TREND MICRO

TREND MICRO
Portable Security 2™
User's Guide

Endpoint Security

Document Part No.: TPEM26430/140512

Release Date: July 2014

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

Chapter 2: Setting Up

Chapter 3: Using the Management Program

Chapter 4: Using the Scanning Tool

Chapter 5: Additional Tools

Chapter 6: Uninstallation

Chapter 7: Getting Help

Chapter 1

Introduction

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

Topics in this chapter:

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 *Management Program on page 1-2*.
- **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. Refer to *Scanning Tool (USB Device) on page 1-4*.

Management Program

The Management Program can configure scan settings for and import log data from multiple Scanning Tools. To download pattern file and scan engine updates, you must install the Management Program on a computer with access to the Internet.

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

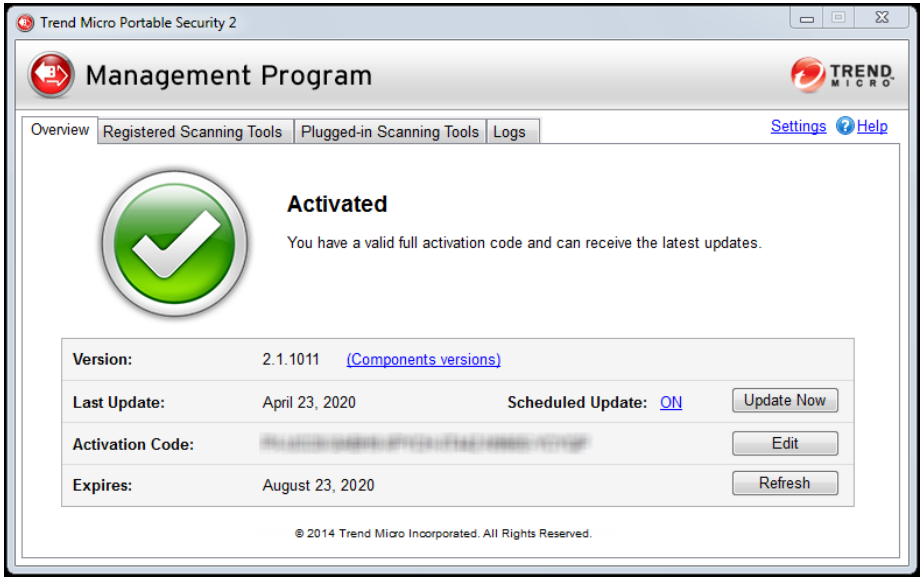


FIGURE 1-1. Main screen of the Management Program

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.

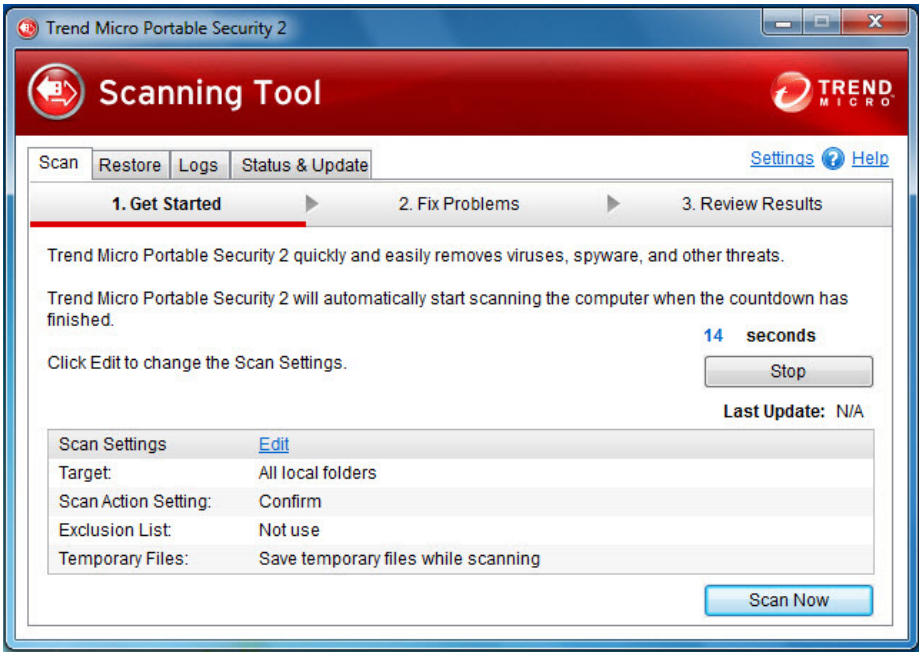


FIGURE 1-2. The Scanning Tool screen

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 1-5* 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 on page 5-9*.

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

	MANAGEMENT PROGRAM CONTROL	STANDALONE SCANNING TOOL
Updates	Downloads specified components from the Management Program.	Downloads all components from the Trend Micro ActiveUpdate server from any computer with an Internet connection.
Scan settings	Same as the Management Program or configured from the Scanning Tool.	Change the scan settings directly from the Scanning Tool console.
Logs	• Exported to the Management Program • Imported from another Scanning Tool	Imported from or exported to a computer.

Note

You can only use the Scanning Tool on computers without the Management Program. 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, refer to *Scan Settings (Advanced) on page 3-18*.

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

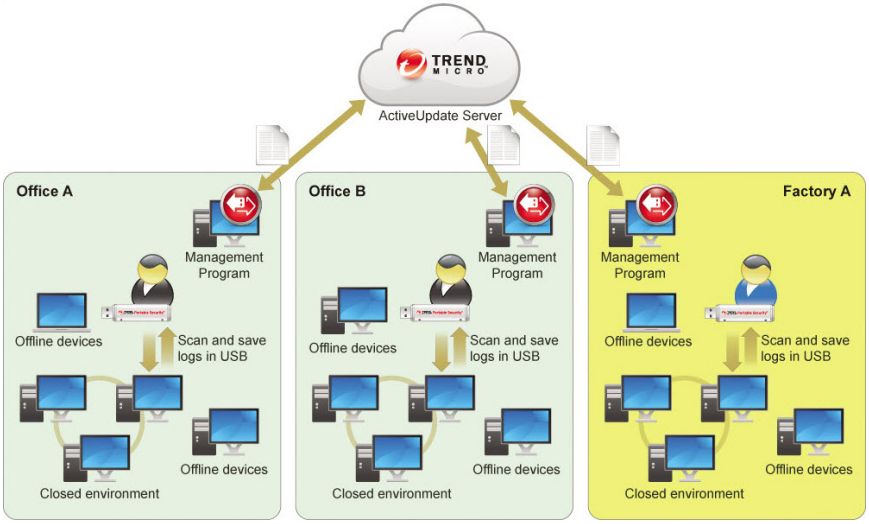
scanning tool devices can get the updates and scan settings from the Management Program and you can also upload all the logs from each device.

In this mode, there are two (2) 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.

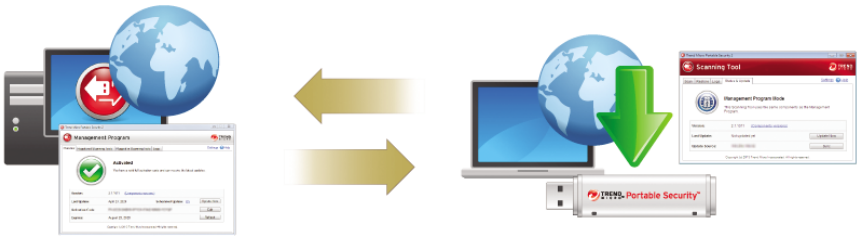


- Remote connection

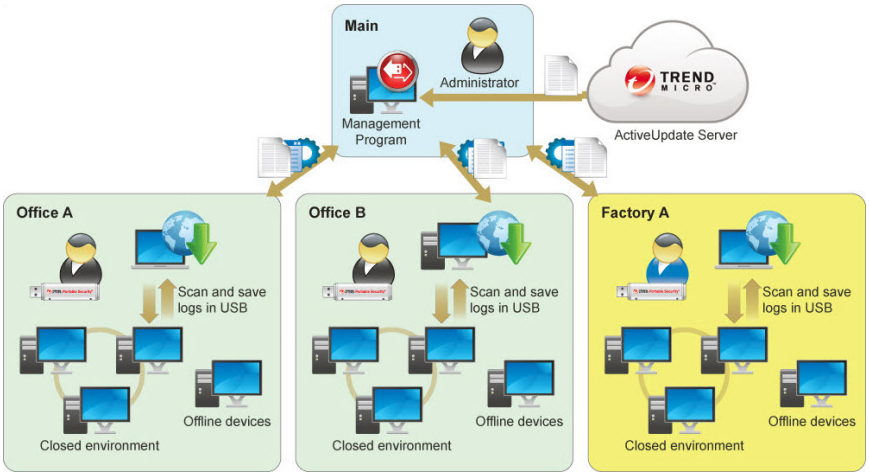
  You can plug in the device from any computer with an Internet connection and then connect to the Management Program online to get the updates, settings, or to transfer logs.

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

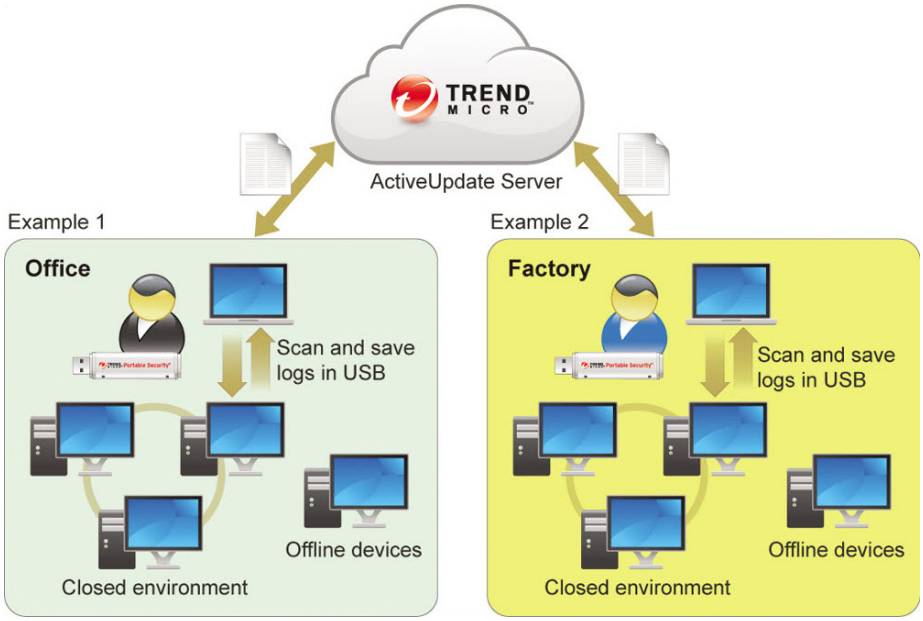
The Standalone Scanning Tool mode uses the Scanning Tool as a standalone device, wherein you can use any computer that has Internet connection to update the components, change scan settings, or check the logs.

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

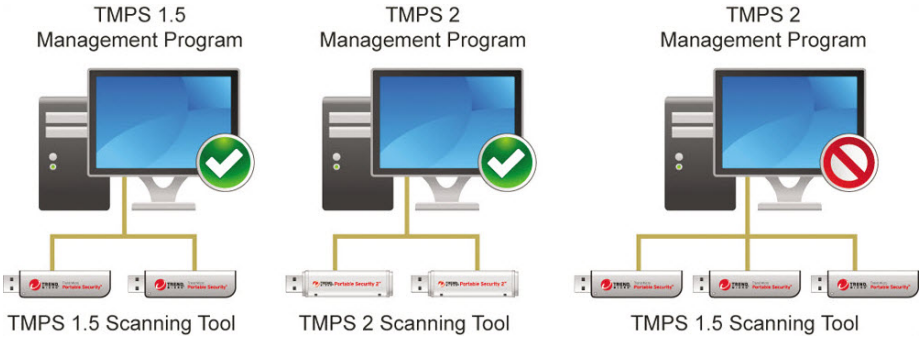
Trend Micro recommends regularly updating the components before scanning any device to make sure that the latest threats can be fixed and quarantined.

Here are some sample scenarios.



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

This chapter describes Trend Micro Portable Security 2™ installation, upgrade, and activation procedures.

Topics in this chapter:

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 to the Management Program locally or remotely.

Note

You must install the Management Program on a computer with access to the Internet.

Procedure

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

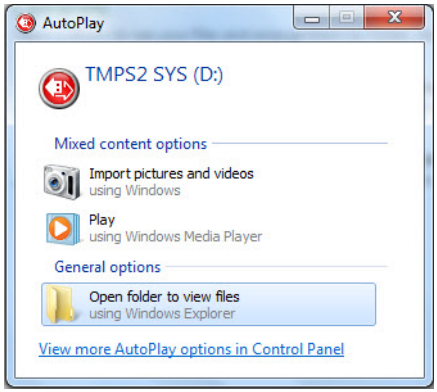
   Note

   Make sure you have Administrator privileges on this computer.

   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**.



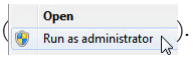
Tip

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 `Setup.exe` file (

).

Note

For some operating systems, you have to make sure you right-click the file and select **Run as administrator** (

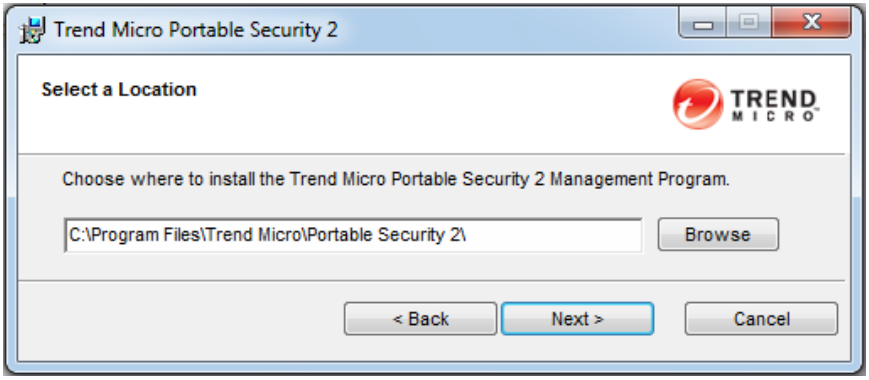
).

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

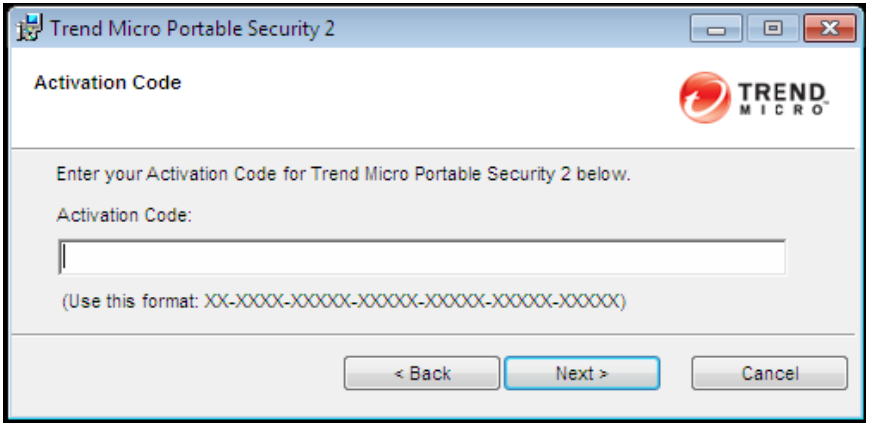
5. When the **Select Location** window opens, you can select a different folder, or click **Next**.

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**.



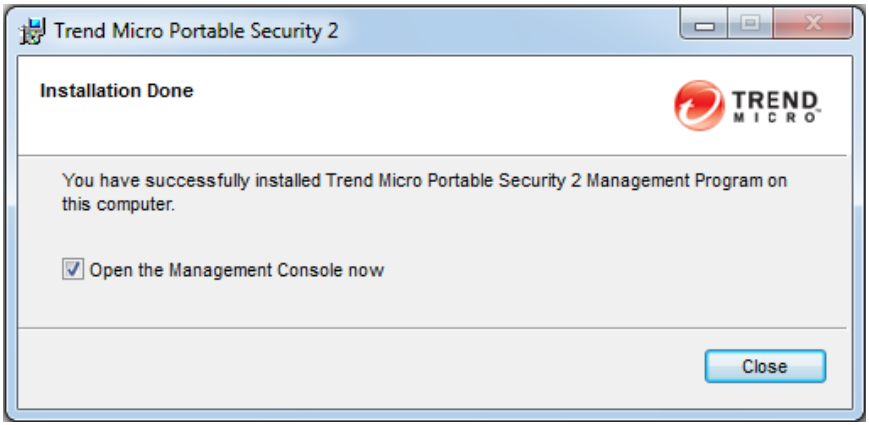
7. When the **Management Port and Password** window appears, specify the port number and the password twice.

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 5-12*.

Activation Status

When looking at the **Status and Update** tab of the scanning tool console, or the **Overview** tab of the Management Program, different messages will 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.
	• 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 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.

Note

To activate a standalone device, refer to *Activating a Standalone Tool on page 2-9*.

Procedure

- Option 1: Simple Activation

  1. *Install the Management Program on page 2-2*.

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.

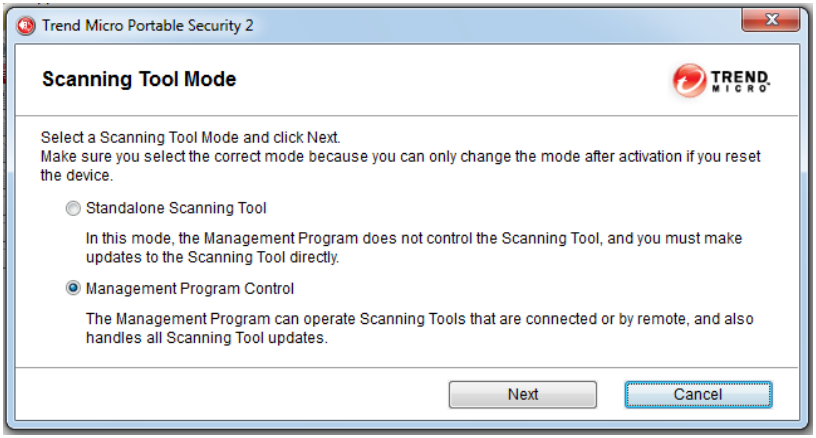
- Option 2: Alternative Activation Procedure

1. Plug-in the new Scanning Tool or any Scanning Tool that has not yet been activated on a computer without the Management Program.

Note

If there is a firewall between the Management Program and the Scanning Tool, accept and give permission to the `C:\Program Files\Trend Micro \Portable Security 2\Sfsrvcom.exe` process to continue.

The **Scanning Tool Mode** screen opens.

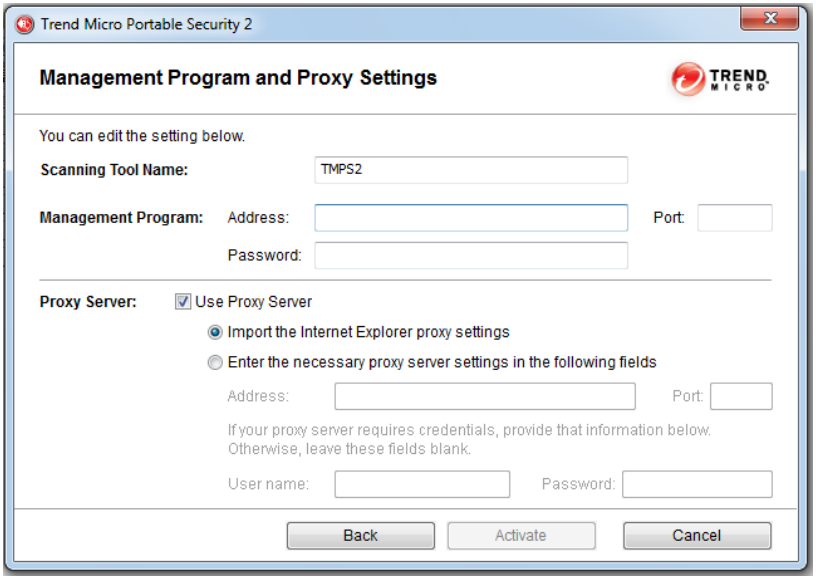


Note

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.



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 Tool

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

Note

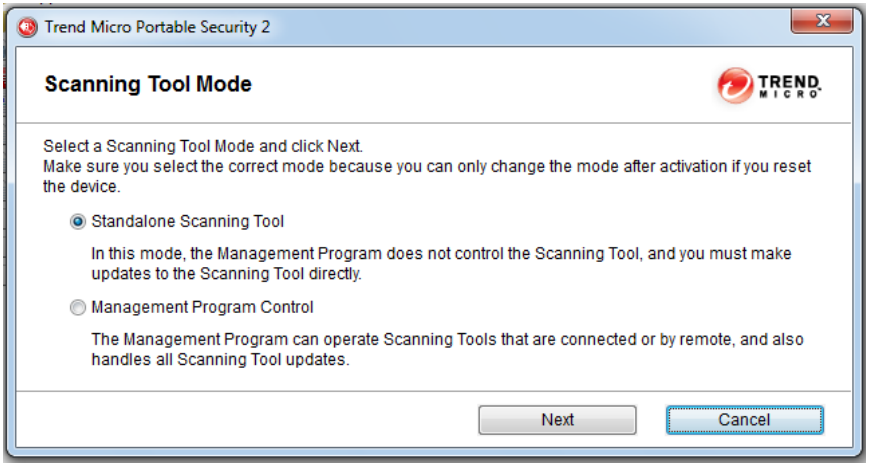
To activate a managed device, refer to *Activating Managed Devices on page 2-7*

Procedure

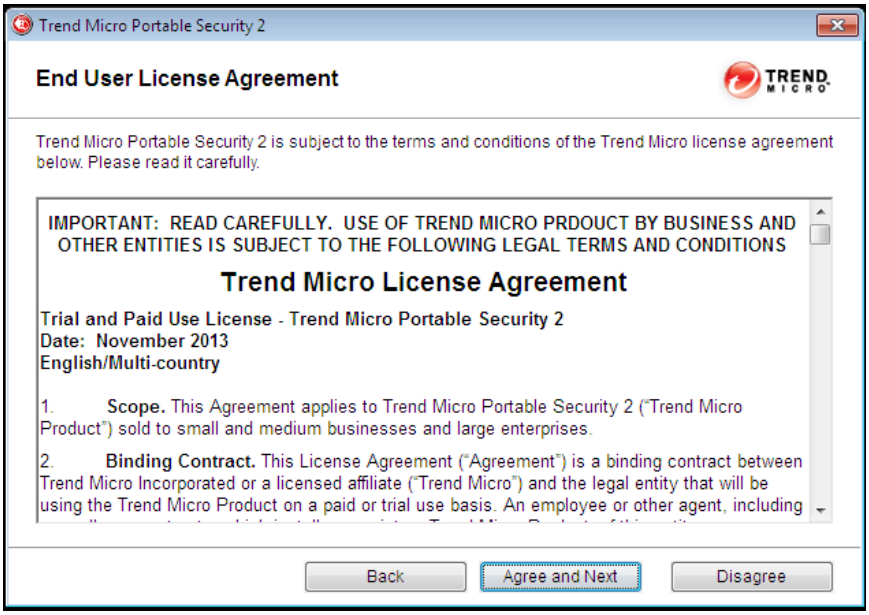
1. Plug-in the new Scanning Tool or any Scanning Tool that has not yet been activated to a computer with an Internet connection. Trend Micro Portable Security 2 will automatically open.

Note

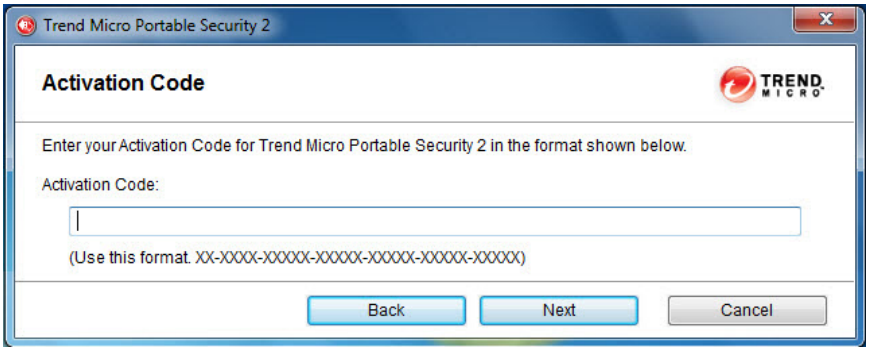
If Trend Micro Portable Security 2 does not open, your security software or computer may have blocked the autorun process. Open Windows Explorer and double-click `Launcher.exe` from the `TMPS2_SYS` partition to start the program.



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



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



4. Specify your activation code and click **Next**.

5. Open the **Status & Update** tab of the Scanning Tool console and click **Update Now** to start downloading the latest components.

Upgrades

Trend Micro will releases updates to the Trend Micro Portable Security 2 Management Program 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*.

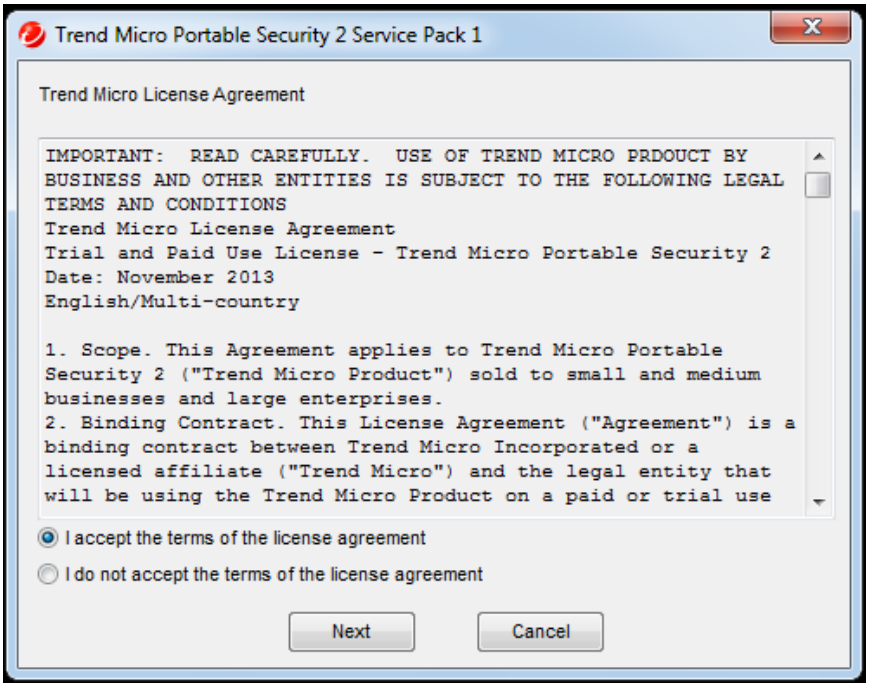
Upgrading the Management Program

Note

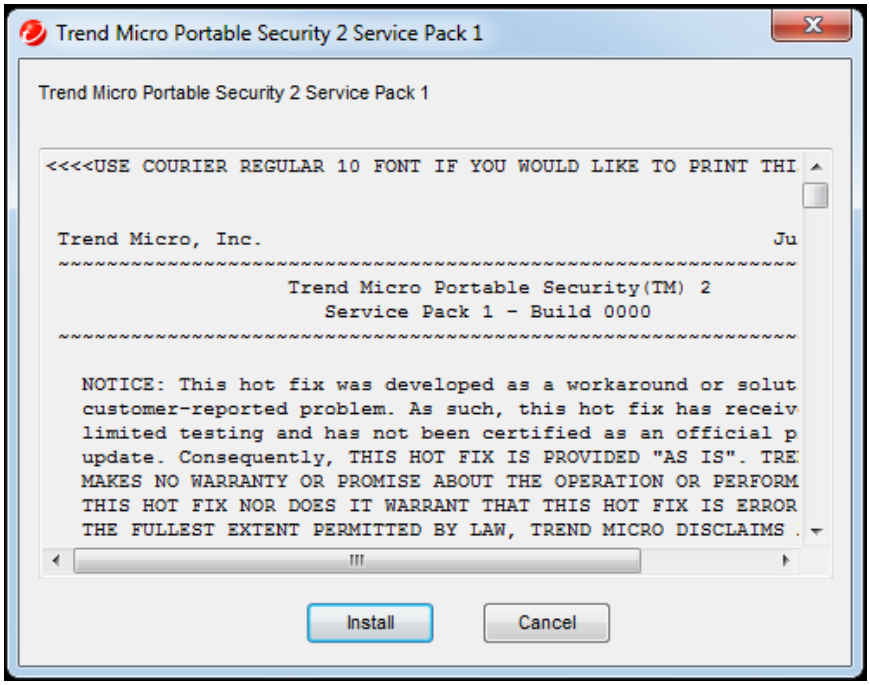
Trend Micro Portable Security 2 does not support upgrades from Trend Micro Portable Security 1.5. For more information, refer to *Trend Micro Portable Security 1.5 and Older Versions on page 1-12*.

Procedure

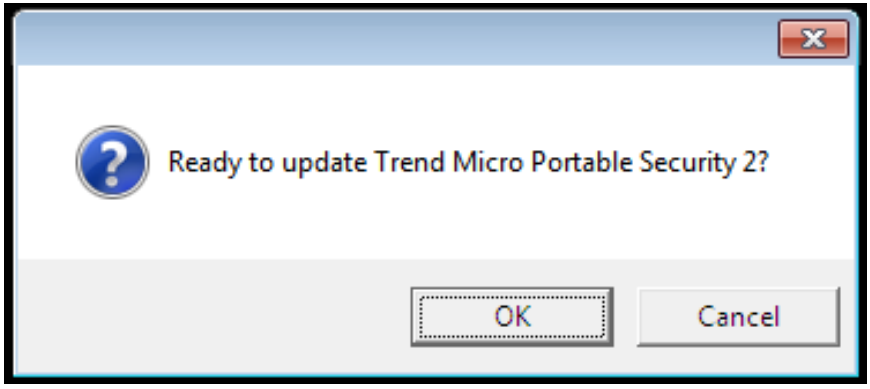
1. Download and double-click the setup package. The **License Agreement** page appears.



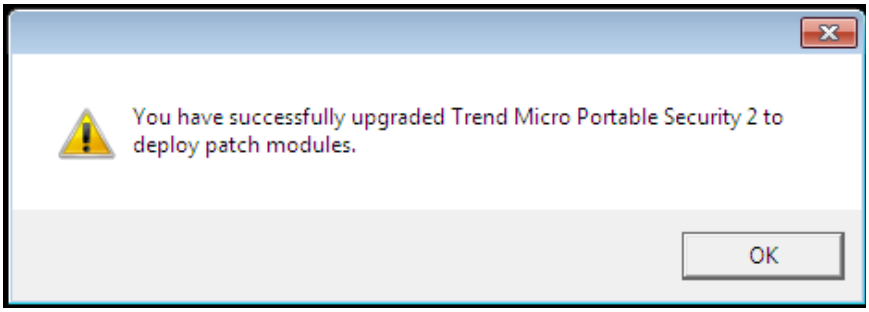
2. Read the Trend Micro License Agreement and select **I accept the terms of the license agreement** if you agree. Otherwise, click **Cancel**. Click **Next**. The Trend Micro Portable Security 1 Service Pack 1 readme appears.



3. Click **Install**. The system will start to check your system. A confirmation popup will appear.



4. Click **OK**. A confirmation popup will appear.



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

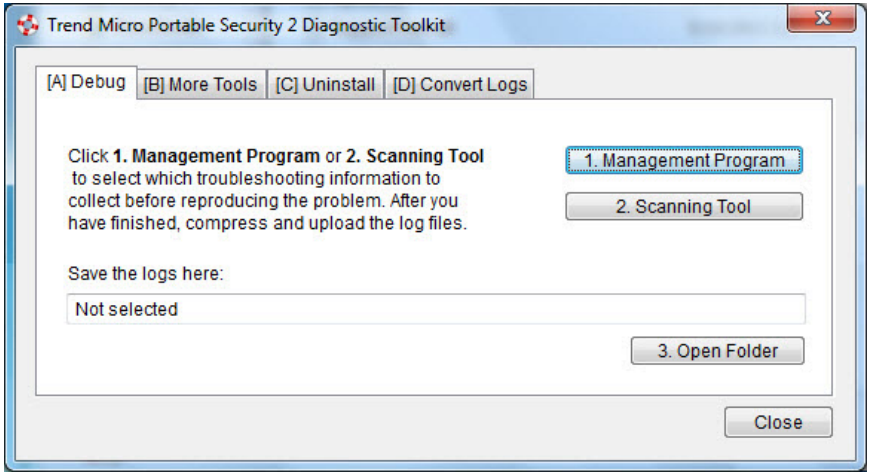
1. Close the Scanning Tool console if it is open.
2. Log on to the computer using an account with administrator privileges and connect the Scanning Tool.
3. Download the Trend Micro Portable Security 2 service pack.
4. Extract the contents of the service pack to a local folder on the computer where you have connected the Scanning Tool.
5. Open the Trend Micro Portable Security 2 Diagnostic Toolkit console.

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

   For the Scanning Tool:

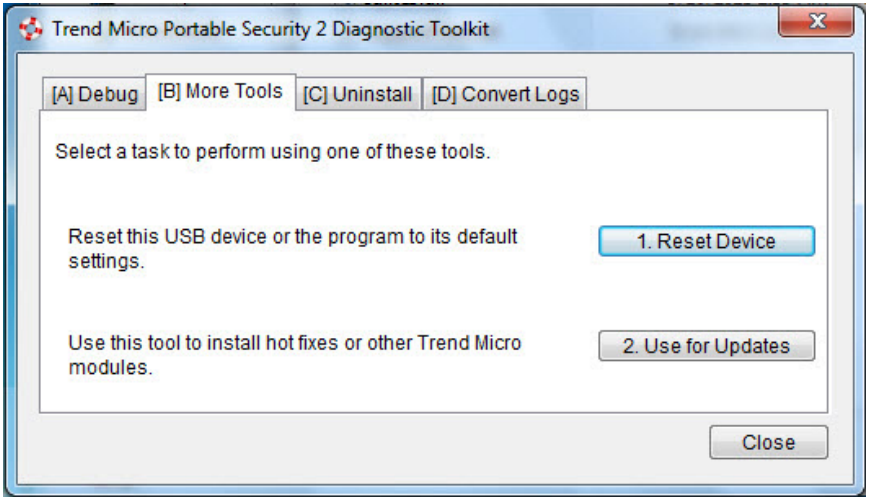
- Copy the `SupportTool` folder from the USB device into your local drive.
- Double-click the `TMPSSuprt.exe` file ().

The Trend Micro Portable Security 2 Diagnostic Toolkit console opens.



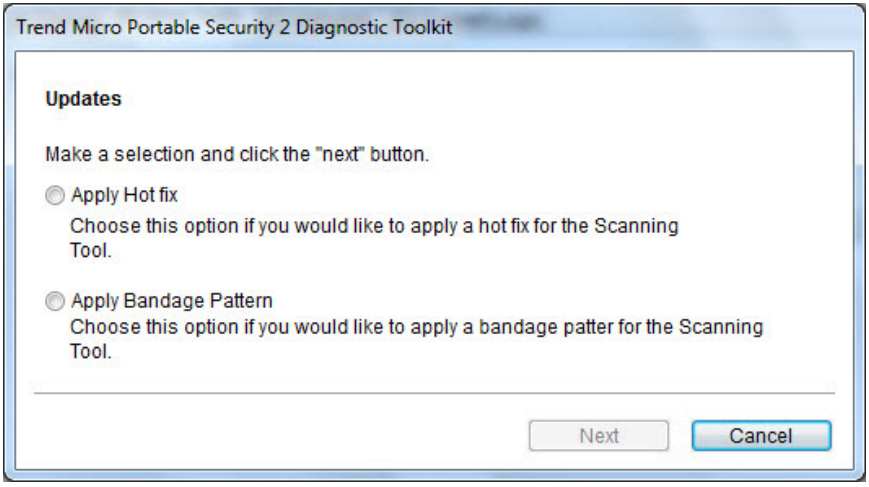
6. Go to the **More Tools** tab.

The **More Tools** tab opens.



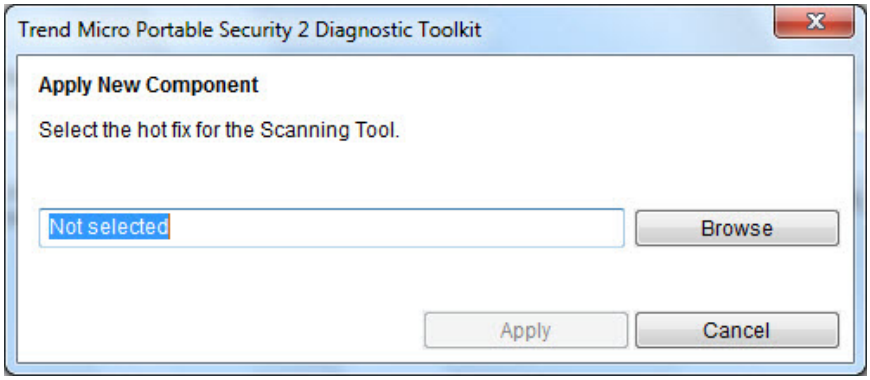
7. Click the **Use for Updates** button.

   The **Updates** window opens.



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

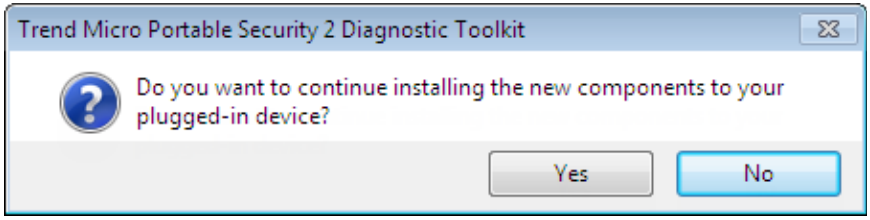
   The **Apply New Components** window opens.



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

10. Click **Apply**.

    A confirmation window opens.



11. Click **Yes**.

    The **Apply to Next Device** window appears.

12. Click **Done**.

Chapter 3

Using the Management Program

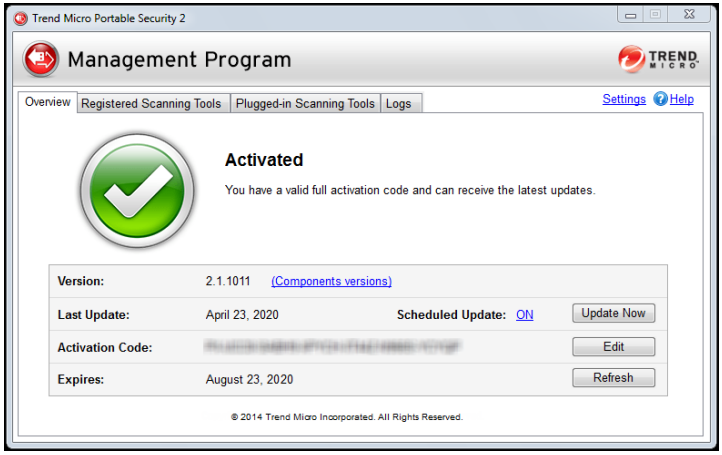
This chapter describes how to use and configure the Trend Micro Portable Security 2™ Management Program.

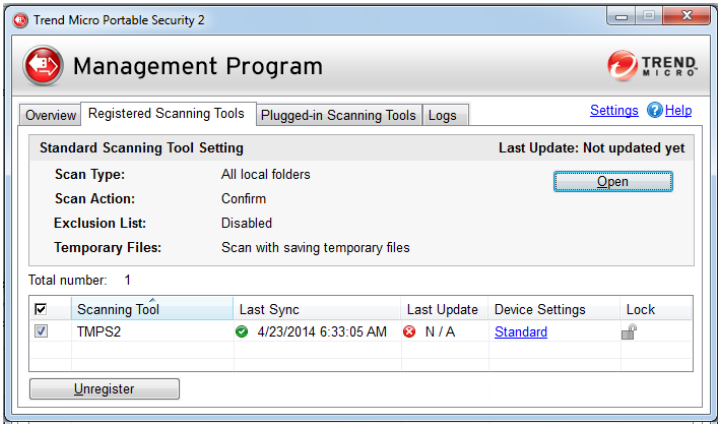
Topics in this chapter:

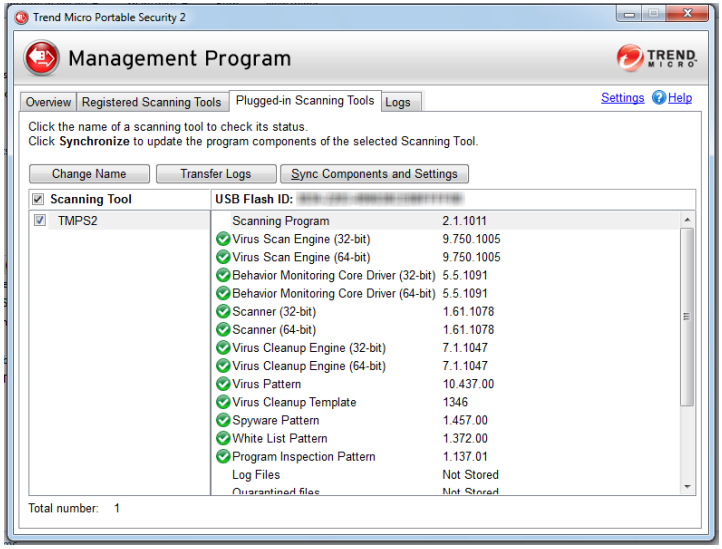
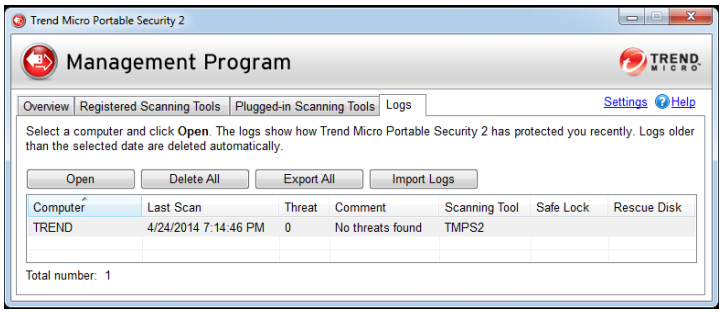
Understanding the Management Program Console

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

TABLE 3-1. How to use the console

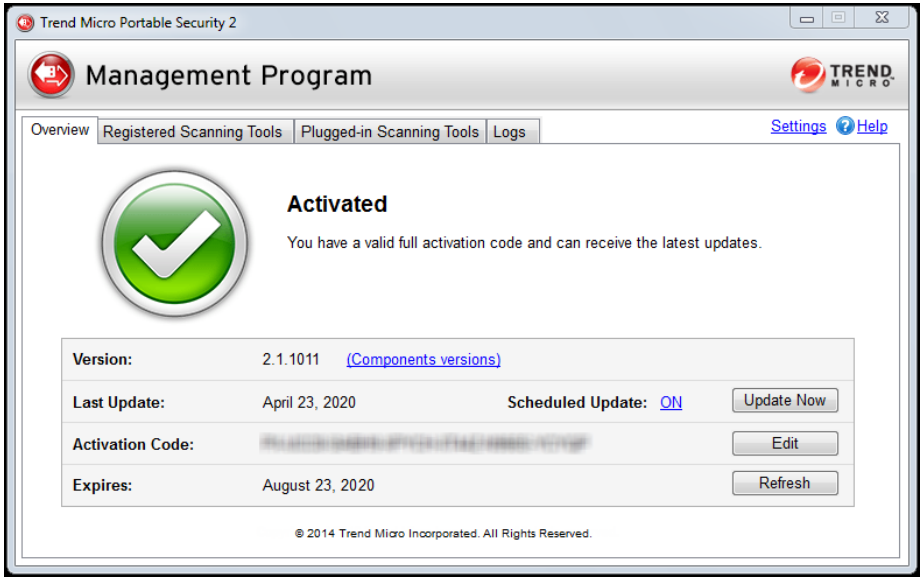
TAB OR BUTTON	DESCRIPTION
Settings	Click this link to check or change the Management Program settings. Refer to *Management Program settings on page 3-47*.
Help	Click this link to open the help file and to find more information about how to use this console.
Overview tab	 Check the status of the components and perform an update, if needed. Refer to *Overview Tab on page 3-5*.

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

Tab or Button	Description
Plugged-in Scanning Tools tab	 Check the status of the Scanning Tool devices that are currently plugged into the Management Program computer. Refer to *Plugged-in Scanning Tools on page 3-7*.
Logs tab	 Check the results of earlier scans performed by the Scanning Tool. Refer to *Logs Tab on page 3-8*

Overview Tab

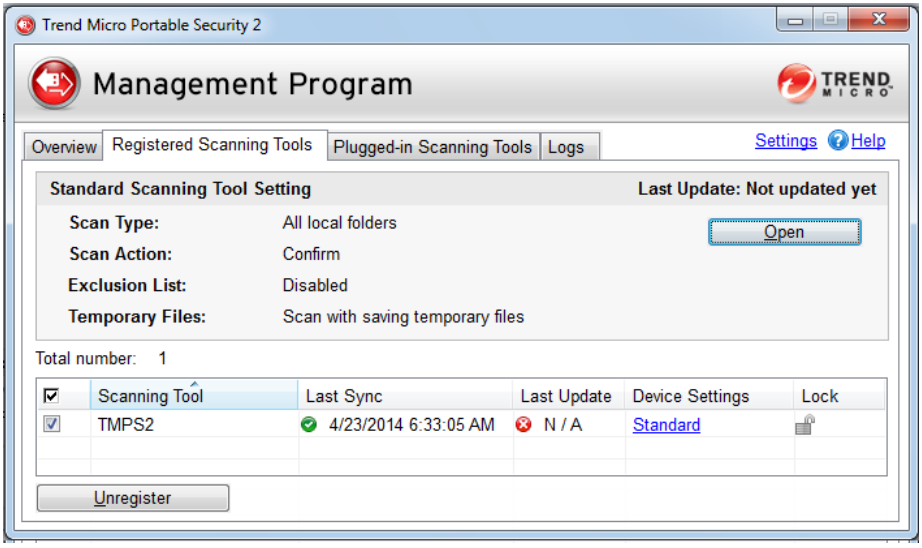
The Overview tab shows the Management Program status and enables changes to program settings.



- **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 *Update Settings on page 3-26*.
- **Update Now**: Click this button to manually start updating the components.
- **Edit**: Click this button to change or update the activation code. Refer to *Changing the Activation Code on page 3-44*.
- **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.

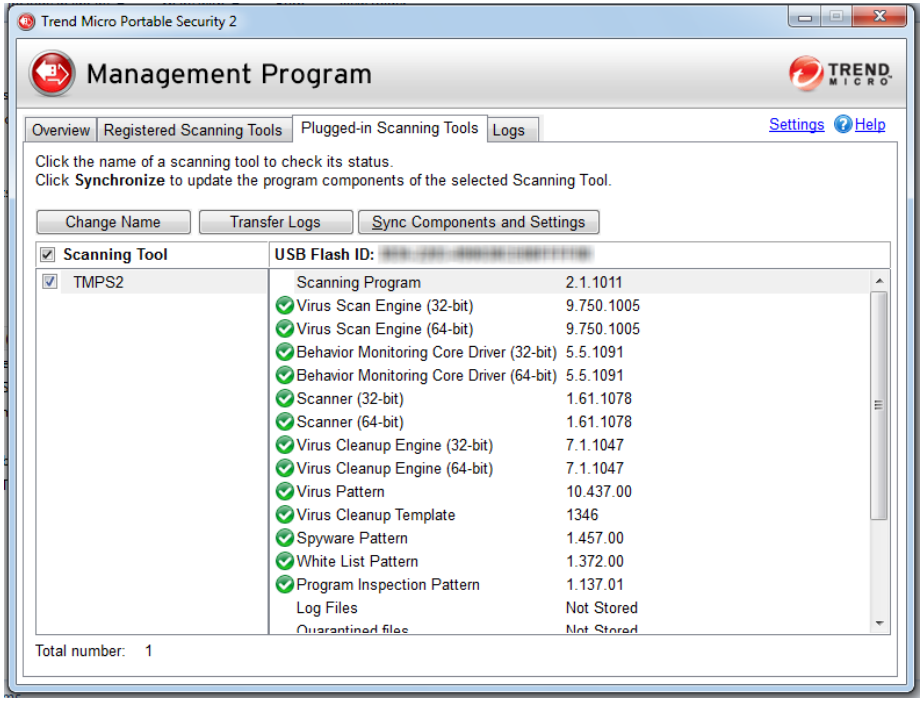


- **Open**: Click this link to open the standard scan setting for all devices registered to this device.
- **Standard/Custom**: This link under Device Settings shows whether the device uses the standard scan setting or if the scan setting for this device is specific to this device.
- **Lock/Unlock**: 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.

Plugged-in Scanning Tools

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

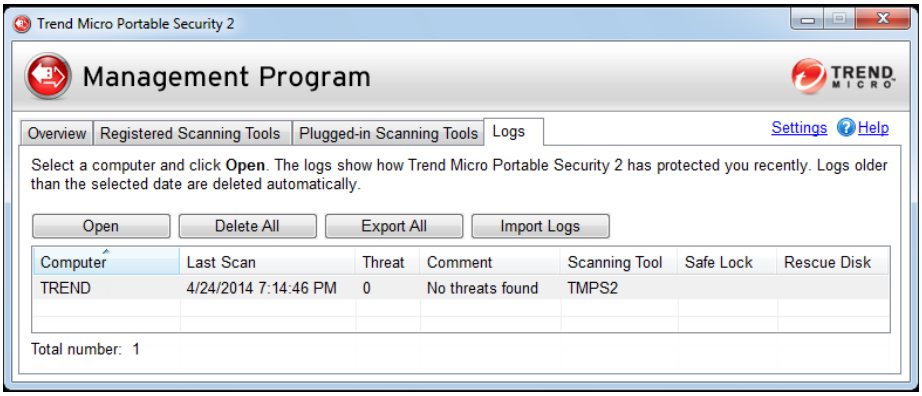


- **Change Name**: Click this button to change the name of the Scanning Tool. Refer to *Changing the Name of the Scanning Tool on page 3-22*.

- **Transfer Logs**: Click this button to transfer logs from the Scanning Tool device to the Management Program. Refer to *Transferring Logs from the Scanning Tool on page 3-40*.
- **Sync Components and Settings**: Click this button to download components and settings from the Management Program to the Scanning Tool.

Logs Tab

Check the results of earlier scans performed by the Scanning Tool.



- **Open**: Click this button to open the scan result page and shows more detailed information. Refer to *Viewing the Logs on page 3-31*.
- **Delete All**: Click this button to delete all log entries.

> **Note**
>
> Trend Micro recommends exporting logs before deleting them.

- **Export All**: Click this button to export all the logs into database or csv format. Refer to *Exporting Logs on page 3-36*.

- **Import Logs**: Click this button to import database format logs. *Importing Logs on page 3-35*.

Scan Settings

Change the scan settings by clicking **Open** at the **Standard Scanning Tool Setting** section of the **Registered Scanning Tools** tab of the Management Program or Edit from the **Scan** tab of the Scanning Tool console.

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:

Note

Whatever option you chose, after making the changes to the Management Program scan settings, the user still has to synchronize the Scanning Tool settings to the Management Program to apply the changes.

- **Standard**: The Scanning Tool uses the Management Program scan settings for registered devices.

  Note

  You will not be able to open the **Advanced** and **Others** tab.

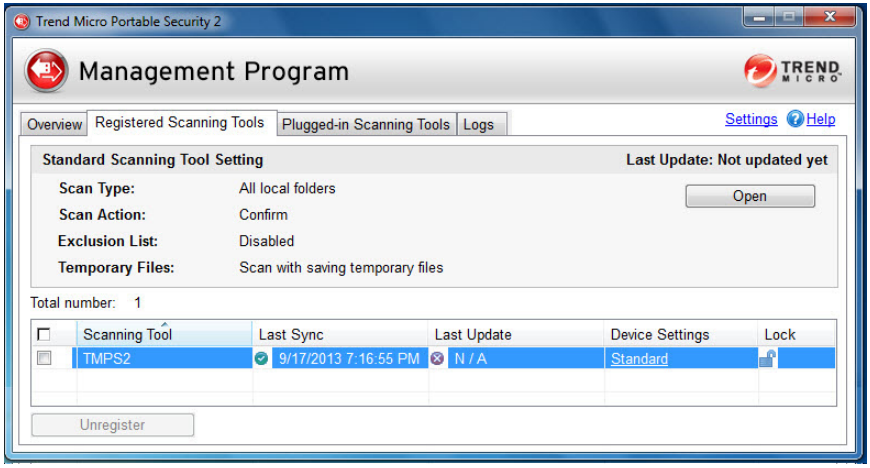
- **Custom**: The scan setting is specific to this device. This can be changed from the Scanning Tool or Management Program console.

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 3-18*
   - *Scan Settings (Others) on page 3-20*
5. Click **Save**.
6. Go to the Scanning Tool console and click the **Status & Update** tab.

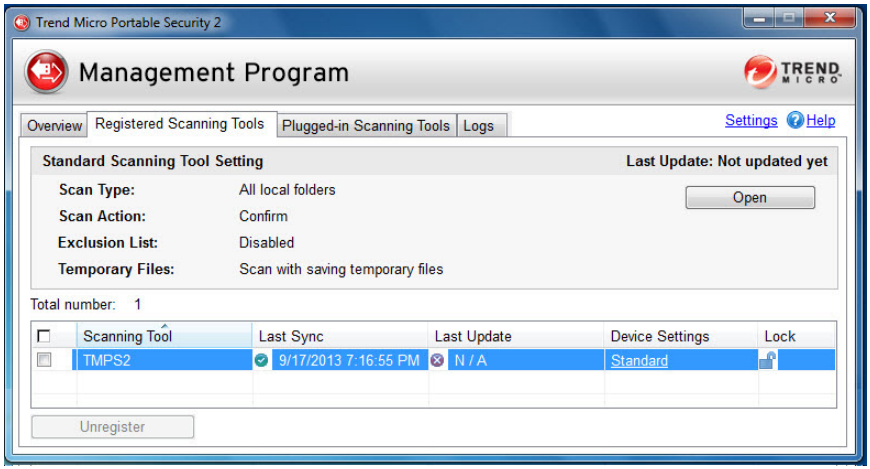
7. Click **Sync Logs and Settings**.

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 3-18*
   - *Scan Settings (Others) on page 3-20*

5. Click **Save**.

6. Go to the Scanning Tool console and click the **Status & Update** tab.

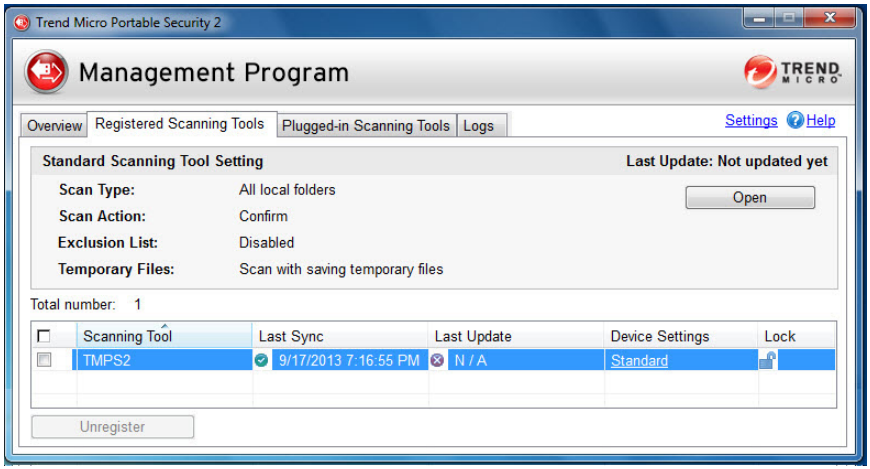
7. Click **Sync Logs and Settings**.

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

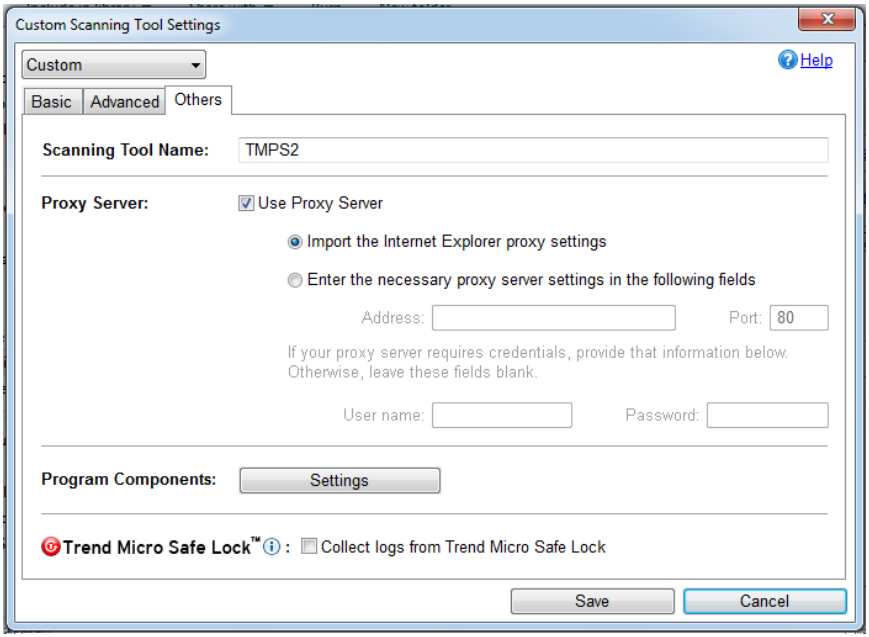
1. Open the Trend Micro Portable Security 2 Management Program.
2. Click the **Registered Scanning Tools** tab.



3. Choose one of the following:

   - To change the setting of all registered scanning tools, click **Open** in the Standard Scanning Tools section.
   - Click the **Custom** or **Standard** link for the selected Scanning Tool under the Device Settings column to change the setting of one device.

4. Go to the **Others** tab.



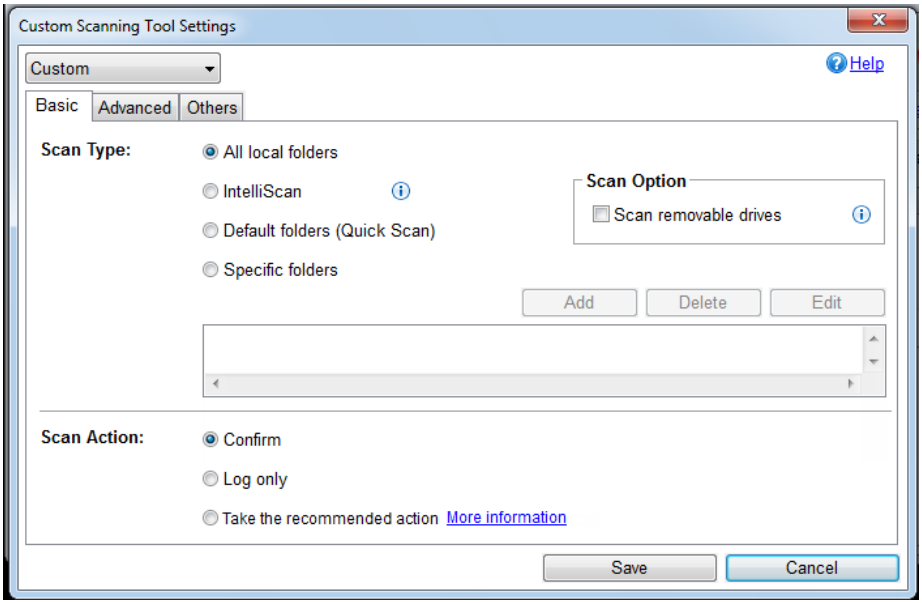
5. Mark the **Use a proxy server** option if your computer is required to use a proxy server to connect to the Management Program. Then choose one of the following options:

   - **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 basic scan 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. Refer to *Scan setting on page 3-9*.
- **Scan Type**: This determines the type of scan the tool will perform. Refer to *Scan Types on page 3-17*.
- **Scan Action**: This specifies what action the Scanning Tool will perform when it detects a threat. Refer to *Scan Action on page 3-17*.
- **Scan removable drives**: Enable the option to include removable drives when scanning.

Changing the Scan Types

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).
- **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 removable drives**: Enabling this option makes the scan check removable drives, as well.

Changing the Scan Action

The scan action setting determines what the scan will do.

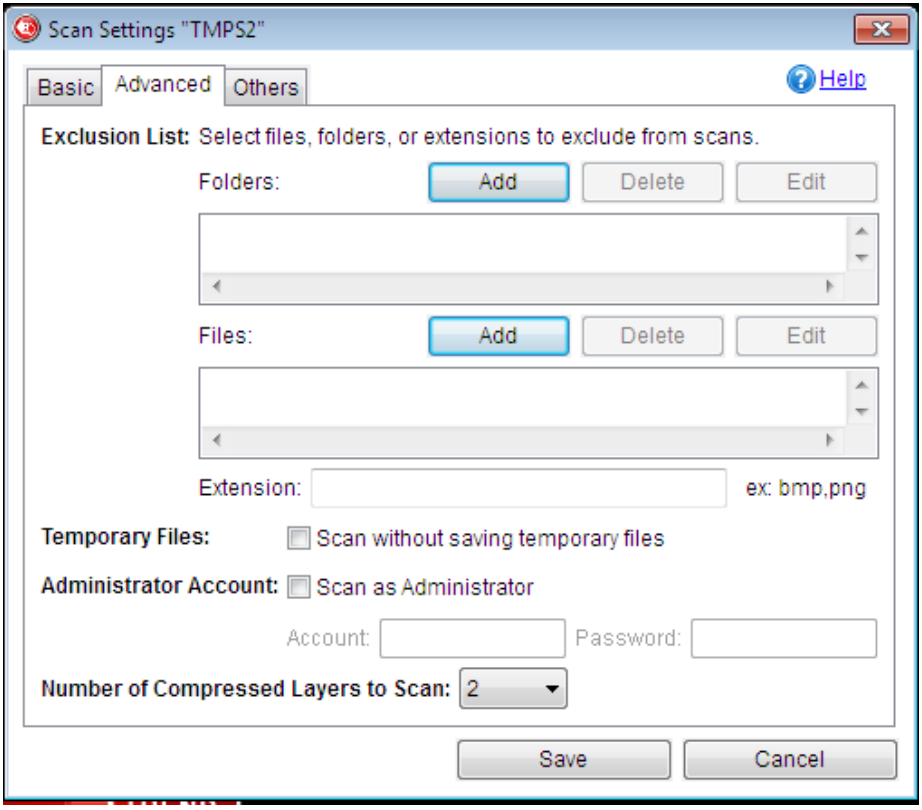
- **Confirm**: The scan will identify security threats and then ask what action to perform.
- **Log only**: The scan will only identify security threats, without taking any action against them.
- **Take the recommended action**: The scan will automatically respond to security threats according to the 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)

Change advanced scan settings of the Scanning Tool device. You can change the following:



- **Exclusion List**: Add files or folders that you do not want to be scanned. Refer to *Exclusion List on page 3-19*.
- **Scan without saving temporary files**: The Scanning Tool will not copy files to the target computer. Using this option reduces scanning capability for certain types of malware.

Note

Scanning and cleaning may still save some files on the 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.

Scan Settings (Others)

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

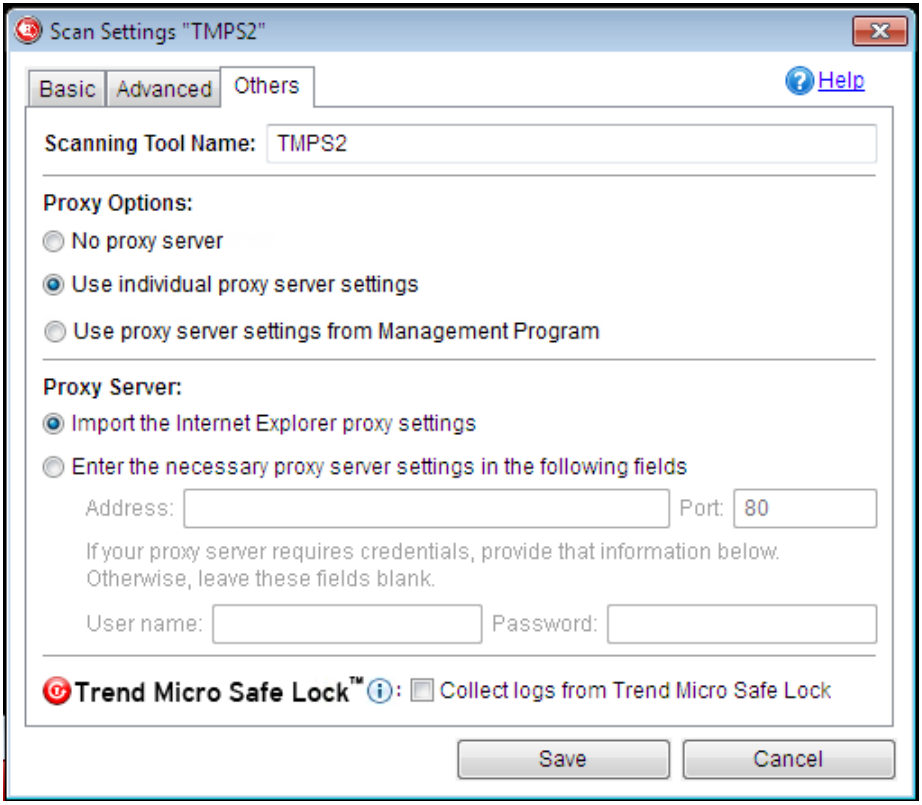


FIGURE 3-1. Scan settings for the Scanning Tool

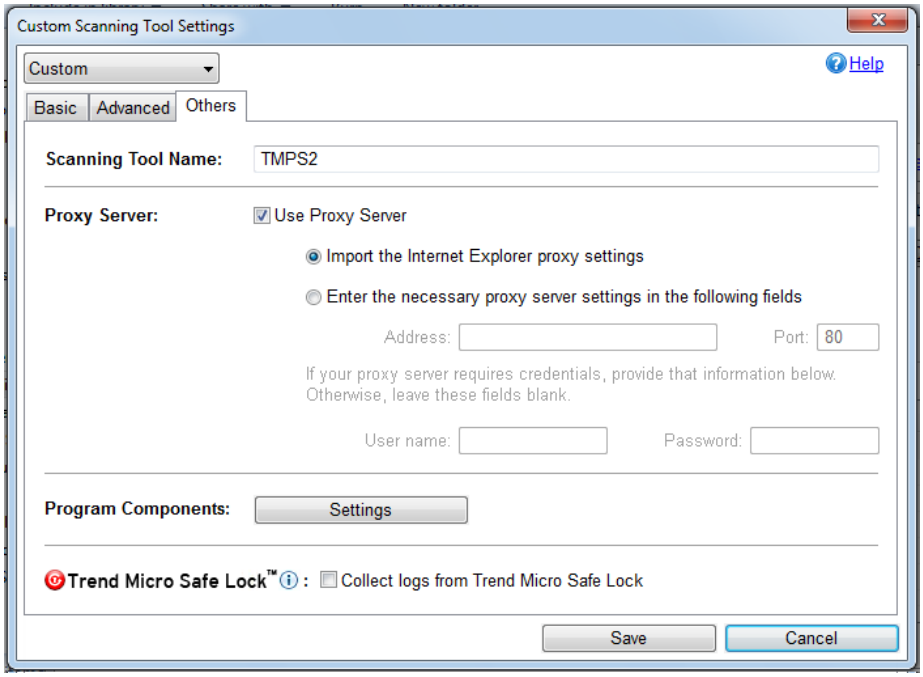


FIGURE 3-2. Scan settings for a managed Scanning Tool

- **Scanning Tool Name**: Change the name of the Scanning Tool device. Refer to *Changing the Name of the Standalone Scanning Tool on page 4-26*.

  Alternatively, you can change the name from the Management Program. Refer to *Changing the Name of the Scanning Tool on page 3-22*.

- **Proxy Options**: Specify if you want to use a proxy server or configure the proxy server for this device. You can select one of the following:

  Note

  This option will only show for the scanning tool.

  - **No proxy server**: Select this option if you do not want to use a proxy server to connect to the Internet.

- **Use individual proxy server settings**: Select this option to configure the proxy server settings for this device.
- **Use proxy server settings from the Management Program**: Select this option if you want to use the proxy server settings specified by the Management Program.

Note

This option is disabled for the Standalone Scanning Tool.

- **Proxy Server**: Enable this option if your computer is required to use a proxy server to connect to the Internet or 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.
- **Collect logs from Trend Micro Safe Lock**: Enable this option to collect logs from computers with Trend Micro Safe Lock. 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.

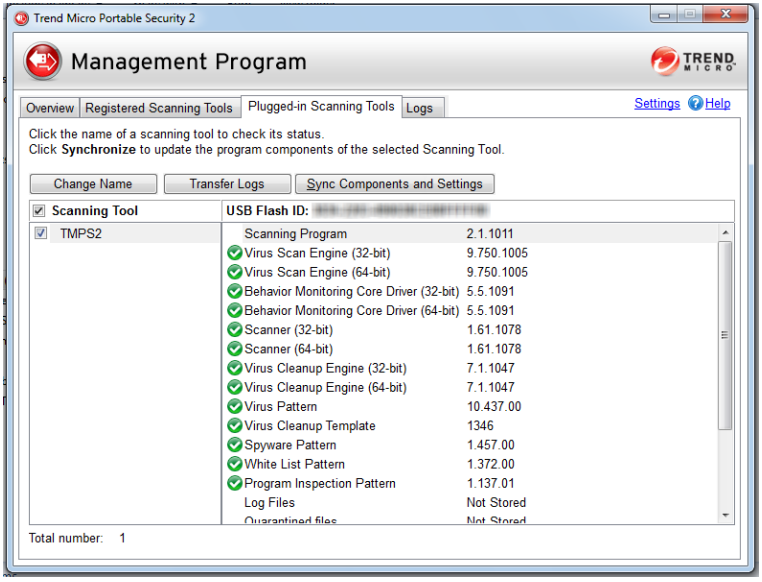
Procedure

1. Open the Trend Micro Portable Security 2 Management Program.

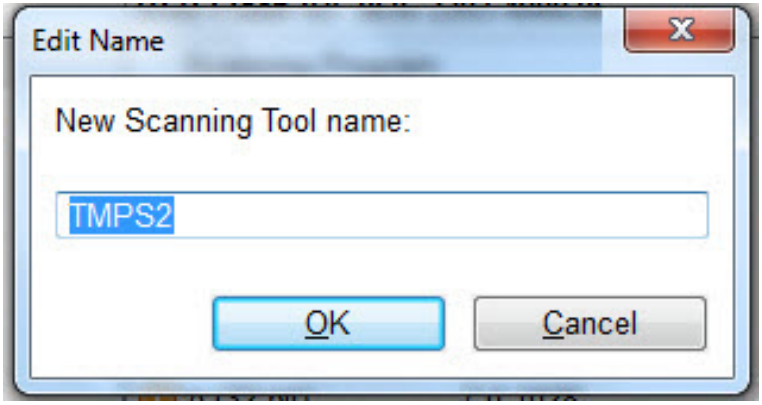
   - Option 1: From the **Plugged-in Scanning Tools** tab.

     a. Plug-in the Scanning Tool to the Management Program computer.

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



c. Click **Change Name**.

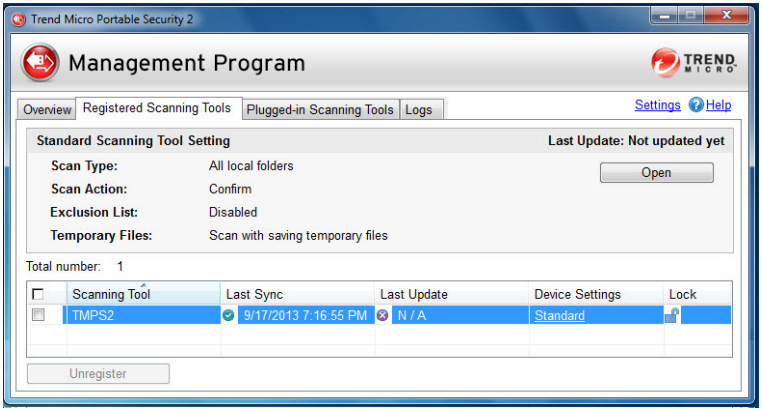


d. Type the new name.

e. Click **OK**.

- Option 2: 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 selected Scanning Tool.

Note

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

c. Type the new name.

d. Click **Save**.

e. Go to the **Plugged-in Scanning Tools** tab and click **Sync Components and Settings**. If you are not connected to the Management Program computer, refer to *Synchronizing Logs and Settings on page 4-16*.

- Option 3: From the Scanning Tool console. Refer to *Changing the Name of the Standalone Scanning Tool on page 4-26*.

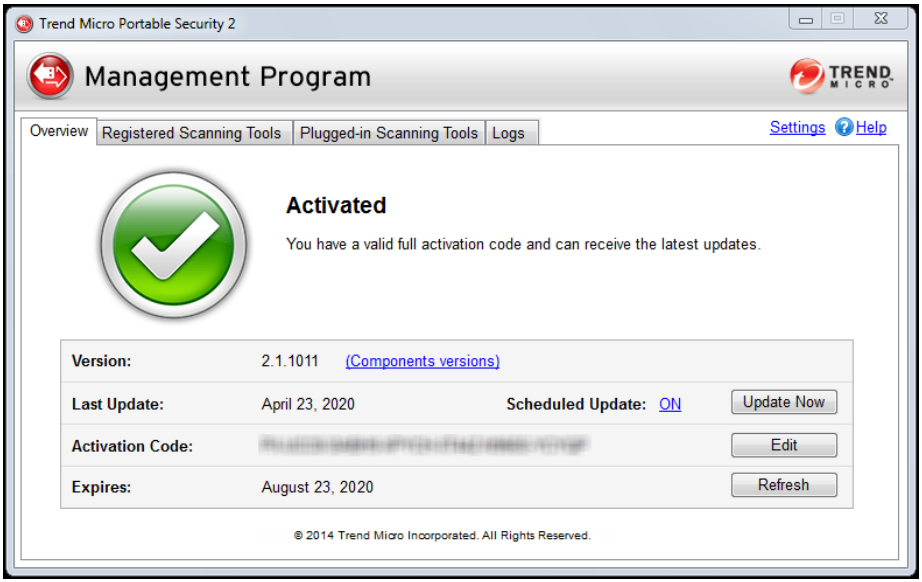
2. Safely unplug the Scanning Tool and then plug it in again.

Updates

Regularly update the components to ensure that you get the latest components. You can manually download the latest components or set Trend Micro Portable Security 2 to automatically download the latest components.

Checking the Latest Components

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.



Changing Update Settings

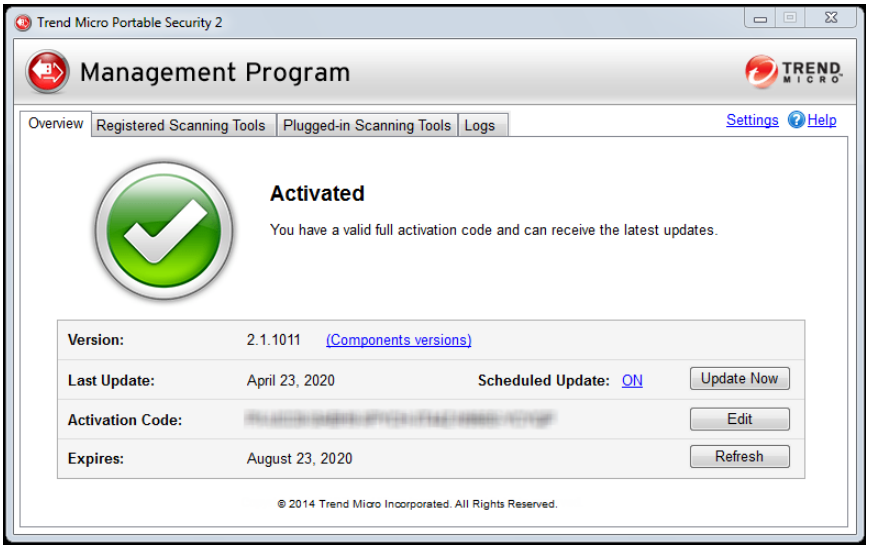
Enable Scheduled Update to automatically download the most recent components from Trend Micro.

Procedure

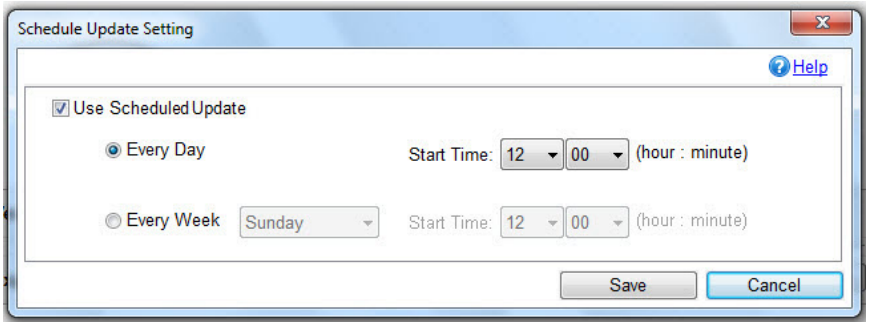
1. From the **Overview** tab, click the link beside **Scheduled Update**.

Note

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



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



3. Select the update frequency and the start time.

4. Click **Save**.

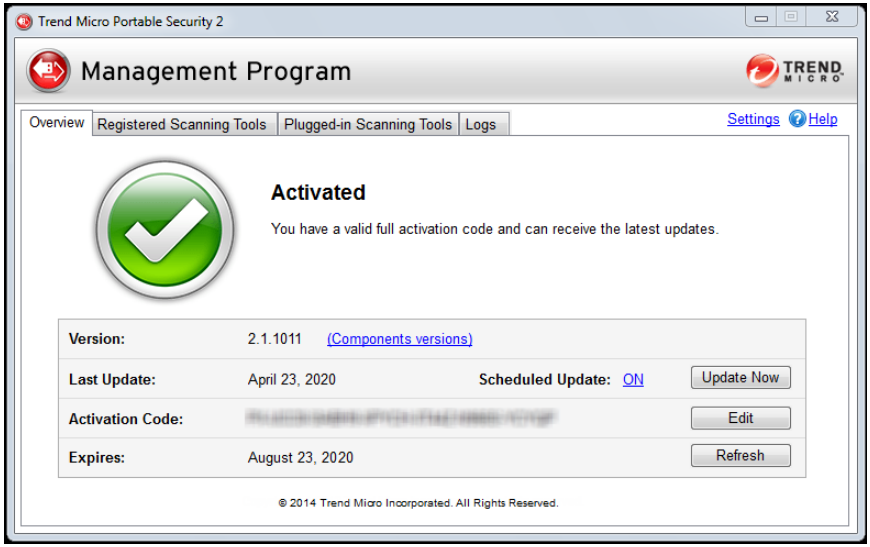
   After making changes, the link in the **Overview** tab should change, depending on whether the scheduled update option has been enabled or disabled.

Updating the Management Program

Regularly connect to Trend Micro to get the latest updates. This ensures that you are using the latest components when synchronizing components with the Scanning Tool.

Procedure

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



2. (Optional) Enable *Scheduled Updates on page 3-26*.

Synchronizing Updates

Synchronize the latest components and settings with the Scanning Tool. If you updated the components and did not synchronize the Scanning Tool, the Scanning Tool will continue to use the older components when scanning.

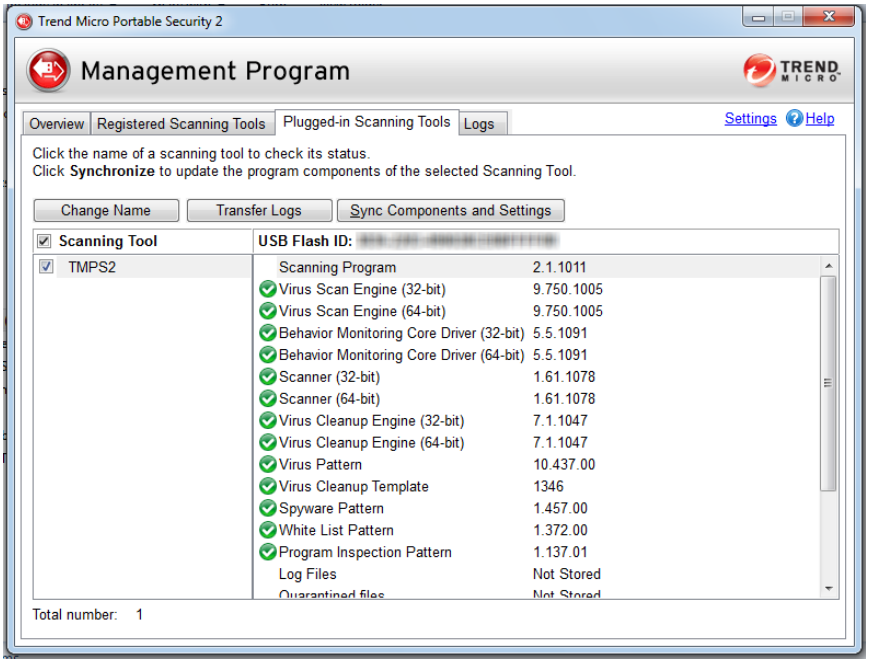
Alternatively, you can click **Update Now** from the Scanning Tool console to download components from the Management Program. Refer to *Updating the Scanning Tool on page 4-13*.

Procedure

1. Update the components on the Management Program.
2. Connect the Scanning Tool to the Management Program.

Note

You can connect the Scanning Tool directly to the Management Program computer or connect remotely from a computer with an Internet connection.



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

Logs

The **Logs** 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 the Logs

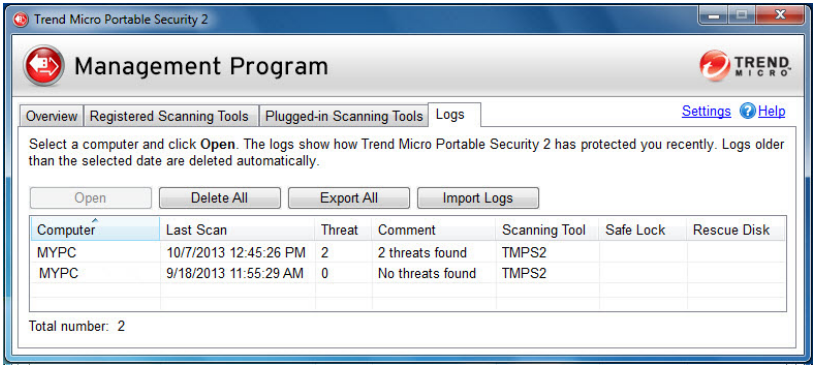
Whenever the Scanning Tool performs a scan, it keeps a detailed log report of the scanned computers and any threats that had been fixed or ignored. You can view these logs from the Scanning Tool console or through the Management Program console.

Procedure

- Management Program console

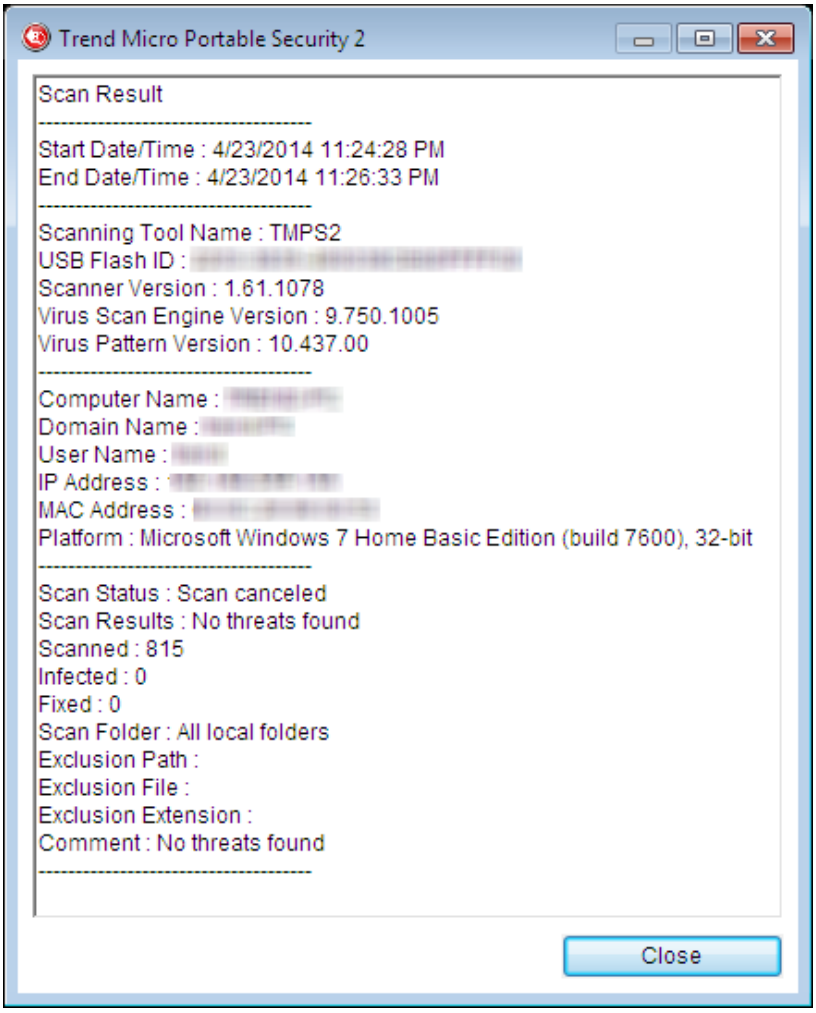
  a. Open the Trend Micro Portable Security 2 Management Program.

  b. Click the **Logs** tab.



  c. Select an item from the list and click **Open**.

  d. The Scan Result screen shows the date and time of the scan, the Scanning Tool name, the pattern file version, the scan engine version, the results of the scan, and the names of any security threats found.



Note

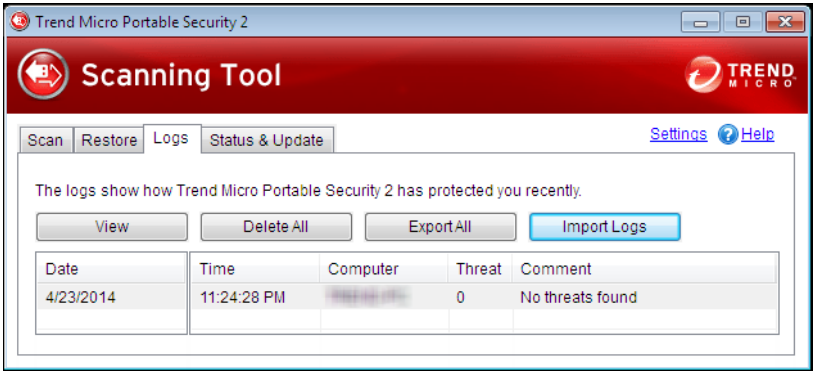
To delete the log data, click **Delete All**. You cannot delete log data files individually.

- Scanning Tool console

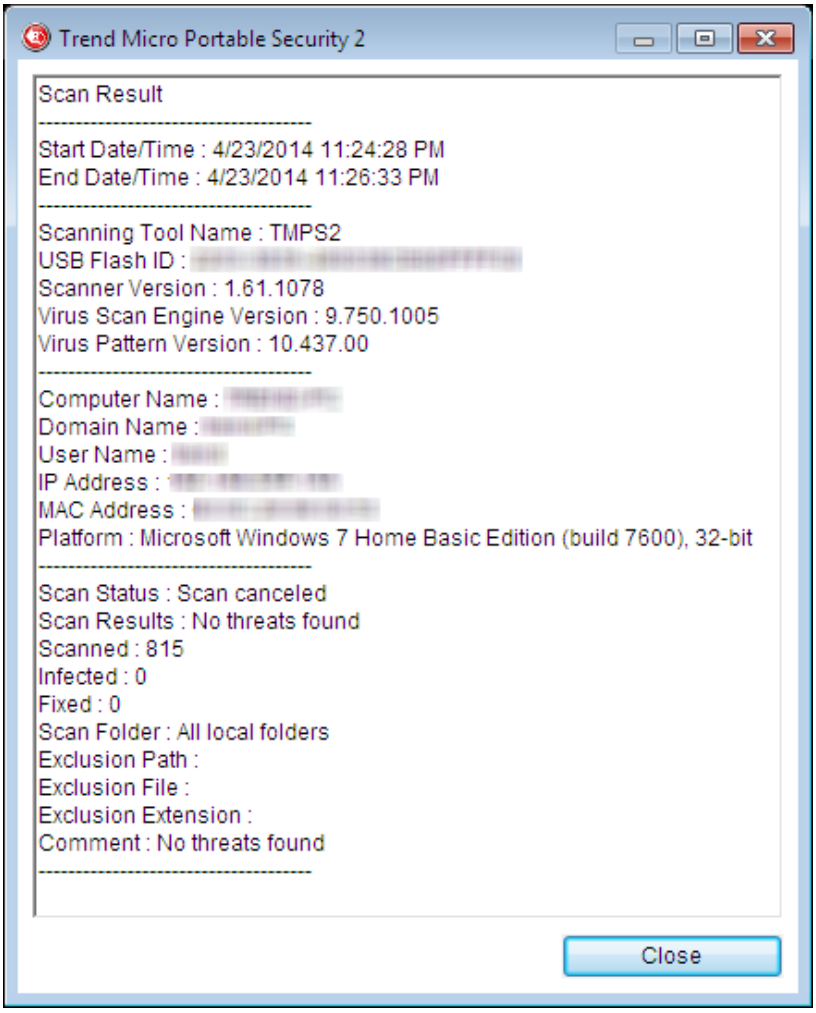
a. Plug in the Scanning Tool on a computer.

b. Open the Scanning Tool console.

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



d. Select a log date and click **View**.


Trend Micro Portable Security 2
Scan Result

Start Date/Time : 4/23/2014 11:24:28 PM
End Date/Time : 4/23/2014 11:26:33 PM

Scanning Tool Name : TMPS2
USB Flash ID :
Scanner Version : 1.61.1078
Virus Scan Engine Version : 9.750.1005
Virus Pattern Version : 10.437.00

Computer Name :
Domain Name :
User Name :
IP Address :
MAC Address :
Platform : Microsoft Windows 7 Home Basic Edition (build 7600), 32-bit
---
Scan Status : Scan canceled
Scan Results : No threats found
Scanned : 815
Infected : 0
Fixed : 0
Scan Folder : All local folders
Exclusion Path :
Exclusion File :
Exclusion Extension :
Comment : No threats found

Close

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

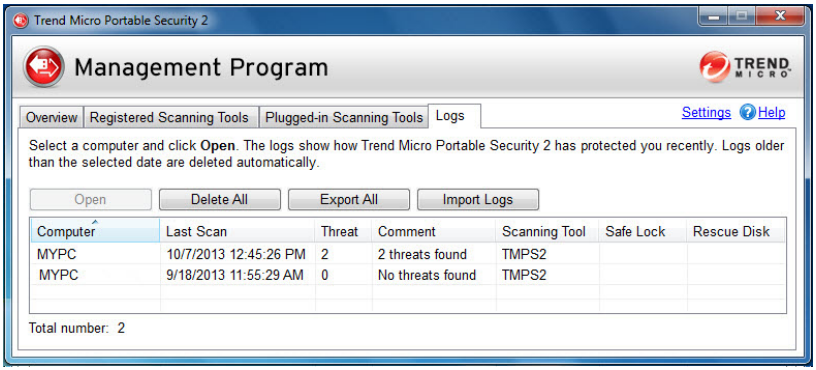
Trend Micro Portable Security 2 can only import database files.

Procedure

- Management Program console

  a. Open the Trend Micro Portable Security 2 Management Program.

  b. Click the **Logs** tab.



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

d. Locate the database file.

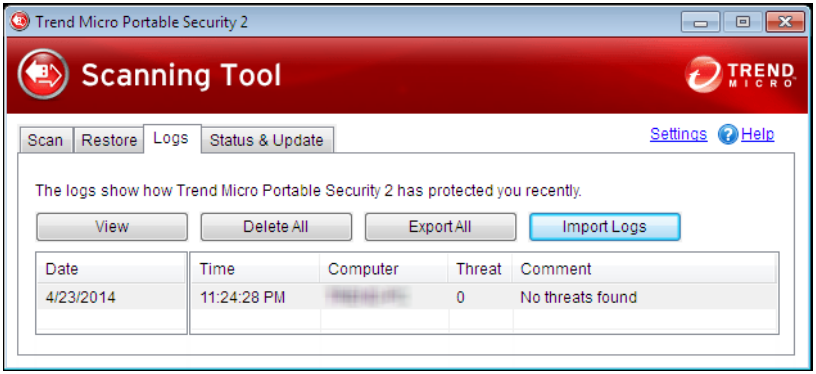
e. Click **OK**.

- Scanning Tool console

a. Plug in the Scanning Tool on a computer with an Internet connection.

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

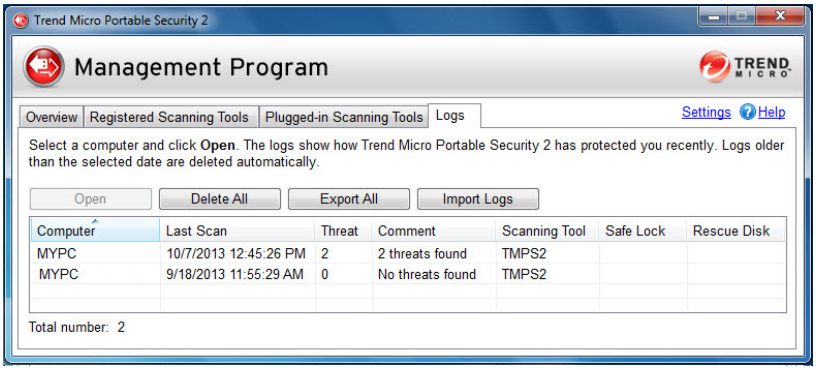
Trend Micro recommends regularly exporting log data and then deleting them from the scanning tool. This ensures that the scanning tool will always have enough space to be able to scan computers properly and save the quarantined files, if needed.

Procedure

- Management Program console

a. Open the Trend Micro Portable Security 2 Management Program.

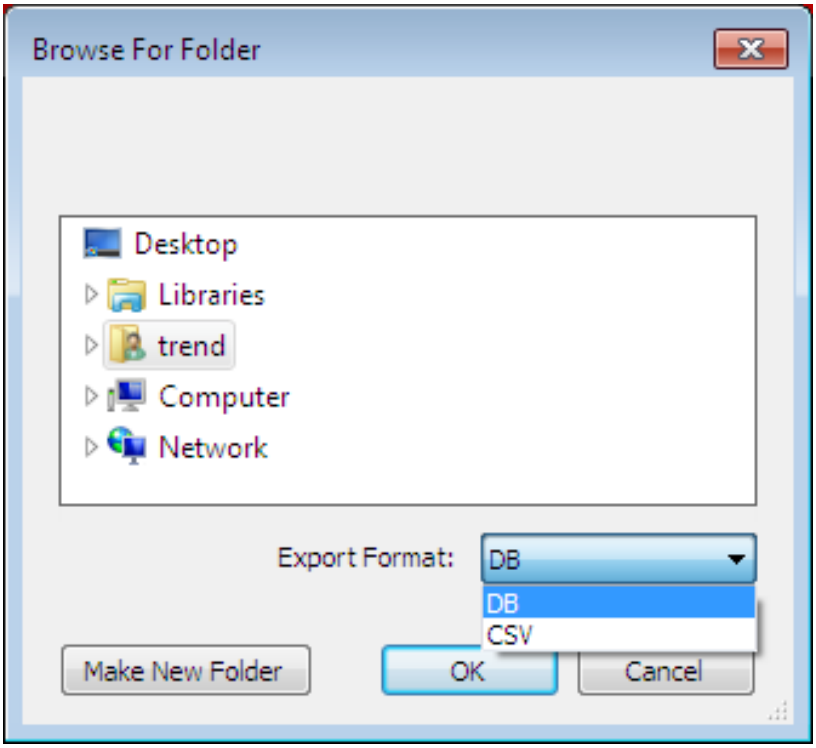
b. Click the **Logs** tab.



c. Click the **Export All** button.

d. Specify a location and choose the export format.

- 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.



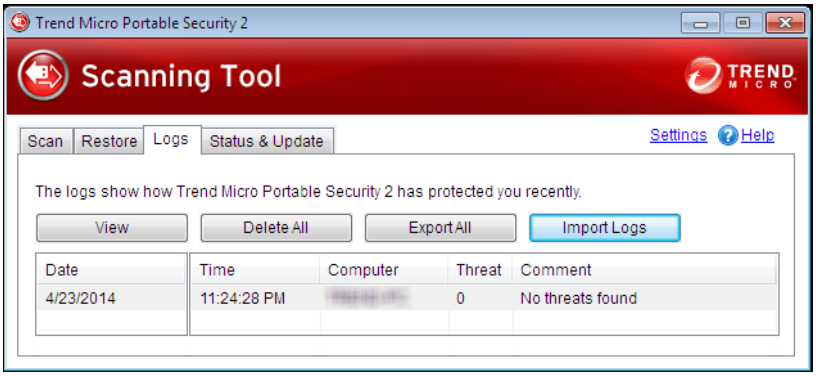
e. Click **OK**.

- Scanning Tool console

  a. Plug in the Scanning Tool on a computer with an Internet connection.

  b. Open the Scanning Tool console.

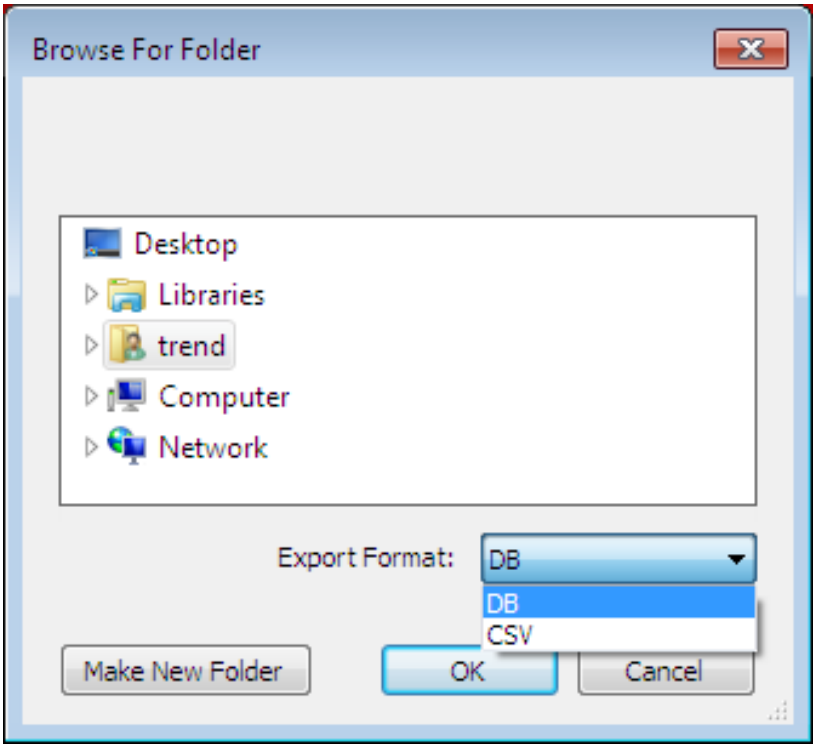
  c. Go to the **Logs** tab.



d. Click the **Export All** button.

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

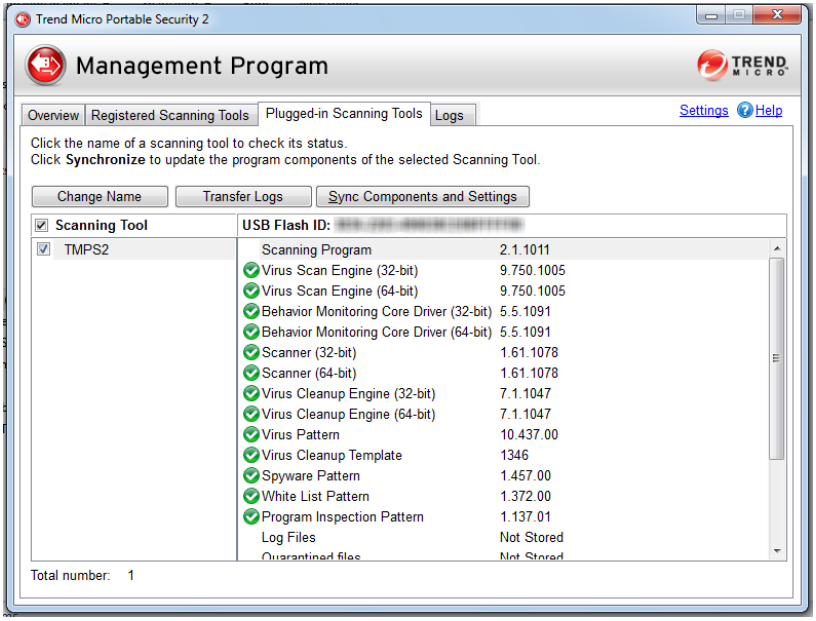
Transfer the logs from the plugged-in Scanning Tool to the Management Program.

Procedure

- Option 1: Connect the Scanning Tool to the Management Program computer

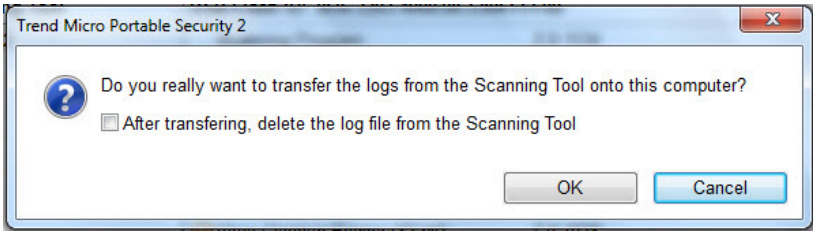
  1. Plug in the Scanning Tool to the computer with the Management Program.
  2. Open the Trend Micro Portable Security 2 Management Program.

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



4. Select the Scanning Tool.

5. Click **Transfer Logs**. A pop message appears.



6. (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

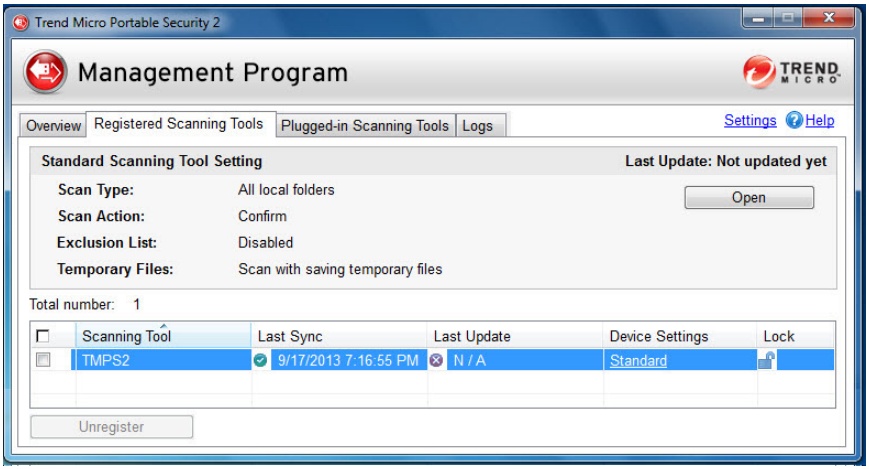
Trend Micro Portable Security 2 has the option of collecting logs from computers that have Trend Micro™ Safe Lock™. For more information, refer to Safe Lock.

Note

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

Procedure

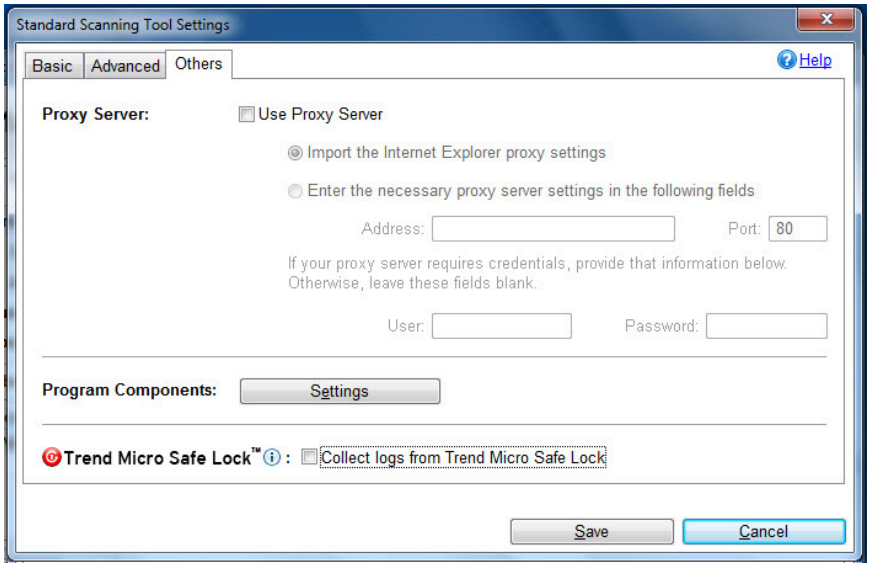
1. Open the Trend Micro Portable Security 2 Management Program.
2. Click the **Registered Scanning Tools** tab.



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 device, click the **Custom** or **Standard** link for the selected Scanning Tool under the Device Settings column.

4. Go to the **Others** tab.



5. Enable or disable the **Collect logs from Trend Micro Safe Lock** option.
6. Click **Save**.
7. Synchronize the Scanning Tool settings with Management Program.

Other Settings

Change other Management Program settings.

Changing the Activation Code

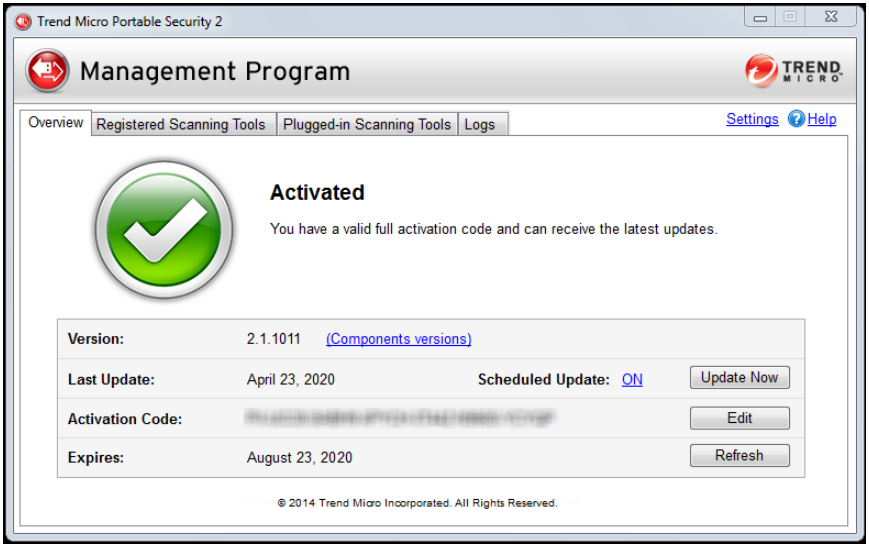
The date next to Expires shows when you need to get another activation code. If you have not connected to the Internet for a while, or if you recently entered a new activation code, click **Refresh** next to Expires to get the latest expiration date or click **Edit** to change the activation code.

For more information, refer to *Activation Status on page 2-6*.

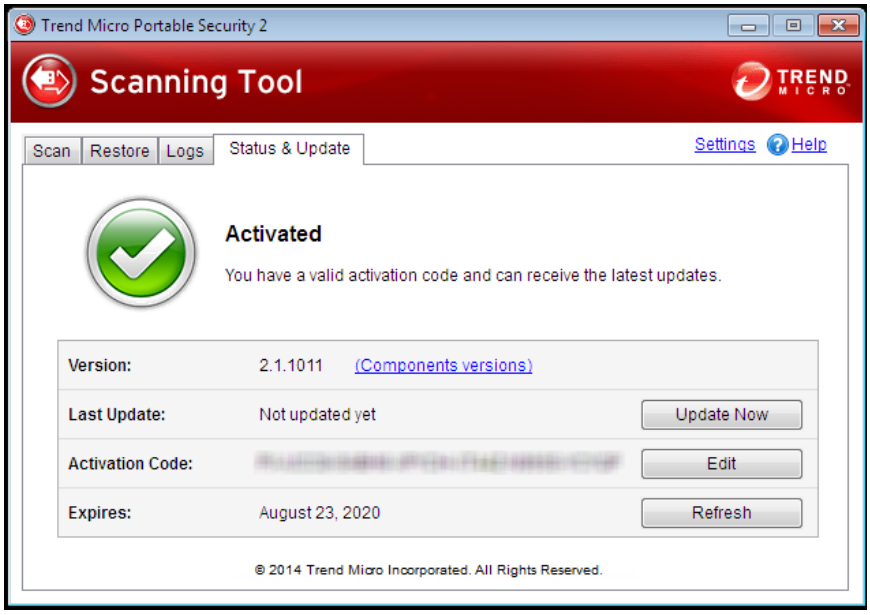
Procedure

1. Open the console.

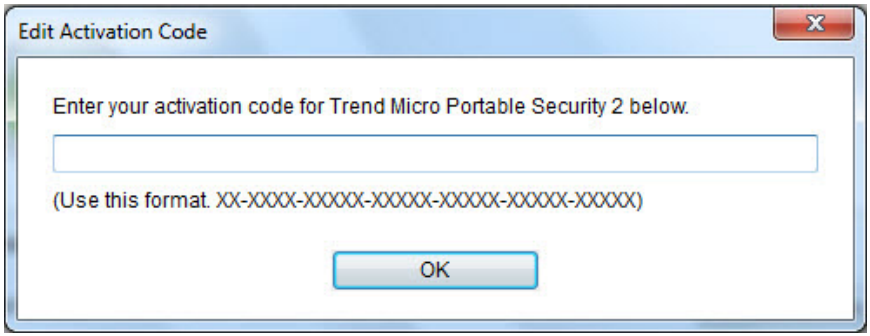
> **Note**
>
> For the Management Program, skip the next step.



2. Go to the **Status & Update** tab.



3. Click **Edit**.



4. Specify a new activation code.

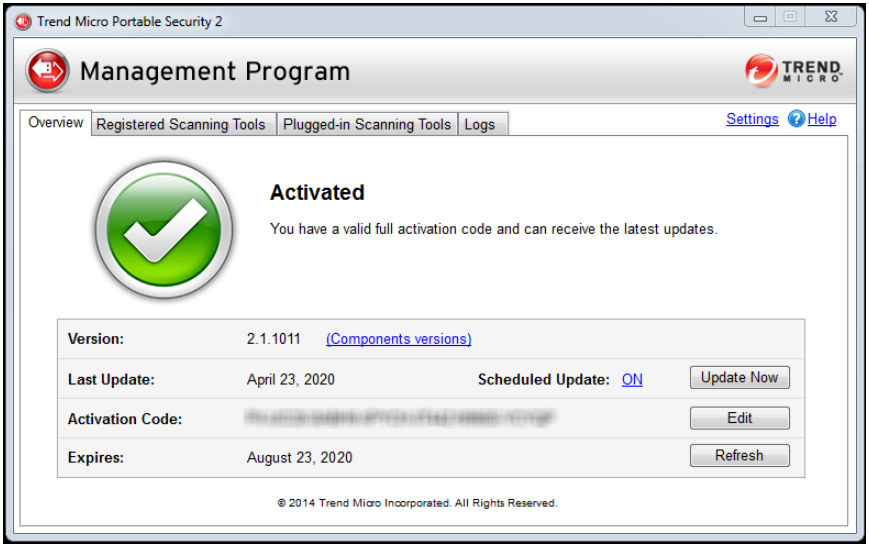
5. Click **OK**.

Changing the Management Program Settings

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

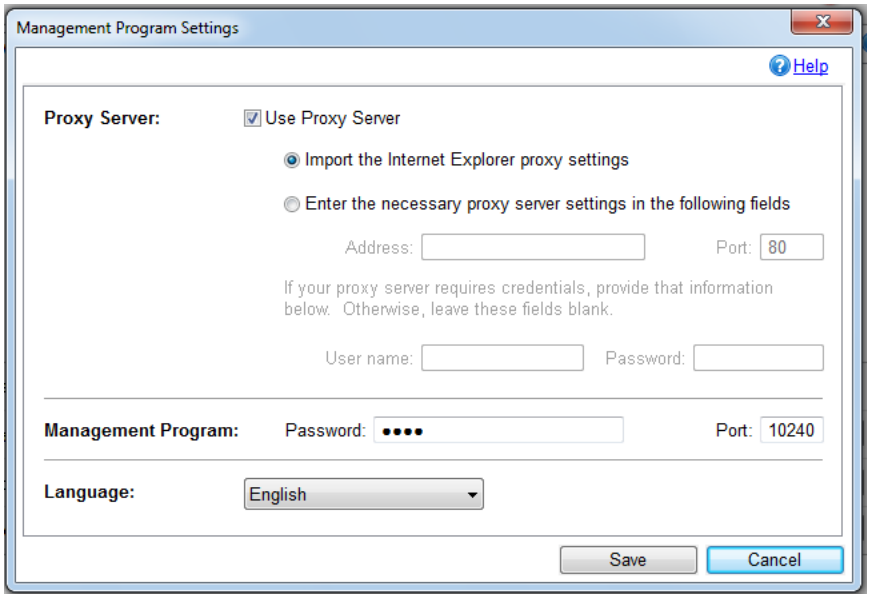
Procedure

1. Open the Management Program console.



2. Click **Settings**.

The **Management Program Settings** page opens.



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 Trend Micro Portable Security 2™ Scanning Tool.

Topics in this chapter:

Getting Started

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 Devices on page 2-7* or *Activating a Standalone Tool on page 2-9* 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.

Changing the Activation Code

The date next to Expires shows when you need to get another activation code. If you have not connected to the Internet for a while, or 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.

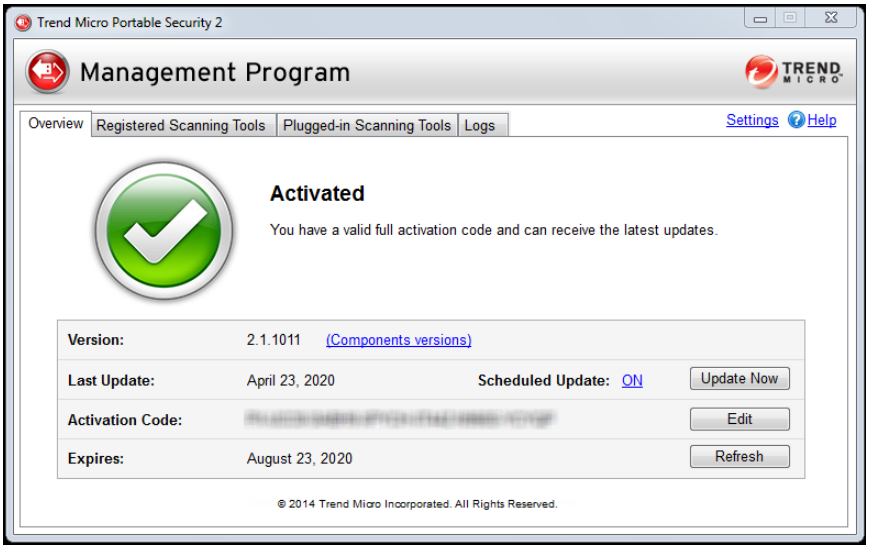
For more information, refer to *Activation Status on page 2-6*.

Procedure

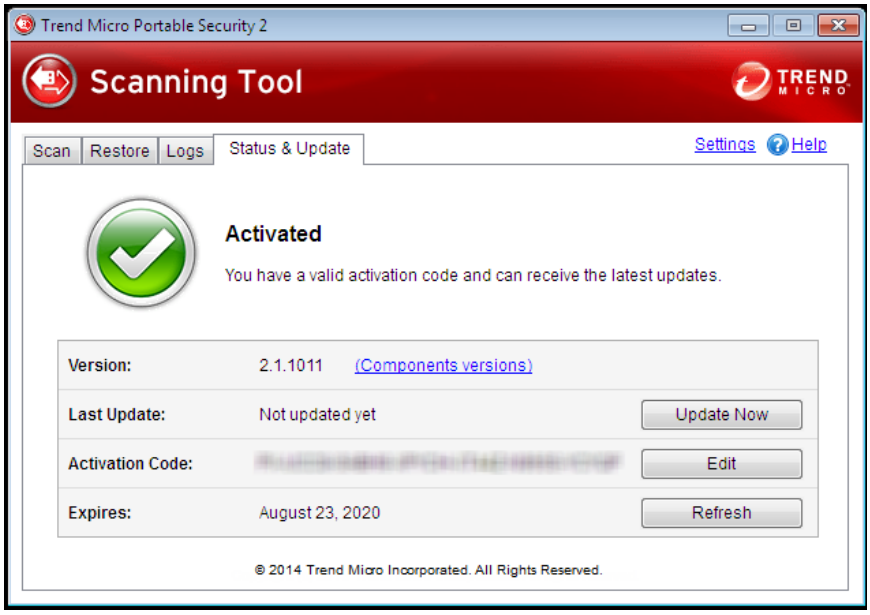
1. Open the console.

Note

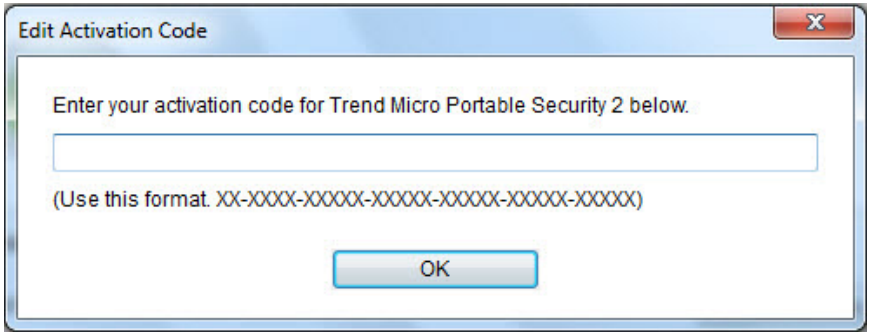
For the Management Program, skip the next step.



2. Go to the **Status & Update** tab.



3. Click **Edit**.



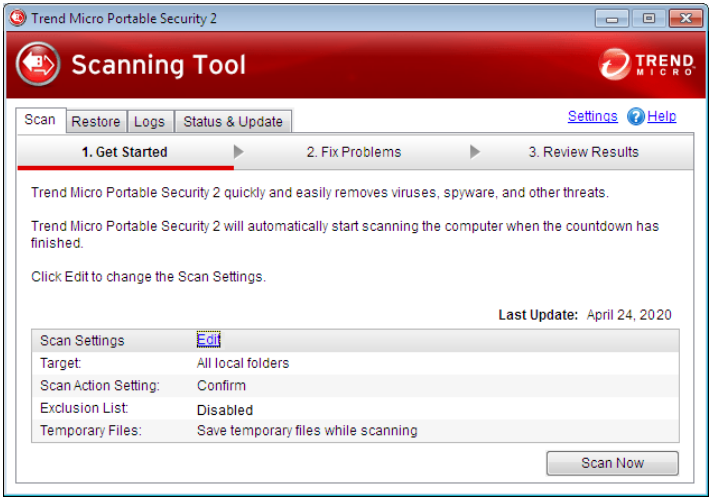
4. Specify a new activation code.

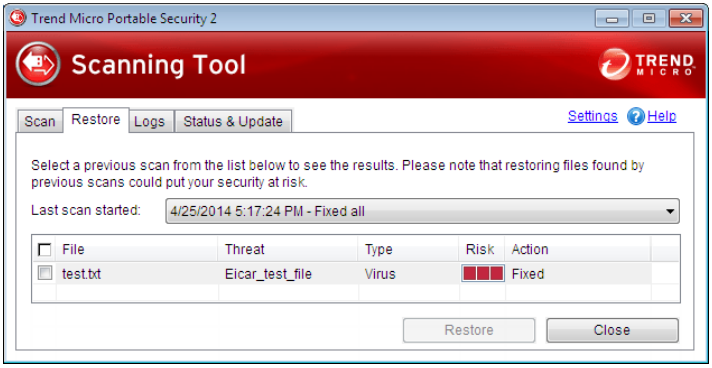
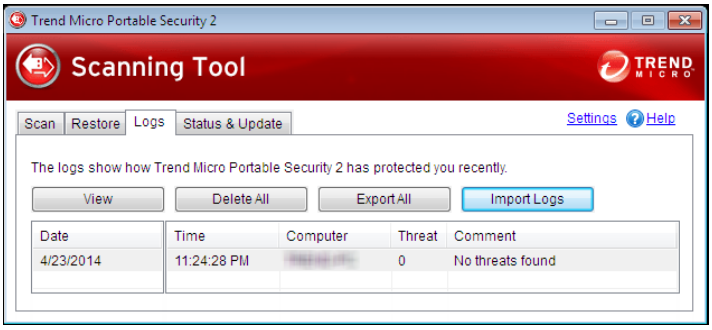
5. Click **OK**.

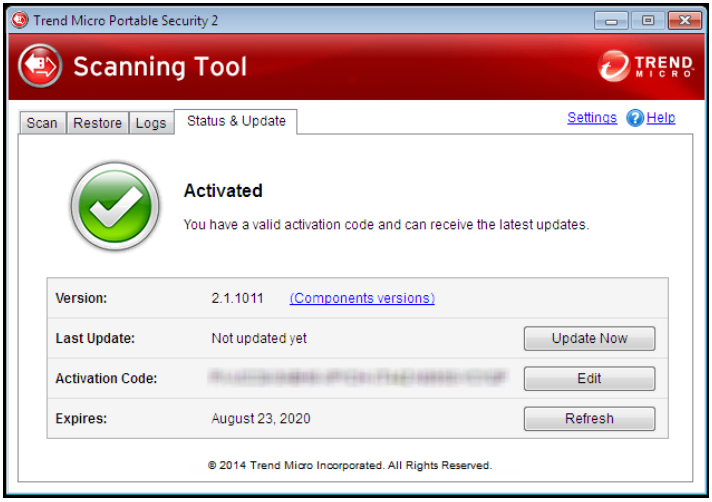
Understanding the Scanning Tool Device Console

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	Click this link to check or change the settings of the scanning tool device. Refer to *Scanning Tool Settings on page 4-23*.
Help	Click this link to open the help file and to find more information about how to use this device.
Scan tab	 Show the scan process and settings. Refer to *Scan Tab on page 4-8*.

TAB OR BUTTON	DESCRIPTION
Restore tab	 Check the quarantined files that the scan process found and performed an action on. Refer to *Restore Tab on page 4-9*. **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.
Logs tab	 Check the results of earlier scans done on the computer connected to the Scanning Tool. Refer to *Logs Tab on page 4-10*.

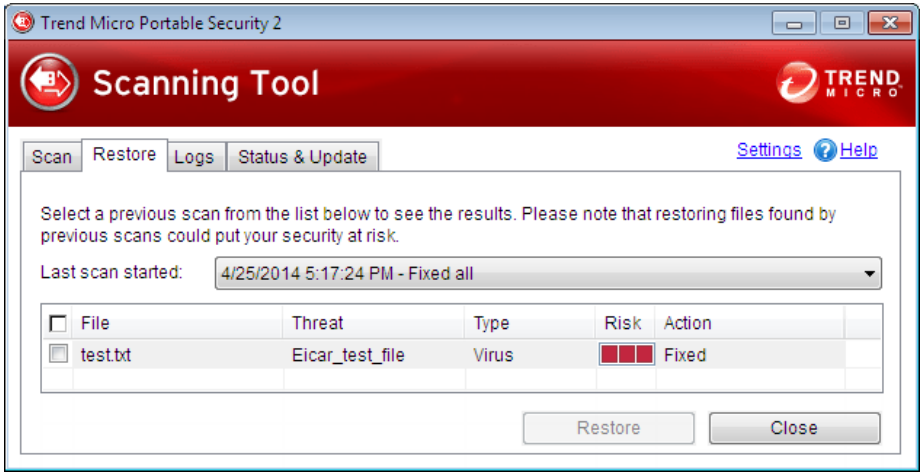
Tab or Button	Description
Status & Update tab	 **Figure 4-1. Standalone device**  **Figure 4-2. Managed device** Check the status of the components and perform an update, if needed. Refer to *Status & Update tab on page 4-10*.

Scan Tab

- **Edit**: Click this link to check or change the scan settings. Refer to *Scan settings on page 4-29*.
- **Scan Now**: Click this button to manually start the scanning process. Refer to *Performing a Scan on page 4-18*.
- **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. Refer to *Security Threats Found on page 4-21*.
- **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.

Restore Tab



Note

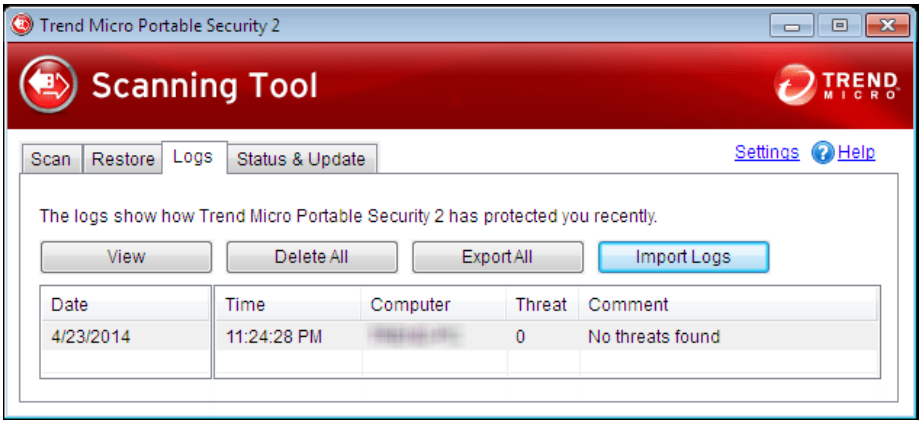
You can store quarantined files in the USB device, instead of on the target computer but you cannot use the Scanning Tool to store other files.

- **Last scan started**: Select the time that the scan was performed to view the logs and actions done at that time.
- **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 4-22*.

WARNING!

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

Logs Tab



- **View**: Click this button to open the scan result page and shows more detailed information. Refer to *Viewing the Logs on page 3-31*.
- **Delete All**: Click this button to delete all log entries.

> **Note**
>
> Trend Micro recommends exporting logs before deleting them.

- **Export All**: Click this button to export all the logs into database or csv format. Refer to *Exporting Logs on page 3-36*.
- **Import Logs**: Click this button to import database format logs. *Importing Logs on page 3-35*.

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 2-6*.

- **Version**: The build number of the Trend Micro Portable Security 2 Management Program or the Scanning Tool appears next to **Version**. Click the **Component versions** link to see the component details and the date of the last update.
- **Update Now**: Click this button to manually start updating the components. Refer to *Updating the Scanning Tool on page 4-13*.
- **Refresh**: Click this button when you have changed the activation code and it still says expired.

Updates

You can plug in the Scanning Tool to the Management Program computer or any computer with an Internet connection and download 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.

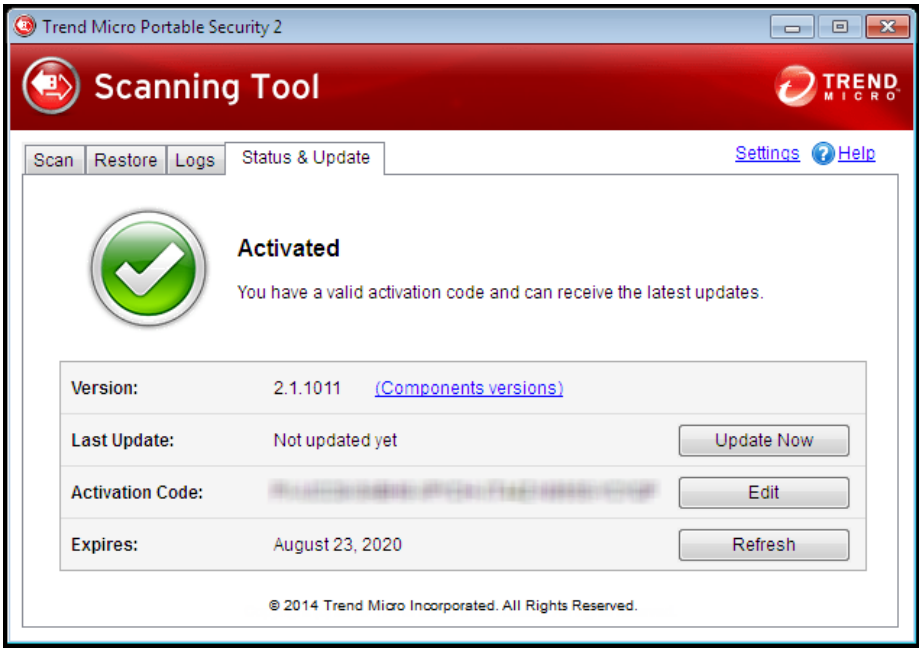


FIGURE 4-3. The Status & Update tab of the Standalone Scanning Tool

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

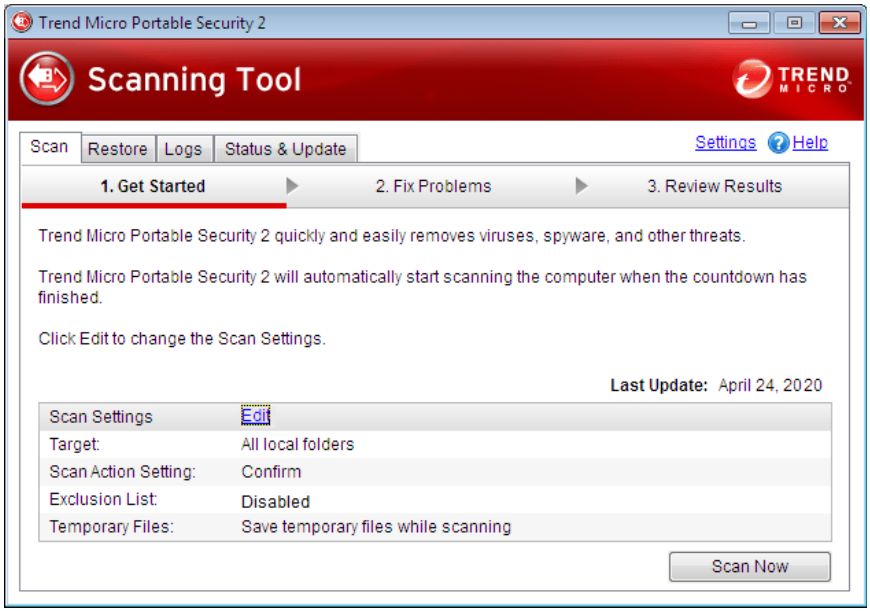
Updating the Scanning Tool

Regularly connect to Trend Micro or your Management Program to get the latest updates. This ensures that you are using the latest components when scanning computers or devices.

Alternatively, you can click **Sync Components and Settings** from the Management Program to download the components from the Management Program. Refer to *Synchronizing Updates on page 3-29*.

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.

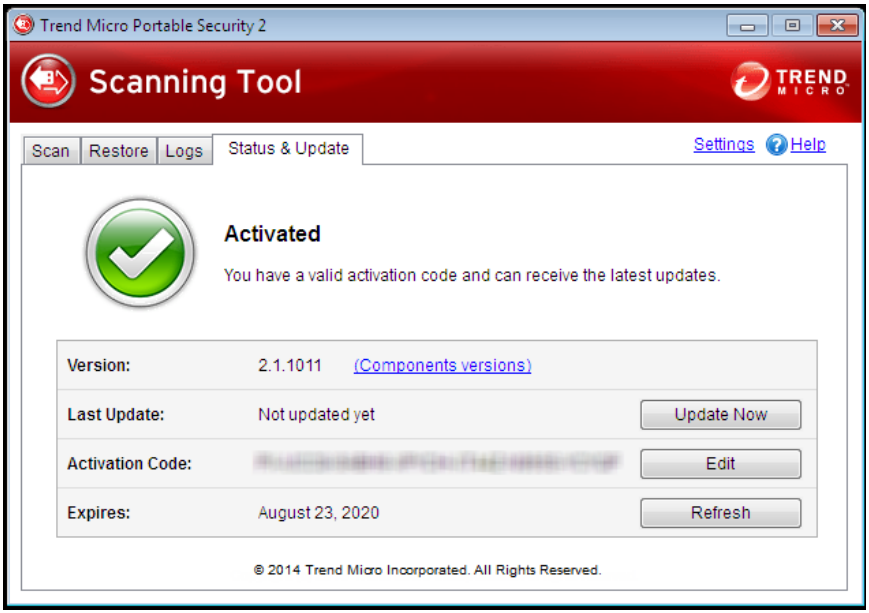


FIGURE 4-5. Standalone device

FIGURE 4-6. Managed devices

4. Click **Update Now**.

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 Updates on page 3-29*.

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**.

Synchronizing Updates

Synchronize the latest components and settings with the Scanning Tool. If you updated the components and did not synchronize the Scanning Tool, the Scanning Tool will continue to use the older components when scanning.

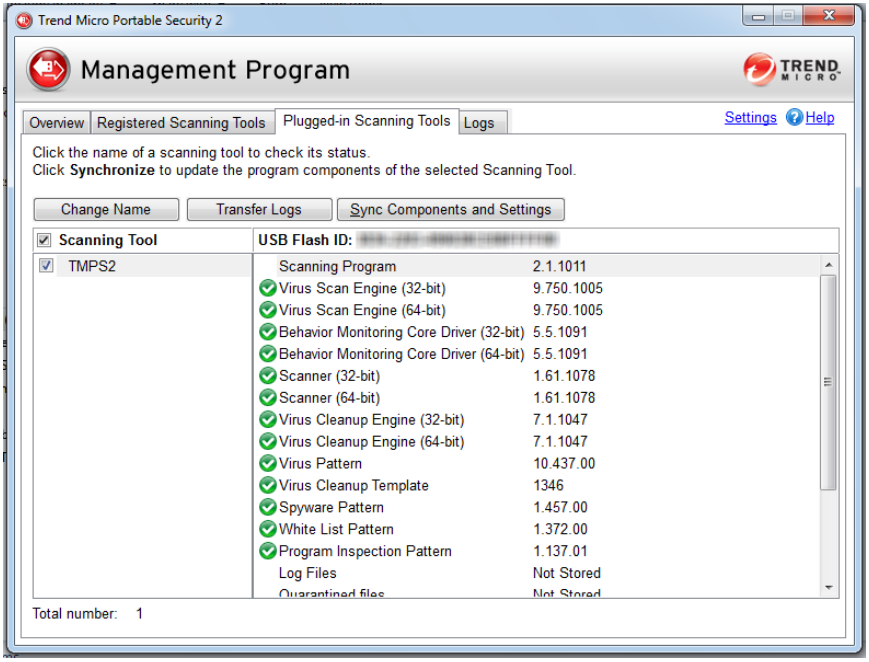
Alternatively, you can click **Update Now** from the Scanning Tool console to download components from the Management Program. Refer to *Updating the Scanning Tool on page 4-13*.

Procedure

1. Update the components on the Management Program.
2. Connect the Scanning Tool to the Management Program.

Note

You can connect the Scanning Tool directly to the Management Program computer or connect remotely from a computer with an 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	The Scanning Tool did not find any threats.
Yellow	The Scanning Tool found some threats and was able to clean the computer.
Red	The Scanning Tool found some threats but was unable to clean the computer.
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.

   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

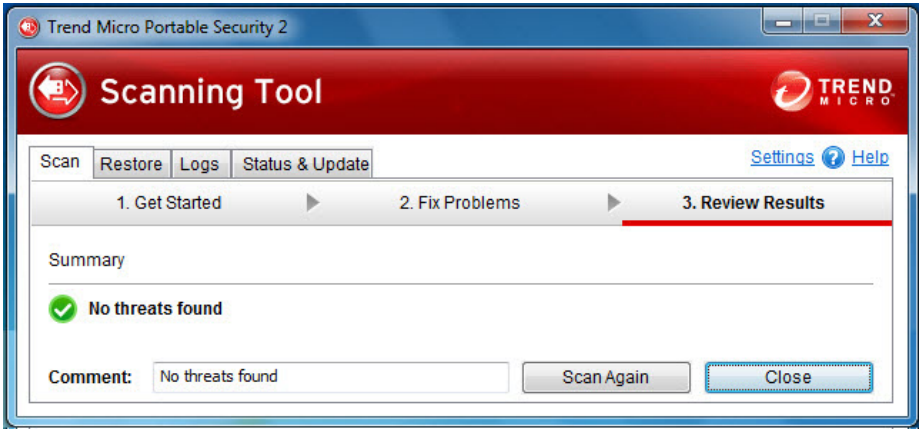
Follow the appropriate directionsbased on the results of the scan.

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.

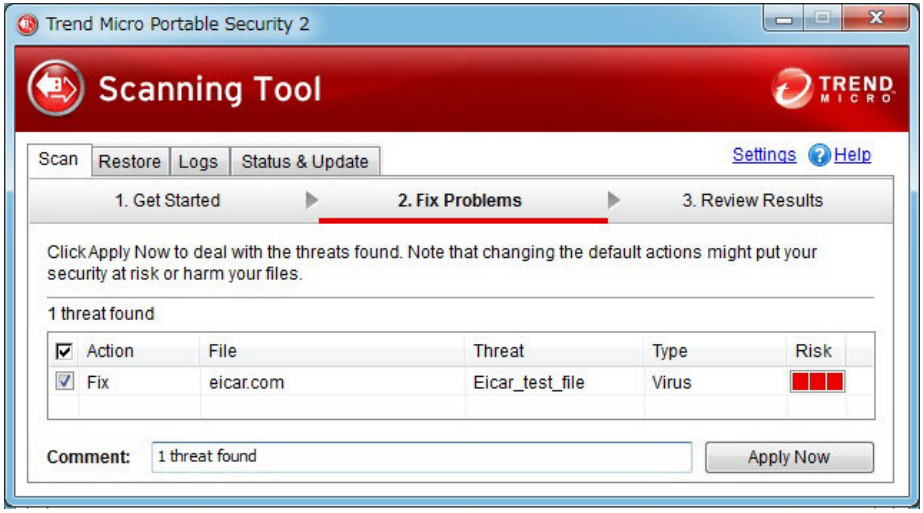
Tip

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 about the scan when you use the Management Program to *check the results on page 3-31*. The name of the computer is the default value of this field.

Restoring Quarantined Files

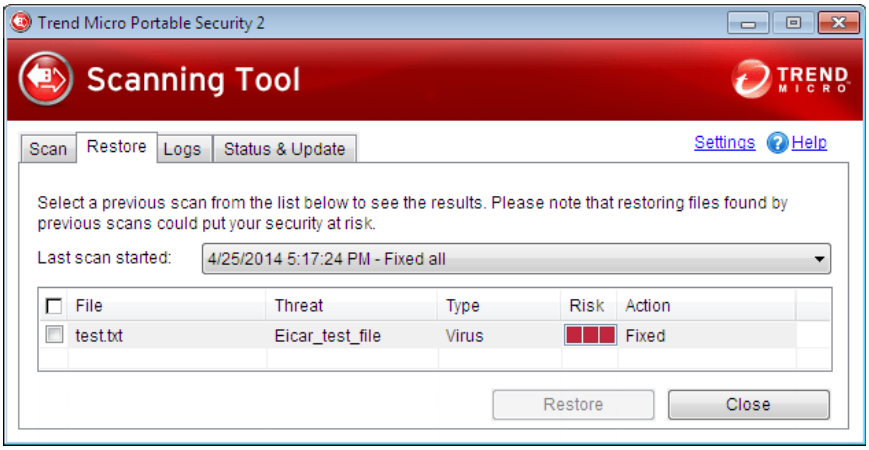
You can restore files if Trend Micro Portable Security 2 fixed and quarantined files that you need.

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

Register your Scanning Tool to the Management Program to be able to sync the components, settings and logs. You can also change the Scanning Tool language.

Procedure

1. Open the Scanning Tool console.

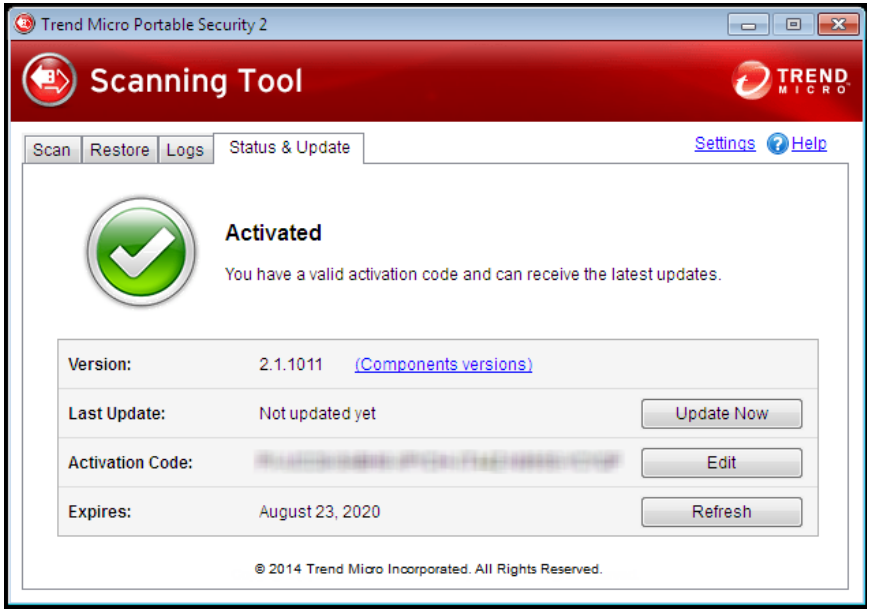
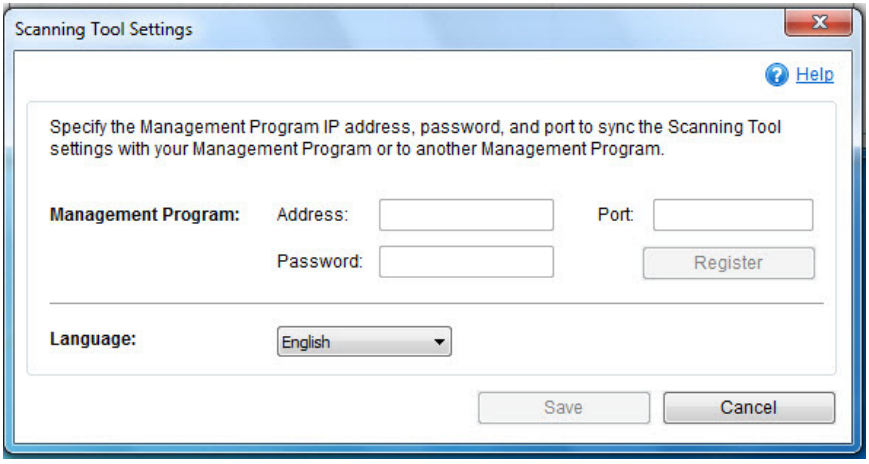


FIGURE 4-7. The Standalone Scanning Tool console

FIGURE 4-8. The Managed Scanning Tool console

2. Click **Settings**.



Note

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

3. Specify the Management Program IP address, port, and password.
4. Click **Register**.
5. (Optional) Select a language from the drop-down menu to change the Scanning Tool language.
6. Click **Save**.

Changing the Name of the Standalone 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.

You can also change the name from the Management Program. Refer to *Changing the Name of the Scanning Tool on page 3-22*.

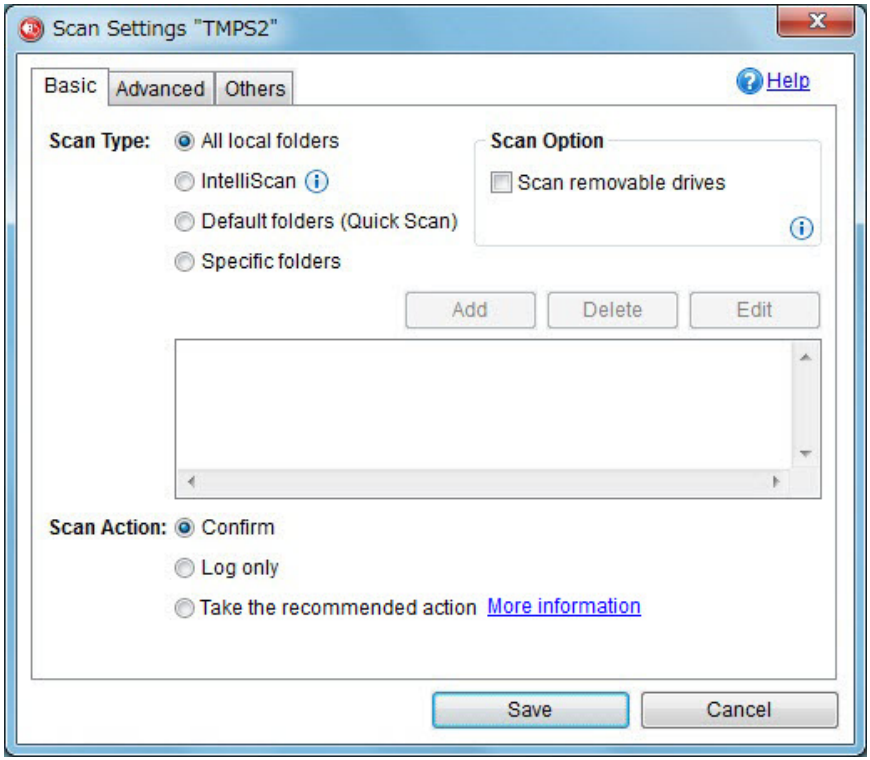
Procedure

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

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

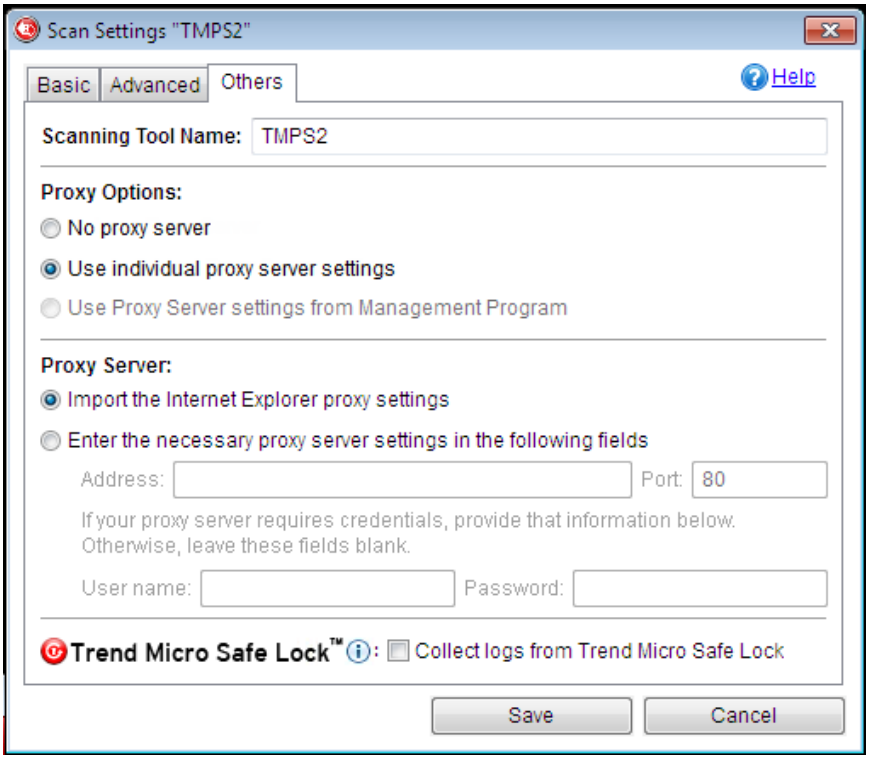
3. Click **Edit**.

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**.

Changing the Scan Settings of a Scanning Tool

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 on page 3-29*, the Management Program settings will replace the Scanning Tool settings.

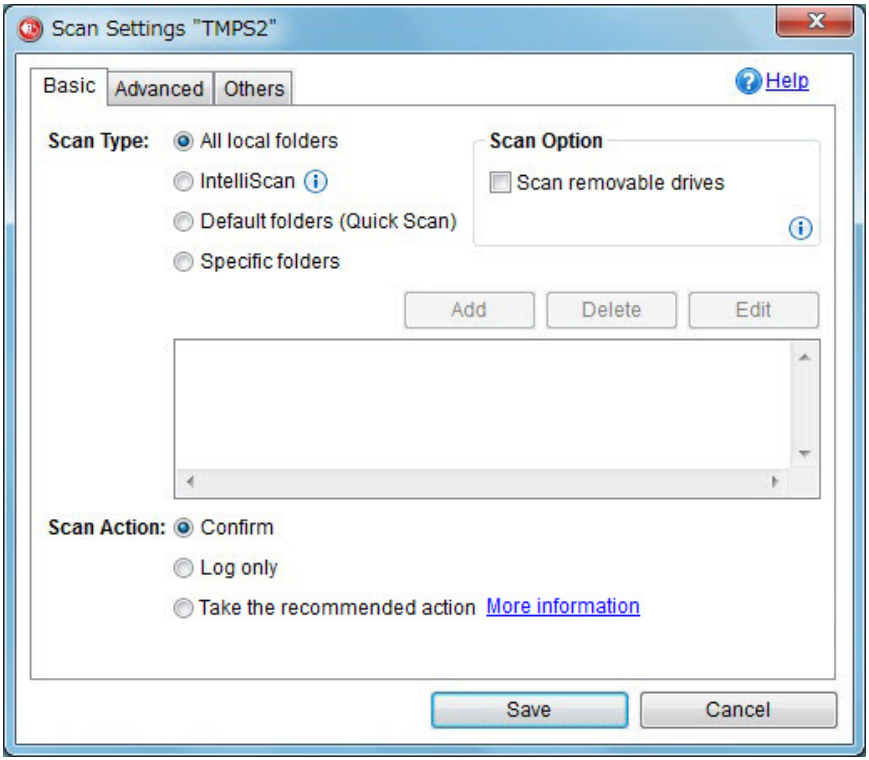
If you are using the Trend Micro Portable Security 2 device as a standalone Scanning Tool, you can use the **Edit** link to change the scan settings of the USB device. Any changes made will only be for this Scanning Tool.

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 3-18*
   - *Scan Settings (Others) on page 3-20*
5. Click **Save**.
6. Click **Scan Now** to start scanning with the new scan 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

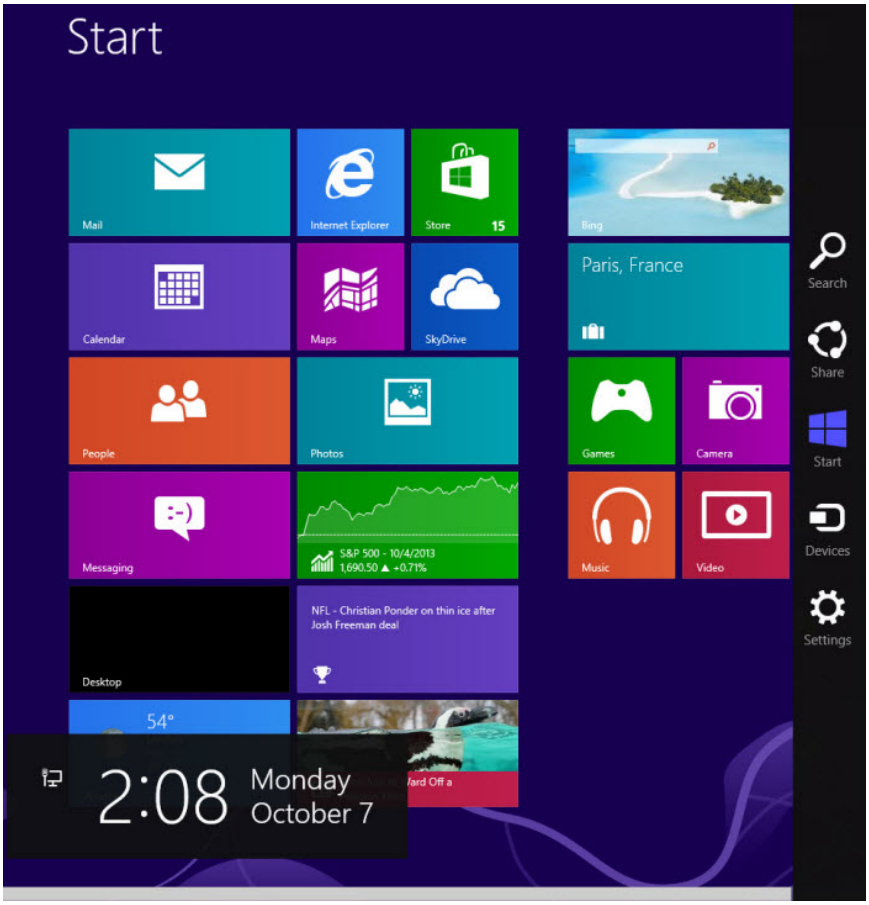
Remove the Scanning Tool only after the lights on the USB device have finished flashing.

For Windows 8

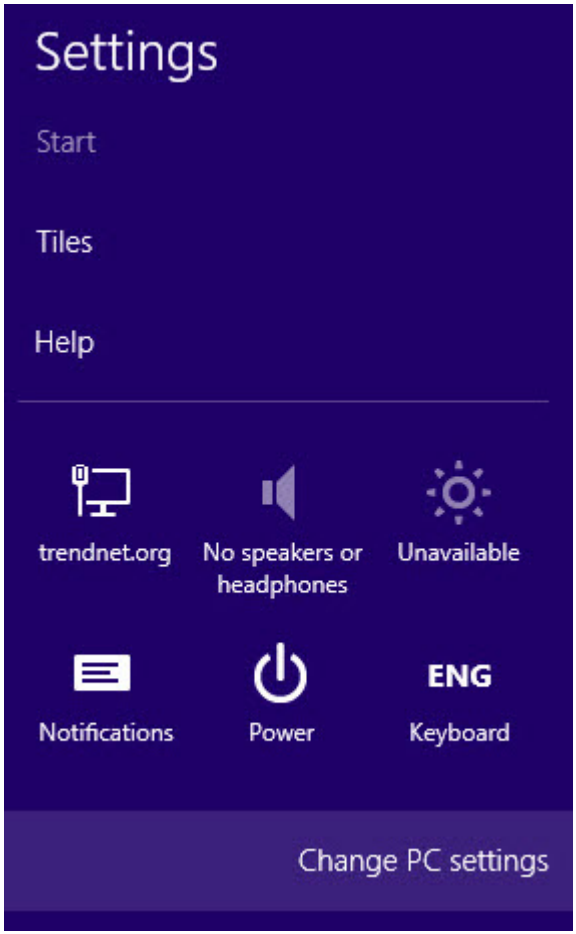
From the Windows 8 desktop, you can follow the same steps as the ones in *Windows 7 on page 4-36*. You can also follow the steps below to remove the tool from the Modern UI.

Procedure

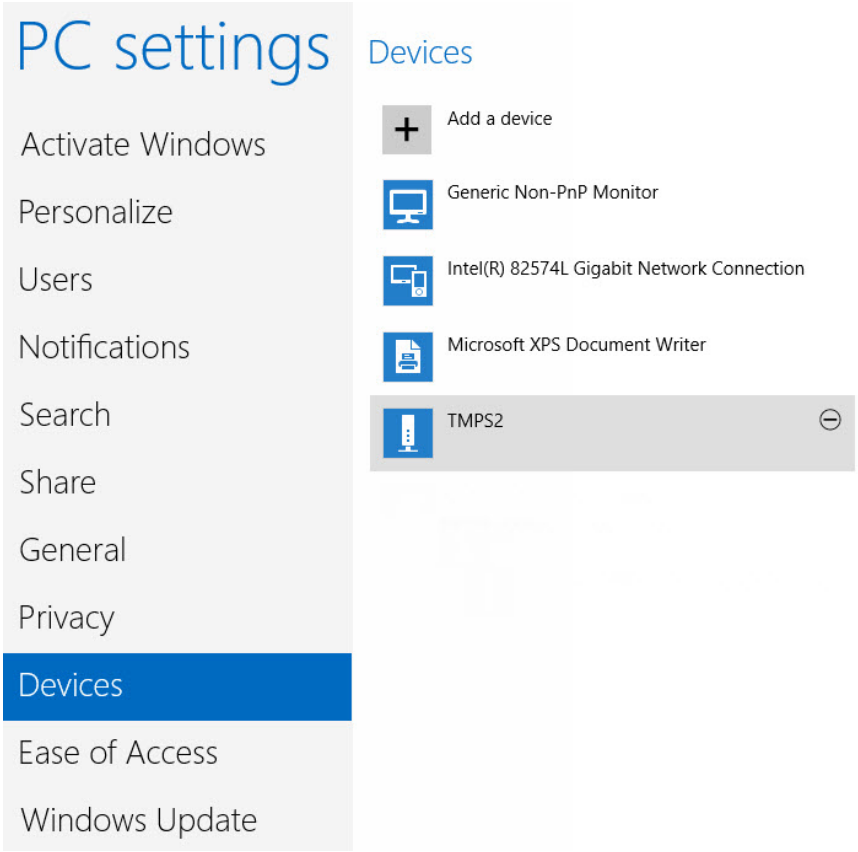
1. From the Windows 8 Start screen, point to the right part of the screen to bring out the available charms.



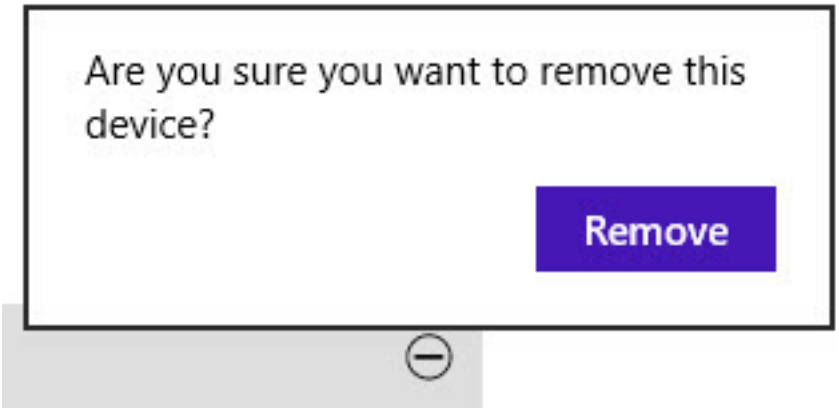
2. Click **Settings**.



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.



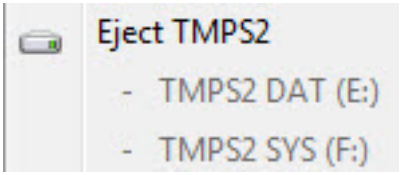
6. Click **Remove**.

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**.

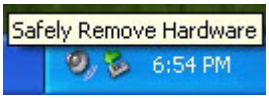


4. Unplug the Scanning Tool from the computer.

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.

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

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. Standalone Scanning Tool users have to copy the support tool folder from the USB device to their computer.

Features:

- *Debug on page 5-2*
- *Reset Device on page 5-9*
- *Support Updates on page 5-14*
- *Convert Logs on page 5-18*
- *Uninstallation on page 6-4*

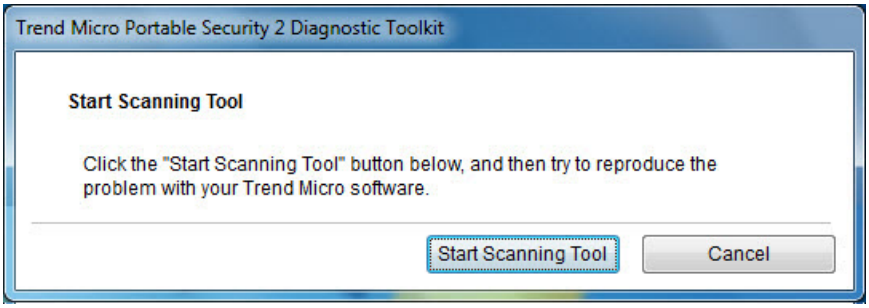
Debug

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

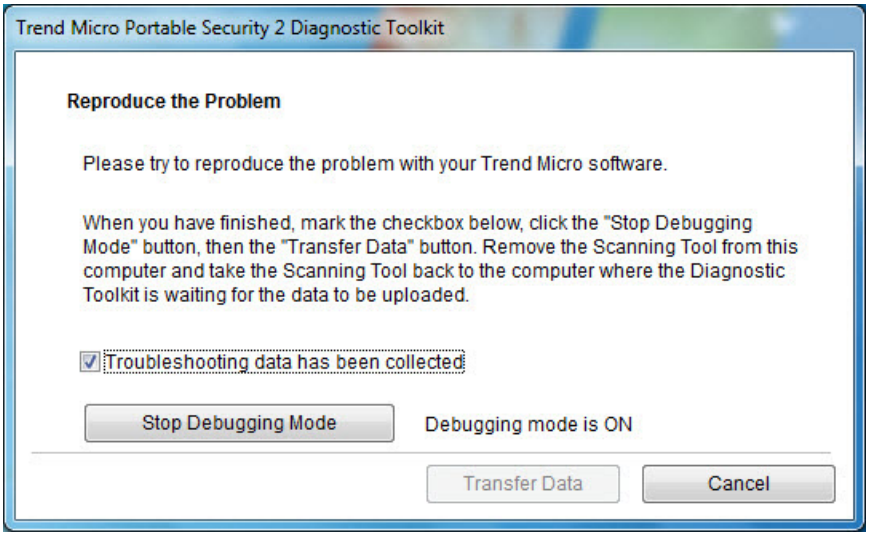
Generating Debug Logs (Scanning Tool)

Procedure

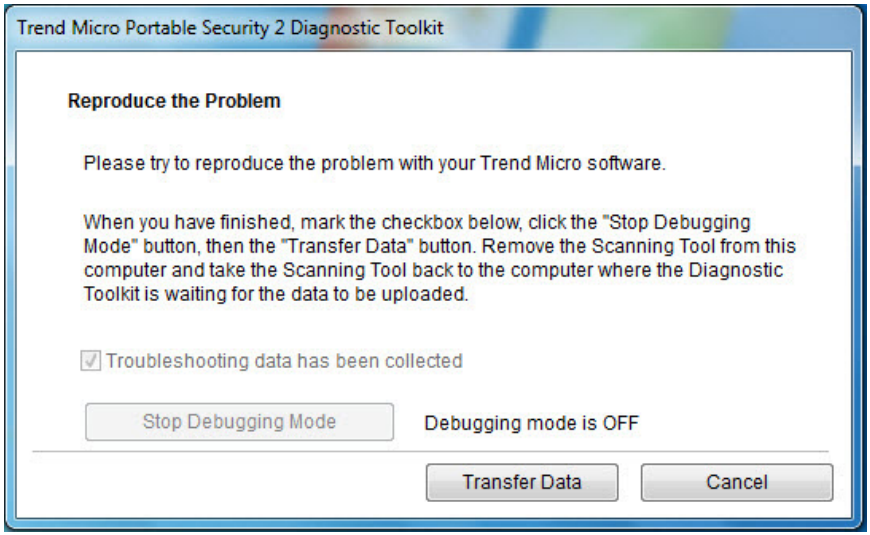
1. Plug-in the Trend Micro Portable Security 2 Scanning Tool to the computer.
2. Double-click the `SmallDebugTool.exe` file ().



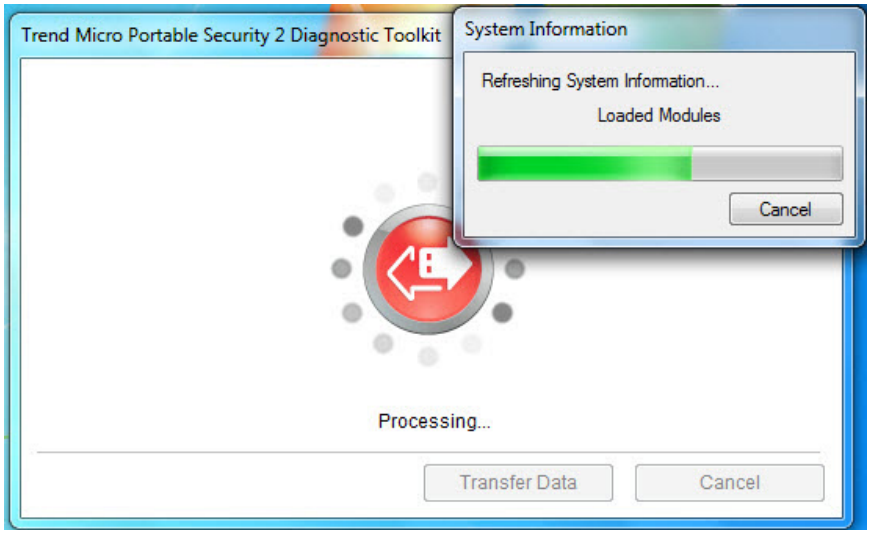
3. Click the **Start Scanning Tool** button.
4. Reproduce the issue.
5. Enable the check box to gather troubleshooting data.



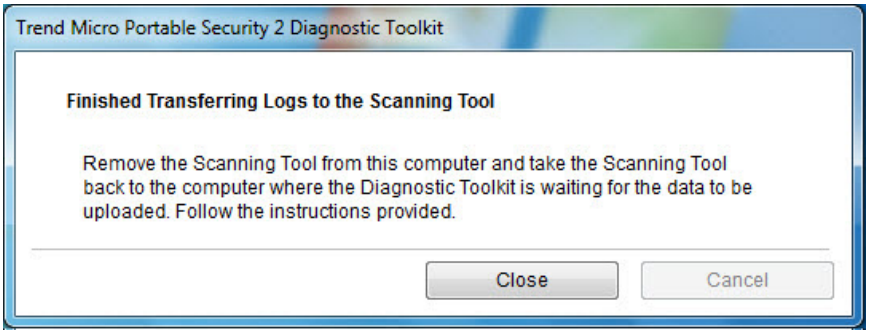
6. Click **Stop Debugging Mode**.



7. Click **Transfer Data**.



8. Click **Close**.



Collecting Debug Logs from the Standalone Scanning Tool

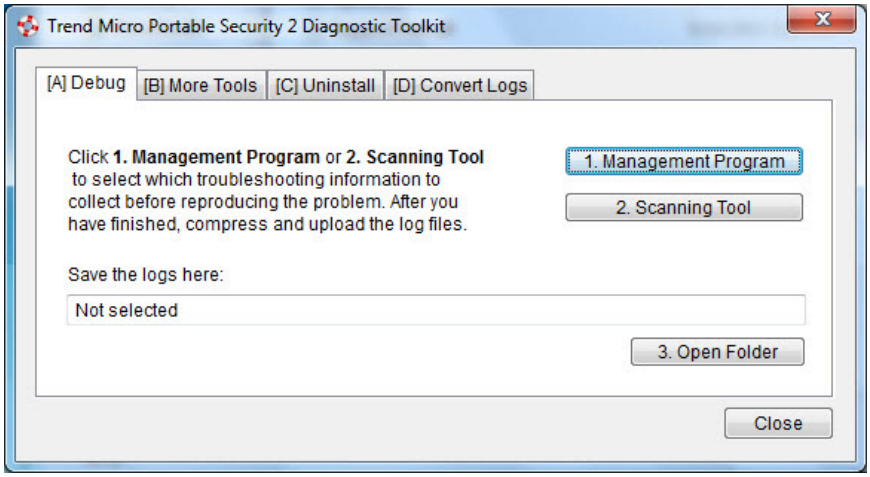
Use the Trend Micro Portable Security 2 Diagnostic Toolkit to collect debug logs from standalone scanning tools.

Procedure

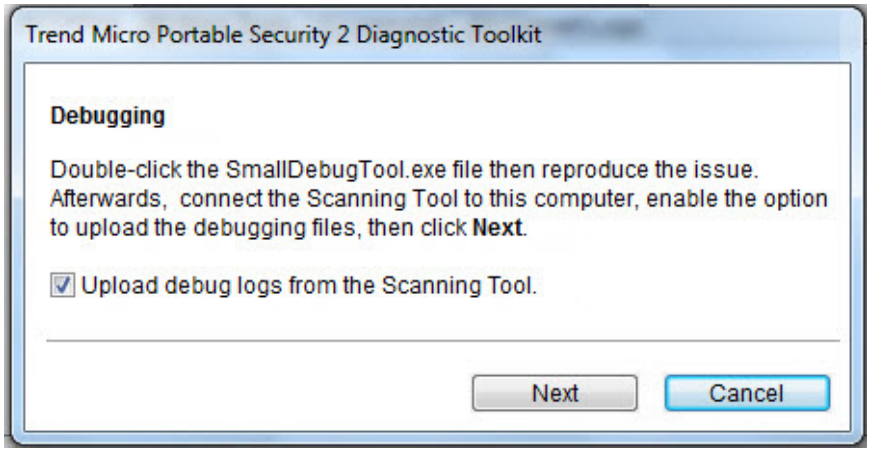
1. *Collect debug logs from the Scanning Tool on page 5-2*.
2. Copy the `SupportTool` folder from the USB device into your local drive.
3. Double-click the `TMPSSuprt.exe` file ()l.

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.



4. In the **Debug** tab, click the **2. Scanning Tool** button.



5. Enable the **Upload debug logs from the Scanning Tool** option.
6. Click **Next** > **Finish**.

7. Click the **3. Open Folder** button and make sure that there is a zipped file with a set of debug logs.

Collecting Debug Logs from the Management Program

Use the Trend Micro Portable Security 2 Diagnostic Toolkit to collect debug logs from the management program computer.

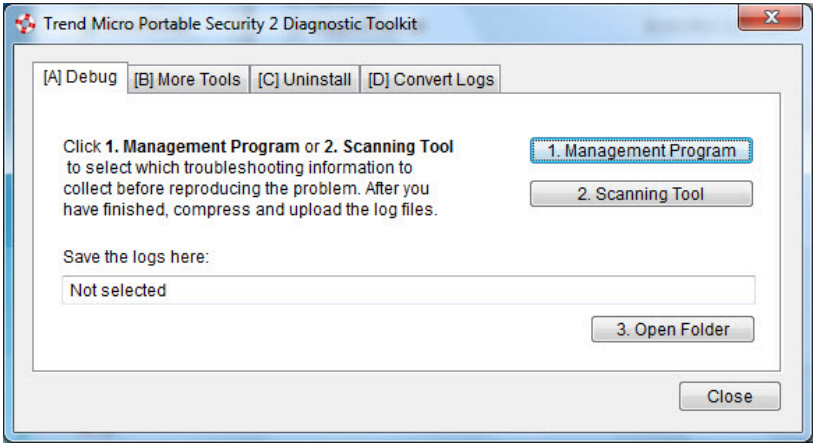
Procedure

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.

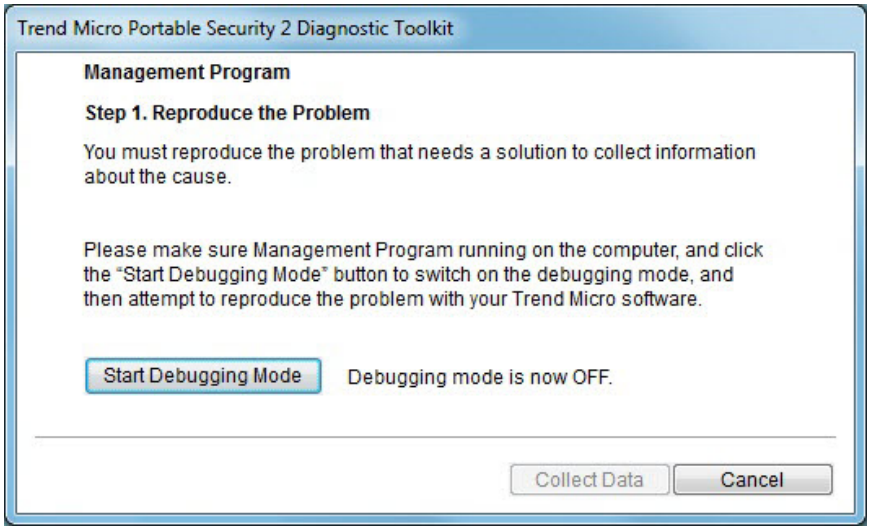
   b. Copy the `SupportTool` folder from the USB device into your local drive.

   c. Double-click the `TMPSSuprt.exe` file ( ).

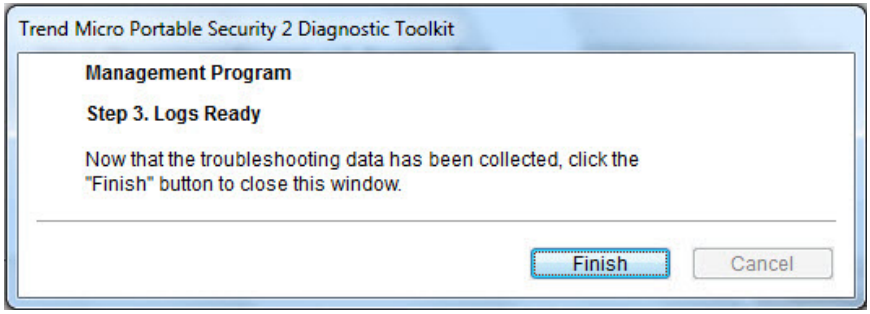


2. In the **Debug** tab, click the **1. Management Program** button.

3. Click the **Start Debugging Mode** button.



4. Reproduce the issue on the Management Program.
5. Click the **Stop Debugging Mode** button.
6. Click the **Collect Data** button.



7. Click **Finish**.

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.

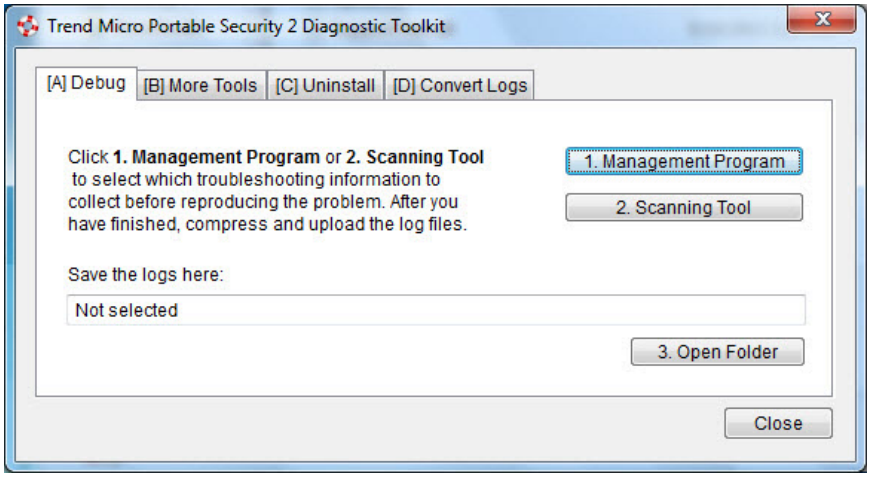
Note

You can only reset one device at a time.

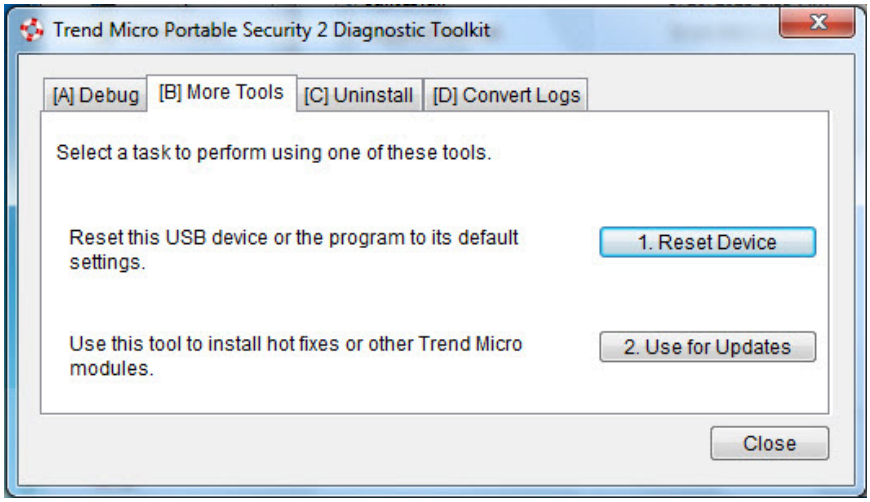
Resetting the Program

Procedure

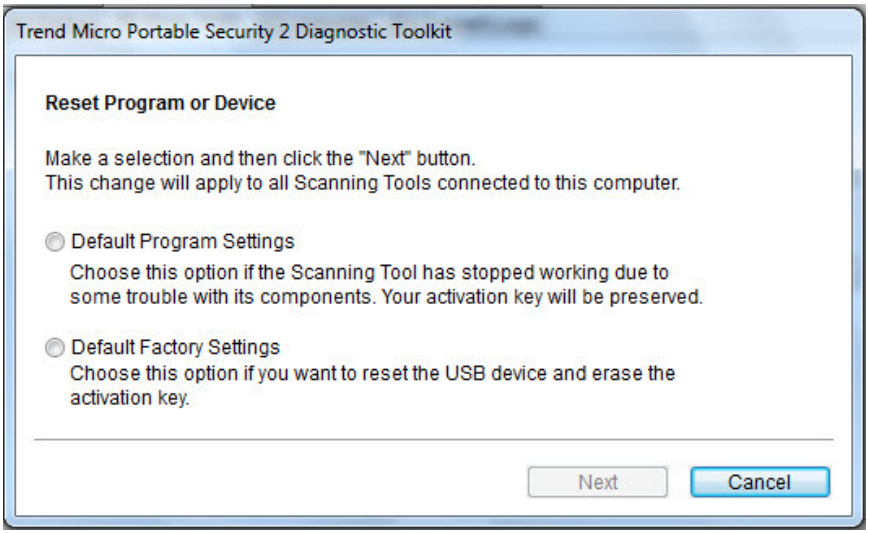
1. Plug-in the Trend Micro Portable Security 2 Scanning Tool to the computer.
2. Copy the `SupportTool` folder from the USB device into your local drive.
3. Double-click the `TMPSSuprt.exe` file ().



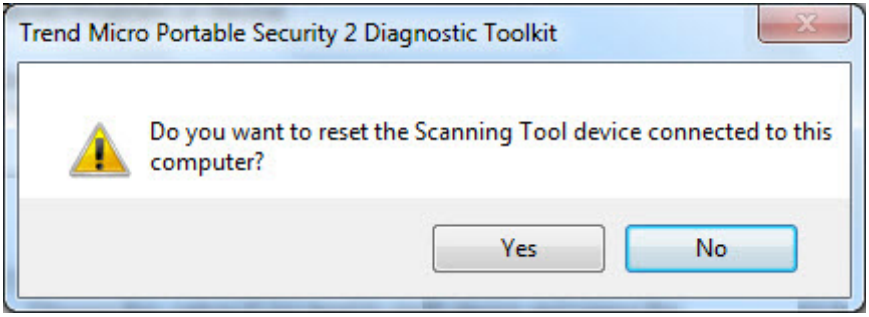
4. Go to the **More Tools** tab.



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



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



7. Confirm the reset.

Note

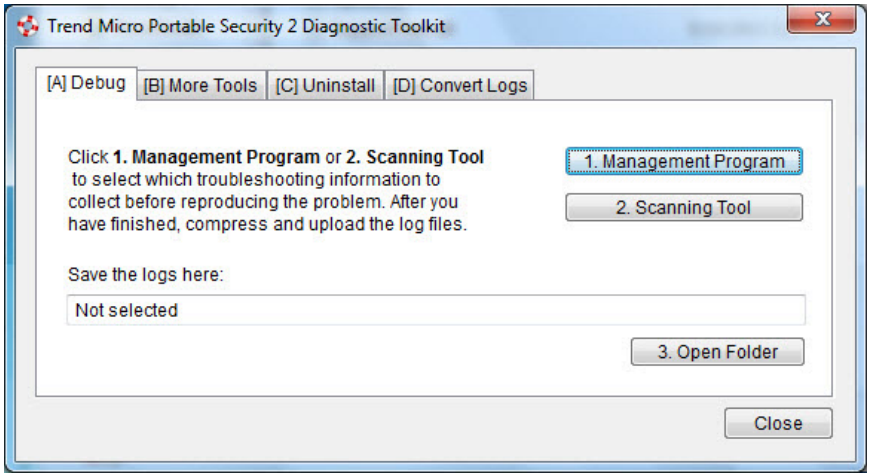
Do not unplug the Scanning Tool until the reset process has completed and a popup appears stating **You have successfully reset the device** appears.

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

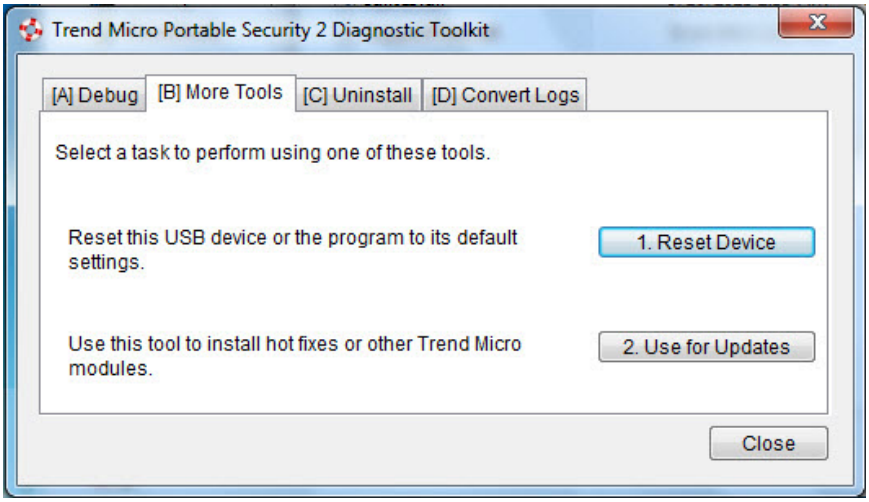
Resetting the Device

Procedure

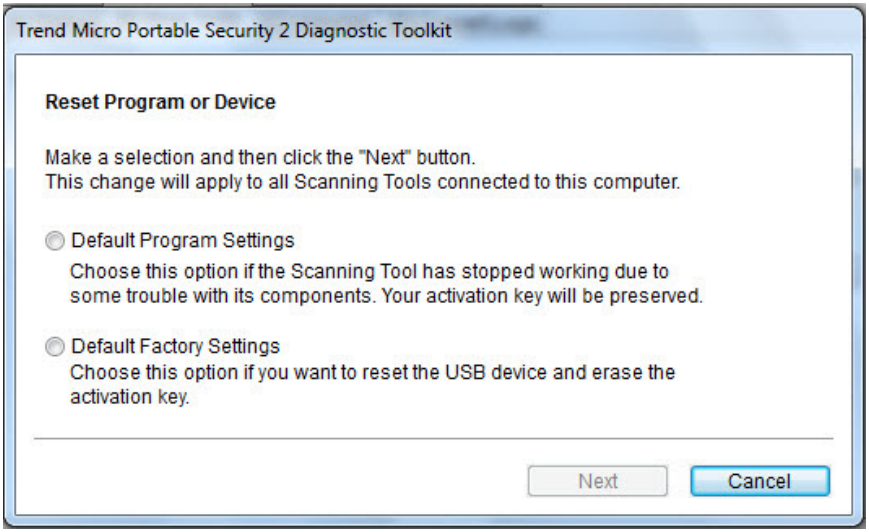
1. Plug-in the Trend Micro Portable Security 2 Scanning Tool to the computer.
2. Copy the `SupportTool` folder from the USB device into your local drive.
3. Double-click the `TMPSSuprt.exe` file ( ).



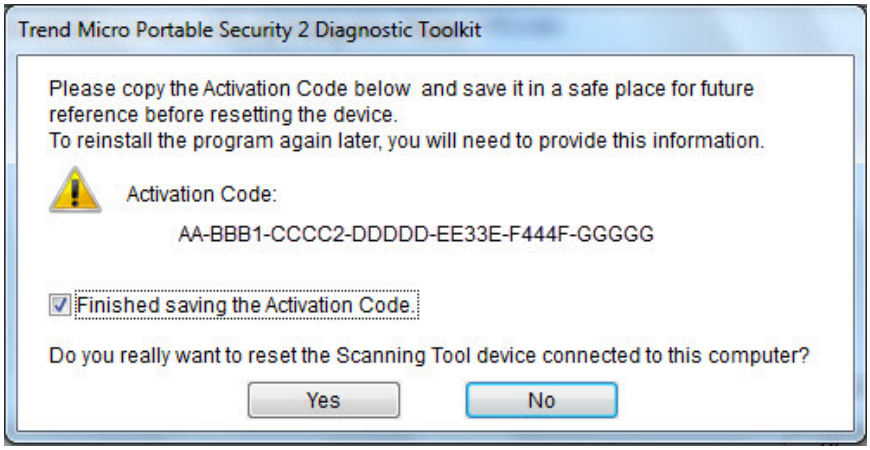
4. Go to the **More Tools** tab.



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.

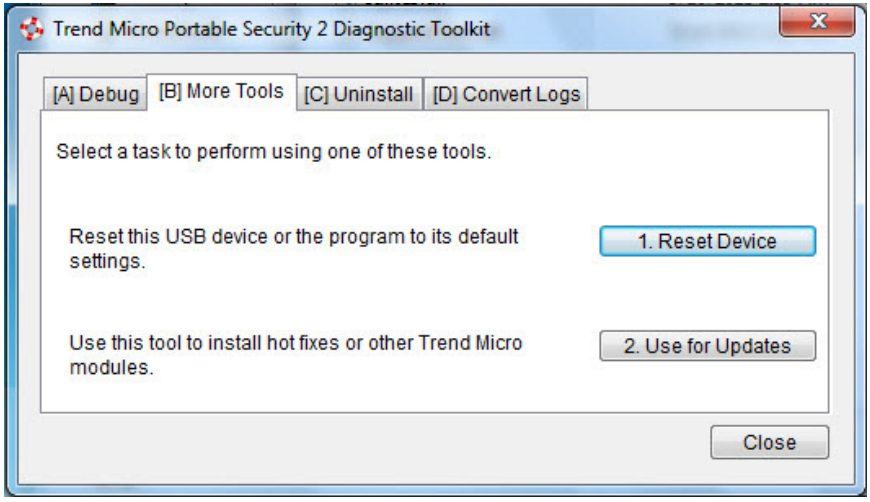
WARNING!

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

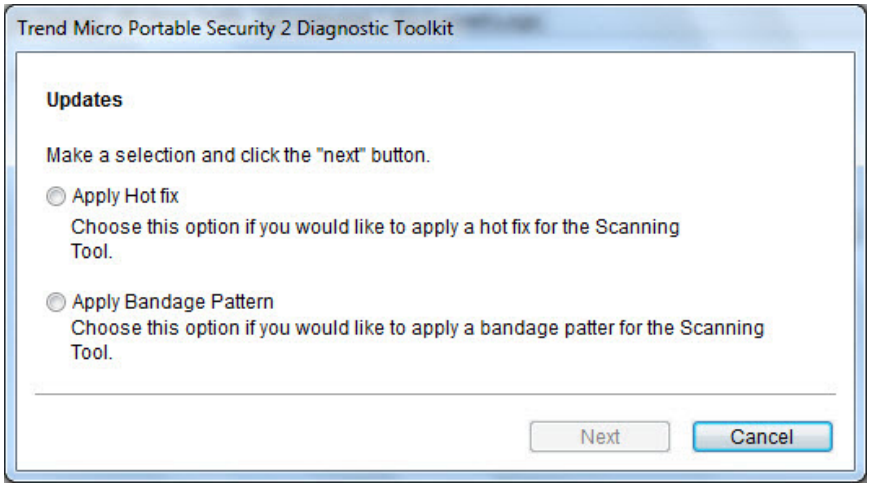
1. Copy the `SupportTool` folder from the USB device into your local drive.
2. Open the Trend Micro Portable Security 2 Diagnostic Toolkit console.
3. Go to the **More Tools** tab.

The **More Tools** tab opens.



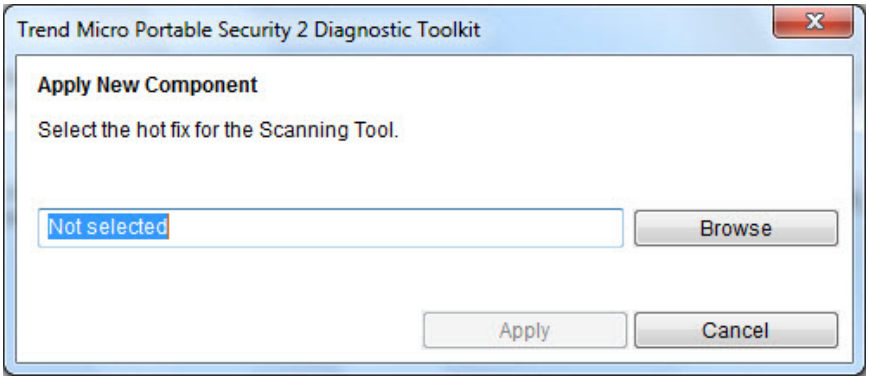
4. Click the **Use for Updates** button.

   The **Updates** window opens.



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

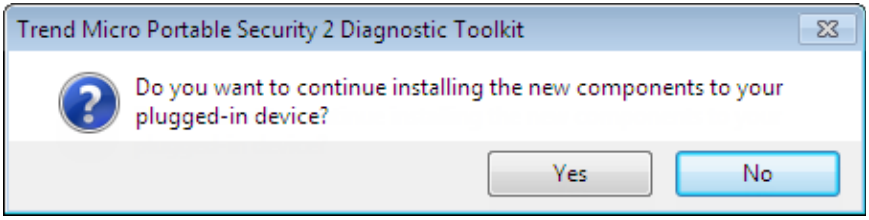
   The **Apply New Components** window opens.



6. Select the hot fix file provided by Trend Micro.

7. Click **Apply**.

   A confirmation window opens.



8. Click **Yes**.

   The **Apply to Next Device** window appears.

9. Repeat steps 6 to 8 if you have to apply the hot fix to another device.

10. Click **Done** if you have finished applying the hot fix to all applicable devices.

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.
5. 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 Microsoft Windows. 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.

To use rescue disk, do the following:

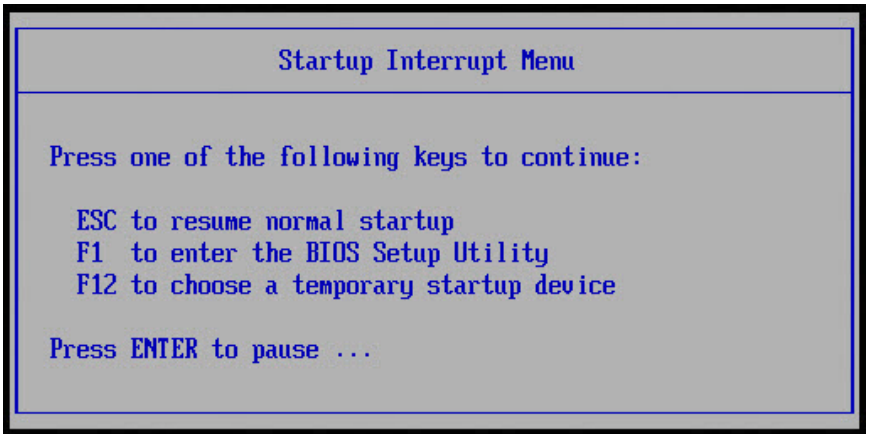
1. *Preparation on page 5-19*

2. *Using the Rescue Disk on page 5-21*
3. *Scanning on page 5-24*

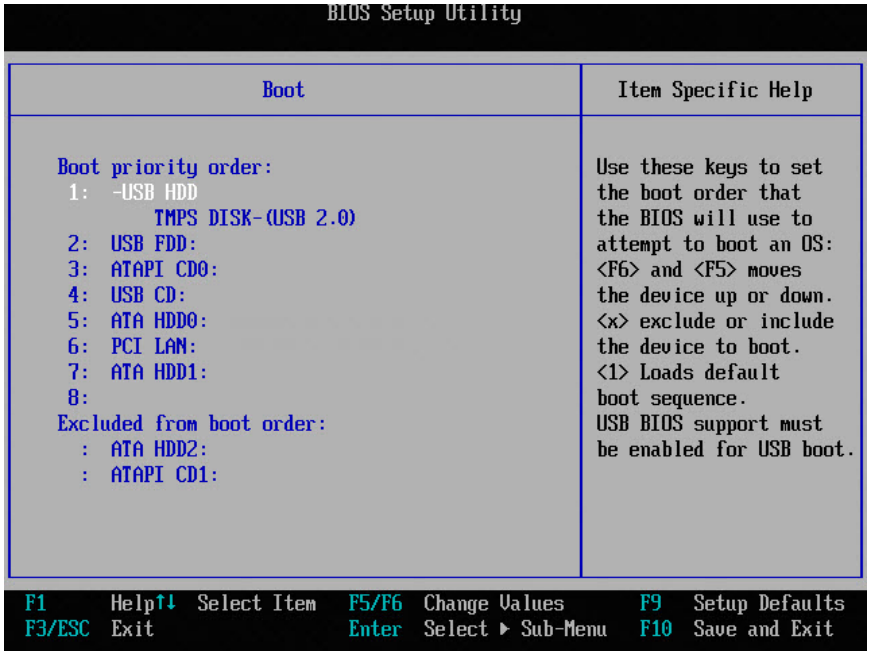
Step 1: Preparation

Procedure

1. Insert the USB device into the computer.
2. Restart the computer.
3. When the computer powers up again, open the BIOS Setup Utility.

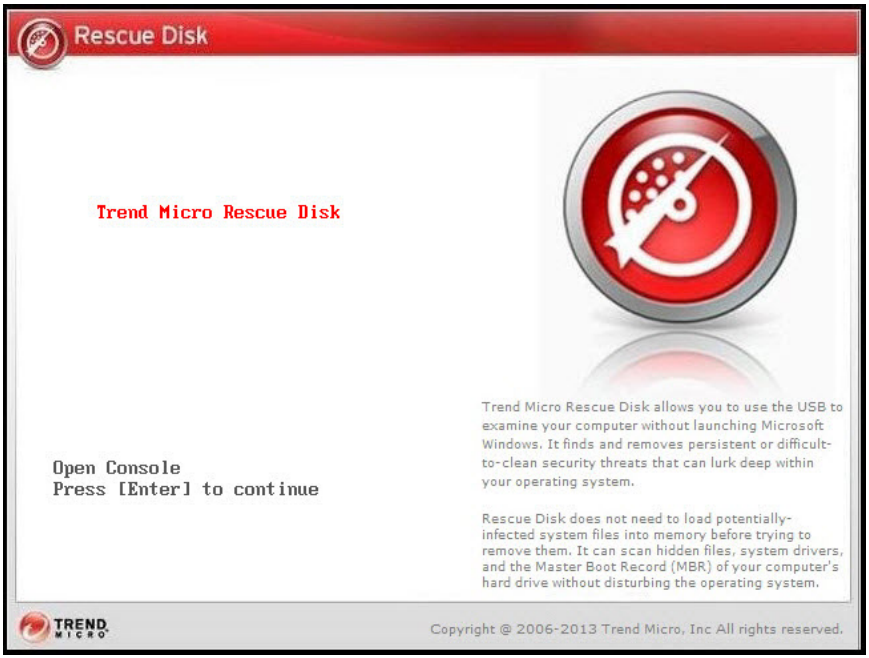


4. Look for Boot, Boot Order, or Boot Options in the menu and change the First Boot Device to the USB device.



5. Exit the menu.

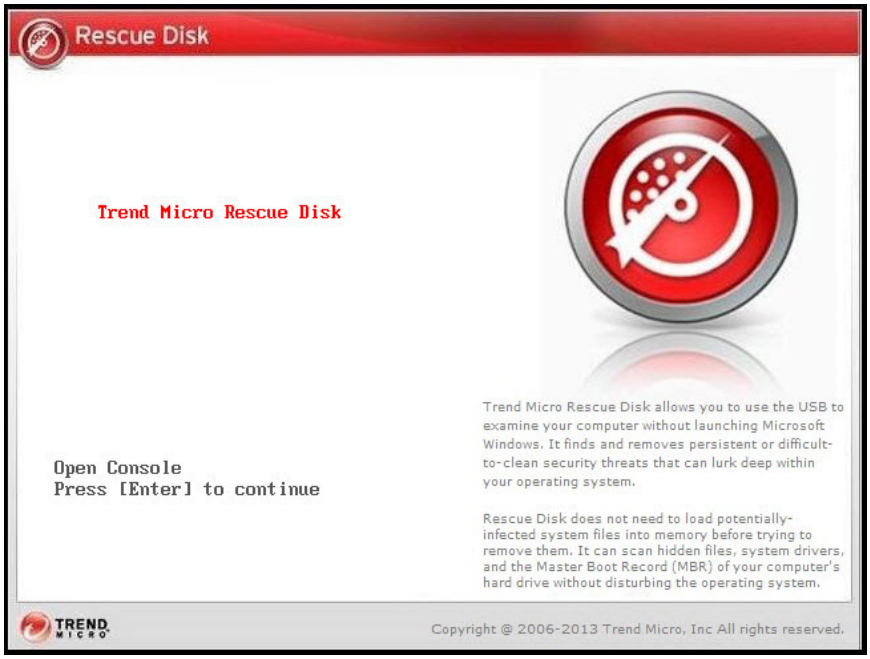
Trend Micro Rescue Disk should automatically open after restarting.



Step 2: Using the Rescue Disk

Procedure

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

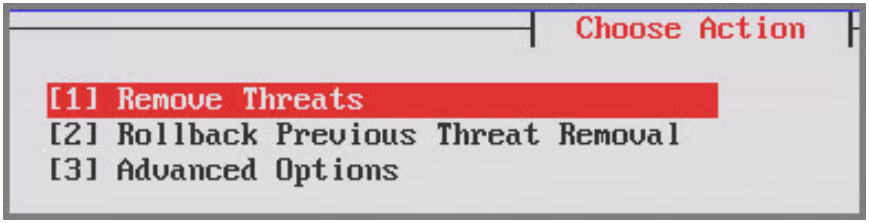


2. Press the **Enter** key or wait for a while.

The **Confirm Disk Log** window appears.

3. Select **Yes**.

   The **Choose Action** window appears.

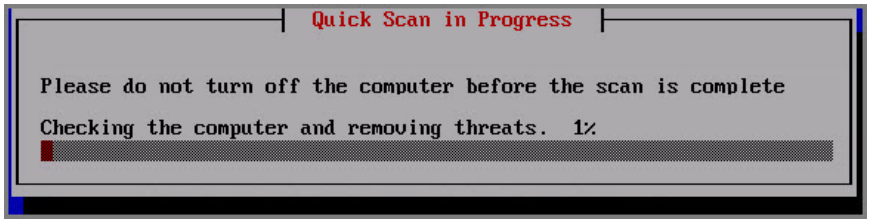


4. Select **[1] Remove Threats**.

The **Remove Threats** window appears.

5. Select **[1] Quick Scan** or **[2] Full Scan**.

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



6. After completing the scan, the screen will show **Please remove the USB from the drive then press [Enter] key to restart the machine**.

7. Remove the Scanning Tool from the computer and then press the **Enter** key to restart the computer.

Step 3: Scanning

Procedure

1. After the computer restarts, sign into Windows.

2. Plug the Scanning Tool into the computer you just scanned with Rescue Disk.

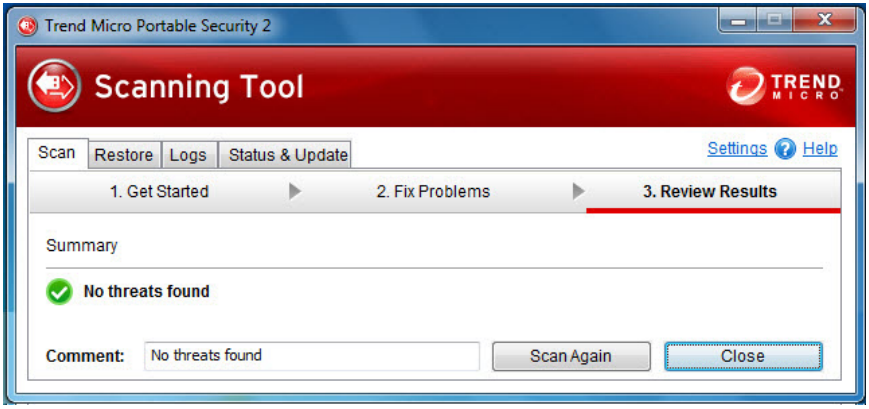
3. Open Windows Explorer and double-click `Launcher.exe` from the `TMPS2_SYS` partition to open the Scanning Tool console.

   The Scanning Tool automatically start scanning the computer.

Important

Do not skip this step. If you close the Scanning Tool console without scanning, Rescue Disk will not be able to save the logs in the Scanning Tool.

4. After completing the scan, close the Scanning Tool console.



   Wait while Rescue Disk automatically saves the logs in the Scanning Tool.

5. *Transfer the collected logs from the Scanning Tool to the Management Program on page 3-40*.

6. *Check the logs on page 3-31*.

Chapter 6

Uninstallation

This chapter describes Trend Micro Portable Security 2™ uninstallation methods.

Topics in this chapter:

Uninstallation

You can use 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.

Option A: From the Windows Start Menu

Procedure

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

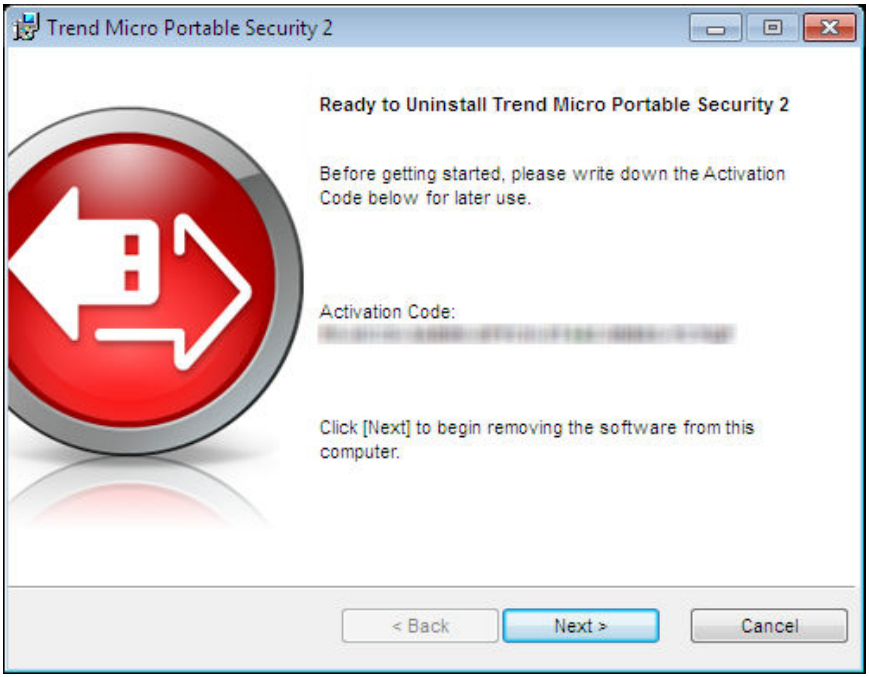
   

   Note

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

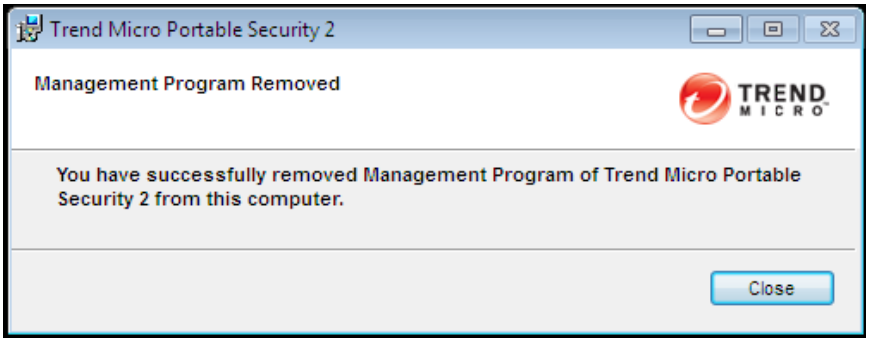
2. Select **Uninstall Trend Micro Portable Security 2**.

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)

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, make sure to follow the Removing the Scanning Tool instructions on *Removing the Scanning Tool on page 4-32*, or else the data may become corrupted.

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/complianceandenforcement/ListsToCheck.htm

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.

Technical Support

Activating and registering Trend Micro Portable Security 2 qualifies you to receive a variety of support services.

The Trend Micro support website provides the latest information on security threats. Please visit it if you have found a security threat, or if you would like to learn more about the support services available.

http://esupport.trendmicro.com/

The content of support services is subject to change without notice. Please contact Trend Micro if you have any questions. You can reach the support center by telephone, FAX, or email. The Trend Micro website lists contact numbers for different regions worldwide.

Support is available for a period of one year once you have completely finished activating your software, although this policy may differ for some licenses.

Please make sure to renew your subscription before it expires. If you do not renew your subscription, you will no longer receive security pattern file and scan engine components. For details on how to renew your subscription, contact Trend Micro or an authorized reseller.

Important

You must activate the Scanning Tool before using it. Refer to *Activating Managed Devices on page 2-7* or *Activating a Standalone Tool on page 2-9* for more information.

About Trend Micro

As a global leader in cloud security, Trend Micro develops Internet content security and threat management solutions that make the world safe for businesses and consumers to exchange digital information. With over 20 years of experience, Trend Micro provides top-ranked client, server, and cloud-based solutions that stop threats faster and protect data in physical, virtualized, and cloud environments.

As new threats and vulnerabilities emerge, Trend Micro remains committed to helping customers secure data, ensure compliance, reduce costs, and safeguard business integrity. For more information, visit:

http://www.trendmicro.com

Contacting Trend Micro

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

Address	Trend Micro, Inc. 10101 North De Anza Blvd., Cupertino, CA 95014
Phone	Toll free: +1 (800) 228-5651 (sales) Voice: +1 (408) 257-1500 (main)
Fax	+1 (408) 257-2003
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

TrendLabs

TrendLabs℠ is a global network of research, development, and action centers committed to 24x7 threat surveillance, attack prevention, and timely and seamless solutions delivery. Serving as the backbone of the Trend Micro service infrastructure, TrendLabs is staffed by a team of several hundred engineers and certified support personnel that provide a wide range of product and technical support services.

TrendLabs monitors the worldwide threat landscape to deliver effective security measures designed to detect, preempt, and eliminate attacks. The daily culmination of these efforts is shared with customers through frequent virus pattern file updates and scan engine refinements.

Learn more about TrendLabs at:

http://cloudsecurity.trendmicro.com/us/technology-innovation/experts/index.html#trendlabs

Third-party Licenses

License Attributions

==========

This product includes or may include the following:

Google Protocol Buffers License Agreement

==========

Copyright 2008, Google Inc.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT

(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Code generated by the Protocol Buffer compiler is owned by the owner of the input file used when generating it. This code is not standalone and requires a support library to be linked with it. This support library is itself covered by the above license.

jsoncpp License Agreement

==========

Copyright (c) 2007-2010 Baptiste Lepilleur

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

libCURL License Agreement

==========

COPYRIGHT AND PERMISSION NOTICE

Copyright (c) 1996 - 2013, Daniel Stenberg, <daniel@haxx.se>.

All rights reserved.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

libmd5-rfc License Agreement

==========

Copyright (C) 2002 Aladdin Enterprises. All rights reserved.

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

libxml2 License Agreement

==========

Copyright (C) 1998-2003 Daniel Veillard. All Rights Reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE DANIEL VEILLARD BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of Daniel Veillard shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization from him.

mongoose License Agreement

==========

Copyright (c) 2004-2010 Sergey Lyubka

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE

WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

OpenSSL License Agreement

==========

Copyright (c) 1998-2008 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

   "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

   "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

==========

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

*/

Original SSLeay License

==========

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.

This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

   The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

   "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT

OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

Expat XML Parser License Agreement

==========

Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd and Clark Cooper

Copyright (c) 2001, 2002, 2003, 2004, 2005, 2006 Expat maintainers.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

zlib License Agreement

==========

Copyright (C) 1995-2004 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

TREND MICRO INCORPORATED

10101 North De Anza Blvd. Cupertino, CA., 95014, USA

Tel:+1(408)257-1500/1-800 228-5651 Fax:+1(408)257-2003 info@trendmicro.com

www.trendmicro.com

Item Code: TPEM26430/140512