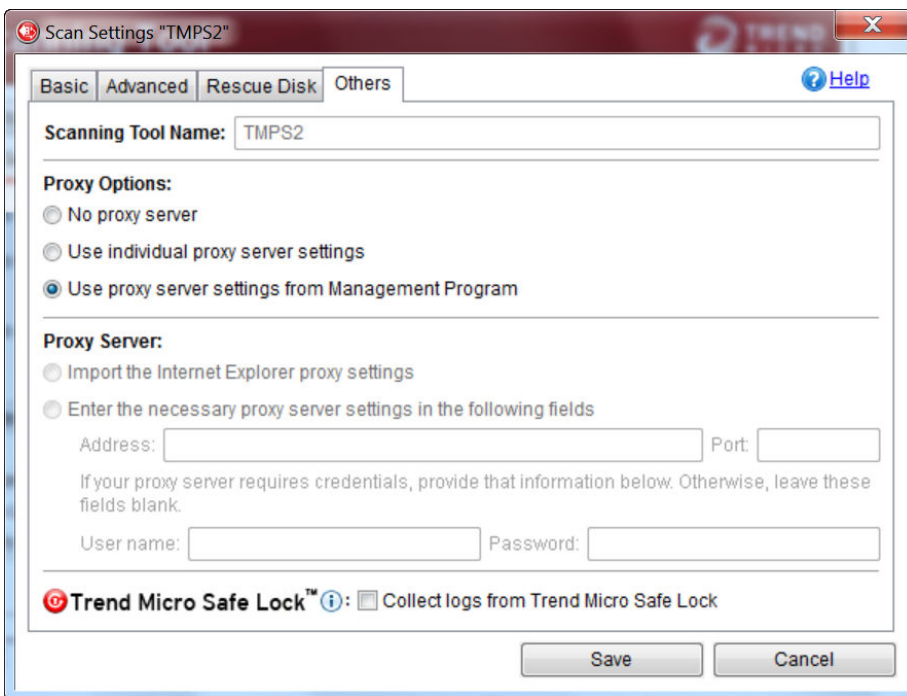


FIGURE 3-2. Scan Settings for a Standalone Scanning Tool

- **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 or 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 details, see *Checking the Latest Components on page 3-28*.

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

For a detailed procedure, see *Collecting Logs from Trend Micro Safe Lock™ on page 3-48*. For more information, refer to [Safe Lock](#).

Changing the Name of the Scanning Tool

Trend Micro recommends giving each Scanning Tool an individual name to easily identify which Scanning Tool is being used.

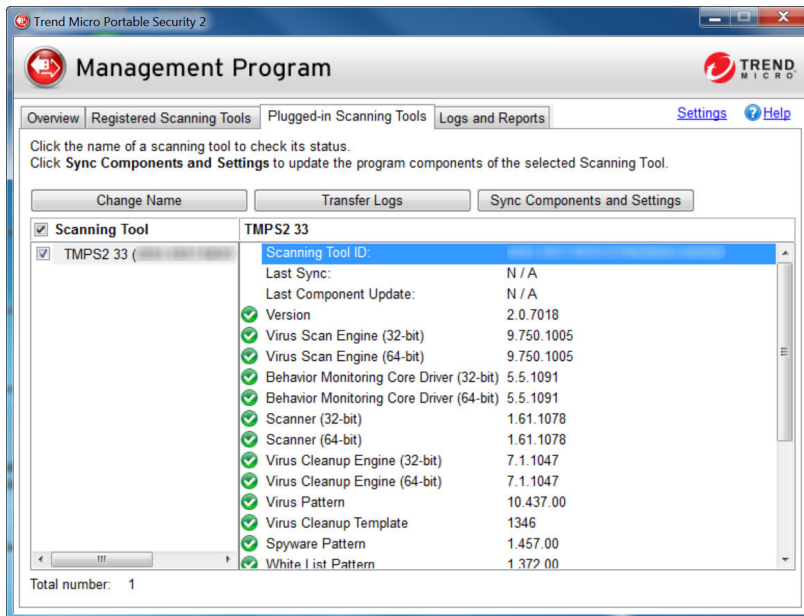


Note

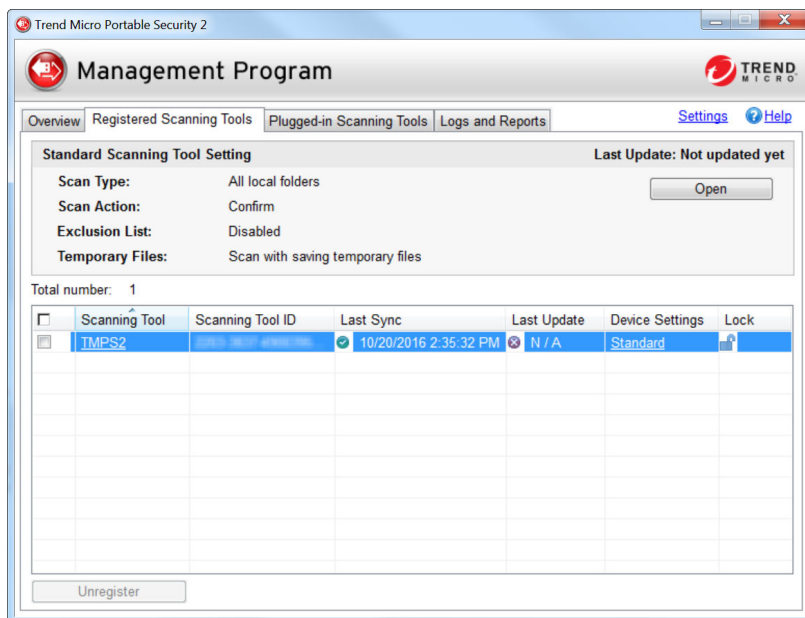
The Scanning Tool name can be 128 alphanumeric characters or 64 double-byte characters. TMPS2 is the default value for the Scanning Tool name.

Procedure

- From the **Plugged-in Scanning Tools** tab
 - a. Plug in the Scanning Tool to the Management Program computer.
 - b. Click the **Plugged-in Scanning Tools** tab.



- c. Click the **Change Name** button.
 - d. Type the new name and click **OK**.
- From the **Registered Scanning Tools** tab
 - a. Click the **Registered Scanning Tools** tab.



- b. Under the Device Settings column, click the **Custom** or **Standard** link for the Scanning Tool you want to configure.



Note

If it is current set as **Standard**, select **Custom** from the drop-down list before proceeding.

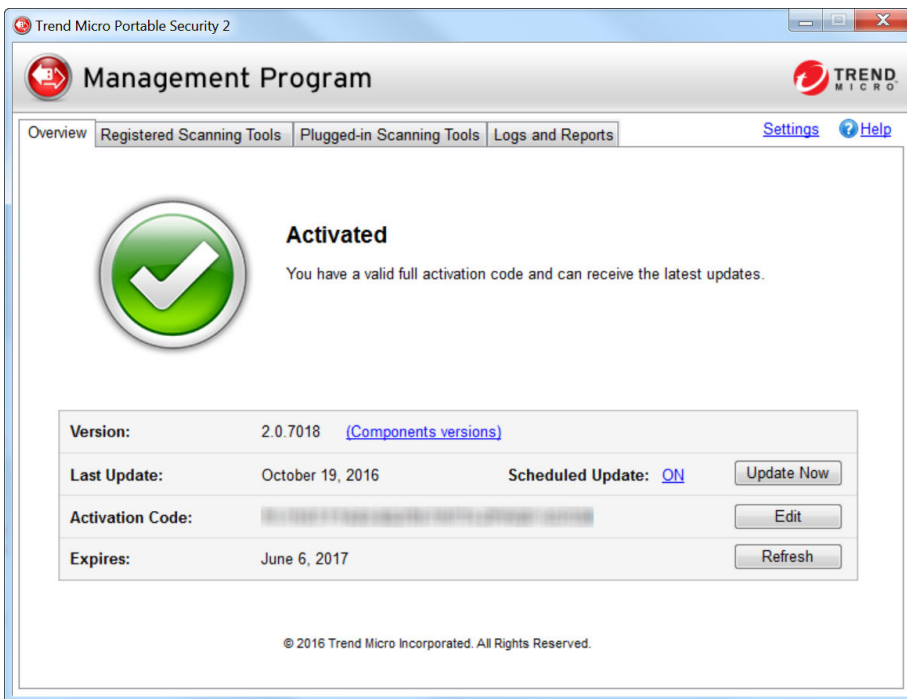
- c. Type the new name and click **Save**.
- d. Go to the **Plugged-in Scanning Tools** tab and click **Sync Components and Settings**.
- To change the Scanning Tool name from the Scanning Tool console, see [Scanning Tool Name Setting on page 4-26](#).

Component Updates

Regularly update the Management Program to ensure that you are using the latest components when synchronizing components with the Scanning Tool. You can update the Management Program on-demand, by schedule, or by importing from a Scanning Tool.

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 3-23.

TABLE 3-2. Trend Micro Portable Security 2 Components

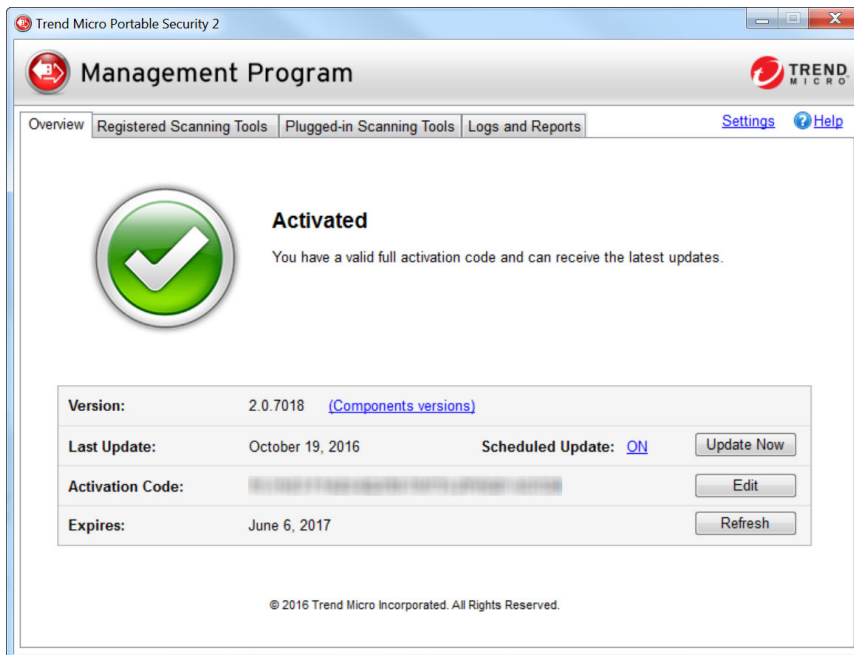
COMPONENT	DESCRIPTION
Virus Scan Engine (32-bit/64-bit)	<p>At the heart of all Trend Micro products lies the scan engine, which was originally developed in response to early file-based computer viruses. The scan engine today is exceptionally sophisticated and capable of detecting different types of viruses and malware. The scan engine also detects controlled viruses that are developed and used for research.</p> <p>Rather than scanning every byte of every file, the engine and pattern file work together to identify the following:</p> <ul style="list-style-type: none"> • Tell-tale characteristics of the virus code • the precise location within a file where the virus resides
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.
Virus Cleanup Engine (32-bit/64-bit)	Scans for and removes Trojans and Trojan processes.
Virus Pattern	<p>Contains information that helps Security Agents identify the latest virus/malware and mixed threat attacks.</p> <p>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.</p>
Virus Cleanup Template	Used by the Virus Cleanup Engine to identify Trojan files and processes so the engine can eliminate them.
Spyware Pattern	Identifies spyware/grayware in files and programs, modules in memory, Windows registry, and URL shortcuts.
White List 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.

Updating Components On-Demand

Procedure

1. From the **Overview** tab, click **Update Now**.



- (Optional) Enable *Scheduled Update on page 3-31*.

Scheduled Update

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

Procedure

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



Note

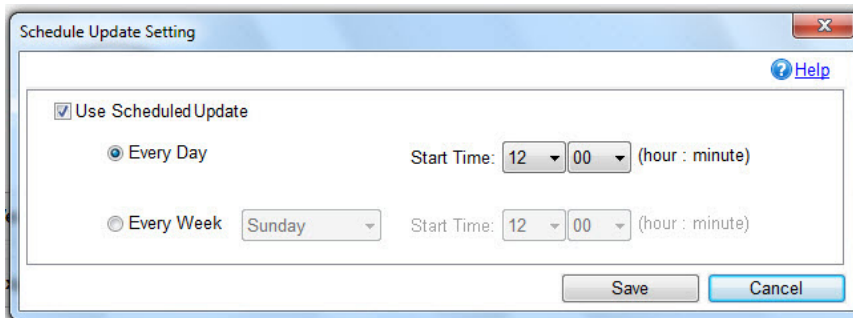
The link may show ON or OFF, depending on the current status of the update setting. If the link shows as **ON**, you have enabled scheduled updates. If the link shows as **OFF**, you have not enabled scheduled updates and will only get updates if you manually click the **Update Now** button.

The screenshot shows the 'Management Program' window with the 'Overview' tab selected. A large green checkmark icon is displayed next to the word 'Activated'. Below this, a message states: 'You have a valid full activation code and can receive the latest updates.' A table below provides the following details:

Version:	2.0.7018	(Components versions)
Last Update:	October 19, 2016	Scheduled Update: ON <input type="button" value="Update Now"/>
Activation Code:	<input type="text" value="XXXXXXXXXXXXXXXXXXXXXXXXXXXX"/>	
Expires:	June 6, 2017	<input type="button" value="Refresh"/>

© 2016 Trend Micro Incorporated. All Rights Reserved.

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.

Updating Components through a Scanning Tool

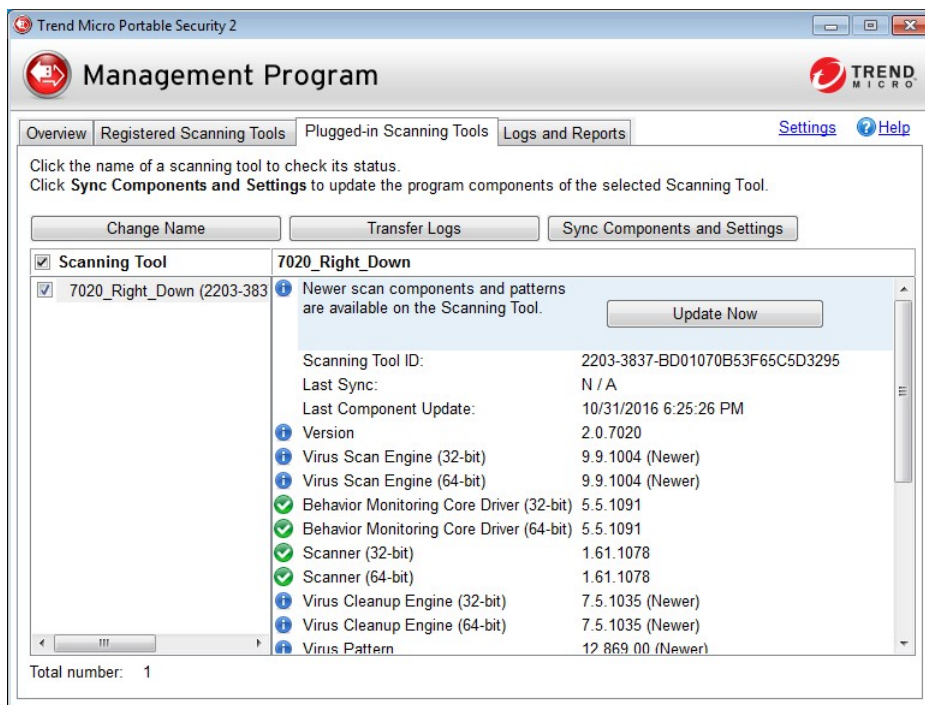
You can update the Management Program by importing components from a Scanning Tool which contains the latest components. This update method is suitable for scenarios that satisfy the following conditions:

- 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.



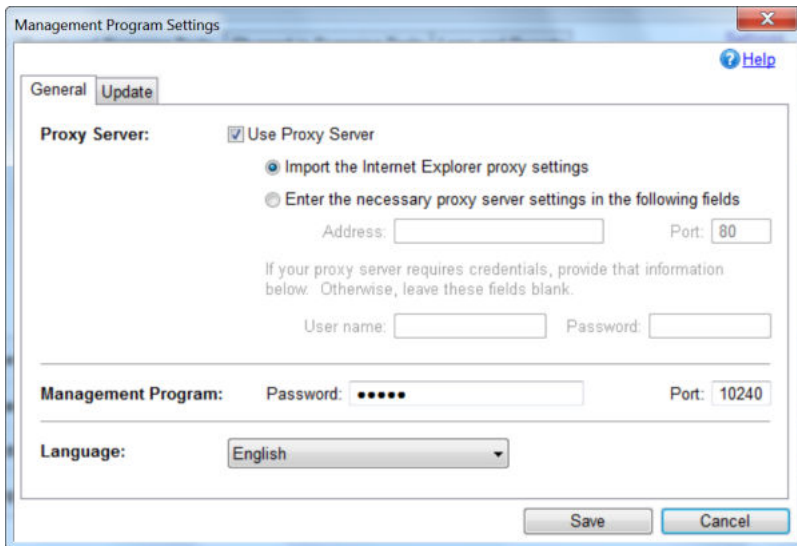
4. Click the **Update Now** button to start the update.

Changing the Update Source

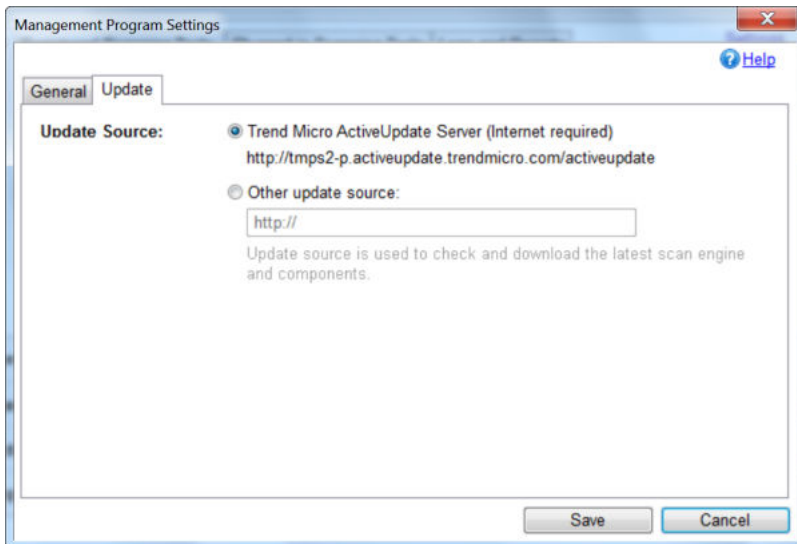
Follow the steps below to change the update source for Management Program.

Procedure

1. From the Management Program console, click the **Overview** tab and click **Settings**.



2. Click the **Update** tab.



3. The default update source is the **Trend Micro ActiveUpdate Server**. Otherwise select **Other update source**.

Logs and Reports

The **Logs and Reports** tab allows you to view, delete, and export log data imported from a Scanning Tool. You can also import log data to the Management Program that you previously exported from another Management Program.



Note

Some older logs might not be compatible with the current program.

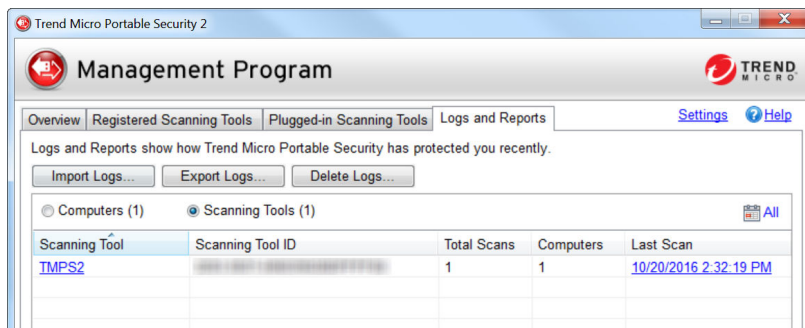
Viewing Logs and Reports

Whenever the Scanning Tool performs a scan, it keeps a detailed log report of the scanned computer and any threats that had been fixed or ignored.

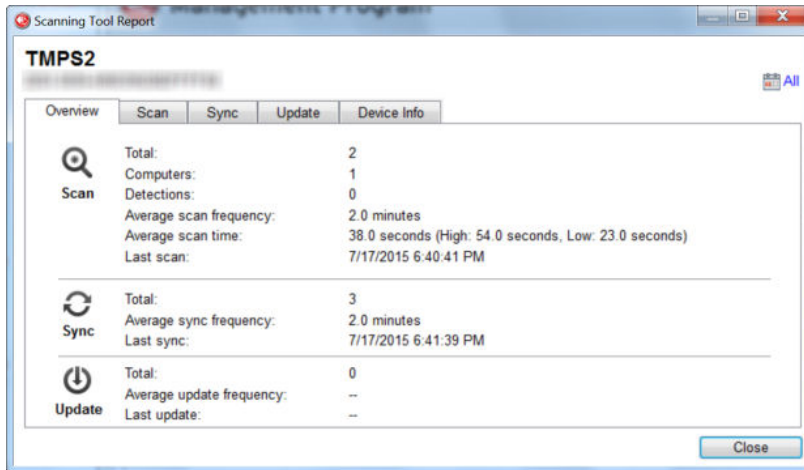
View these logs from the Scanning Tool or the Management Program console.

Procedure

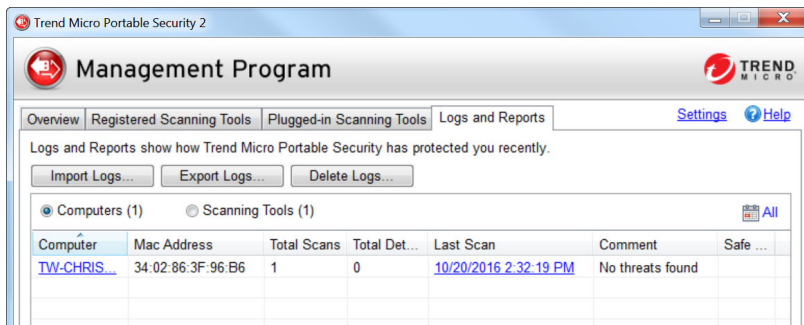
- Viewing scan logs listed by Scanning Tools (Management Program console)
 - a. Open the Trend Micro Portable Security 2 Management Program.
 - b. Click the **Logs and Reports** tab and select **Scanning Tools**.



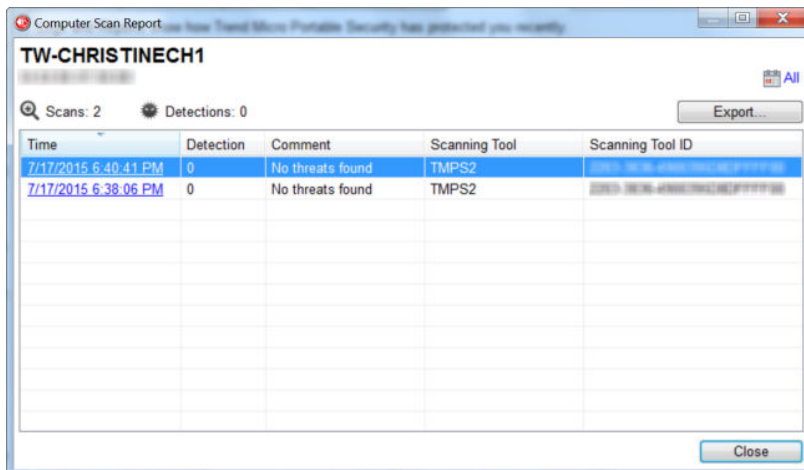
- c. Click an item from the Scanning Tool column. The Scanning Tool Report window appears. This window contains logs on the scan, synchronization, and update that the selected Scanning Tool has performed and its components versions.



- Viewing scan logs listed by computers (Management Program console)
 - a. Open the Trend Micro Portable Security 2 Management Program.
 - b. Click the **Logs and Reports** tab and select **Computers**.



- c. Click an item from the Computer column. This window appears.



Computer Scan Report

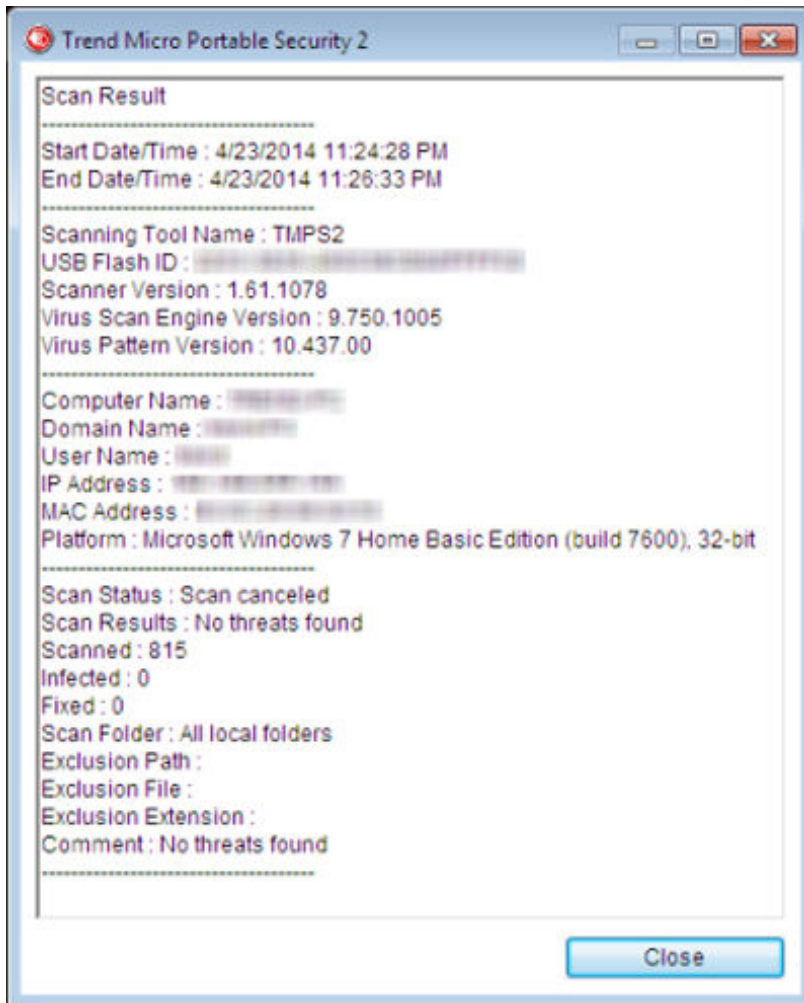
TW-CHRISTINECH1

Scans: 2 Detections: 0 Export...

Time	Detection	Comment	Scanning Tool	Scanning Tool ID
7/17/2015 6:40:41 PM	0	No threats found	TMPS2	2015-06-26-08:00:00-00000000
7/17/2015 6:38:06 PM	0	No threats found	TMPS2	2015-06-26-08:00:00-00000000

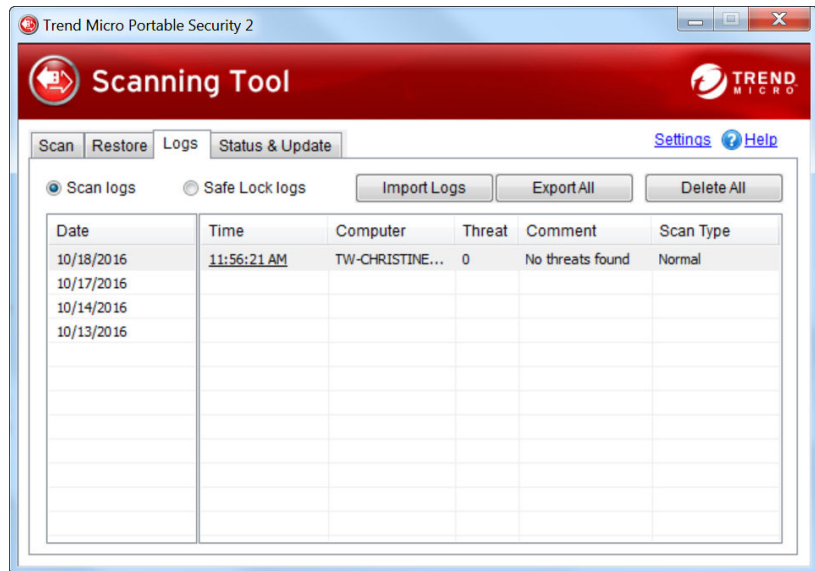
Close

- d. Click an item from the Time column to view scan log for the selected time. This log shows date and time of the scan, the name and ID of the Scanning Tool, and the number of time the computer has been scanned. Click on an item from the Computer column to view detailed results including the pattern file version, the scan engine version, the results of the scan, and the names of any security threats found.

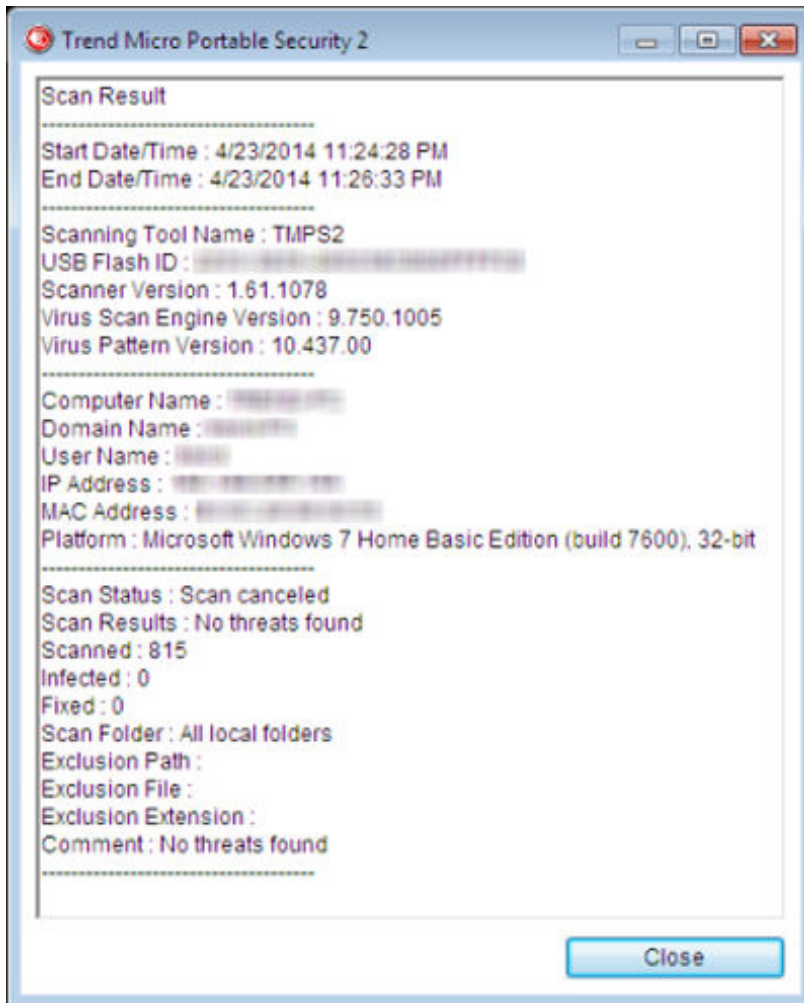


- Viewing scan logs (Scanning Tool console)
 - a. Plug the Scanning Tool to a computer.
 - b. Open the Scanning Tool console.

- c. Go to the **Logs** tab.



- d. Click an item from the Time column.



Importing or Exporting Logs from the Management Program

Administrators can export or import logs from the Scanning Tool or Management Program. The supported formats are database and csv files.

Importing Logs

To import log data from exported database files, click **Import Logs**, then select the folder containing the log data that you wish to import. To import log data, you must specify the complete path to the folder containing the files. For example, to import the log data in `C:\SAMPLE\{log data}`, you must specify `C:\SAMPLE` to find the files.

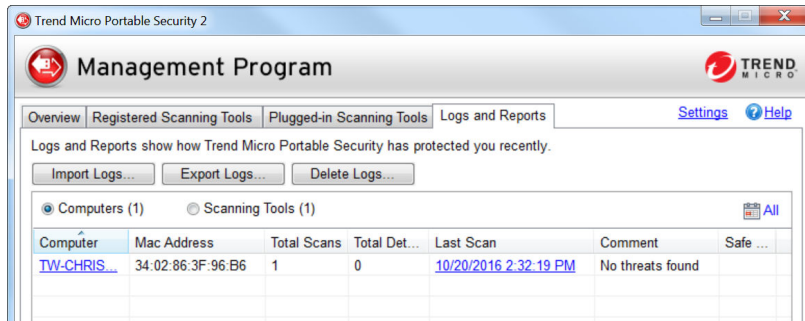


Note

Trend Micro Portable Security 2 can only import database files.

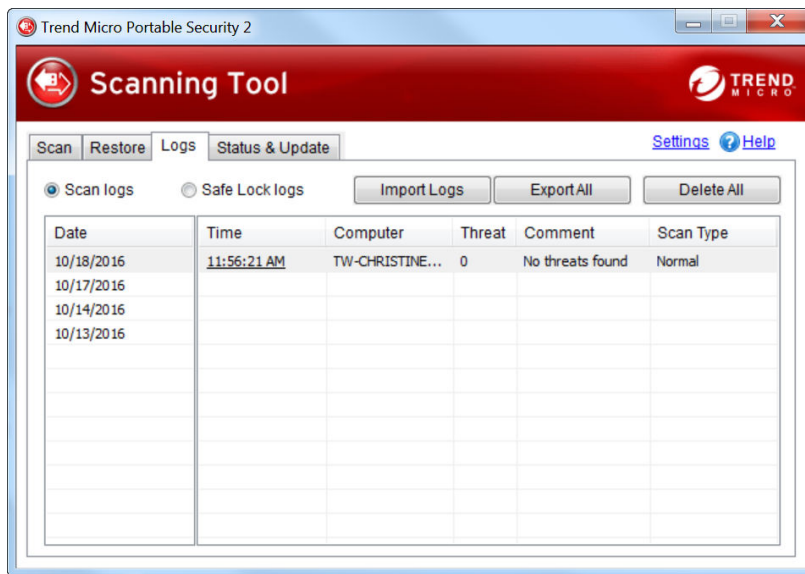
Procedure

- Management Program console
 - a. Open the Trend Micro Portable Security 2 Management Program.
 - b. Click the **Logs and Reports** tab.



- c. Click the **Import Logs** button.

- d. Locate the database file.
 - e. Click **OK**.
- Scanning Tool console
 - a. Plug in the Scanning Tool to the computer where log files are saved.
 - b. Open the Scanning Tool console.
 - c. Go to the **Logs** tab.



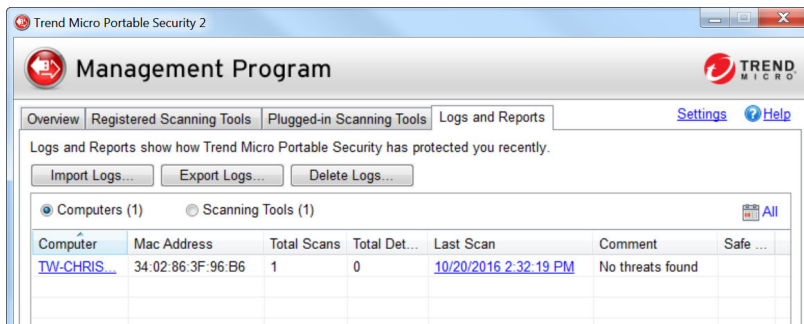
- d. Click the **Import Logs** button.
 - e. Locate the database file.
 - f. Click **OK**.
-

Exporting Logs

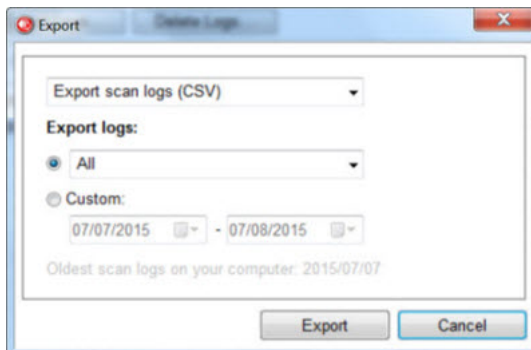
Trend Micro recommends regularly exporting log data and then deleting them from the scanning tool. This ensures that the scanning tool will always have enough space to be able to scan computers properly and save the quarantined files, if needed.

Procedure

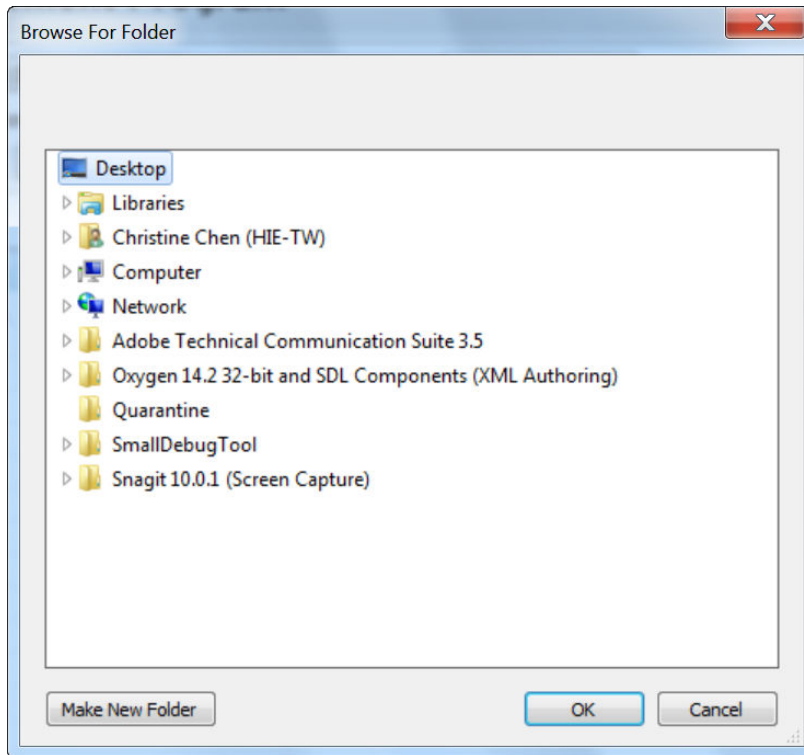
- Management Program console
 - a. Open the Trend Micro Portable Security 2 Management Program.
 - b. Click the **Logs and Reports** tab.



- c. Click the **Export Logs** button. The **Export** window appears.

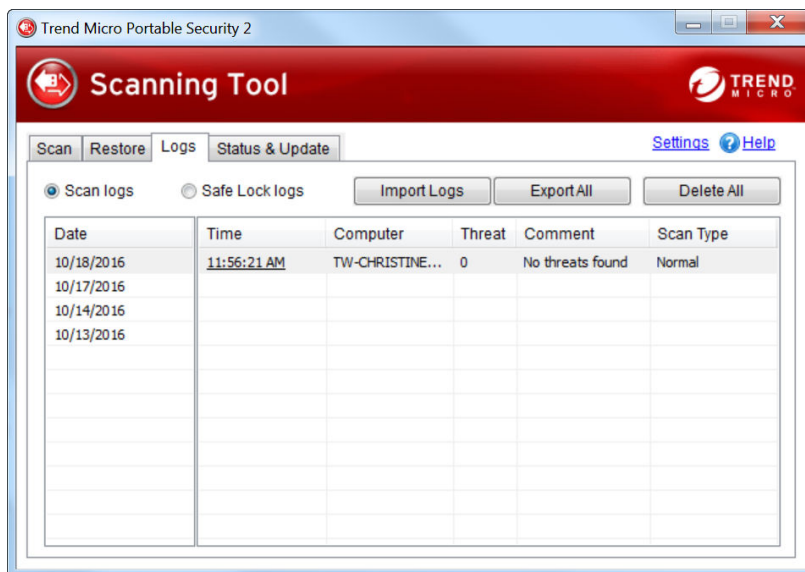


- d. Choose the file format and time frame, and then click **Export**.
- DB: This is the database format. You can export and import this file.
 - CSV: This is the comma-separated values (.csv) file. You can export the file but you will not be able to import this file.

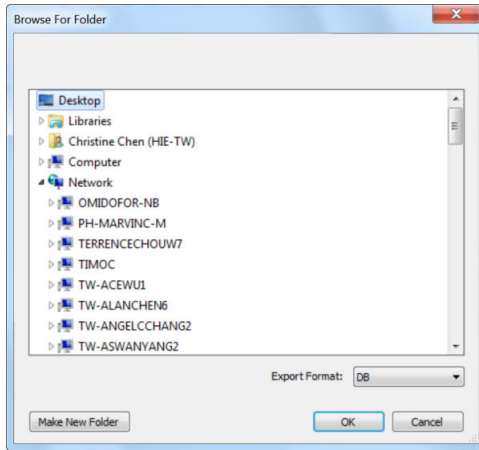


- e. Select a location for the export and click **OK**.
- Scanning Tool console
 - a. Plug the Scanning Tool to a computer where you wish to export the log files.
 - b. Open the Scanning Tool console.

- c. Go to the **Logs** tab.



- d. Select **Scan logs** or **Safe Lock logs**, and then click **Export All**.
- e. Specify a location and choose the export format.
- DB: This is the database format.
 - CSV: This is the comma-separated values (.csv) file.



- f. Click **OK**.
-

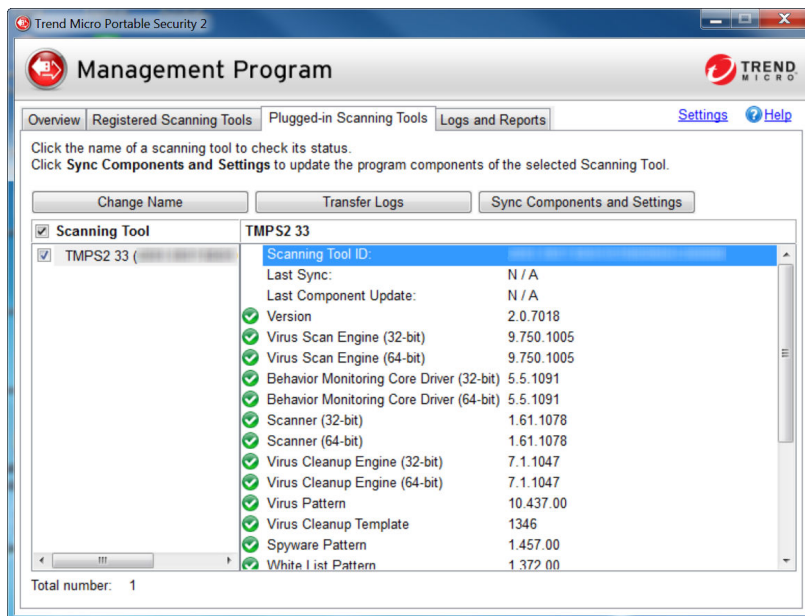
Transferring Logs from the Scanning Tool

Transfer the logs from the plugged-in Scanning Tool to the Management Program.

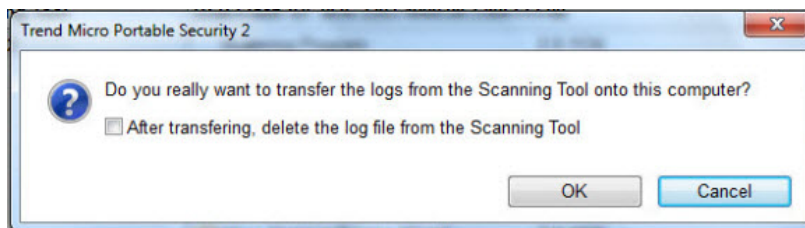
Procedure

- Option 1: Connect the Scanning Tool to the Management Program computer
 1. Plug in the Scanning Tool to the computer with the Management Program.
 2. Open the Trend Micro Portable Security 2 Management Program.

- Go to the **Plugged-in Scanning Tool** tab.



- Select the Scanning Tool.
- Click **Transfer Logs**. A pop message appears.



- (Optional) Select the **After transferring, delete the log file from the Scanning Tool**. option.



Note

Trend Micro recommends selecting this option to ensure that the Scanning Tool device will always have enough space to scan and save quarantined files.

7. Click **OK**.
- Option 2: Transfer the logs remotely
 1. Plug in the Scanning Tool to a computer with Internet connection and remotely connect to the Management Program.
 2. Go to the **Status & Update** tab.
 3. Click **Sync Logs and Settings**.
-

Collecting Logs from Trend Micro Safe Lock™

Trend Micro Portable Security 2 has the option of collecting logs from computers that have Trend Micro Safe Lock™.

For more information, refer to [Safe Lock](#).

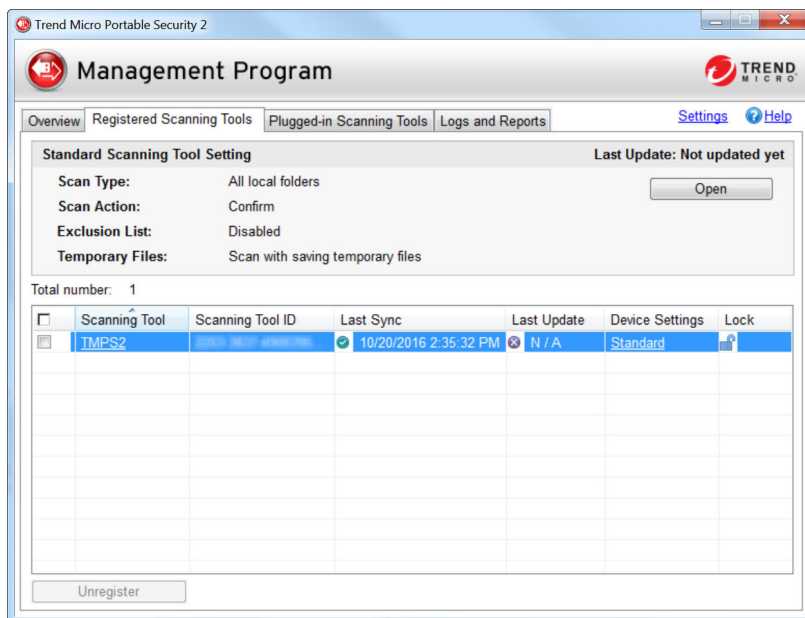


Note

These logs will only be collected after the Scanning Tool has scanned computers that have Trend Micro Safe Lock™.

Procedure

- For a Managed Scanning Tool
 - a. Open the Trend Micro Portable Security 2 Management Program.
 - b. Click the **Registered Scanning Tools** tab.

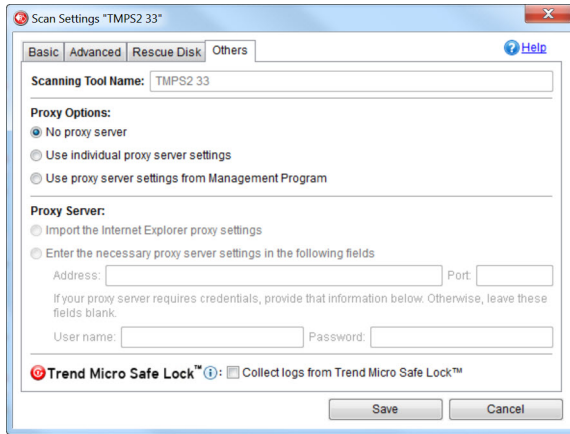


- c. Choose one of the following:

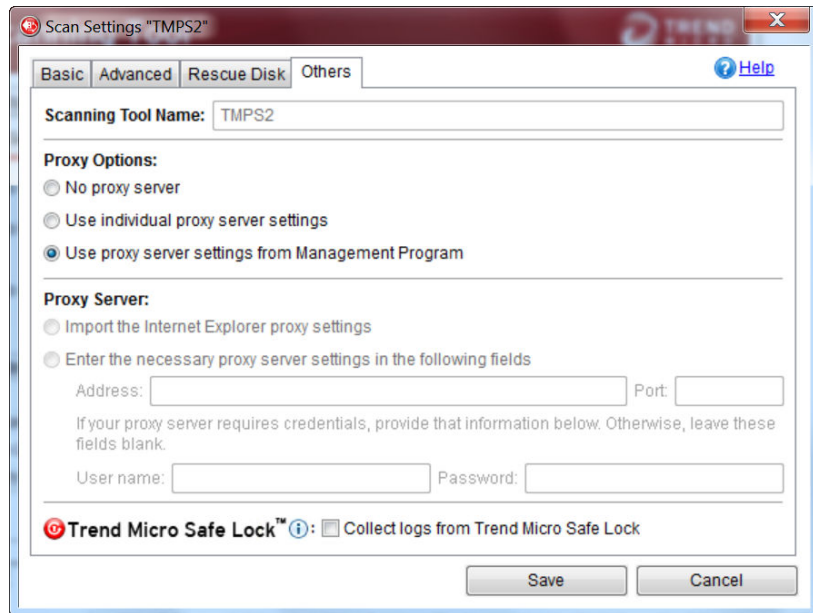
To change the setting of all registered scanning tools, click **Open** in the Standard Scanning Tools section.

To change the setting of one device, click the **Custom** or **Standard** link for the selected Scanning Tool under the Device Settings column.

- d. Go to the **Others** tab.



- e. Enable the **Collect logs from Trend Micro Safe Lock** option and click **Save**.
 - f. Synchronize the Scanning Tool settings with Management Program.
 - g. Launch the Scanning Tool and run a scan.
 - h. After the scan is complete, re-launch the Scanning Tool. Logs from Trend Micro Safe Lock™ are transferred to the Scanning Tool under **Safe Lock logs** of the **Logs and Reports** tab.
- For a Standalone Scanning Tool
 - a. From the Scanning Tool console, click **Edit** and click **Others**.



- b. Enable the **Collect logs from Trend Micro Safe Lock** option and click **Save**.
- c. Scan the computer with the Scanning Tool.
- d. After the scan is complete, re-launch the Scanning Tool. Logs from Trend Micro Safe Lock™ are transferred to the Scanning Tool under **Safe Lock logs** of the **Logs** tab.

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 will not be 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**.

Other Settings

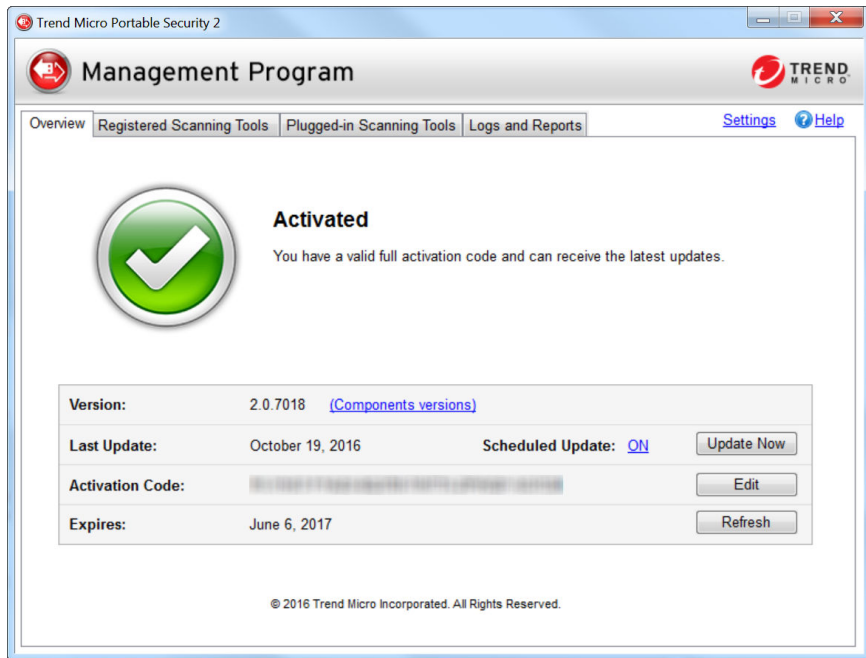
Change other Management Program settings.

Changing the Management Program Settings

Use the **Settings** link to make changes to the Management Program settings.

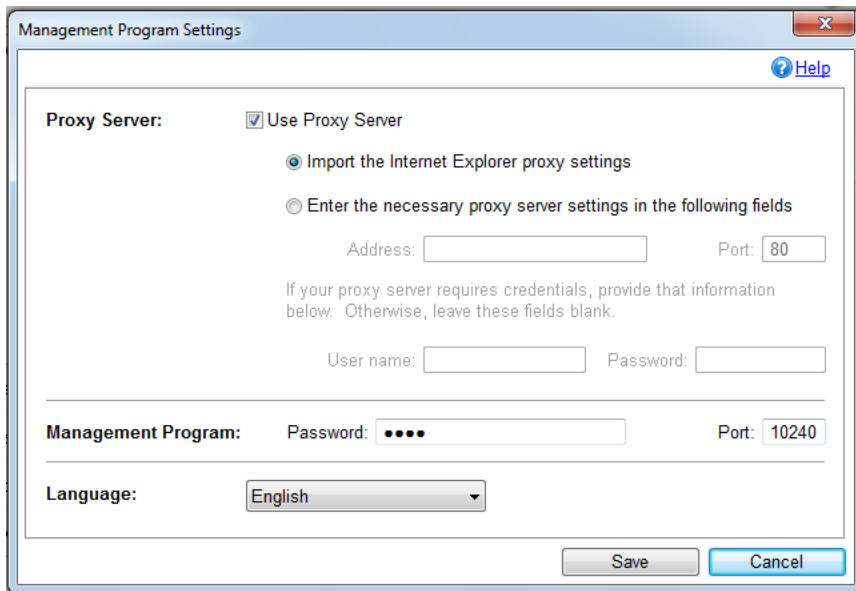
Procedure

1. Open the Management Program console.



2. Click **Settings**.

The **Management Program Settings** page opens.



The screenshot shows a dialog box titled "Management Program Settings" with a "Help" button in the top right corner. The "Proxy Server" section is active, with the "Use Proxy Server" checkbox checked. Two radio buttons are present: "Import the Internet Explorer proxy settings" (selected) and "Enter the necessary proxy server settings in the following fields". Below the second radio button are input fields for "Address", "Port" (set to 80), "User name", and "Password". A note states: "If your proxy server requires credentials, provide that information below. Otherwise, leave these fields blank." The "Management Program" section has a "Password" field (masked with dots) and a "Port" field (set to 10240). The "Language" section has a drop-down menu currently set to "English". "Save" and "Cancel" buttons are at the bottom right.

3. Mark the **Use a proxy server** 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.
4. Specify the Management Program port and password.
5. (Optional) Select a language from the drop-down menu to change the Management Program language.
6. Click **Save**.

Chapter 4

Using the Scanning Tool

This chapter describes how to use and configure the Scanning Tool.


Topics in this chapter:

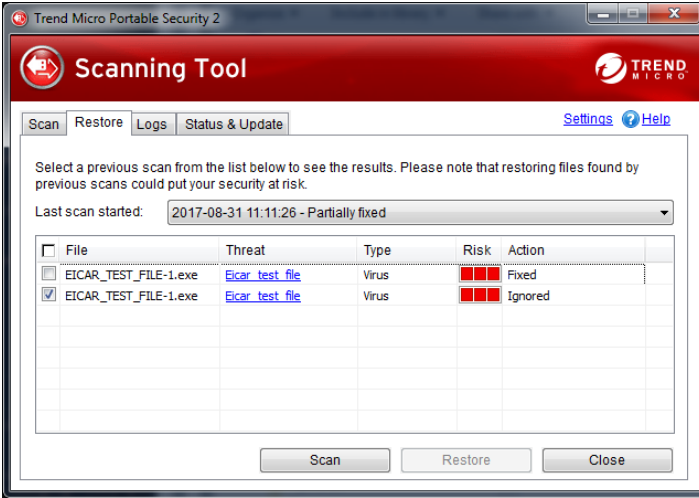

- *Understanding the Scanning Tool Device Console on page 4-2*
- *Component Updates on page 4-12*
- *Performing a Scan on page 4-16*
- *Changing the Scanning Tool Settings on page 4-23*
- *Removing the Scanning Tool on page 4-32*
- *Using the Scanning Tool Agent on page 4-40*

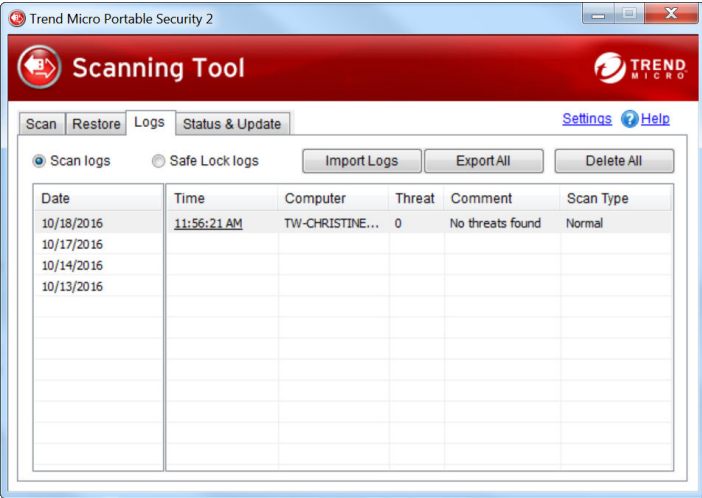
Understanding the Scanning Tool Device Console

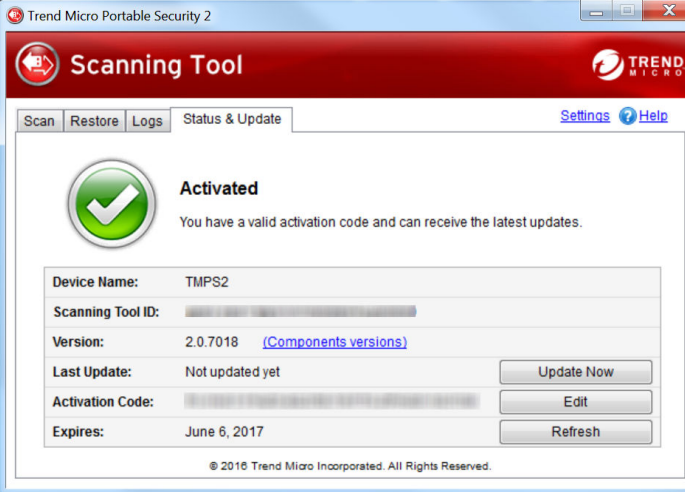
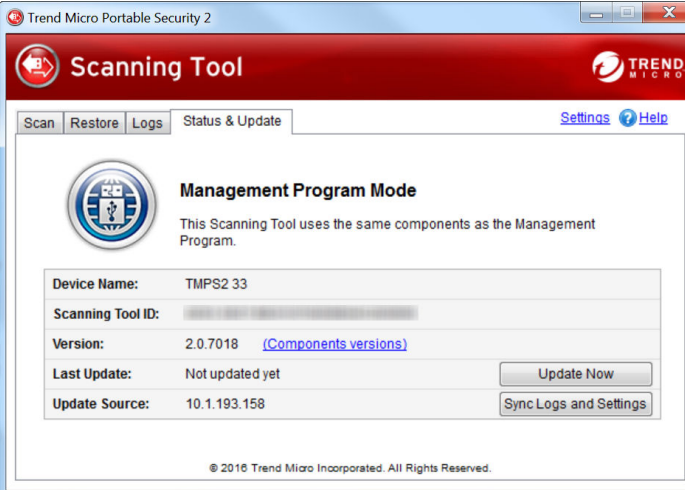
This is a short guide on how to use the console of this device.

TABLE 4-1. How to use the console

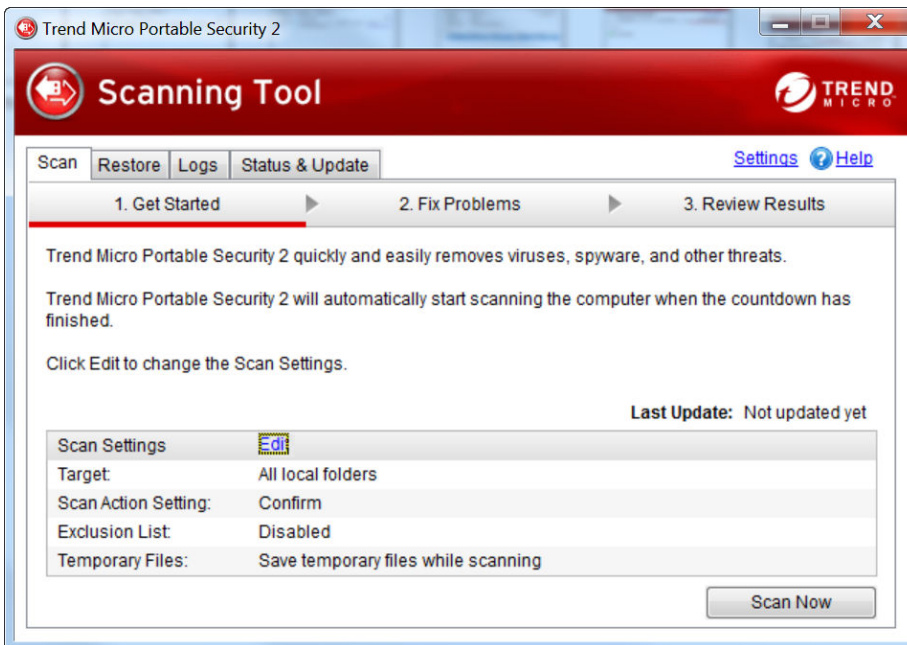
TAB OR BUTTON	DESCRIPTION
Settings	<p>Click this link to check or change the settings of the scanning tool device.</p> <p>Refer to Changing the Scanning Tool Settings on page 4-23.</p>
Help	<p>Click this link to open the help file and to find more information about how to use this device.</p>
Scan tab	 <p>Show the scan process and settings.</p> <p>See Scan Tab on page 4-6.</p>

TAB OR BUTTON	DESCRIPTION
Restore tab	 <p>Check the quarantined files that the scan process found and performed an action on.</p> <p>See Restore Tab on page 4-7.</p> <hr/> <p> Note</p> <p>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.</p>

TAB OR BUTTON	DESCRIPTION
Logs tab	 <p data-bbox="387 813 1089 867">Check the results of earlier scans done on the computer connected to the Scanning Tool.</p> <p data-bbox="387 883 1089 911">See Logs Tab on page 4-8.</p>

TAB OR BUTTON	DESCRIPTION
<p>Status & Update tab</p>	 <p>FIGURE 4-1. Standalone device</p>  <p>FIGURE 4-2. Managed device</p> <p>Check the status of the components and perform an update, if needed.</p> <p>See Status & Update tab on page 4-10.</p>

Scan Tab



- **Edit:** Click this link to check or change the scan settings.
See *Scan Settings* on page 3-10.
- **Scan Now:** Click this button to manually start the scanning process.
See *Performing a Scan* on page 4-16.
- **Stop:** You will see this button when the device is scanning the computer. Click this button to stop scanning immediately.
- **Apply Now:** You will see this button after the device has finished scanning the computer and has found a threat. Click this button to perform the selected action.
See *Security Threats Found* on page 4-20.

- **Scan Again:** You will see this button after you have applied the selected action. You can perform another scan to make sure you did not have any more threats.
- **Close:** Click this button to close the console.
- **Suspend:** Click this button to suspend a current scan.

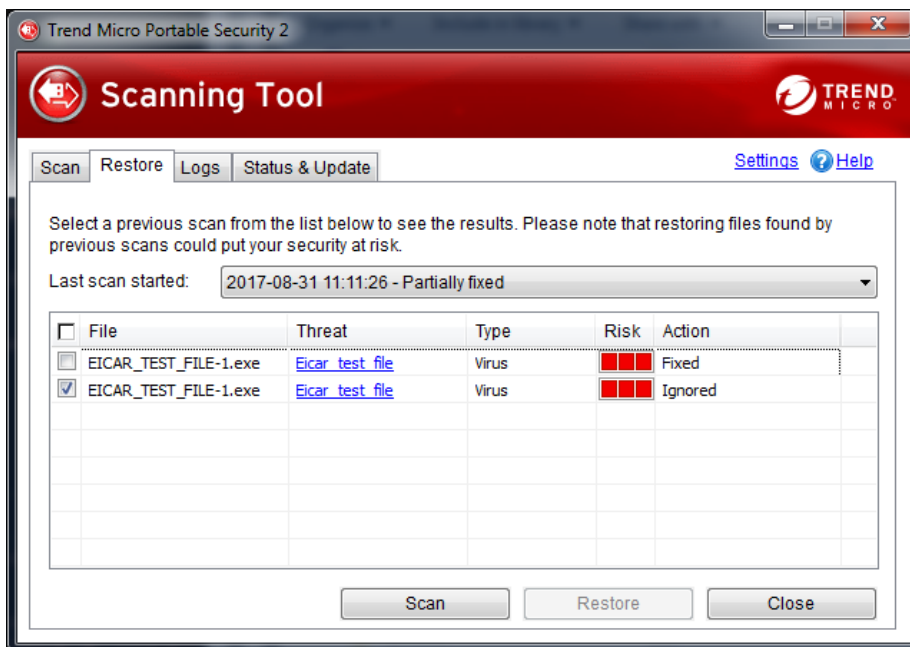


Note

- To enable the Suspend button, go to the **Scan Tab, Scan Settings > Edit**, then select **Enable Suspend scan**.
- Suspending a scan stores the scanning environment. Users may resume scanning immediately after the Scanning Tool is relaunched.

Refer to *Performing a Scan on page 4-16*.

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). For more information, see [Scan Action on page 3-18](#).

- **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 4-21](#).



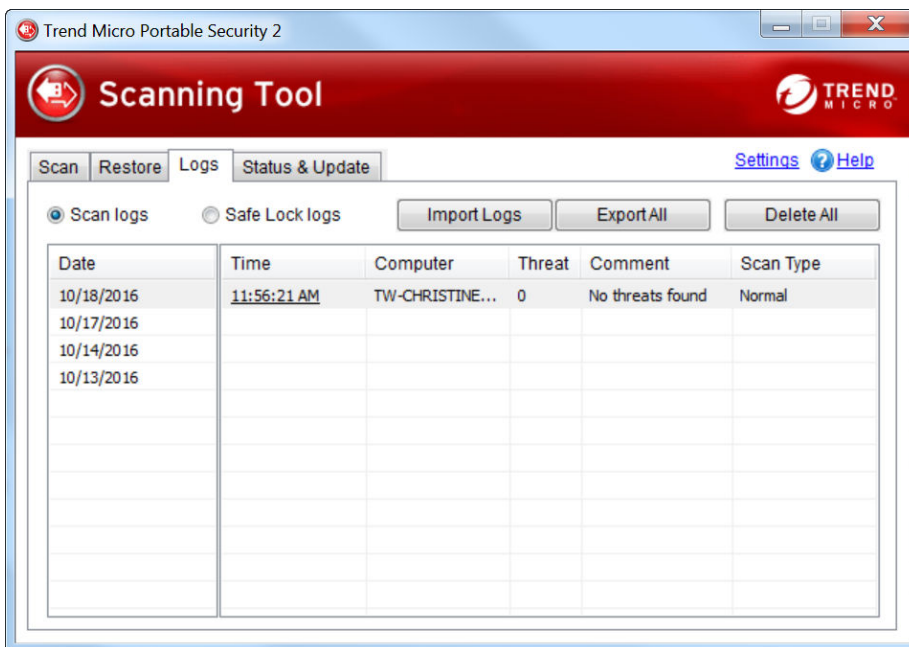
WARNING!

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**.

See *Viewing Logs and Reports on page 3-35*.



- **Import Logs:** Click this button to import database format logs.
See *Importing Logs on page 3-41*.
- **Export All:** Click this button to export all the logs into database or csv format.
See *Exporting Logs on page 3-43*.
- **Delete All:** Click this button to delete all log entries.



Note

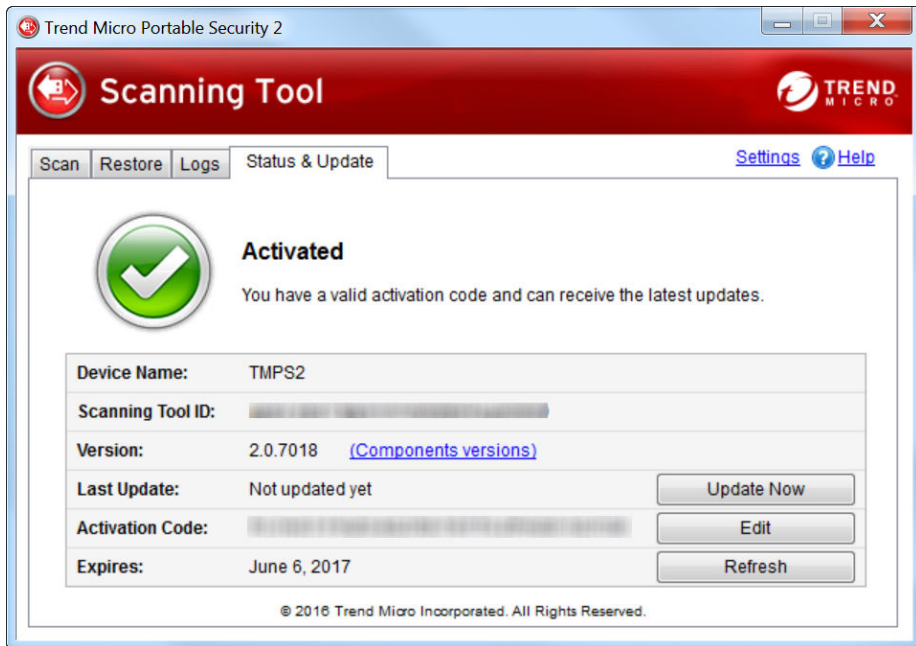
Trend Micro recommends exporting logs before deleting them.

Status & Update tab

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

For more information on the device activation status, refer to *Activation Status on page 2-8*.





- **Device Name:** This is the name of the Scanning Tool.
To change this name, refer to [Scanning Tool Name Setting on page 4-26](#).
- **Scanning Tool ID:** The Scanning Tool ID is a unique identification number given to every Scanning Tool device.
- **Version:** The build number of the Trend Micro Portable Security 2 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 2-14](#).

- **Expires:** Shows the expire date of the activation code. Click **Refresh** after you have changed the activation code and it still says expired.
- **Sync Logs and Settings:** Click this button to start downloading settings and uploading logs to the Management Program.

Component Updates

Make sure to update your Scanning Tool for the most recent security pattern file or scan engine from Trend Micro. The date next to Last Update shows the last time you updated the components. For details on update components, refer to *Checking the Latest Components on page 3-28*.

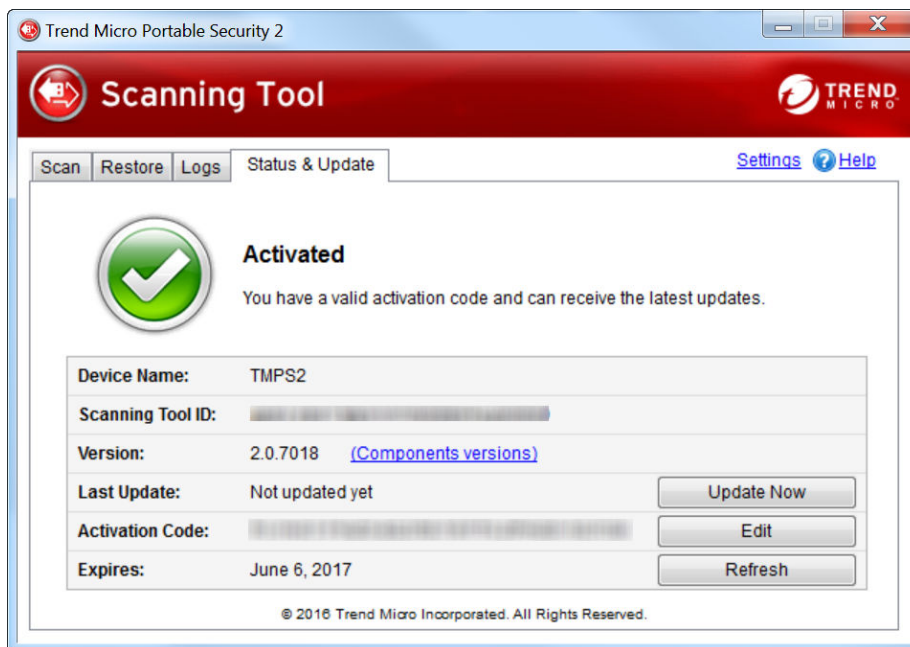


FIGURE 4-3. The Status & Update tab of the Standalone Scanning Tool



FIGURE 4-4. The Status & Update tab of the Managed Scanning Tool

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 4-23](#).

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

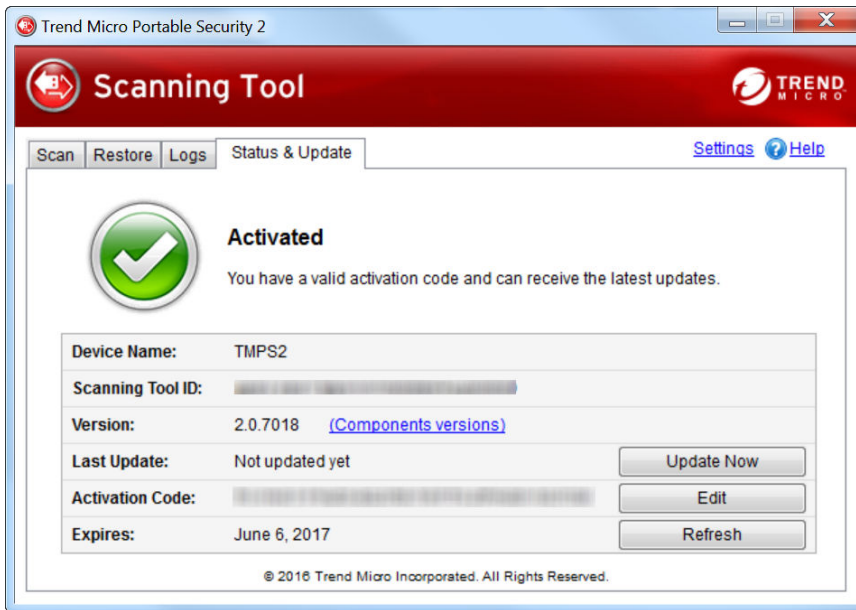


FIGURE 4-5. Standalone device



FIGURE 4-6. Managed devices

3. Click **Update Now**.

Synchronizing Component Updates

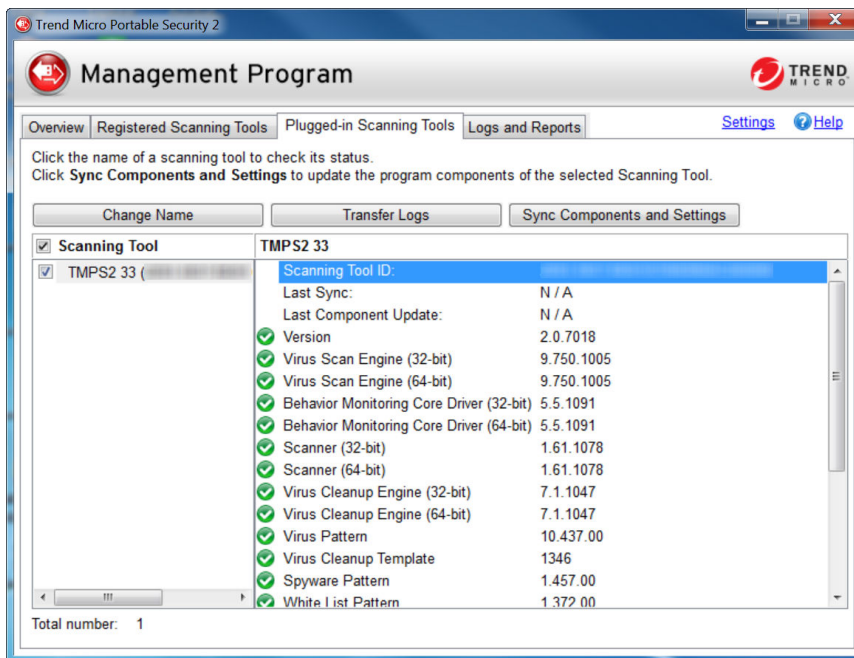
Update the Scanning Tool for the latest components, hot fixes, and settings by synchronizing with Management Program. If you updated the components on the Management Program and did not synchronize the Scanning Tool, the Scanning Tool will continue to use the older components when scanning.

Procedure

1. Update the components on the Management Program.
2. Plug in the Scanning Tool to the Management Program computer.

**Note**

You can plug in the Scanning Tool locally on a Management Program computer or connect it remotely from a computer with Internet connection.



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

Performing a Scan

Refer to the LED lights on the Trend Micro Portable Security 2 Scanning Tool device to determine what the scan status is.

TABLE 4-2. Scanning Tool indicator lights.

INDICATOR LIGHTS	DESCRIPTION
Blue (Blinking)	Information is being written to or retrieved from the Scanning Tool.
Blue	The scan is complete and no threats were found.
Yellow	The scan is complete and all threats are cleaned.
Red	The scan is complete and threats are found. Need to take actions to deal with the threats.
Blue, Yellow, and Red (Continuous)	The Scanning Tool is currently scanning the computer.

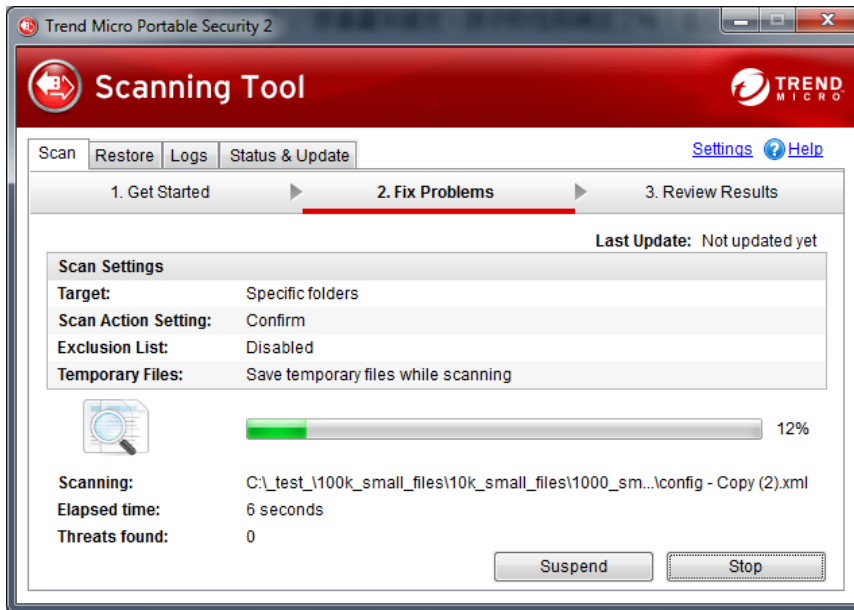
Procedure

1. Connect the Scanning Tool to the computer that you want to check.
2. Choose **Run Trend Micro Portable Security 2** in the window that automatically opens.

**Note**

If the Scanning Tool does not start, you can open Windows Explorer and double-click `Launcher.exe` from the `TMPS2_SYS` partition.

3. The scan will automatically begin 30 seconds after the Scanning Tool window opens.

**Note**

Click **Stop** if you want to stop scanning the computer.

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.

**WARNING!**

Trend Micro does not recommend unplugging the Scanning Tool while the LED is flashing or while the Scanning Tool console is open. For more information, refer to [Removing the Scanning Tool on page 4-32](#).

Checking the Scan Results

Follow the appropriate directions based on the results of the scan.

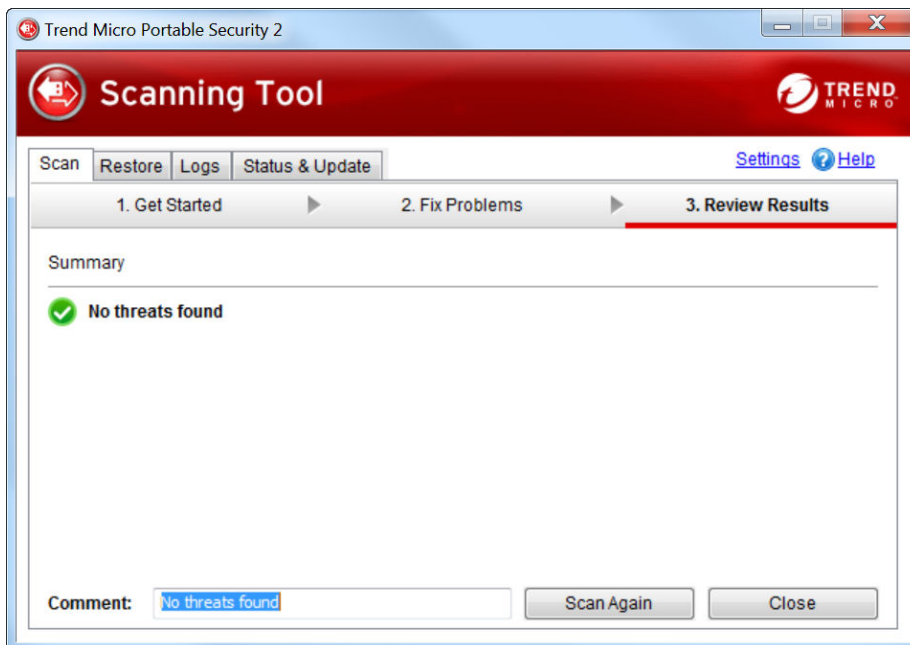
No Security Threats Found

If the scan found no threats, then you do not need to take any action. Click **Close** to shut the window.



Tip

To run another scan, click **Scan Again**.



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:** Trend Micro Portable Security 2 will not take any action against the threat.
 - **Fix:** Trend Micro Portable Security 2 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.

See *Viewing Logs and Reports on page 3-35*.

Restoring Quarantined Files

You can restore files if Trend Micro Portable Security 2 fixed and quarantined files that you need.

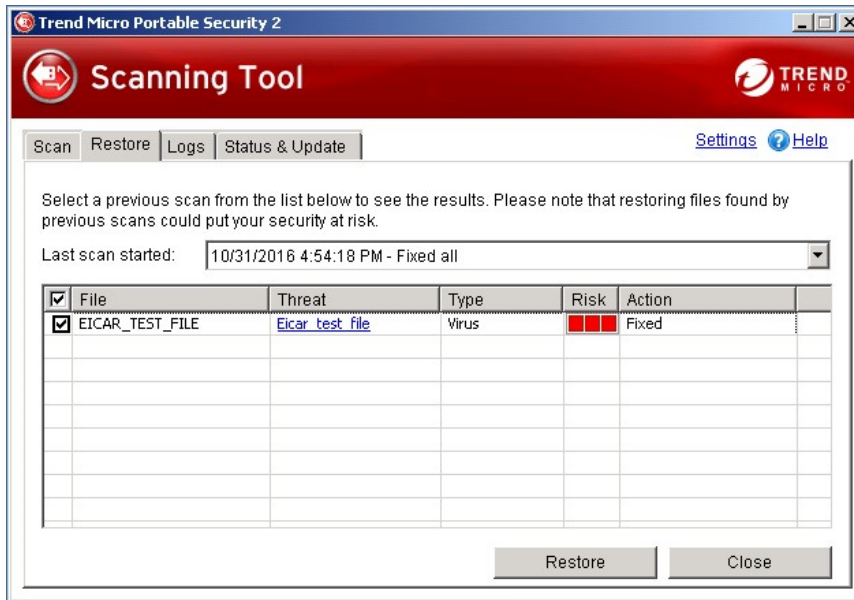
**WARNING!**

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 Trend Micro Portable Security 2 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**.
-

Changing the Scanning Tool Settings

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

Procedure

1. Open the Scanning Tool console.



FIGURE 4-7. The Managed Scanning Tool console

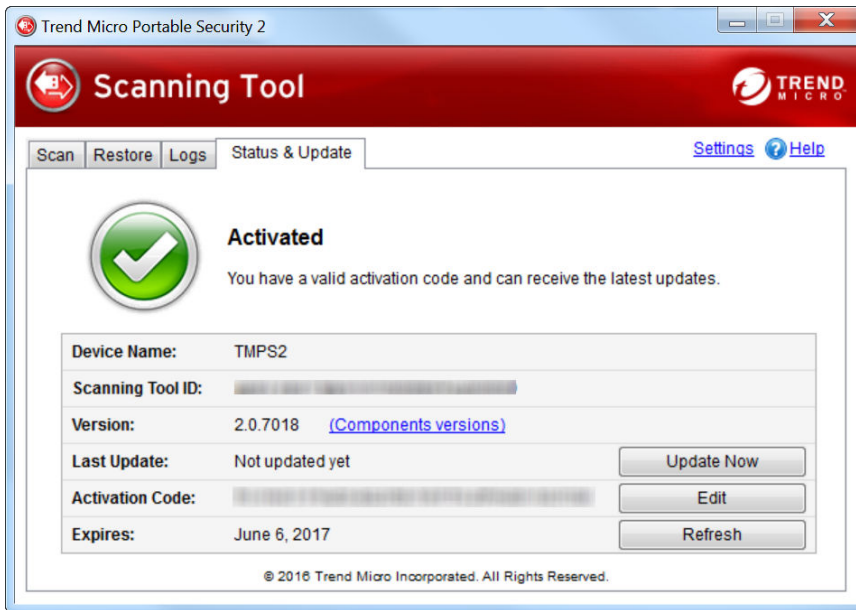


FIGURE 4-8. The Standalone Scanning Tool console

2. Click **Settings**.

Scanning Tool Settings

Specify the Management Program IP address, password, and port to sync the Scanning Tool settings with your Management Program or to another Management Program.

Management Program: Address: 10.1.65.55 Port: 10240
 Password: ••••• Register

Update Source:

- Management Program
- Trend Micro ActiveUpdate Server (Internet required)
 http://tmps2-p.activeupdate.trendmicro.com/activeupdate
- Other update source
 http://
 Update source is used to check and download the latest scan engine and components.

Language: English

Save Cancel

**Note**

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

3. Specify an update source.
 - **Management Program:** Obtain updates from the specified Management Program locally and remotely. Specify the Management Program IP address, port, and password, and then click **Register**.
 - **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.



Note

Remote connection to Management Program is only supported for Trend Micro Portable Security 2 SP2.

4. (Optional) Select a language from the drop-down menu to change the Scanning Tool language.
 5. Click **Save**.
-

Scanning Tool Name Setting



Note

The Scanning Tool name can be 128 alphanumeric characters or 64 double-byte characters. TMPS2 is the default value for the Scanning Tool name.

You can also change the name from the Management Program. Refer to [Changing the Name of the Scanning Tool on page 3-25](#).

Procedure

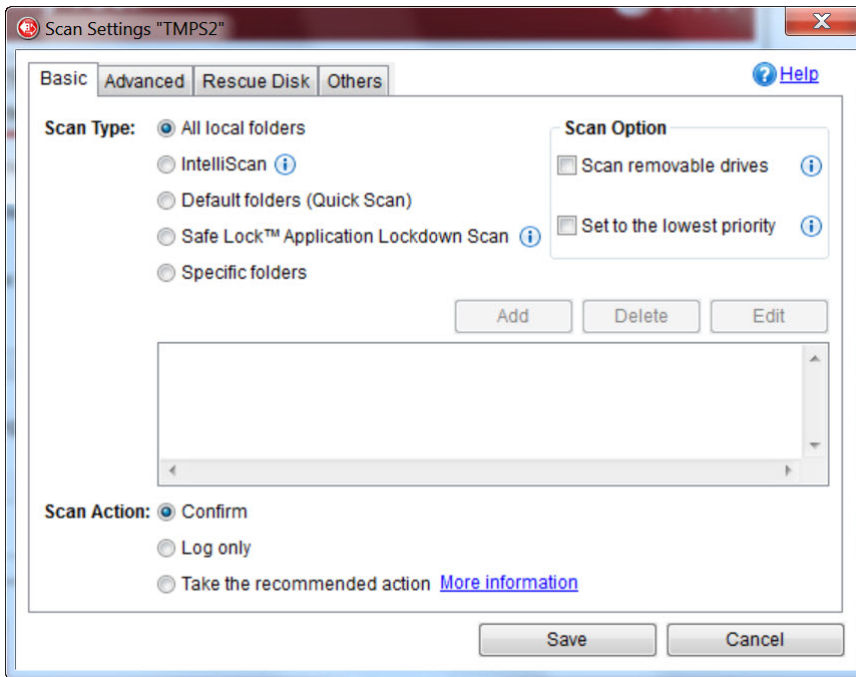
1. Open the Scanning Tool console.
2. Click **Stop**.

The Scan settings options will display on the **Scan** tab.



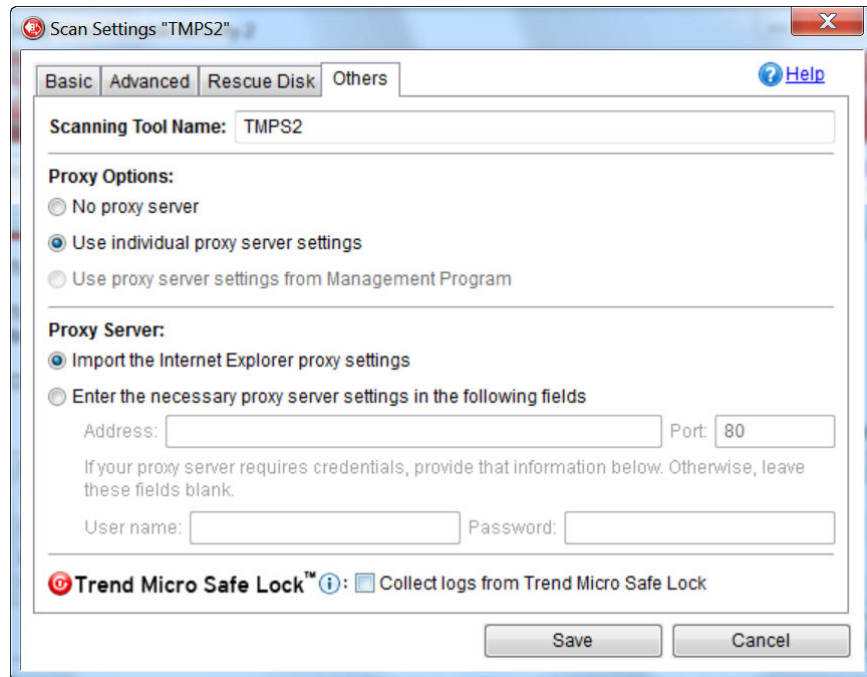
3. Click **Edit**.

The Scan settings page will display.



4. Click the **Others** tab.

The **Others** tab page will display.



5. Change the Scanning Tool name.
6. Click **Save**.

Scan Settings

If you are using the Trend Micro Portable Security 2 as a managed device, Trend Micro recommends synchronizing the settings with the Management Program instead of using this option. If you make changes to the Scanning Tool and then synchronize updates and settings with the Management Program, the Management Program settings will replace the Scanning Tool settings.

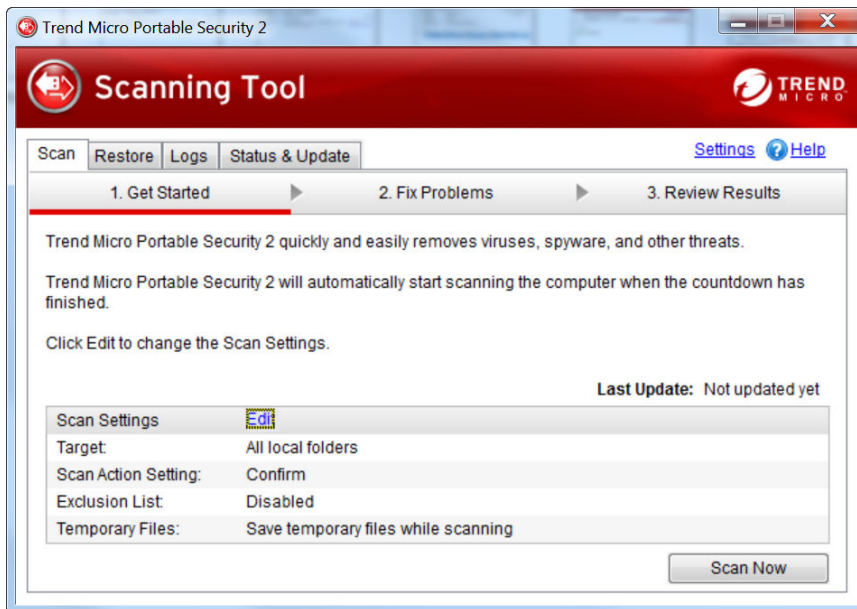
See [synchronize updates and settings with the Management Program on page 4-15](#).

If you are using the Trend Micro Portable Security 2 device as a standalone Scanning Tool, you can use the **Edit** link to change the scan settings of the USB device. Any changes made will only be for this Scanning Tool.

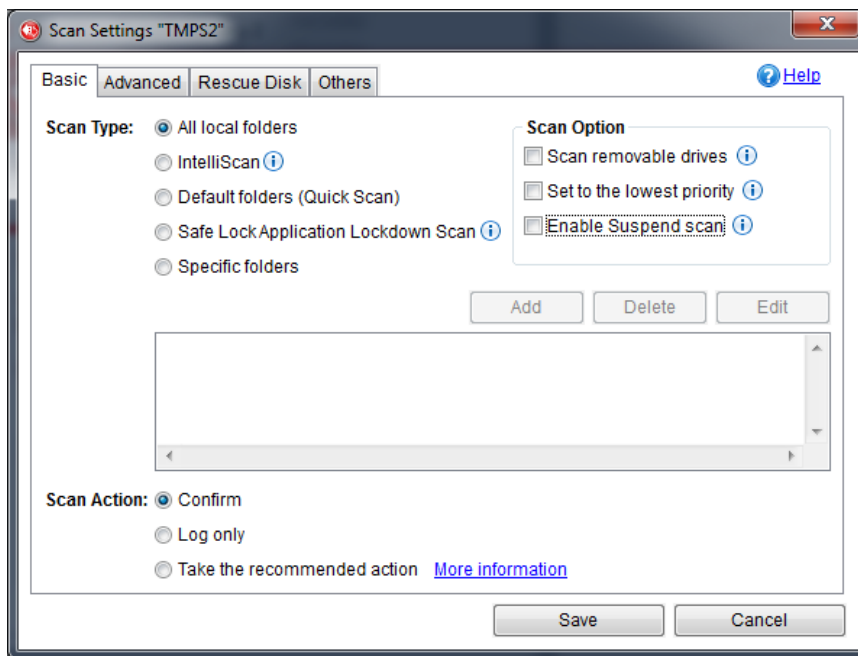
Procedure

1. Open the Scanning Tool console.
2. Click **Stop**.

The Scan settings page will display.



3. Click **Edit**.



4. Change the following settings:
 - *Scan Settings (Basic) on page 3-16*
 - *Scan Settings (Advanced) on page 3-19*
 - *Rescue Disk on page 3-22*
 - *Scan Settings (Others) on page 3-23*
5. Click **Save**.
6. Click **Scan Now** to start scanning with the new scan settings.

Synchronizing Logs and Settings

Regularly connect to your Management Program to get the latest settings or to upload the logs from the Scanning Tool.

You can also click **Sync Components and Settings** or **Transfer Logs** from the Management Program. Refer to *Synchronizing Component Updates on page 4-15*.

Procedure

1. Plug in the Scanning Tool on a computer with an Internet connection.
2. Open the Scanning Tool console.
3. Go to the **Status & Update** tab.



4. Click **Sync Logs and Settings**.
-

Removing the Scanning Tool

Follow the procedure below when removing the Scanning Tool from any computer to avoid corrupting the data on the Scanning Tool.

**Important**

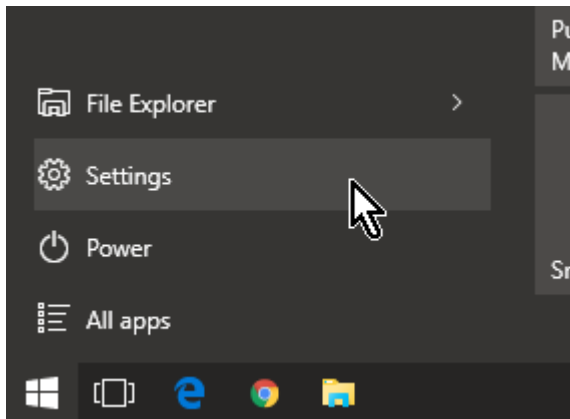
Remove the Scanning Tool only after the lights on the USB device have finished flashing.

For Windows 10

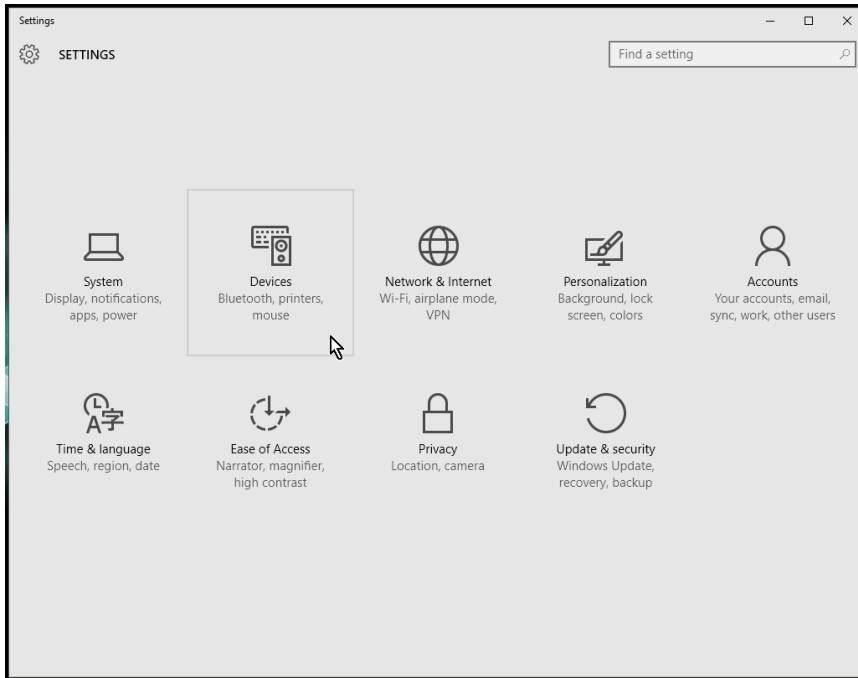
Perform the following steps to safely remove the Scanning Tool from a Windows 10 desktop:

Procedure

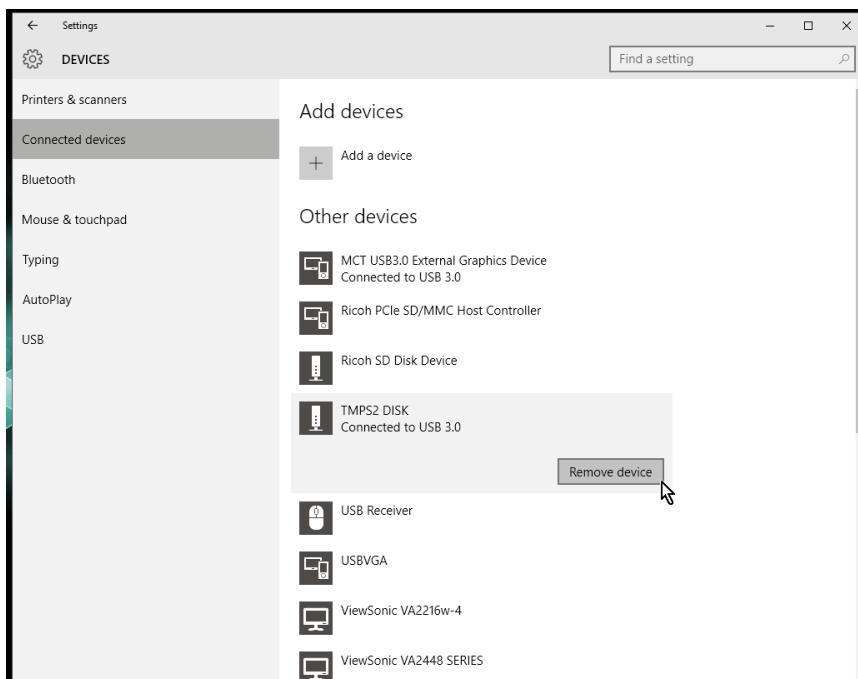
1. Locate and select **Settings** from the **Start** menu on the Windows 10 desktop.



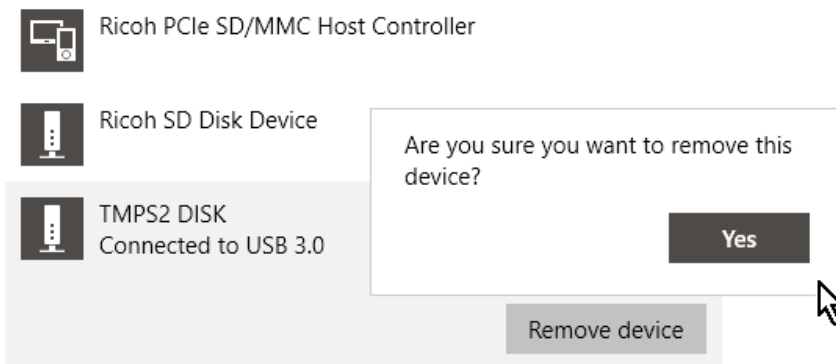
2. On the **Settings** screen, select **Devices**.



3. On the left panel, select **Connected devices** > **TMPS2 DISK** > **Remove device**



4. The **Are you sure you want to remove this device?** message appears.



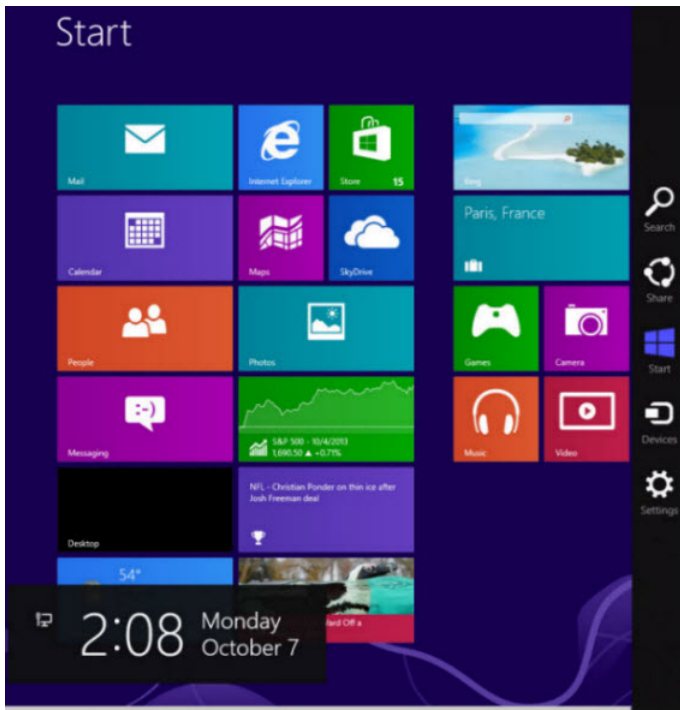
5. Click **Yes**.
-

For Windows 8

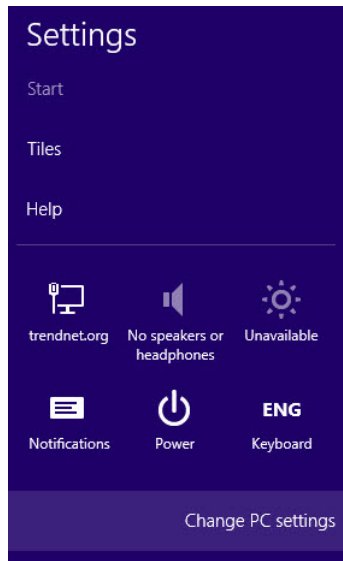
From the Windows 8 desktop, you can follow the same steps as the ones in [Windows 7 on page 4-39](#). You can also follow the steps below to remove the tool from the Modern UI.

Procedure

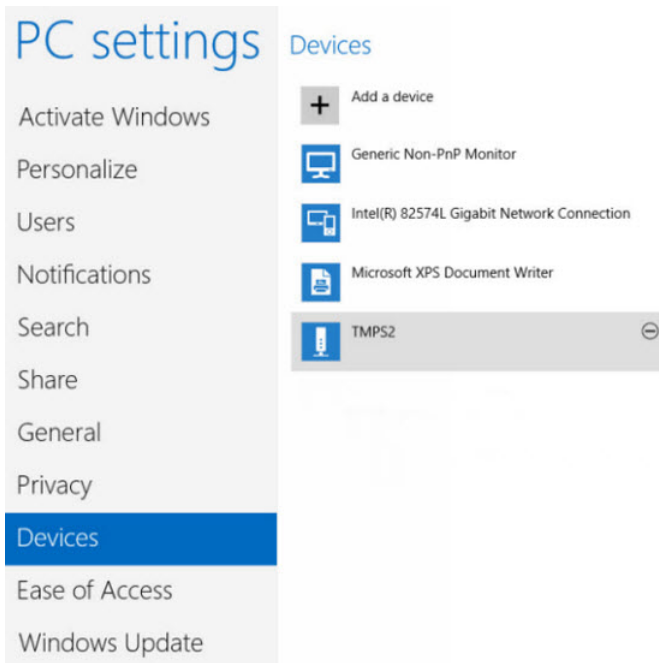
1. From the Windows 8 Start screen, point to the right part of the screen to bring out the available charms.



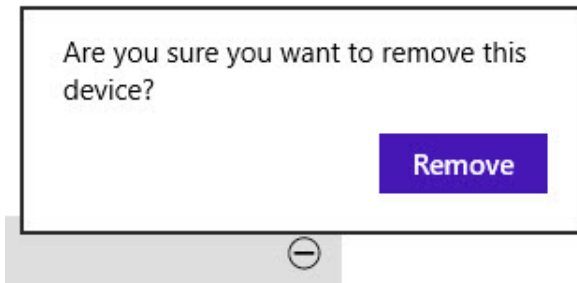
2. Click **Settings**.



3. Click **Change PC settings**.



4. Click **Devices > TMPS2 DISK**.
5. Click the minus icon. The **Are you sure you want to remove this device?** message appears.

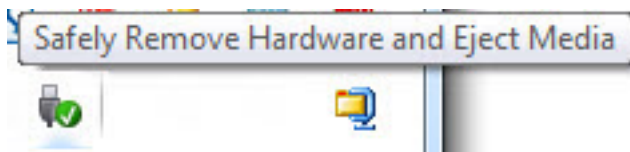


6. Click **Remove**.
-

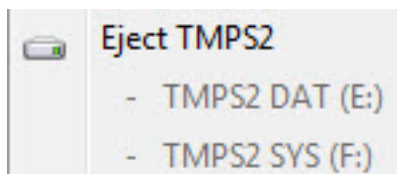
For Windows 7

Procedure

1. Click the system tray icon in the bottom right corner of the Windows desktop to see additional icons.
2. Click the icon to display a list of connected devices.



3. Click **Eject TMPS2 DISK**.

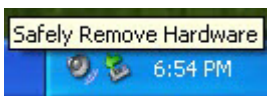


4. Unplug the Scanning Tool from the computer.
-

For Windows Vista or Windows XP

Procedure

1. Double-click the system tray icon in the bottom right corner of the Windows desktop to open the **Safely Remove Hardware** window.



2. Select a Scanning Tool from the list and click **Stop** to open the **Stop a Hardware Device** window.
 3. Click **OK** to make the ... **can now be safely removed from the system** message appear on the bottom right corner of the Windows desktop.
 4. Click **Close** in the **Safely Remove Hardware** window.
 5. Detach the Scanning Tool from the computer.
-

Using the Scanning Tool Agent

The Scanning Tool Agent is used to specify update, scan, and synchronization settings of a Scanning Tool when it is plugged into an endpoint.

Installing the Scanning Tool Agent



Important

Scanning Tool Agent cannot be installed on an endpoint installed with Management Program.

Follow the steps below to install the Scanning Tool Agent.

Procedure

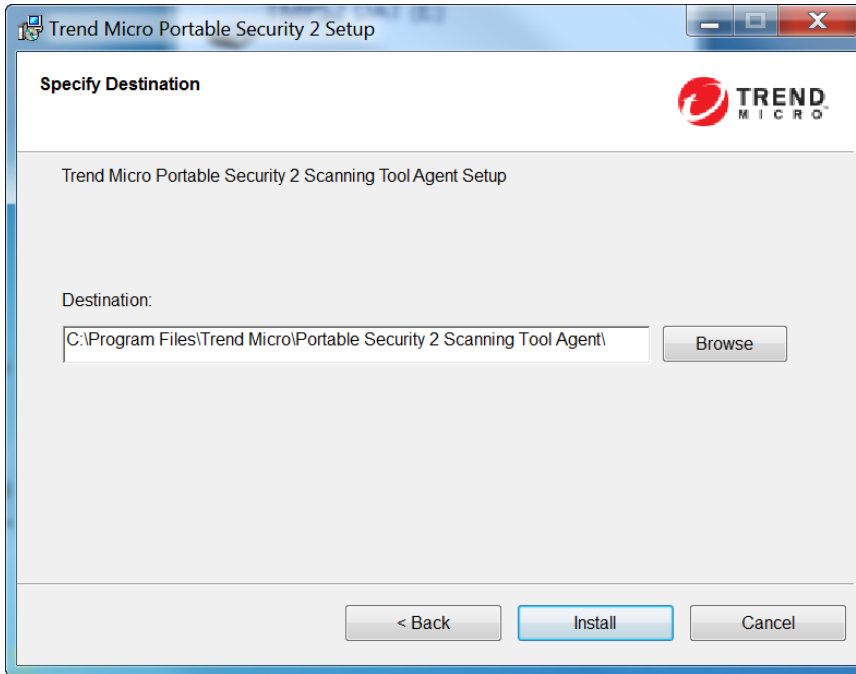
1. Plug in the Scanning Tool USB device to the computer where you want to install the Scanning Tool Agent.
2. When a window opens, click **Open folder to view files**.



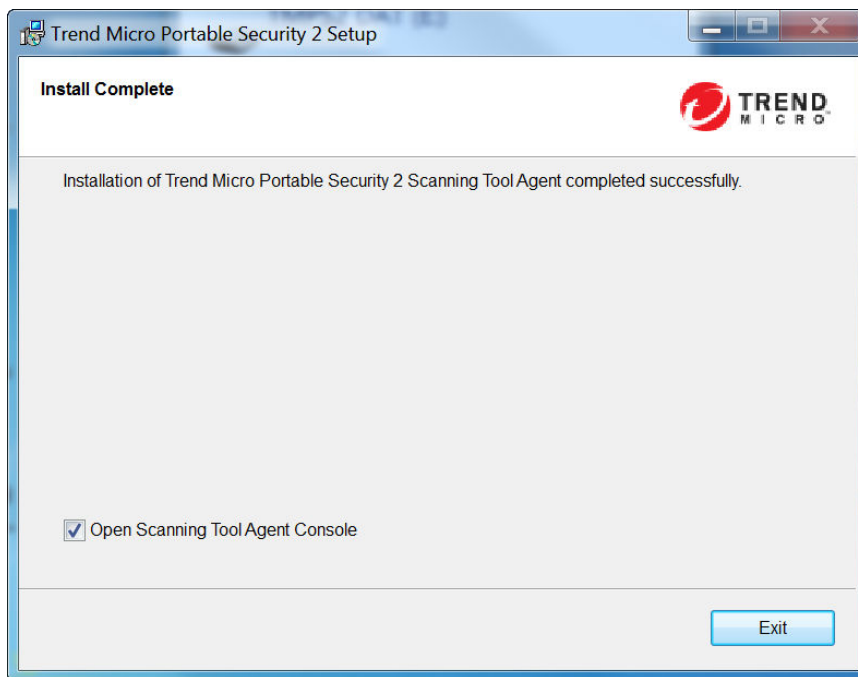
3. Open the TmpsAgent folder in the TMPS2_SYS drive, and double-click the Setup.exe file (Setup.exe).
4. When the **End-User License Agreement** window appears, read the agreement and click **Agree and Continue**.



5. When the **Specify Destination** window opens, type or browse for a folder and click **Install**.



6. When the **Installation Complete** window appears, click **Exit**.



By default, the Scanning Tool Agent console will open. To disable this function, unselect **Open Scanning Tool Agent Console**.

Uninstalling the Scanning Tool Agent



Note

Make sure to unlock Trend Micro Safe Lock™ before uninstalling the Scanning Tool Agent.

Follow the steps below to uninstall the Scanning Tool Agent.

Procedure

1. From the Windows Start Menu, select **All Programs > Trend Micro Portable Security 2 Scanning Tool Agent**.

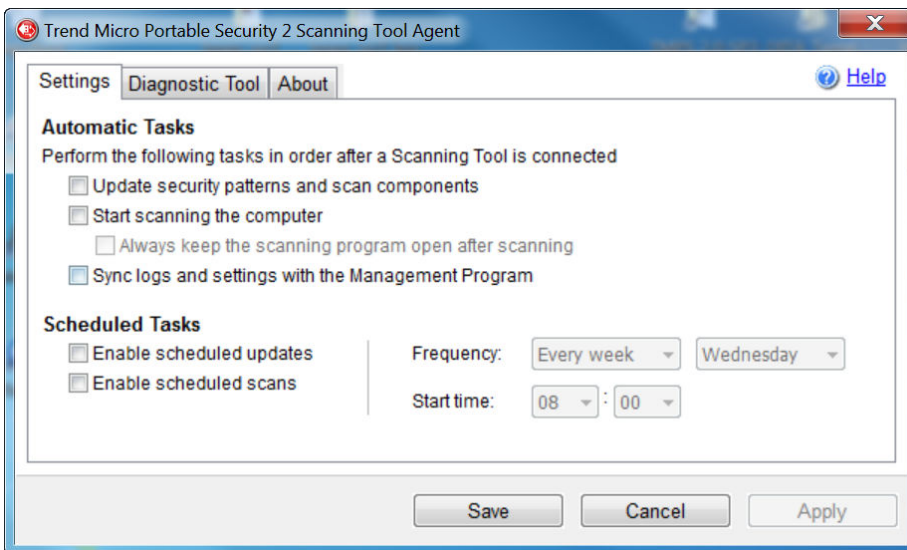
**Note**

Make sure the Scanning Tool is not plugged into the computer before continuing.

2. Select **Uninstall**.
-

Settings Tab

Click the **Settings** tab to access the following functions.



- **Update security patterns and components:** Select this option to automatically update the Scanning Tool for the latest security patterns and components.

- **Start scanning the computer:** Select this option 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**.

**Note**

By enabling **always keep the scanning program open after scanning**, the automatic execution of tasks by Scanning Tool Agent will be interrupted. Any enabled tasks after scanning (synchronization or scheduled update) will not be performed.

- **Sync logs and settings with the Management Program:** Select this option to synchronize logs and settings of the Scanning Tool with those on the Management Program.
- **Enable scheduled updates:** Select this option to have the Scanning Tool updated at the defined frequency and start time.
- **Enable scheduled scans:** Select this option for a Scanning Tool to scan the your device at the defined frequency and start time.

**Note**

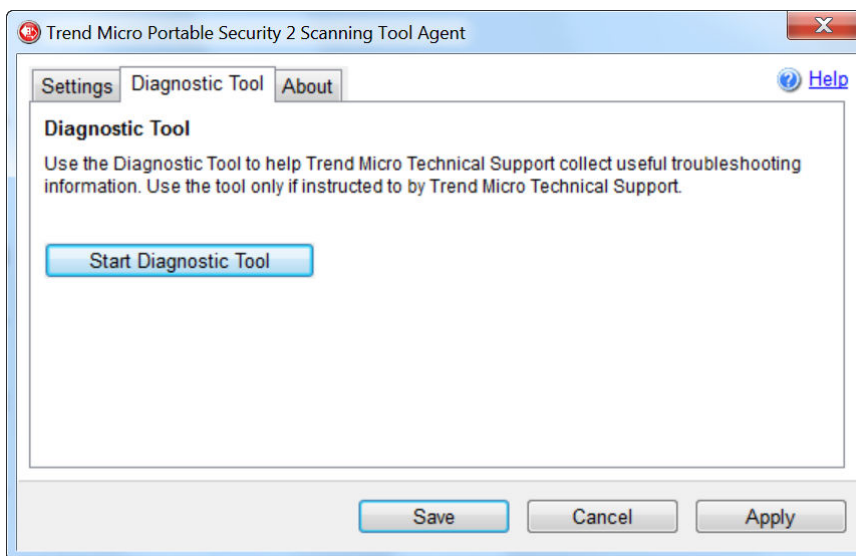
1. If both the scheduled updates and scheduled scans are enabled, Scanning Tool will always update first.
 2. The Scanning Tool console will be closed when the above tasks are complete.
 3. The execution of all automatic tasks for a Scanning Tool will be interrupted and cancelled when any of the following occurs. If you also have more than one Scanning Tools plugged in, Trend Micro recommends to close the current Scanning Tool console for the automatic tasks of another Scanning Tool to be executed.
 - There is a failure to carry out any of the tasks. This can include manual cancellation or network connection failure.
 - Threats are found while scanning.
-

Diagnostic Tool for the Scanning Tool Agent

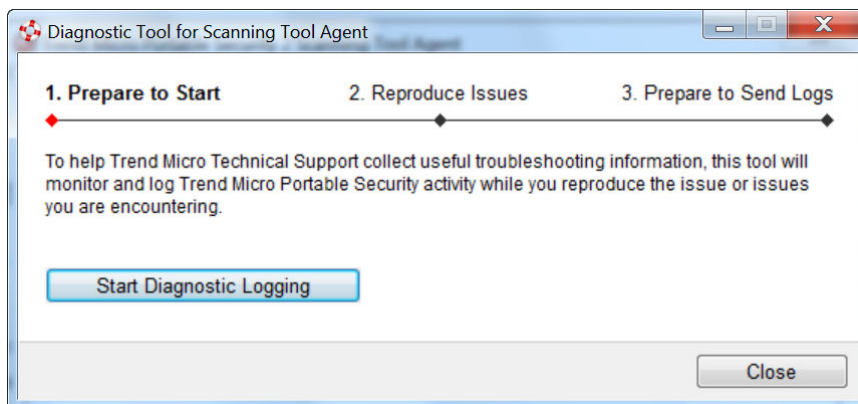
Use this Diagnostic Tool to help Trend Micro Technical Support collect useful troubleshooting information. Only use the tool when instructed by Trend Micro Technical Support.

Procedure

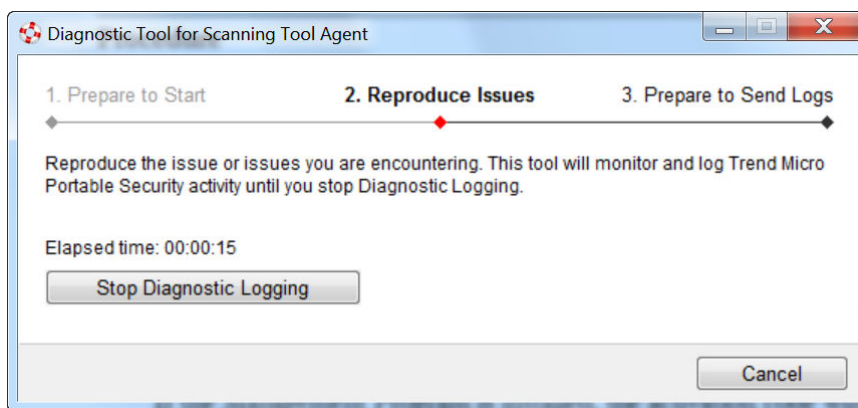
1. From the Scanning Tool Agent console, click the **Diagnostic Tool** tab.



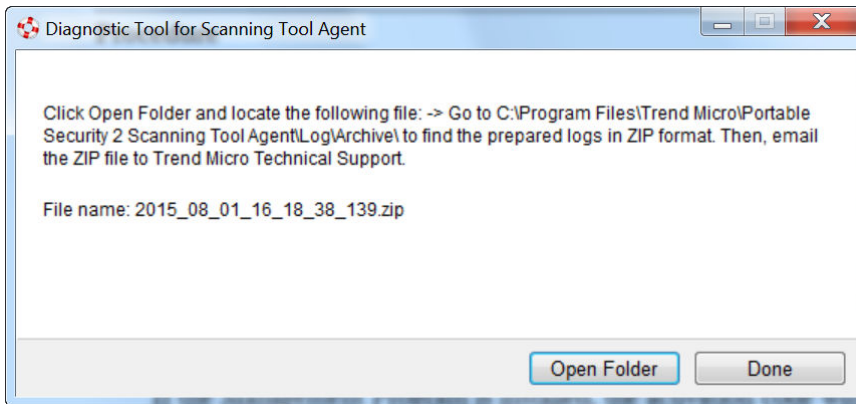
2. Click **Start Diagnostic Tool** to start this function. This window appears.



3. Click **Start Diagnostic Logging** to start collecting information and click **Stop Diagnostic Logging** to stop.



4. The collected logs will be saved to the local drive for later analysis. Click **Open Folder** to access the collected information.



Chapter 5

Additional Tools

This chapter describes the additional tools provided with Trend Micro Portable Security 2™ and how to use these tools.

Topics in this chapter:

- *Trend Micro Portable Security 2 Diagnostic Toolkit on page 5-2*
- *Trend Micro Rescue Disk on page 5-25*
- *Scanning Tool Agent on page 5-32*

Trend Micro Portable Security 2 Diagnostic Toolkit

The Trend Micro Portable Security 2 Diagnostic Toolkit has features applicable to the Scanning Tool and Management Program. This tool is installed with the Management Program and can be accessed from the Windows Start Menu.

Features:

- *Debug on page 5-2*
- *Reset Device on page 5-15*
- *Support Updates on page 5-21*
- *Converting Logs on page 5-24*
- Uninstallation (For details, refer to *Option C: Use the Trend Micro Portable Security 2 Diagnostic Toolkit on page 6-4*)

Debug

Users can use the support tool to generate debug logs that can be checked if there is an issue with the product.

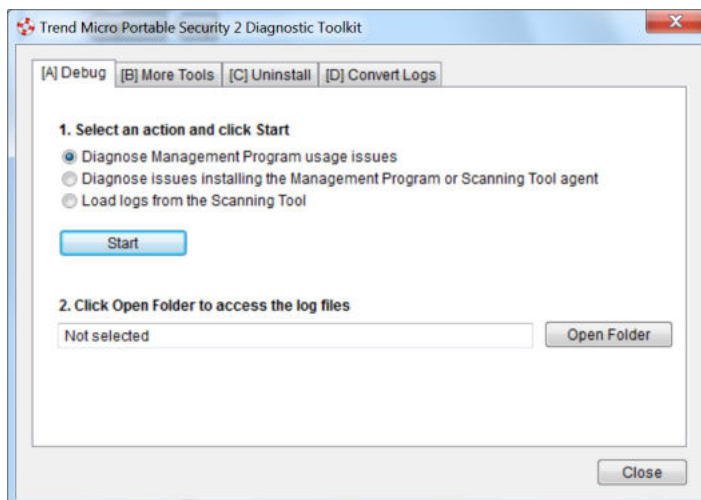
Generating Debug Logs for Management Program

Follow the steps below to generate debug logs for Management Program usage issues.

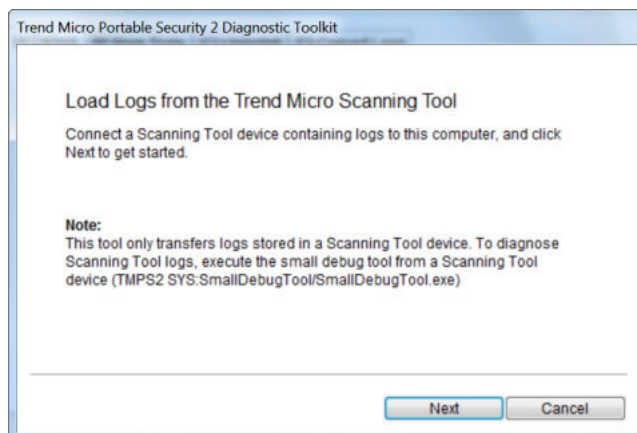
Procedure

1. From the Start menu of the Management Program computer, click **Trend Micro Portable Security 2 > Trend Micro Portable Security 2 Diagnostic Toolkit**. If you are using a different computer, you can do the following:
 - a. Plug-in the Trend Micro Portable Security 2 Scanning Tool to the computer.
 - b. Copy the SupportTool folder from the USB device into your local drive.

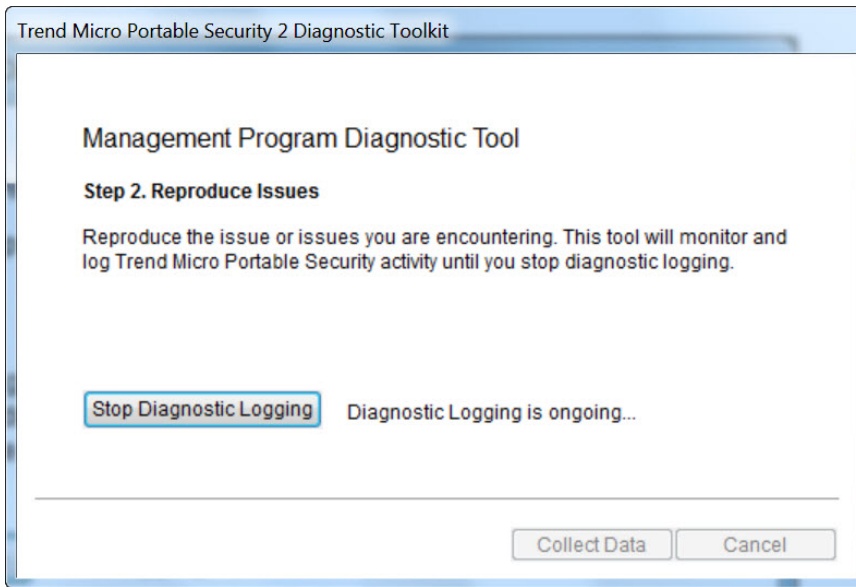
- c. Double-click the TMPSSuprt .exe file .



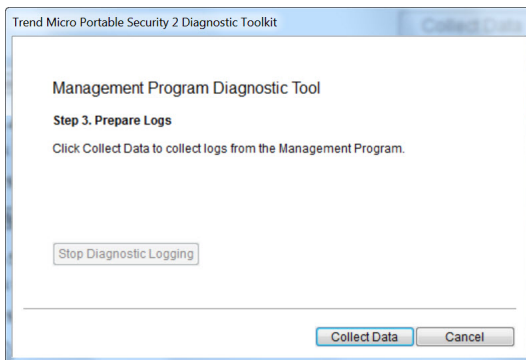
2. In the **[A] Debug** tab, select **Diagnose Management Program usage issues**, and click **Start**.



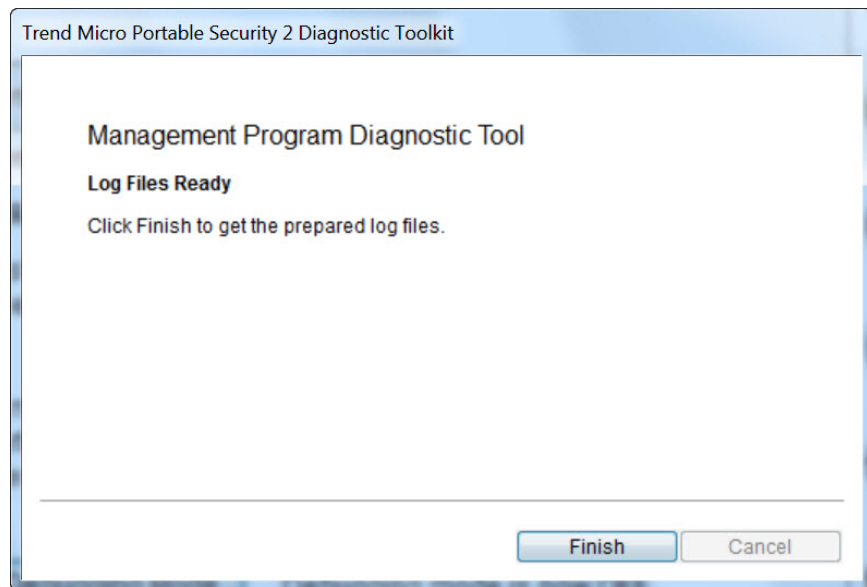
3. Click **Start Diagnostic Logging** to reproduce the issue.



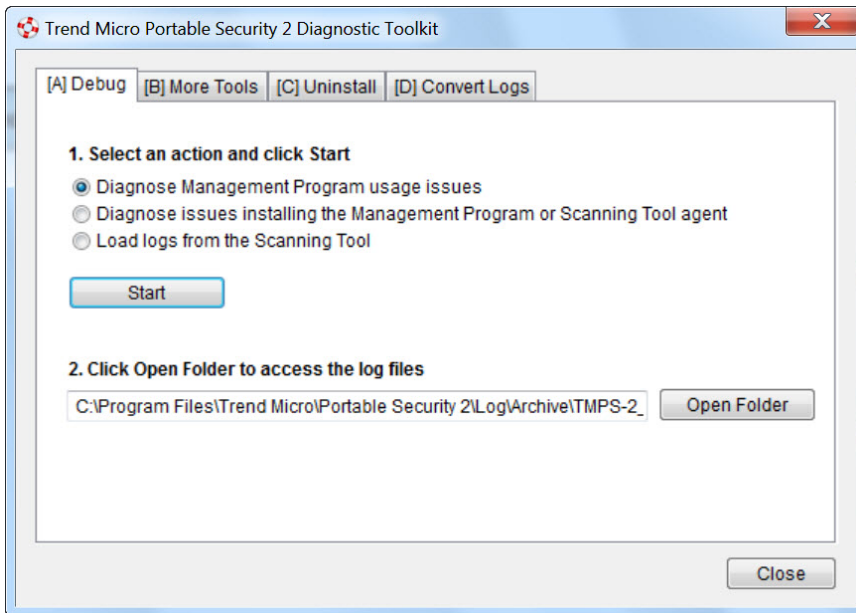
4. Click **Stop Diagnostic Logging**.



5. Click the **Collect Data** button.



6. Click **Finish** and the storage path of the logs are indicated.




7. Click **Open Folder** and make sure that there is a zipped file with a set of debug logs.

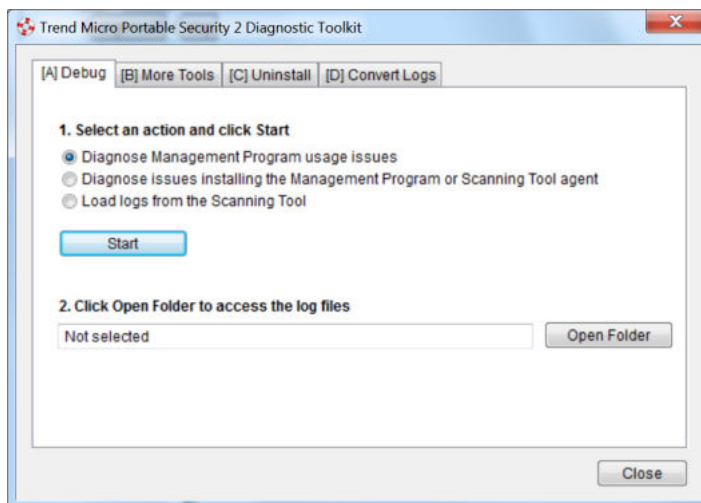
Generating Debug Logs for Installation Issues

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

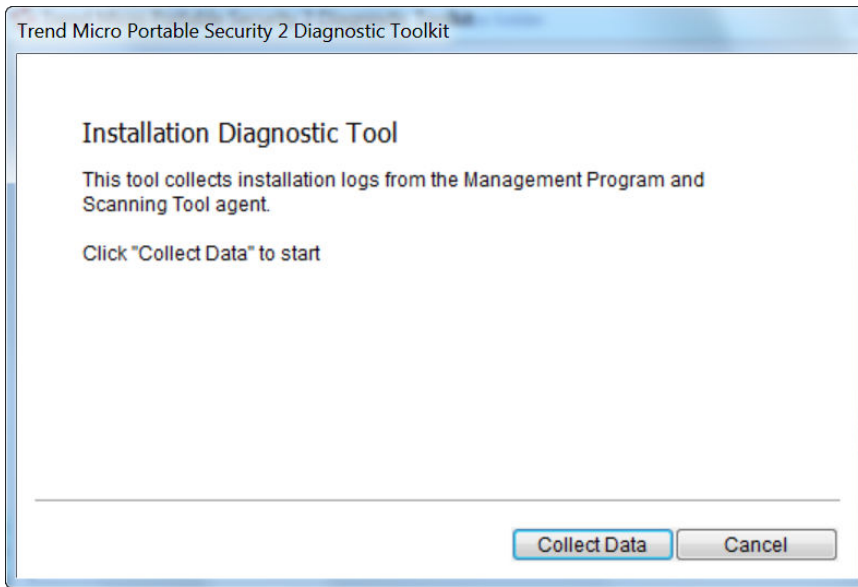
Procedure

1. From the Start menu of the Management Program computer, click **Trend Micro Portable Security 2 > Trend Micro Portable Security 2 Diagnostic Toolkit**. If you are using a different computer, you can do the following:
 - a. Plug-in the Trend Micro Portable Security 2 Scanning Tool to the computer.

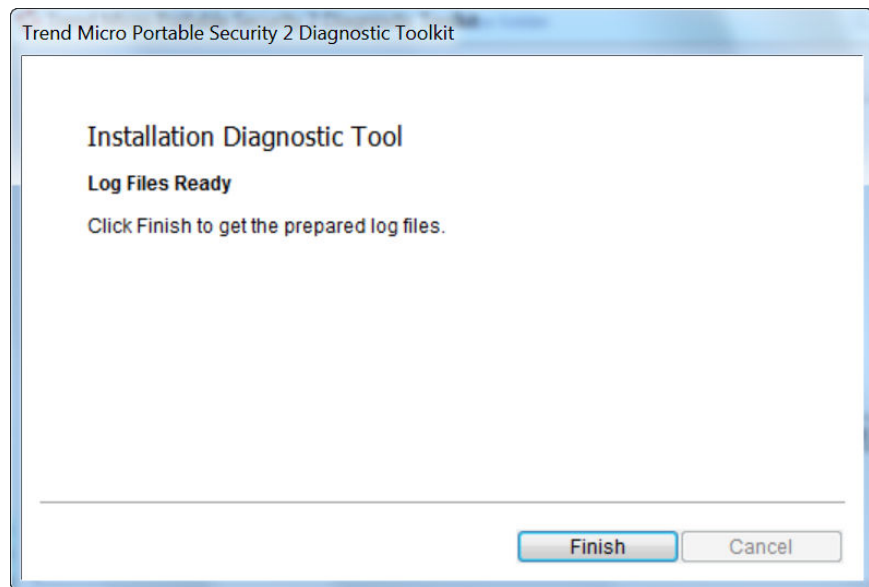
- b. Copy the SupportTool folder from the USB device into your local drive.
- c. Double-click the TMPSSuprt.exe file .



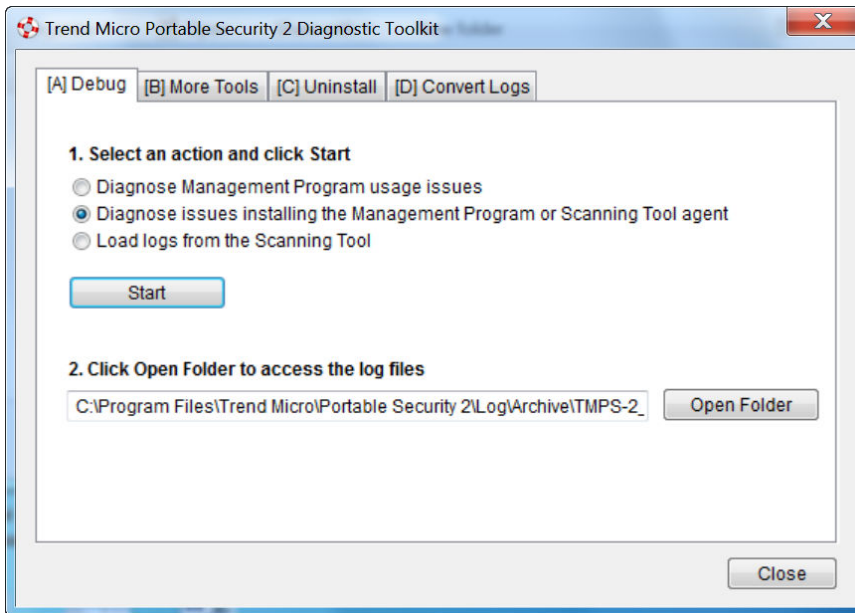
2. In the **[A] Debug** tab, select **Diagnose issues installing the Management Program or Scanning Tool Agent** and click **Start**.



3. Click **Collect Data**. Log files are prepared shortly.




4. Click **Finish**. The file location is indicated.

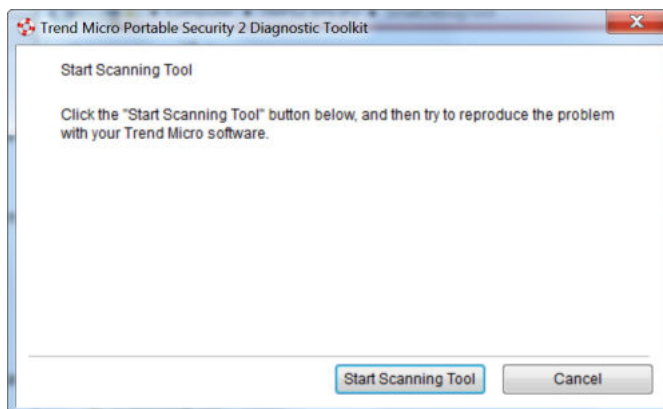


5. Click **Open Folder** and make sure that there is a zipped file with a set of debug logs.

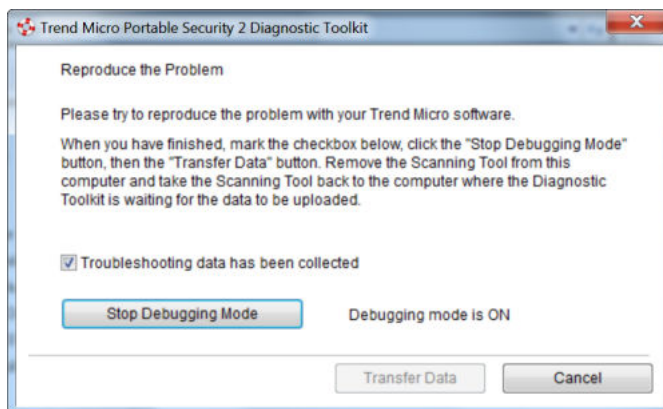
Generating Debug Logs for Scanning Tools

Procedure

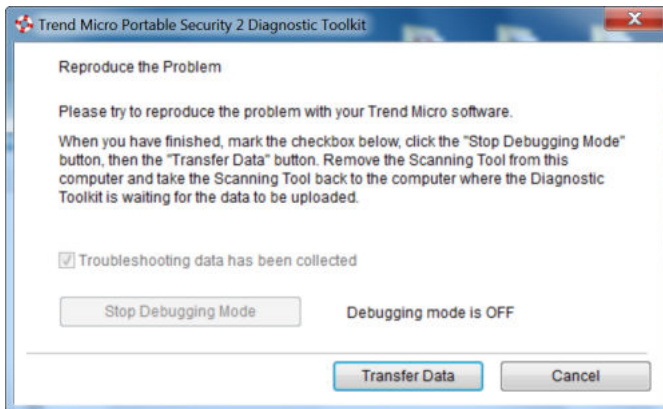
1. Plug-in the Trend Micro Portable Security 2 Scanning Tool to the computer.
2. Double-click the `SmallDebugTool.exe` file .



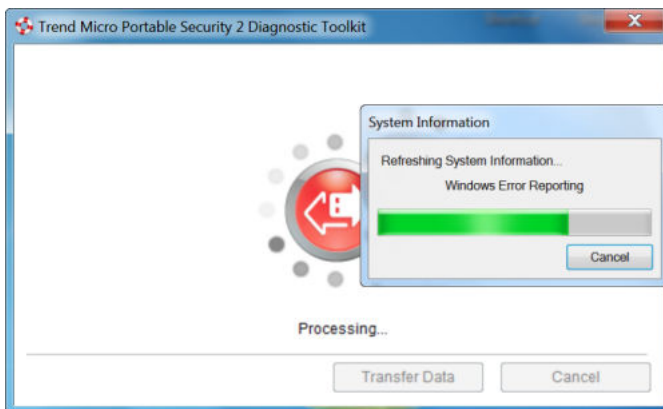
3. Click the **Start Scanning Tool** button.
4. Enable the check box to gather troubleshooting data.



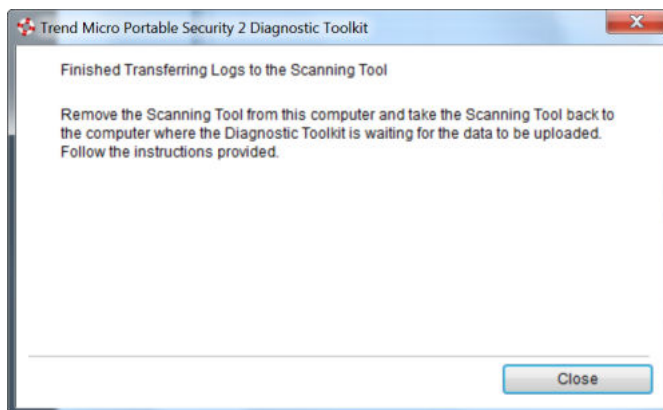
5. Click **Stop Debugging Mode**.




6. Click **Transfer Data**.



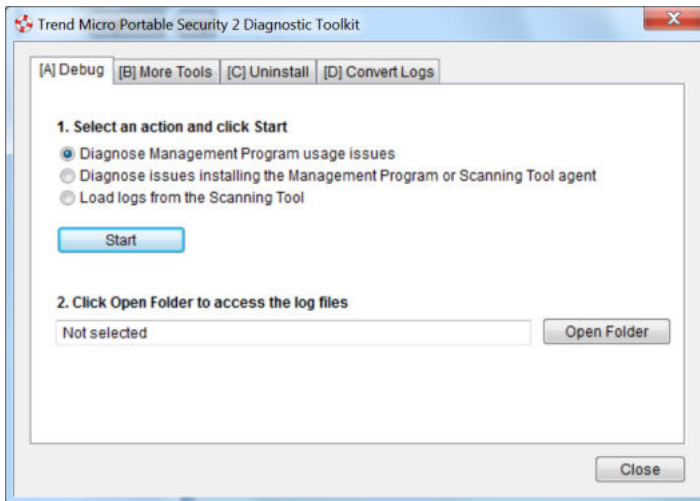
7. Click **Close**.



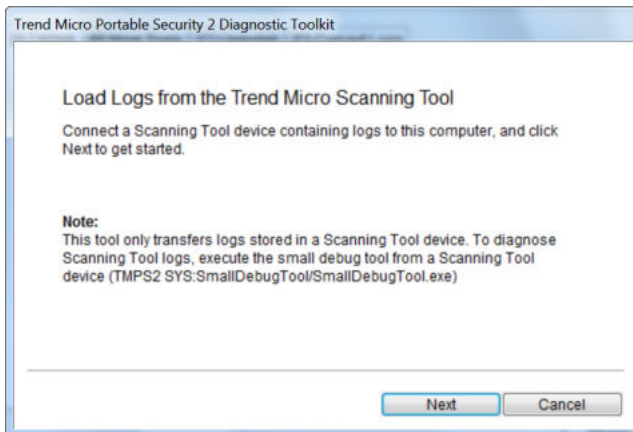
8. Copy the SupportTool folder from the USB device into your local drive.
9. Double-click the TMPSSuprt.exe file .

**Note**

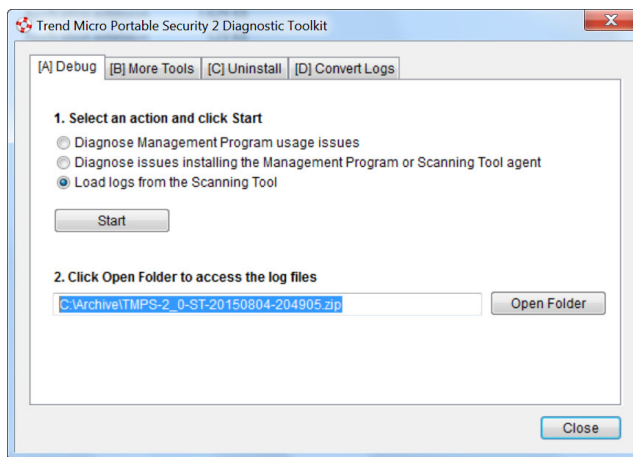
Use of the TMPSSuprt.exe file is dependent on your operating system. If you are using a 32-bit operating system, execute TMPSSuprt.exe from the Win 32 folder and if you are using a 64-bit operating system, execute TMPSSuprt.exe from the x64 folder.



10. In the **Debug** tab, select **Load logs from the Scanning Tool** and click **Start**.



11. Connect the Scanning Tool to the endpoint and click **Next**. The storage path of the logs are indicated.



12. Click **Open Folder** and make sure that there is a zipped file with a set of debug logs.

Reset Device

You can use the Trend Micro Portable Security 2 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 will keep the activation code and status.
- **Factory Reset:** Select this option to reset to factory status.




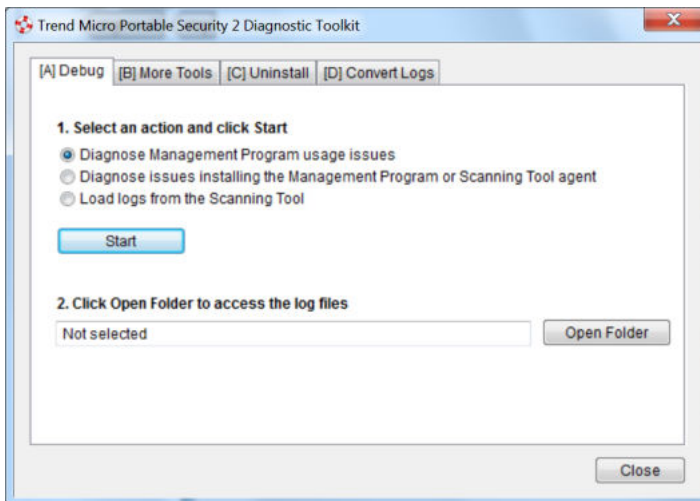
Note

You can only reset one device at a time.

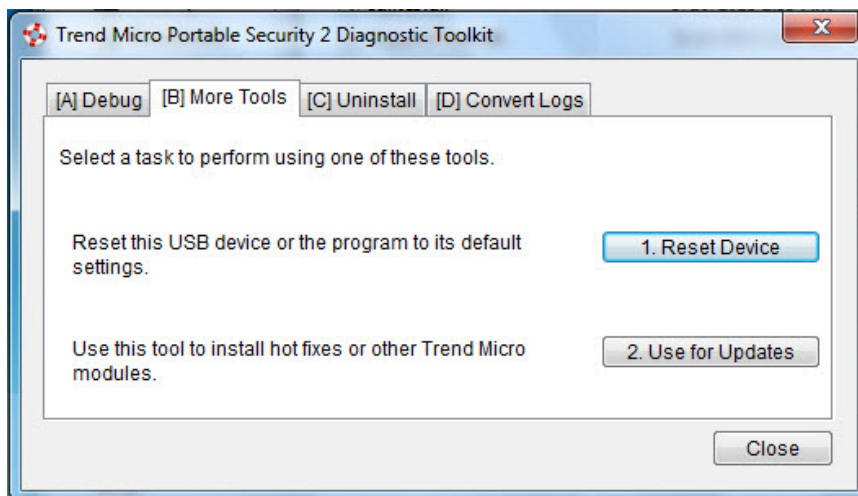
Resetting the Program

Procedure

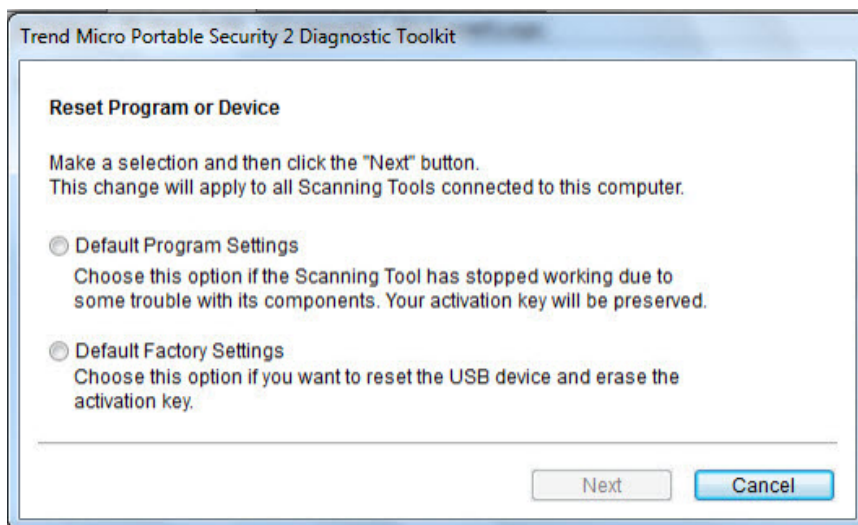
1. Plug-in the Trend Micro Portable Security 2 Scanning Tool to the computer.
2. Copy the SupportTool folder from the USB device into your local drive.
3. Double-click the TMPSSuprt.exe file .



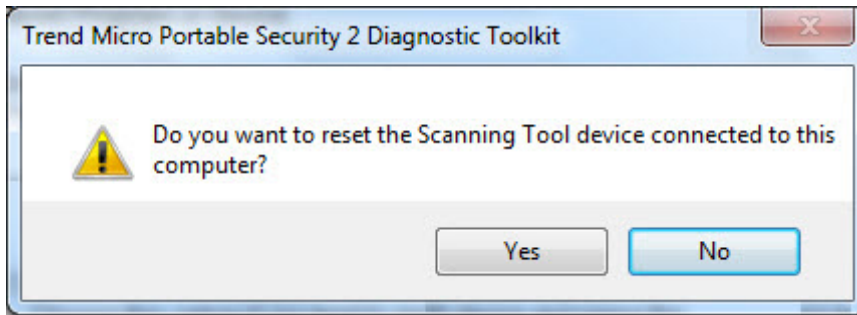
4. Go to the **More Tools** tab.



5. Click the **1. Reset Device** button.



6. Select **Default Program Settings** and click **Next**.



7. Confirm the reset.




Note

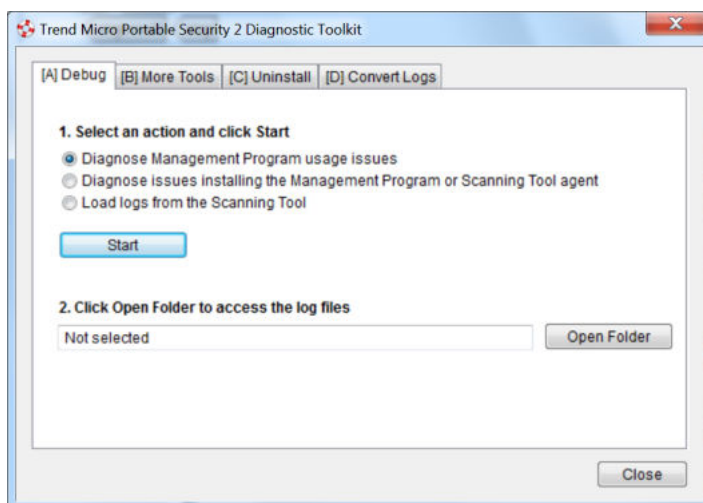
Do not unplug the Scanning Tool until the reset process has completed and a popup appears stating **You have successfully reset the device** appears.

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

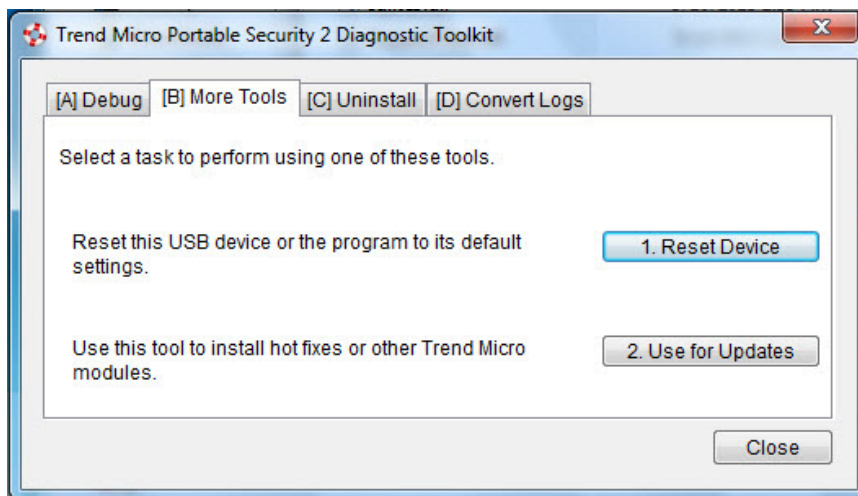
Resetting the Device

Procedure

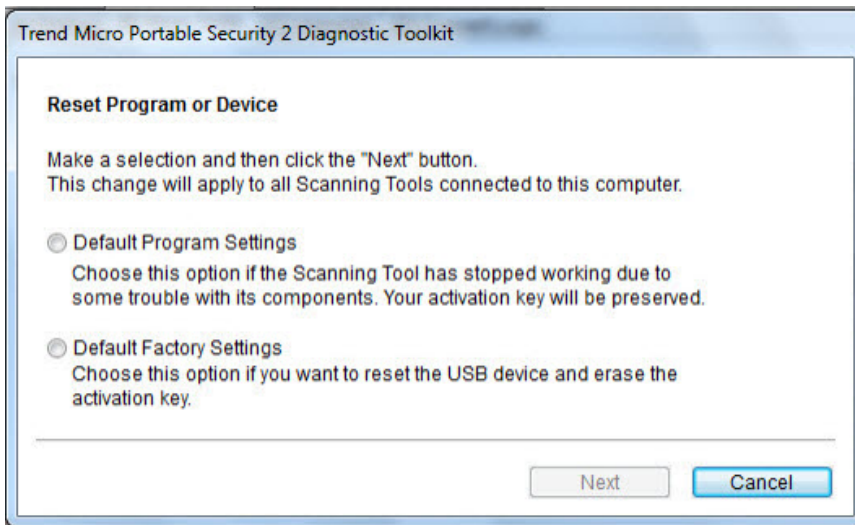
1. Plug-in the Trend Micro Portable Security 2 Scanning Tool to the computer.
2. Copy the SupportTool folder from the USB device into your local drive.
3. Double-click the TMPSSuprt.exe file .



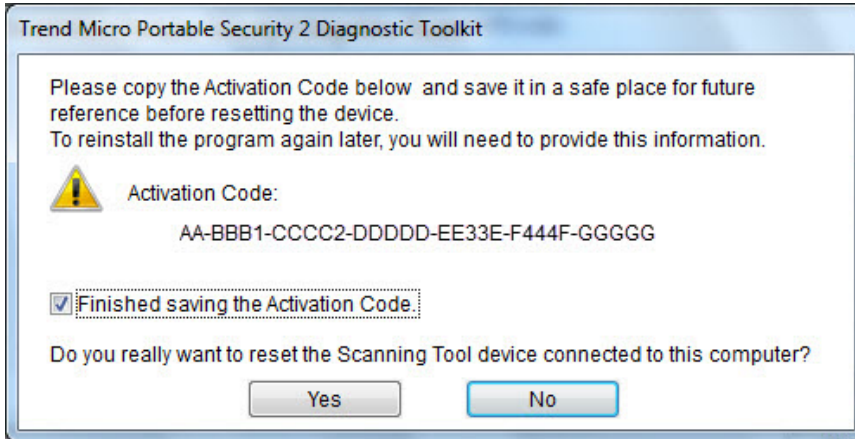
4. Go to the **More Tools** tab.



5. Click the **1. Reset Device** button.



6. Select **Default 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 popup appears stating **You have successfully reset the device** appears.

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

Support Updates

Use the Trend Micro Portable Security 2 Diagnostic Toolkit to apply hot fixes 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 not have 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 will provide the hot fix to an individual customer. Hot fixes use the `xxx.bin` format.

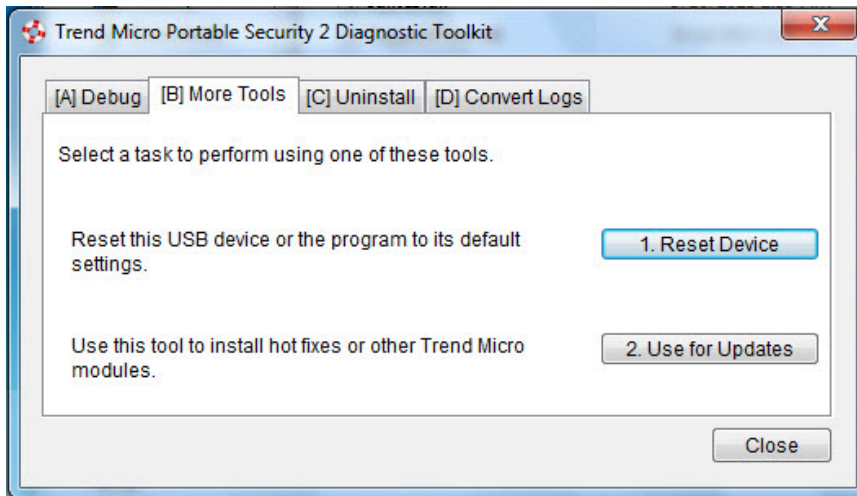
**WARNING!**

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

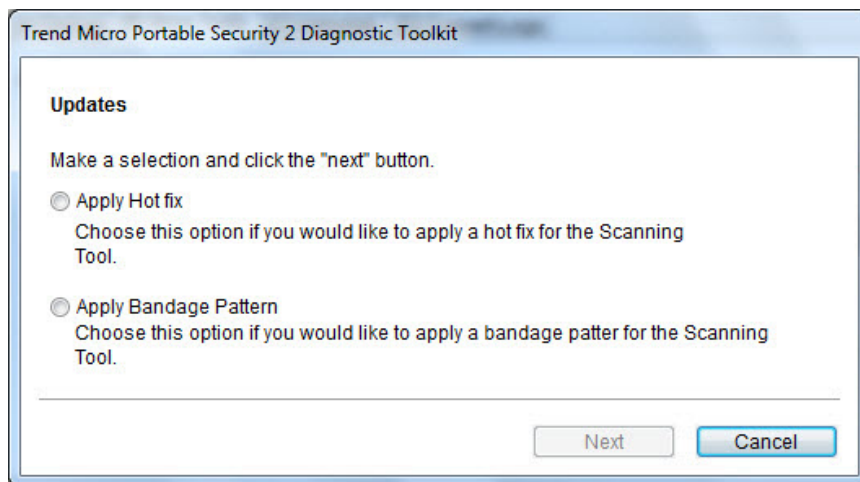
1. Copy the SupportTool folder from the USB device into your local drive.
2. Open the Trend Micro Portable Security 2 Diagnostic Toolkit console.
3. Go to the **More Tools** tab.

The **More Tools** tab opens.



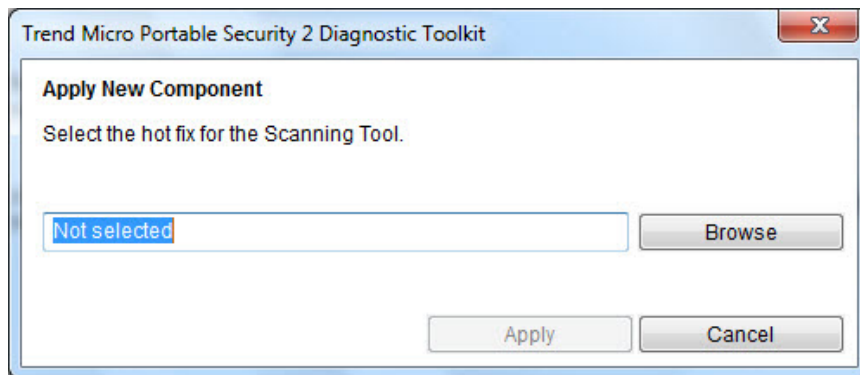
4. Click the **Use for Updates** button.

The **Updates** window opens.



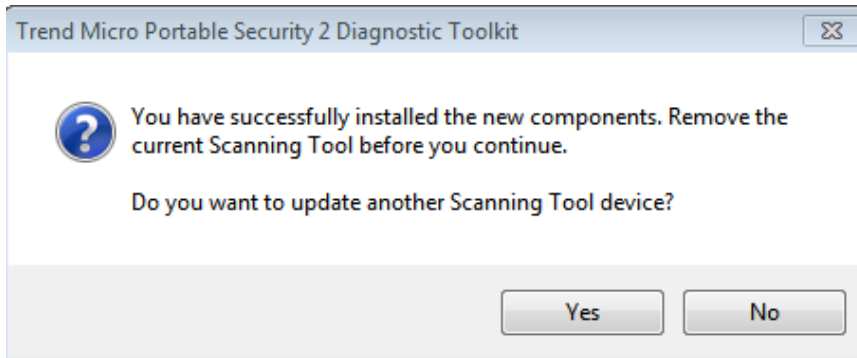
5. Select **Apply Hot fix** and click **Next**.

The **Apply New Components** window opens.



6. Select the hot fix file provided by Trend Micro.
7. Click **Apply**.

A confirmation window opens.



8. To update another Scanning Tool, click **Yes** and follow steps 6 to 8. To finish the update, select **No** and replug the device for the update to take effect.

Converting Logs

Trend Micro Portable Security 2 uses a different log format from previous releases of Trend Micro Portable Security. Previous releases used xml while Trend Micro Portable Security 2 uses the database format.

Use the Trend Micro Portable Security 2 Diagnostic Toolkit to convert xml logs to the database format log.

Procedure

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

The **Select Logs to Convert** window opens.

- Select the location of the older logs and click **Convert**.

Trend Micro Portable Security 2 saves the converted logs to the same location as the older logs.

Trend Micro Rescue Disk

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

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




Note

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

Rescue Disk supports the following file systems:

OPERATING SYSTEM	FILE SYSTEM
Windows	NTFS and FAT
Linux	EXT, EXT2, EXT3, EXT4 and XFS



Note
Rescue Disk runs on any Linux distribution installed on a supported file system.

To use the rescue disk, perform the following:

- Step 1: Preparation on page 5-26.*

- *Step 2: Using the Rescue Disk on page 5-28.*
- *Step 3: Viewing the Logs on page 5-31.*

Step 1: Preparation

Procedure

1. Insert the USB device into the computer.
2. Restart the computer.
3. When the computer 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.

BIOS Setup Utility	
Boot	Item Specific Help
Boot priority order: 1: -USB HDD TMPS DISK-(USB 2.0) 2: USB FDD: 3: ATAPI CD0: 4: USB CD: 5: ATA HDD0: 6: PCI LAN: 7: ATA HDD1: 8: Excluded from boot order: : ATA HDD2: : ATAPI CD1:	Use these keys to set the boot order that the BIOS will use to attempt to boot an OS: <F6> and <F5> moves the device up or down. <x> exclude or include the device to boot. <1> Loads default boot sequence. USB BIOS support must be enabled for USB boot.
F1 Help ↑ Select Item F3/ESC Exit	F5/F6 Change Values Enter Select ▶ Sub-Menu F9 Setup Defaults F10 Save and Exit

5. Exit the menu.

Trend Micro Rescue Disk should automatically open after restarting.



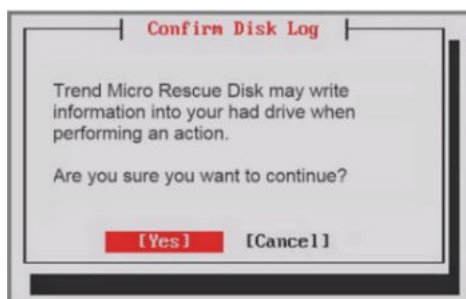
Step 2: Using the Rescue Disk

Procedure

1. After you have restarted the computer, Trend Micro Rescue Disk console will open automatically.



2. Press the **Enter** key or wait for a while. The **Confirm Disk Log** window appears.

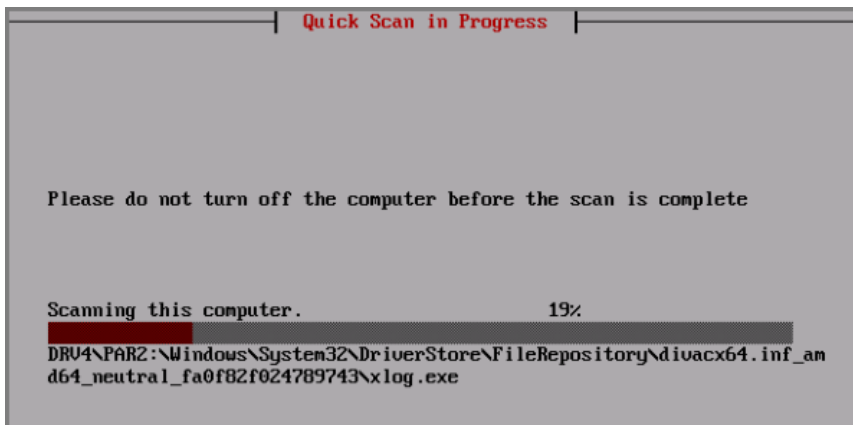


3. Select **Yes**. The **Choose Action** window appears.



4. Select **[1] Scan for Security Threats** and then select **[1] Quick Scan** or **[2] Full Scan**.

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



5. If any threats are detected and if you have configured the Rescue Disk to scan and quarantine objects and to inform users before the quarantine starts, you will be prompted with the message "Are you sure you want to resolve these objects?" Select **Yes** to remove threats.
6. After scan logs are saved to the Scanning Tool, you will be prompted to remove the Scanning Tool from the computer.
7. Press the **Enter** key to restart the computer.

8. To scan another computer, repeat *Step 1: Preparation on page 5-26* and *Step 2: Using the Rescue Disk on page 5-28* before moving on to view the logs.
-

Step 3: Viewing the Logs

Procedure

1. Transfer the collected logs from the Scanning Tool to the Management Program. Refer to *Transfer Logs from the Scanning Tool on page 3-46*.
2. Check the logs.

Rescue Disk gathers the following log information from the scan:

- State Date/Time
- End Date/Time
- Scanning Tool Name
- Scanning Tool ID
- Scanner Version
- Virus Scan Engine Version
- Virus Pattern Version
- IP Address
- MAC Address
- Scan Status
- Scan Results
- Scanned
- Infected
- Fixed

- Comment
-

Scanning Tool Agent

The Scanning Tool Agent is designed for automatic update, scanning, synchronization, and schedule update on a target computer when a Scanning Tool is detected. For details, refer to [Using the Scanning Tool Agent on page 4-40](#).

Chapter 6

Uninstallation

This chapter describes Trend Micro Portable Security 2™ uninstallation methods. There are several ways to remove Trend Micro Portable Security 2 from your computer:



Note

- You only need to remove the Management Program from the computer where you previously installed it. You do not need to do anything to the computers that you have scanned.
 - Make sure to unlock Trend Micro Safe Lock™ before uninstalling Trend Micro Portable Security 2.
-

Topics in this chapter:

- *Option A: From the Windows Start Menu on page 6-2*
- *Option B: From the Control Panel on page 6-3*
- *Option C: Use the Trend Micro Portable Security 2 Diagnostic Toolkit on page 6-4*

Option A: From the Windows Start Menu

Procedure

1. From the Windows Start Menu, select **All Programs > Trend Micro Portable Security 2**.

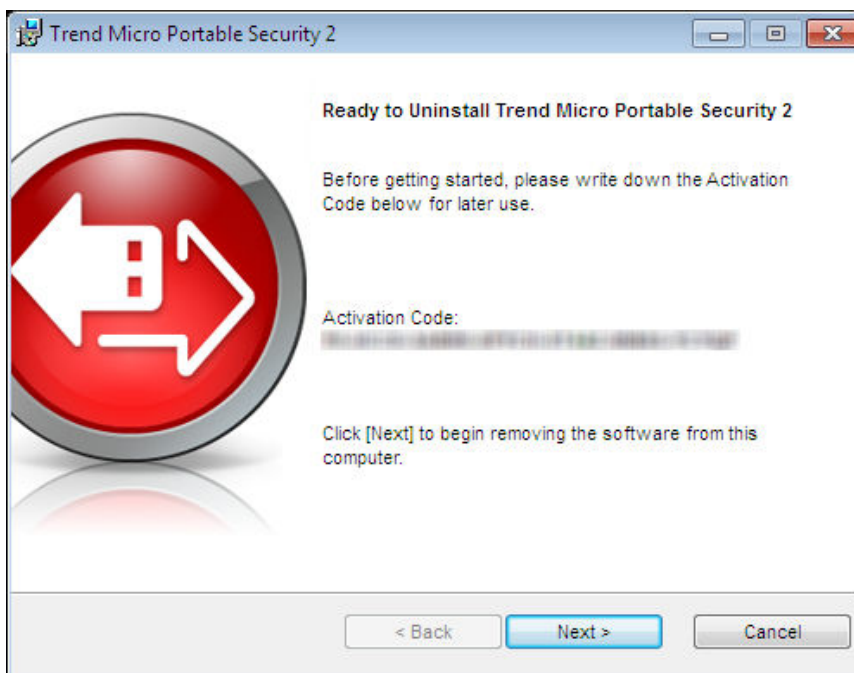


Note

Make sure the Scanning Tool is not plugged into the computer before continuing.

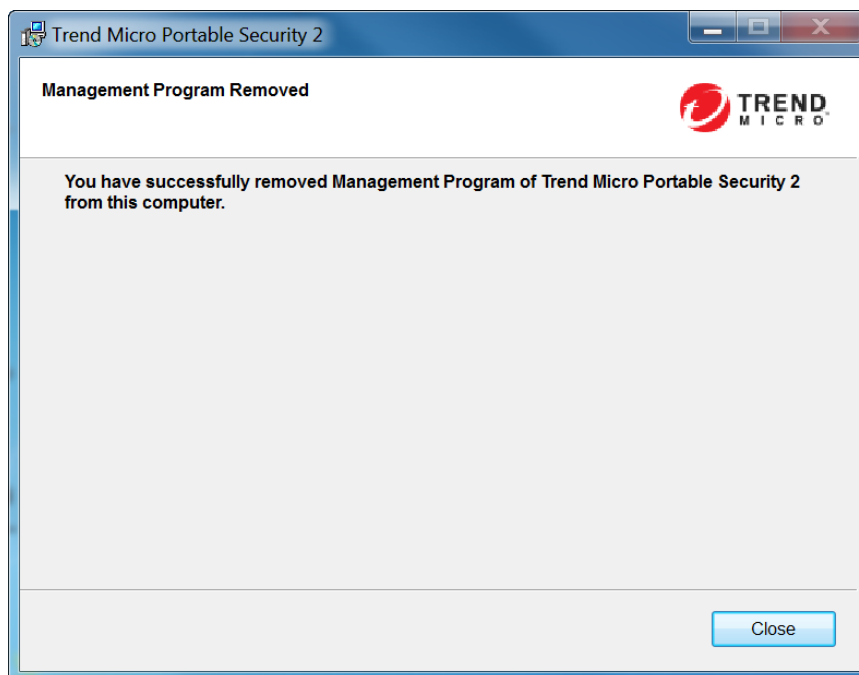
2. Select **Uninstall Trend Micro Portable Security 2**.

The Ready to Uninstall Trend Micro Portable Security 2 page opens.



3. Click **Next**.

The Program Uninstalled window opens.



4. Click **Close**.
5. Restart your computer.

Option B: From the Control Panel

Procedure

1. From the Windows Start Menu, go to the **Control Panel** and select **Add or Remove Programs** or **Program and Features**.



Note

Make sure the Scanning Tool is not plugged into the computer before continuing.

2. Double-click Trend Micro Portable Security 2 from the window that opens.

This should start the uninstallation process.

3. Click **Yes** when the confirmation window opens.
 4. Restart your computer.
-

Option C: Use the Trend Micro Portable Security 2 Diagnostic Toolkit

Use the Trend Micro Portable Security 2 Diagnostic Toolkit to uninstall the program only if you are unable to uninstall the program using the control panel. This tool will do the following:

- Stop and delete the Management Program service.
- Clean up the Management Program registry keys.
- Clean up the registry keys added by MSI for installation and uninstallation.
- Delete all modules and ActiveUpdate temp files.
- Delete imported scan and debug logs.

Procedure

1. Open the Trend Micro Portable Security 2 Diagnostic Toolkit console.
2. Go to the **Uninstall** tab.



Note

Make sure there are no Scanning Tool devices plugged in before continuing.

3. Click the **1. Uninstall** button.

If the Management Program is installed, the activation code window opens.

4. Copy and save the activation code in a separate location.
 5. Enable the **Finished saving the activation code** option.
 6. Click **Uninstall**.
 7. Confirm uninstallation.
 8. Click **Yes** and restart the computer to finish uninstallation.
-

Chapter 7

Getting Help

This chapter describes troubleshooting issues that may arise and how to contact support.

Topics in this chapter:

- *Frequently Asked Questions (FAQs) on page 7-2*
- *Data Transmissions to Trend Micro on page 7-4*
- *Export Controls on page 7-5*
- *Multi-year Contracts on page 7-6*

Frequently Asked Questions (FAQs)

Where can I find more information about a threat found?

Search the Trend Micro Threat Encyclopedia for the name of a threat shown in the imported log data on this website:

[Trend Micro Threat Encyclopedia](#)

Why was the log data not saved?

- Do not remove the Scanning Tool from a computer until the window that displays after you click **Close** has disappeared.
- When removing the Scanning Tool from a computer, ensure that you remove the tool safely or else the data may become corrupted.

Follow the Removing the Scanning Tool instructions on *Removing the Scanning Tool on page 4-32*.

Additionally, you can go to the Trend Micro website, which provides answers to questions commonly asked about the software, and covers many useful topics.

[Knowledge Base](#)

You can search the website using the product name or keywords to find information not included in the manual or Readme file. Trend Micro continually adds and updates the information available online.

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 a product or service from the appropriate drop-down list and specify any other related information.

The **Technical Support** product page appears.

3. Use the **Search Support** box to search for available solutions.
4. If no solution is found, click **Submit a Support Case** from the left navigation and add any relevant details, or submit a support case here:

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

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

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 hardware connected to the endpoint
- Amount of memory and free hard disk space
- Operating system and service pack version
- Endpoint client version
- Serial number or activation code
- Detailed description of install environment
- Exact text of any error message received.

Threat Encyclopedia

Most malware today consists of "blended threats" - two or more technologies combined 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://www.trendmicro.com/vinfo> 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.

Data Transmissions to Trend Micro

About Web Reputation Service, PhishTrap, Harmful Site/URL Filtering, and TrendProtect:

1. Trend Micro uses data received from you to check the security of the pages that you tried to access. Certain information (such as your domain and IP address) about the websites that you have accessed will be encrypted and sent anonymously to Trend Micro for analysis. Trend Micro uses this information to verify the safety of websites and improve the filtering functions.
2. Enabling these features before opening a website may trigger the following results:
 - a. The server providing the page may append information that you have entered to the website as parameters. That means the information you entered (such as your ID, password, etc.) could be sent to Trend Micro as part of the data about the website. Trend Micro uses the data received to check the security of the page you tried to access.
 - b. To check the security of any page that you try to open, Trend Micro examines the specifications of the Web server providing it. Trend Micro also follows a similar process based on URL content parameters when checking a request to open a page.
 - The Trend Micro File Reputation Service sends hash values to Trend Micro to verify the safety of files. Neither the file itself nor any of its content is sent.

- The Software Safety Evaluation Service sends programs or program information to Trend Micro for risk assessment.
- The Virus Tracking / Trendcare Program sends information about any security threats found (including the threat name, number found, region, and the URL of the source website, if applicable) to Trend Micro for statistical purposes.
- The Trend Micro Anti-Spam Toolbar sends the subject line of spam messages to Trend Micro to help improve the accuracy of the spam mail identification system. Trend Micro may disclose the body of the spam mail to government organizations to reduce the quantity of spam mail or the harm caused by it.
- The Email Reputation Service sends information about a sender's mail server to Trend Micro for the purpose of identifying spam messages.
- If a program behaves suspiciously, the Trend Micro Smart Feedback system sends the file checksum, the URL accessed, the size and path of the file, and the name of the executable file to Trend Micro for the purpose of collecting, analyzing, and strengthening protection capabilities. This information is used to determine the safety of the file or program involved. While some personal or confidential information could inadvertently be contained within these files, Trend Micro does not collect or use such information in any way.

For more details on how Trend Micro handles information collected from you, please refer to this website:

<http://www.trendmicro.com/us/about-us/legal-policies/privacy-statement/index.html>

The "Web Reputation Service," "TrendProtect," and other Trend Micro filtering software checks the security of a given website according to proprietary standards set by Trend Micro. Whether or not you can then access a given website may not be entirely up to you after a judgment has been made.

Export Controls

This product and its technology ("Software") may be subject to export controls, the Foreign Exchange and Foreign Trade Act, Export Trade Control Order, Foreign

Exchange Order, and ministerial ordinance or U.S. Export Administration Regulations. It may also be designated an "export control item" by the trade laws of other countries. You may not export or re-export the Software to a company, resident, citizen, or embargoed person or company of any embargoed country or any country with a trade sanction without the appropriate U.S. or foreign government licenses. Nations subject to U.S. embargo include Cuba, Iran, North Korea, Sudan, and Syria as of May 2010. Further information about embargoed countries is available by searching the following websites. You are responsible for any violation of such export control laws related to the Software. You should take appropriate measures to prevent violations.

<http://www.treas.gov/offices/enforcement/ofac/>

<http://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear>

By using the Software, you confirm that you are not a resident or citizen of any country currently embargoed by the U.S., and that you are not otherwise prohibited under the export laws from receiving it. You also agree not to use this product in the development, design, manufacture, or production of nuclear weapons, chemical weapons, biological weapons, or missiles intended as weapons of mass destruction.

Multi-year Contracts

- Even if you pay for multi-year contracts (by paying more than one year of support fees in advance), Trend Micro sets the period during which support for a product shall be provided without regard to your contract term.
- Please note that multi-year contracts do not guarantee product support during the applicable contract period, nor do they guarantee upgrades if the product support period has concluded.

Chapter 8

Technical Support

Learn about the following topics:

- *Troubleshooting Resources on page 8-2*
- *Contacting Trend Micro on page 8-3*
- *Sending Suspicious Content to Trend Micro on page 8-4*
- *Other Resources on page 8-5*

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, 8-6

S

support

 knowledge base, 7-2

 resolve issues faster, 7-3, 8-4



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: TPEM28077/171019