



TREND MICRO™

Titanium™ 2013

Product Guide

Titanium Antivirus+

Titanium Internet Security

Titanium Maximum Security

Titanium Premium Security

US V1.2

Trend Micro, Inc.
10101 N. De Anza Blvd.
Cupertino, CA 95014
T 800.228.5651 / 408.257.1500
F 408.257.2003

www.trendmicro.com

Consumer Technical Product Marketing



Trend Micro Incorporated reserves the right to make changes to this document and to the product described herein without notice. Before implementing the product, please review the readme file and the latest version of the applicable user documentation.

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

Copyright © 2012 Trend Micro Inc., Consumer Technical Product Marketing. All rights reserved.

Trend Micro™ Titanium™ 2013 - Product Guide provides help for analysts, reviewers, and customers who are evaluating, reviewing, or using Trend Micro™ Titanium™ Antivirus+; Trend Micro™ Titanium™ Internet Security; or Trend Micro™ Titanium™ Maximum Security.

This Product Guide can be read in conjunction with the following documents, available at <http://esupport.trendmicro.com/en-us/home/pages/technical-support.aspx>.

Product Guides

- *Trend Micro™ Titanium™ Internet Security for Mac 2.0 - Product Guide*
- *Trend Micro™ Mobile Security 2.6 - Product Guide*
- *Trend Micro™ DirectPass™ 1.3 - Product Guide*
- *Trend Micro™ Online Guardian for Families 1.5 - Product Guide*
- *Trend Micro™ SafeSync™ for Consumer 5.1 - Product Guide*
- *Trend Micro™ SafeSync™ for Business 5.1 – Product Guide*

Whitepaper

- *Trend Micro Titanium 2013 and the Windows Firewall*

At Trend Micro, we are always seeking to improve our documentation. If you have questions, comments, or suggestions about this or any Trend Micro documents, please contact the author at or provide feedback at docs@trendmicro.com. You can also evaluate this document on the following web site:

DOCUMENT PROFILE:

Product: Trend Micro™ Titanium™ 2013 (6.0)

Document Title: Trend Micro™ Titanium 2013 - Product Guide

Document Filename: PG - Trend Micro Titanium 2013 - Product Guide US v1.2

Document Release Date: October 26, 2012

Team: Consumer Technical Product Marketing

Product Guide: Michael Miley, Consumer TPM Manager, michael_miley@trendmicro.com

Table of Contents

Chapter 1: Introduction to Titanium.....	5
Key Features of Titanium 2013	7
System Requirements	8
North America - Availability	9
Contacting Trend Micro.....	9
Consumer Support Line	9
Free Phone, Email and Chat support.....	9
Premium Services.....	9
Chapter 2: Installing and Activating Trend Micro Titanium.....	10
Installing Titanium on Windows 7	10
Installing Titanium on Windows 8	14
Installing Titanium on an Infected Computer and Cleaning Up	21
Using Rescue Disk for Severe Malware Removal	23
Chapter 3: Titanium Overview	28
Quick Start: The Titanium Console	28
Quick Start: Conducting On-Demand Scans	29
Quick Start: Viewing Threat Security Reports	34
Chapter 4: Trend Micro Titanium Antivirus+	37
Protection Overview	37
Getting Started > Additional Protections.....	40
Virus & Spyware Controls: Scan Preferences	41
Virus & Spyware Controls: Schedule Scans	44
Internet & Email Controls: Web Threats Trend Micro Toolbar	45
Internet & Email Controls: Spam & Emailed Files	46
Internet & Email Controls: Network Firewall Booster and Wi-Fi Protection	47
Internet & Email Controls: Instant Messaging	48
Exception Lists: Programs/Folders.....	49
Exception Lists: Websites	51
Exception Lists: Wireless Connection.....	52
Other Settings: System Startup	53
Other Settings: Network Settings	54
Other Settings: Smart Protection Network	55
Other Settings: Password	56
Other Settings: Background Picture.....	57
PC/Mobile: Rescue Disk.....	60
Privacy: Facebook Privacy Scanner	61
Privacy: Social Networking Protection.....	67
Chapter 5: Trend Micro Titanium Internet Security	72
Protection Overview	72
PC/Mobile: System Tuner.....	74
Security Report: System Tuner	80
Data: Data Theft Prevention	81
Data: Secure Erase.....	83
Family: Parental Controls	85

Security Report: Parental Controls	96
Chapter 6: Trend Micro Titanium Maximum and Premium Security	98
Protection Overview	98
Data: Trend Micro Vault	100
Chapter 7: Titanium Help and Support	106
Chapter 8: Applications Bundled with Titanium	111
Introduction	111
Mobile Security	112
Titanium Internet Security for Mac	113
Online Guardian	114
DirectPass	115
SafeSync	116
Chapter 9: Windows 8 Applications	118
SafeGuard Browser	118
Security Center	124
Go Everywhere	129
About Trend Micro	134

Chapter 1: Introduction to Titanium

With enhanced social networking security, Trend Micro™ Titanium™ makes it easy for you to protect yourself and your family. It features:

- A friendly interface - a snap to install and use
- Simple screens and reports – easy to read and understand
- Set-and-forget security – won't annoy you with excessive alerts and pop-ups

With three primary versions to choose from and a premium package that extends you protection on more devices you're sure to find the Internet security you need within your budget.

- **Trend Micro™ Titanium™ Antivirus+** - our entry-level product provides essential protection for netbooks, laptops, and entry level computers.
- **Trend Micro™ Titanium™ Internet Security** – our midrange product provides advanced protection with superior performance.
- **Trend Micro™ Titanium™ Maximum Security** – our high-end product provides all-in-one security for everything you and your family do online and includes cloud storage and protection for mobile devices.
- **Trend Micro™ Titanium™ Premium Security**—our high-end product is enhanced with more storage in the cloud and protection for five devices for the fully connected family or small office.

Each edition of Titanium meets the most stringent tests, qualifying it as a leading security product in each category.

- **Stronger protection**—Titanium's core technologies provide state-of-the-art protection from a wide variety of threats.
- **Better performance**—With the help of Trend Micro's revolutionary Smart Scan technology, which utilizes in-the-cloud reputation services along with an intelligent client, Titanium scans faster, uses less CPU, and has a smaller footprint in memory and on disk than competing security products.
- **Easier to use**—Titanium's user interface is uncluttered, easy to use, and specifically designed for the consumer market.

In addition, you are invited to try the products bundled with Titanium, (available variously with the different editions), to deepen protection for all aspects of your digital life.

- **Titanium™ Internet Security for Mac**—Extends your protection to the Macintosh, compatible with Mountain Lion OS.
- **Mobile Security**—Extends your protection to mobile devices, including Android and iOS.
- **Online Guardian**—Secures your family's internet use with enhanced monitoring and protection for your children.
- **DirectPass™**—Provides secure password management across all your devices.
- **SafeSync™**—Provides sync and backup to the cloud for all your devices.

Available from the Windows App Store

- **Micro™ SafeGuard** is a secure browser for Windows 8 that has security technology built right in. It provides you with a safer browsing experience by including safe search results ratings, social networking security, and more. Browse the web without worry with Trend Micro SafeGuard.
- **Trend Micro™ Security Center** delivers current information about malware outbreaks in your area, offering insights into dangerous websites and malicious file downloads to avoid near you. For Trend Micro™ Titanium™ customers, it also provides up-to date information about your protection status. Surf the web knowing your protection is current and what sites to avoid with Trend Micro Security Center.
- **Trend Micro™ Go Everywhere** protects your Windows 8 tablet from loss or theft. Locate your tablet if lost or stolen with just one click. You can find your missing device on a worldwide Google map or sound a 1-minute alarm. Wherever you misplaced your tablet, Trend Micro Go Everywhere has got you covered.

Key Features of Titanium 2013

Table 1. Titanium 2013 - Key Features

TITANIUM 2013 – Key Features Pink shaded areas are new for that edition. Premium Security provides more sync/backup space in the cloud.	Titanium Antivirus+	Titanium Internet Security	Titanium Maximum Security	Titanium Premium Security
Essential Protection				
Core AV Protection	✓	✓	✓	✓
Rootkit Detection and Removal	✓	✓	✓	✓
Rescue Disk	✓	✓	✓	✓
Web Threat Protection	✓	✓	✓	✓
Anti-Spam	✓	✓	✓	✓
Anti-Phishing	✓	✓	✓	✓
Search Results Ratings	✓	✓	✓	✓
Windows Firewall Booster	✓	✓	✓	✓
Block Malicious Links in Email and IM	✓	✓	✓	✓
Authenticate Wi-Fi Networks and Hotspots	✓	✓	✓	✓
Social Networking Security	✓	✓	✓	✓
Data Protection & Privacy				
Data Theft Prevention		✓	✓	✓
Secure Erase		✓	✓	✓
System Tuner		✓	✓	✓
Facebook Privacy Scanner	✓	✓	✓	✓
Trend Micro Vault with Remote File Lock			✓	✓
DirectPass			✓	✓
SafeSync			5GB	25GB
Family Protection				
Parental Controls with App Blocking		✓	✓	✓
Online Guardian			✓	✓

Table 2. Titanium 2013 - Key Features (Continued)

TITANIUM 2013 – Key Features Pink shaded areas are new for that edition. Premium Security provides more sync/backup space.	Titanium Antivirus+	Titanium Internet Security	Titanium Maximum Security	Titanium Premium Security
Platform Protection				
Trend Micro SafeGuard for Window 8*	✓	✓	✓	✓
Trend Micro Security Center for Windows 8*	✓	✓	✓	✓
Trend Micro Go Everywhere for Windows 8*			✓	✓
Mobile Security for Android			✓	✓
Seat Options / 1 and 2 year subscriptions	1, 3, 5, 10	1, 3, 5, 10	1, 3, 5, 10	5
*Available from the Windows App Store				

System Requirements

Table 3. Trend Micro™ Titanium System Requirements

System Requirements	Minimum Specifications
Processor	350 MHz (800 MHz recommended) for the Windows® XP Family 800 MHz (1 GHz recommended) for the Windows Vista® Family 800 MHz (1 GHz recommended) for the Windows® 7 Family 1 GHz for the Windows® 8 Family
Memory	256 MB (512 MB recommended) for the Windows® XP Family 512 MB (1 GB recommended) for the Windows Vista® Family 1 GB for the Windows® 7 Family 1 GB for the Windows® 8 32-bit Family 2 GB for the Windows® 8 64-bit Family
Operating System	Windows® XP Family (32-bit only) SP3 or higher Windows Vista® Family (32 or 64-bit) SP2 or higher Windows 7® Family (32 or 64-bit) Windows 8® Family (32 or 64-bit)
Disk Space	500 MB (600 MB recommended)
Other Requirements	Specifications
Web browser	Microsoft® Internet Explorer® 7.0, 8.0, 9.0, and 10.0 Mozilla® Firefox® 13.0 or previous versions still supported by Mozilla® (not required) Google Chrome™ 20.0 or previous versions still supported by Google (not required)
Display	High-color display with a resolution of 800x480 pixels or higher
PDF Reader	Any
Internet Connection	Broadband or equivalent high speed connection highly recommended
Note: Trend Micro™ Titanium™ Maximum Security can support RAID 0 (Striping) or RAID 1 (Mirroring)	

Table 4. Trend Micro™ Titanium Internet Security for Mac System Requirements

Operating System	CPU	Memory	Disk Space
Mac OS [™] version 10.8 “Mountain Lion”	Apple [™] Macintosh [™] computer with Intel [™] processor	512 MB	400 MB
Mac OS [™] version 10.7 “Lion”		1 GB Recommended	
Mac OS [™] version 10.6 “Snow Leopard”			
Mac OS [™] version 10.5 “Leopard”			

North America - Availability

September 10, 2012

Contacting Trend Micro

Trend Micro Incorporated
10101 North De Anza Blvd.
Cupertino, CA 95014
Tel: (408) 257-1500 or (800) 228-5651
Fax: (408) 257-2003

info@trendmicro.com

www.trendmicro.com

Further information is available at <http://us.trendmicro.com/us/about/index.html>

Consumer Support Line

(800) 864-6027

Monday - Friday, 5:00AM - 8:00PM Pacific

Free Phone, Email and Chat support

Trend Micro also offers free phone, email, and chat support. For more information, contact eSupport at:

http://esupport.trendmicro.com/support/consumer/consumerhome.do?locale=en_US

You can also contact the Trend Community at:

<http://community.trendmicro.com/>

Premium Services

Trend Micro provides Titanium users with Premium Services for a wide variety of technical issues including installation, virus and spyware removal, PC Tune-ups, etc. These services are offered as a bundle with a purchase of Titanium or as stand-alone and ad-hoc services. For more information, select ? > **Premium Services** in the **Titanium Console**, or go to

<http://www.trendmicro.com/us/home/products/support-services/index.html>

Chapter 2: Installing and Activating Trend Micro Titanium

Trend Micro™ Titanium™ has separate installs for each version of the product:

- Trend Micro™ Titanium™ Antivirus+
- Trend Micro™ Titanium™ Internet Security
- Trend Micro™ Titanium™ Maximum Security

Titanium™ Premium Security simply extends Maximum Security by increasing your sync and backup storage capacity.

In the examples below we install Titanium Maximum Security, but each version of Titanium has an identical installation and activation process.

Installing Titanium on Windows 7

To install Titanium on Windows 7 using a Download or a CD:

By Download:

1. Go to <http://www.trendmicro.com/us/home/products/titanium/index.html> to download Titanium 2013.
2. Click **Free Trial** or **Buy Now** for the edition you wish to download, then follow the instructions for the free or purchased download.
3. When the **Download** page appears, click **Save File**. The download process begins and presents a **TrendMicro Downloader** dialog.
4. Select **Save As** and navigate to the folder where you'll put the **Downloader**, then click **Save**.
5. When the download completes, click **Open Folder** (in IE), then double-click the **Downloader**.

By CD:

6. Insert your Titanium CD. The autorun process launches the installer.

Note: The install process is the same from this point on.

7. In Windows 7 (and Vista), a **User Account Control** pop-up dialog appears, asking if you want to allow the installation program to make changes to the computer.

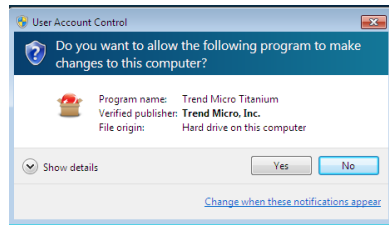


Figure 1. User Account Control

8. Click **Yes**. The **Downloader** will complete the download and begin the installation, unpacking the file and giving you a progress screen.

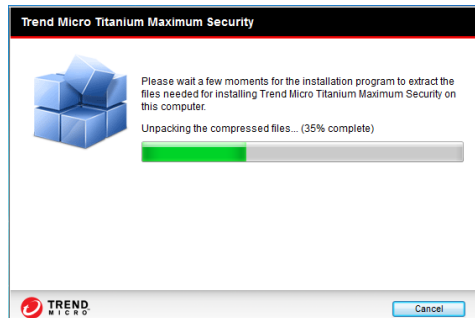


Figure 2. Titanium - Unpacking Files

9. It will check if your computer meets the minimum system requirements and do a quick malware scan. When the process completes, a screen appears asking you to **Choose Your Version**.

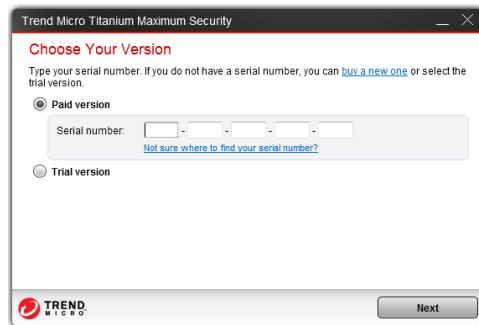


Figure 3. Choose Your Version

10. If you're installing a **Paid version**, enter the **serial number** provided by Trend Micro on the CD envelope or inside the confirmation email received after your online purchase.
11. If you're installing a **trial version**, click the **trial version** button.
12. Click **Next**. The **License Agreement** appears.

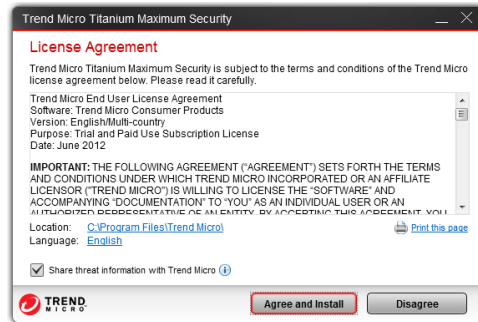


Figure 4. License Agreement

13. Choose among the following:

- Note the item checked by default at the bottom of the screen: **“Share threat information with Trend Micro.”** When new threats attack your computer, this feature provides threat feedback to the Trend Micro™ Smart Protection Network™, improving your protection and that of other Trend Micro users. **Users are strongly urged to leave this checked.** No personal information is collected. If you do not wish to share such threat information, uncheck the checkbox.
- Read the **License Agreement.** (Click **Print this page** to print it out.) If you agree with the License Agreement, click **Agree and Install.**

14. Titanium will begin the installation, copy the necessary files to their proper locations, enable the components, and activate the program. This will take a few minutes. A progress indicator will indicate the stages and progress of the install.



Figure 5. Progress Indicator

15. When the installation is completed, the wizard will indicate **Installation Completed.**

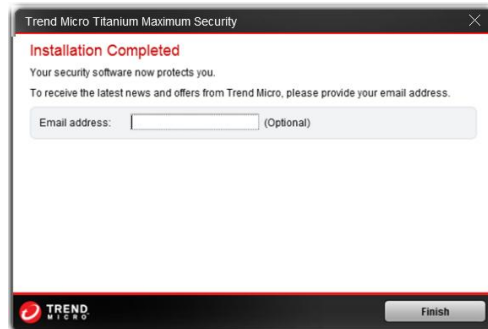


Figure 6. Installation Completed

16. To receive the latest news and offers from Trend Micro, enter your email address and click **Finish**. (An email address may also be required for some trials.) The **Welcome** screen displays.

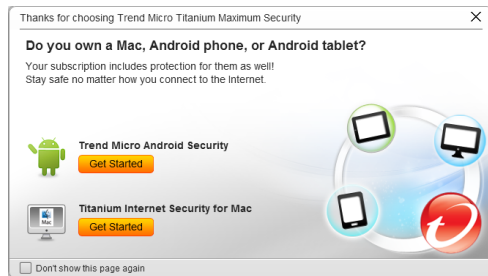


Figure 7. Titanium Welcome (Titanium Maximum – Paid Version)

17. The **Welcome** screen lets you **Get Started** with **Trend Micro Android Security** or **Titanium Internet Security for Mac**. All you need to do is to click the relevant **Get Started** button.

Note: By installing these products, you will be allocating device licenses from your account. For example: if you purchased a three-device license, you can choose to allocate one of these licenses to your Windows PC, one to a Mac, and one to an Android device. Or mix and match to suite your needs. To see how many seats have been allocated and to what device, please visit **MyAccount**.

18. Check the checkbox **Don't show this page again** if you do not wish to see the Welcome screen when you load the **Titanium Console** in the future, then click the **Close** box in the upper right corner to close the Welcome screen. The **Titanium Console** becomes visible.

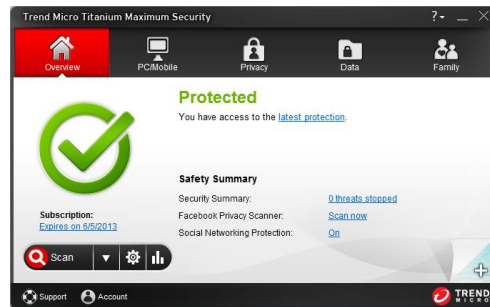


Figure 8. Titanium Maximum Security Console (Paid Version)

19. The features displayed in the **Titanium Console** again depend upon the edition you have installed. The Titanium Console shows threats stopped, lets you execute scans, gives you access to reports, and lets you configure settings, using mouse-clicks from easy-to-use screens. Shown above is the Console for Titanium Maximum Security 2013 (Paid Version). See the following chapters for further details on using the Titanium Console.

Installing Titanium on Windows 8

To install Titanium on Windows 8 using a Download or a CD:

Installing Trend Micro Titanium on Windows 8 is as easy as installing it on Windows 7. Simply follow the instructions below.

Note: For users of Windows 8 smartphones or tablets, “click” instructions below should be read as “tap.”

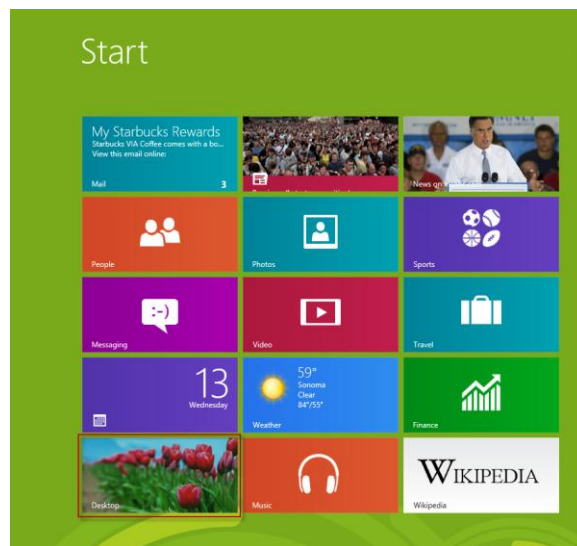


Figure 9. Windows 8

By Download:

1. In the Windows 8 UI, click the **Desktop** icon. Windows 8 toggles to the Desktop.



Figure 10. Windows 8 Desktop

2. Go to <http://www.trendmicro.com/us/home/products/titanium/index.html> to download Titanium 2013.
3. Click **Free Trial** or **Buy Now** for the version you wish to download, then follow the instructions for the free or purchased download.
4. When the **Download** page appears, click the relevant **Download** button. The download process begins and presents a **TrendMicro Downloader** dialog.
5. Select **Save As** and navigate to the folder where you'll put the **Downloader**, then click **Save**.
6. When the download completes, click **Open Folder** (in IE), then double-click the **Downloader**.

By CD:

7. Insert your Titanium CD. The autorun process launches the installer.

Note: The install process is the same from this point on.

8. The Windows 8 **User Account Control** pop-up dialog appears, asking if you want to allow the installation program to make changes to the computer.

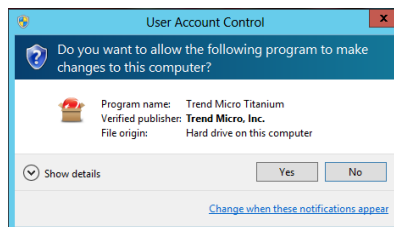


Figure 11. User Account Control

9. Click **Yes**. The **Downloader** will complete the download and begin the installation, unpacking the file and giving you a progress screen.

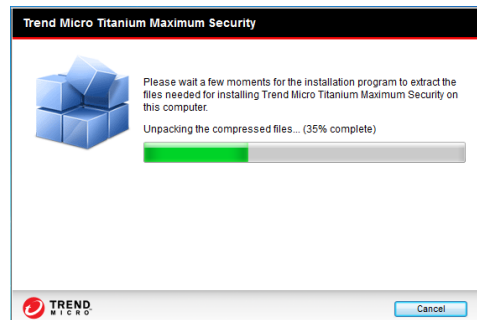


Figure 12. Extracting Files

10. It will then check if your computer meets the minimum system requirements and do a quick malware scan. When the process completes, a screen appears asking you to **Choose Your Version**.

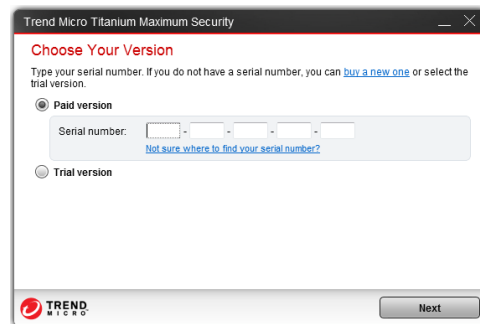


Figure 13. Choose Your Version

11. If you're installing a **paid version**, enter the **serial number** provided by Trend Micro on your retail box or in your confirmation email.
12. If you're installing a **trial version**, click the **trial version** button, then click **Next**. The **License Agreement** appears.

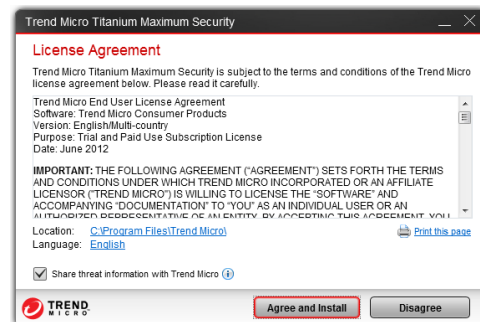


Figure 14. License Agreement

13. Choose among the following:
 - Note the item checked by default at the bottom of the screen: **“Share threat information with Trend Micro.”** When new threats attack your computer, this

feature provides threat feedback to the Trend Micro™ Smart Protection Network™, improving your protection and that of other Trend Micro users. **Users are strongly urged to leave this checked.** No personal information is collected. If you do not wish to share such threat information, uncheck the checkbox.

- Read the **License Agreement**. (Click **Print this page** to print it out.) If you agree with the License Agreement, click **Agree and Install**.
14. Titanium will begin the installation, copy the necessary files to their proper locations, enable the components, and activate the program. This will take a few minutes. A progress indicator will indicate the stages and progress of the install.



Figure 15. Progress Indicator

15. When the installation is completed, the wizard will indicate “Installation Completed.”

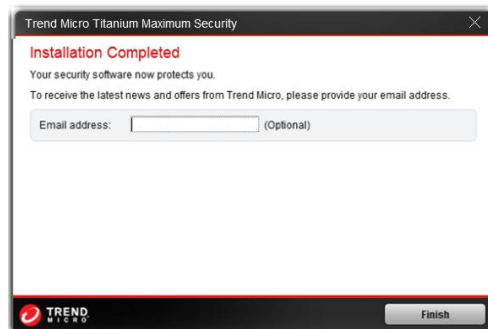


Figure 16. Installation Completed

16. To receive the latest news and offers from Trend Micro, enter your email address and click **Finish**. (An email address may also be required for some Trials.) The **Welcome** screen displays.



Figure 17. Titanium Maximum Security Welcome (Paid Version)

17. Click the **Get Started** buttons to get started with the bundled products. (You can always come back to the Welcome screen later simply by opening the Titanium Console, which also displays the Welcome screen, unless you've chosen to hide it.)

Note: By installing these products, you will be allocating device licenses from your account. For example: if you purchased a three-device license, you can choose to allocate one of these licenses to your Windows PC, one to a Mac, and one to an Android device. Or mix and match to suite your needs. To see how many seats have been allocated and to what device, please visit MyAccount.

18. Check the checkbox **Don't show this page again** if you wish, then click the **Close** box in the upper right corner to close the **Welcome** screen. The Titanium Console becomes visible.

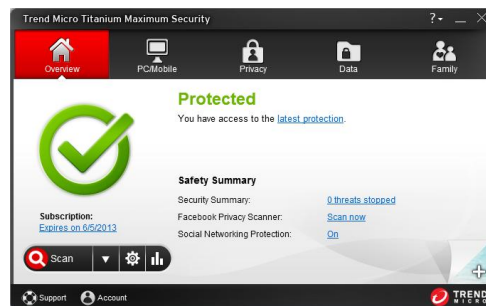


Figure 18. Titanium Maximum Security Console

19. The features displayed in the **Titanium Console** again depend upon the edition you have installed. The Titanium Console shows threats stopped, lets you execute scans, gives you access to reports, and lets you configure settings, using mouse-clicks from easy-to-use screens. Shown above is the Console for Titanium Maximum Security 2013 (Paid Version). See the following chapters for further details.
20. You can access the Titanium Console in Windows 8 Desktop by double-clicking its icon on the desktop, or selecting **Open the Main Console** from the System Tray icon/menu.

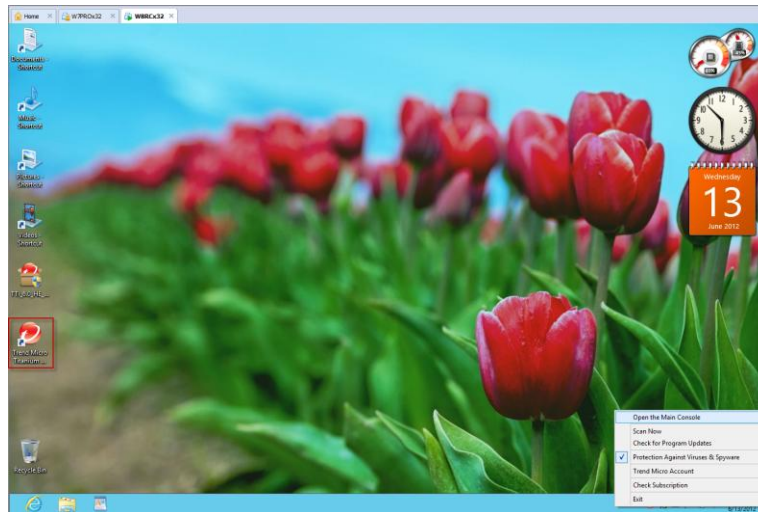


Figure 19. Windows 8 Desktop

21. Toggle back to Windows 8 by tapping the Microsoft Menu key on your keyboard, then scroll to the right to locate the Titanium apps. (Your screen will differ depending upon how many apps you have loaded.)



Figure 20. Windows 8

22. You can click the **Trend Micro Titanium** icon to access the **Titanium Console**. The action will toggle back to Windows 8 Desktop and launch the **Titanium Console**.
23. Once you've finished your installation, Titanium provides a popup that says **Get More Protection** for Windows 8.

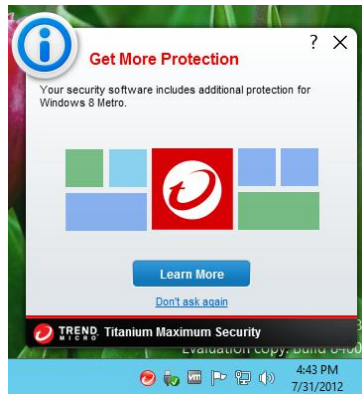


Figure 21. Get More Protection

24. Click **Learn More**. This launches your browser and takes you to the **More Tools** web page, which provides links (among others) to **SafeGuard**, **Security Center**, and **Go Everywhere** in the Windows App Store. (Click **Don't ask again** if you don't wish to see this popup in the future. You can always return to the **More Tools** webpage later by selecting **More Tools** in the ? menu in the upper right-hand corner of the Titanium Console.)



Figure 22. More Tools Web Page

25. Click **Try Now** to try an additional tool, including Windows 8 tools **Trend Micro™ Go Everywhere** and **Trend Micro™ SafeGuard**. **Go Everywhere** lets you locate a missing device on a map or sound a one-minute alarm by remote control to help you find it. The **SafeGuard** browser provides greater security when browsing in Windows 8, providing the cutting-edge protection Titanium users have come to enjoy in their browser.

Installing Titanium on an Infected Computer and Cleaning Up

If Titanium detects malware that's already present on your computer during the install, you may need to change a default setting after installation has finished to obtain the best results for your initial scan and cleanup. Since Titanium chooses a default balance between detection and false positives for the average user, a computer that is already badly infected before Titanium is installed may need to do a more aggressive scan for remediation than is normally required.

To modify Titanium settings for an already-infected computer:

1. Open the Titanium Console and click **PC/Mobile > PC & Internet Security**.



Figure 23. Titanium Maximum Security Console

2. The **Protection Settings** window appears, with **Virus & Spyware Controls > Scan Preferences** selected by default.

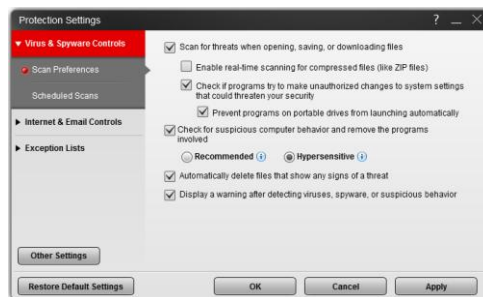


Figure 24. Change to Hypersensitive

3. Click the radio button for **Hypersensitive**.
4. Check **Automatically delete files that show any sign of a threat**.
5. Click **Apply** to apply your changes.
6. Click **OK** to close the **Protection Settings** window.
7. Click the **Overview** tab to return to the main console screen.



Figure 25. Scan > Full Scan

8. Select **Scan > Full Scan** from the **Scan** popup menu. The **Full Scan** begins.



Figure 26. Full Scan in Progress

9. If the scan requires a shut down at the end, reboot your computer.
10. If the scan detects a rootkit that can't be removed using a normal scan, it will prompt you with a message **Additional Cleaning Needed** and provide a button in the **Scan Results** dialog to download an additional tool, i.e., the **Rescue Disk** installer.



Figure 27. Additional Cleaning Needed

11. Click **Get Now** to get it. **Rescue Disk** is also available from the main console. Simply click the **PC/Mobile > Rescue Disk** to connect you to the **Rescue Disk** webpage for downloading.

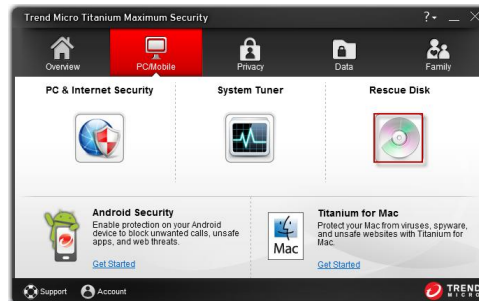


Figure 28. Rescue Disk

12. Instructions for using the **Rescue Disk** are in the following section.

Using Rescue Disk for Severe Malware Removal

Titanium's **Rescue Disk**, available for Titanium through the **Scan Results** dialog or through **PC/Mobile > Rescue Disk**, lets you create a **Rescue Disk** to eliminate rootkits and other hard-to-remove malware from your system. Utilizing Trend Micro's Clean Boot technology, the **Rescue Disk** reboots your computer into a Linux kernel, scans and cleans rootkits and other malware from your system, then reboots back into Windows.

To Create a Rescue Disk for Rootkit Removal:

1. Choose between the following options:
 - If you just conducted a scan and you receive the message in the scan result window "Additional Cleaning Needed," click the **Download Now** button to take you to a **Trend Micro Rescue Disk** web page.
 - OR
 - In Titanium Internet Security or Maximum Security, click **PC/Mobile > Rescue Disk**.
2. Either method launches the **Trend Micro Rescue Disk** web page where you can click the **Download Now** button to download the **Rescue Disk** installer.

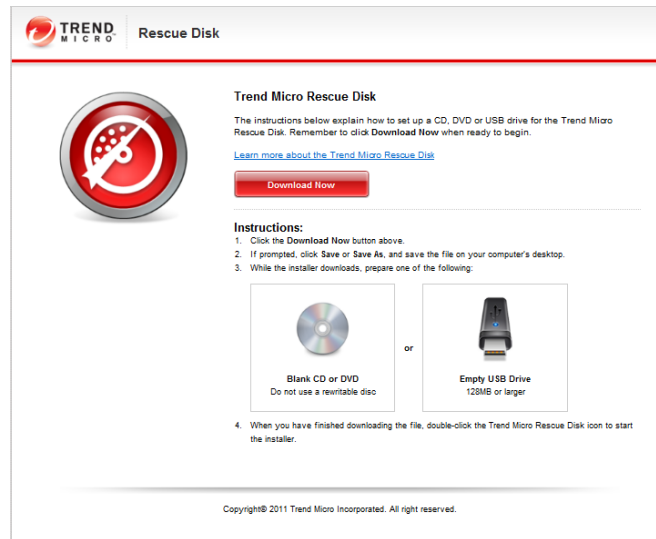


Figure 29. Trend Micro Rescue Disk Download

- Once downloaded, double-click the **Rescue Disk** icon. A security dialog appears, asking if you want to run this program.

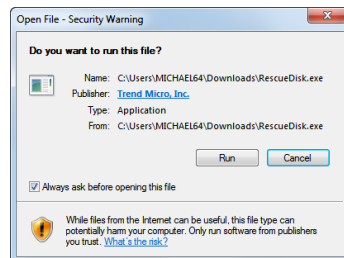


Figure 30. Security Warning

- Click **Run** to continue. The **Rescue Disk License Agreement** appears.



Figure 31. Rescue Disk License Agreement

- Read the license agreement. If you agree, select **I accept the terms of the license agreement** and click **Next**.

- The **Rescue Disk** installer checks online for the most recent version and updates it. A dialog then appears, asking **What kind of Rescue Disk do you want to create?** (USB Device or Blank CD/DVD).



Figure 32. Rescue Disk Types

- In this example, select **Blank CD/DVD**. A device selection dialog appears.



Figure 33. Device Selector

- If you haven't already done so, insert a blank CD/DVD in your drive, close any autorun dialogs, select the CD/DVD burner icon, click **Refresh** if necessary, and click **Create**. A progress dialog appears, showing the drive's progress as it burns the disc.

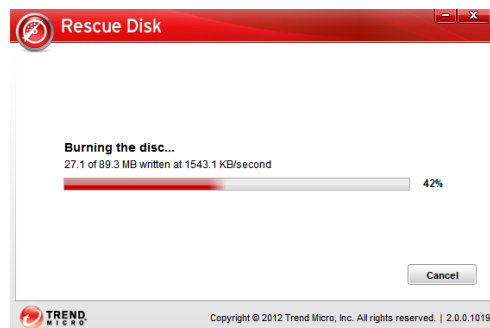


Figure 34. Burning the Rescue Disk

- Once the **Rescue Disk** has been created, you should be notified that disk creation was a success and **Your Rescue Disk is Ready**.



Figure 35. Rescue Disk is Ready

10. Click **Restart Now** to boot from the **Rescue Disk**, (or click **Later** to use the disk later, going through a reboot process after having inserted the disk.)

Note: To use Rescue Disk, you must have previously set up your computer to boot from the CD/DVD Drive first. Most computers are already set to seek the CD/DVD first when booting.

11. When the computer restarts, **Rescue Disk** provides three main options, the first selected by default.
 - **Remove Threats**
 - Quick Scan
 - Full Scan
 - **Rollback Previous Threat Removal**
 - Dates and Times of Previous Removals
 - **Advanced Options**
 - MBR Cleanup (Master Boot Record)
 - MBR Rollback (Master Boot Record)
 - Enter Linux Command Line
12. In this example, leave **Remove Threats** selected, choose **Quick Scan** or **Full Scan**, and allow **Rescue Disk** to scan and remove the threats from your computer.
13. A progress dialog appears, saying “**Please do not turn off computer before the scan is complete. Checking the computer and removing threats.**”
14. Once the scan and clean has completed, the screen provides the results, indicating the threats that have been removed.
15. Click the **Enter** key to restart the computer. A dialog appears, saying “**Are you sure you want to exit?**” with **Cancel** selected by default.
16. Use the left arrow to move the cursor to **Yes** and hit **Enter**. Your computer will eject the CD, so you can remove it.

17. Remove the CD, close the tray, and hit **Enter** again. The will reboot to the Windows Desktop.
18. **Rescue Disk** also lets you roll back the computer to its state before the last threat removal. Just reinsert the **Rescue Disk**, reboot, and when the **Option** window appears, select **Rollback Previous Threat Removal** and the listing you wish to roll back.
19. When **Rescue Disk** is finished rolling back the last threat removal, the eject/reboot process will repeat, rebooting your machine to the Windows desktop.
20. Finally, **Advanced Options** let you do a **MBR Cleanup** of the Master Boot Record or roll an MBR cleanup back. An option also lets you enter the **Linux Command Line**. **MBR Cleanup** must be used with caution, as it can make your computer unbootable.
21. Note that after you've executed a scan using **Rescue Disk**, you can find **Rescue Disk Log** information in the Titanium Log Viewer.

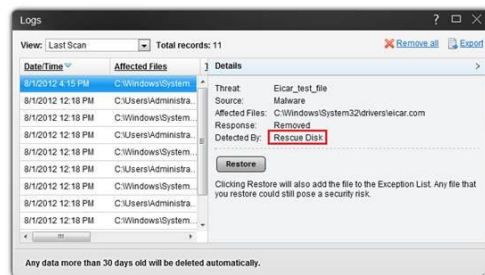


Figure 36. Titanium Rescue Disk Log

Chapter 3: Titanium Overview

In the following chapters, we'll walk through each version of Titanium, explaining the key features provided in each.

Note: If you have a higher-end version of Titanium, you should read the prior chapters devoted to the lower-end versions. The higher-end versions have all the features of their lower-end siblings, but provide additional “premium” features on top of common features.

Quick Start: The Titanium Console

All editions of Titanium provide essentially the same **Titanium Console**, with some functional additions as you step up from **Titanium Antivirus+** to **Titanium Internet Security** and **Titanium Maximum Security**.

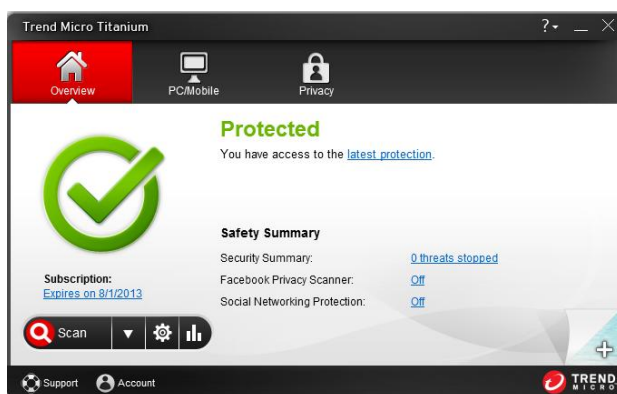


Figure 37. Titanium Antivirus+ Console

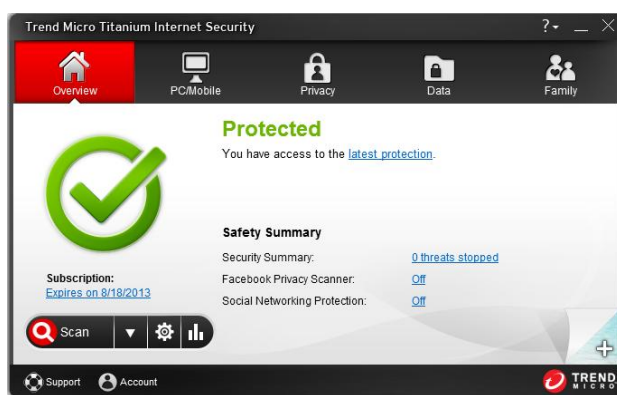


Figure 38. Titanium Internet Security

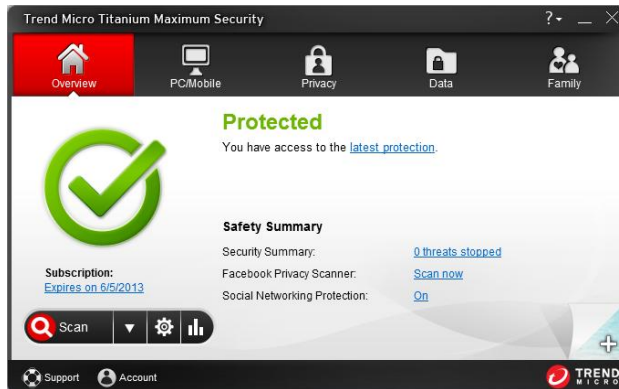


Figure 39. Titanium Maximum Security

All editions of Titanium allow you to scan on-demand or by schedule, and to view security reports. We'll quickly review these features in the following two sections.

Quick Start: Conducting On-Demand Scans

By default, Titanium activates a **real-time scan** when it is installed. This is always present in memory (unless disabled), to proactively protect you from real-time threats. Threats are caught as they try to enter memory or touch the hard drive, preventing infections.

Titanium also provides a **disk scan**—which you can execute on-demand or by schedule—that utilizes Trend Micro revolutionary Smart Scan technology on the client when it scans your hard drive. This references Trend Micro's file reputation services in the cloud—part of the Smart Protection Network—for a shorter "time-to-protect."

Unlike other local-protection-based products that require you to frequently update a large local signature database on your computer, Titanium updates the signature database primarily on Trend Micro Servers in the cloud, so all consumers of the Smart Protection Network are instantly protected whenever the database is updated.

Smart Scan reduces the need to deploy most antimalware signatures on the client, thus reducing network bandwidth usage (for updating/downloading signatures), while saving disk space and memory on the client's computer.

Scanning Your Computer's Disk

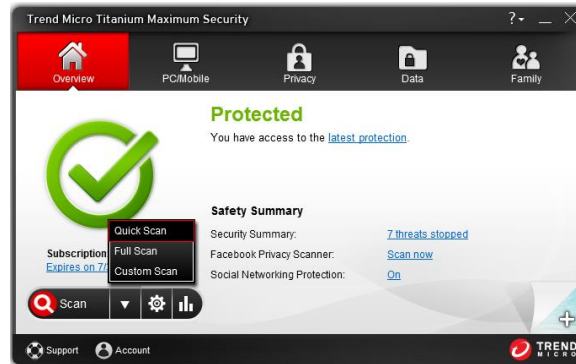


Figure 40. Quick Scan | Scan Menu

To scan your computer disk:

Titanium provides a **Scan Tool** on the console (shown above) which can be used in two ways:

1. Click the spyglass section of the **Scan** tool to execute a **Quick Scan**.
2. Use the **Scan Options** popup menu on the right side of the **Scan** tool to select among the various options:
 - A **Quick Scan** conducts a scan of those directories on your system that are most likely to be infected.
 - A **Full Scan** conducts a full scan of your system.
 - A **Custom Scan** lets you designate which parts of your system you wish to scan.

Quick Scan and Full Scan

To conduct a Quick Scan or a Full Scan:

1. To conduct a **Quick Scan**, click the **Scan** button on the main console, or optionally select **Quick Scan** or **Full Scan** from the **Scan Options** popup menu. A window appears, showing the **Quick** or **Full Scan in Progress** and the percentage completed. Scans can kick off messages when malware is quarantined or deleted.



Figure 41. Quick Scan in Progress

2. You may **Hide**, **Pause**, or **Stop** the scan by clicking the respective button. You may also select **Shut down the computer when this scan is done**.
3. When the scan has completed, a **Scan Results** screen appears, showing **Potential threats found**, as well as **Browser cookies deleted**.



Figure 42. Scan Results

4. Click **What's a cookie?** to obtain a definition of a cookie. The **Definition** screen appears.
5. Click **Details** for more details on the threats found and actions taken. The **Details** screen appears.

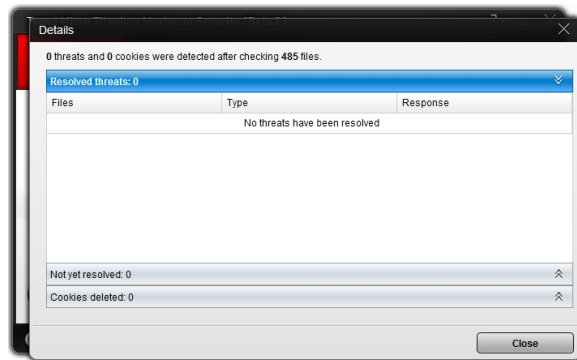


Figure 43. Details

6. Click each of the collapsible panels in turn to show the **Details** tables, which include file names, types, and responses to the threats.
7. Click **Close** to close the **Details** window, then **Close** again to close the **Scan Results** window.

Custom Scan

To conduct a Custom Scan:

1. Choose **Custom Scan** from the **Scan Options** popup menu. A dialog appears, letting you **Select Targets** you wish to scan.



Figure 44. Select Targets

2. Expand the tree by clicking the **+** (**Plus**) signs at any level, then check the checkbox for the chosen target(s).
3. Click **Start Scan** to start the scan.
4. When the scan has completed, the **Scan Results** and **Details** screens appear in the same format as Quick and Full Scans.

Intensive Scan

Titanium performs an **Intensive Scan** whenever a Quick, Full, Custom, or Scheduled Scan detects a high amount of malware on your computer.

Note: In the *real world*, Titanium does not allow a large virus data set to even get onto a user's computer after it has been installed. To obtain this condition artificially, you have to dump a large collection of malware files onto an unprotected system *before you install Titanium*, or you would have to turn off all the proactive features, such as the real-time scan, that would prevent such a large infection from occurring in the first place.

To activate an Intensive Scan on a previously badly infected computer:

1. Click the **Scan > Quick Scan** tool to begin a **Quick Scan**. The **Quick Scan** process begins.



Figure 45. Quick Scan in Progress

2. When the scan detects a large volume of malware, the **Quick Scan** stops and an **Intensive Scan** starts.

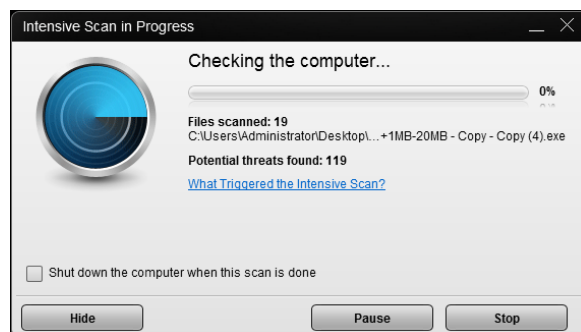


Figure 46. Intensive Scan in Progress

3. Note that the icon changes to indicate that an **Intensive Scan** is in progress. You can get more information about what triggered the scan by clicking **What triggered the Intensive Scan?**

Quick Start: Viewing Threat Security Reports

Titanium allows you to view **Threat Security Reports** at the click of a button. The reports provide a wealth of detail on the dates and types of threats blocked. You can also generate a **Root Cause Analysis Report** to investigate the source of an infection and the effects upon your system.

Note: All versions of Titanium produce a security report for threats that is made up of viruses, spyware, and web threats detected.

To View a Threat Security Report:

1. Click the **Security Report** button on the **Titanium Console**. The **Security Report** screen appears.

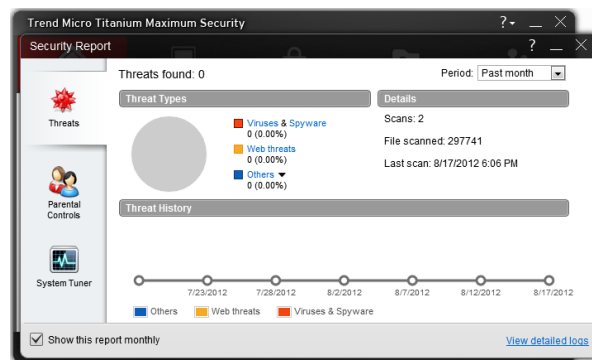


Figure 47. Security Report (Titanium Maximum Security)

2. The **Security Report** provides the following data:
 - **Threats Found** – The number of threats found
 - **Threat Types** are shown in a pie chart by percentage
 - **Details** – Shows number of Scans, number of Files scanned, and Last Scan
 - **Threat History** – A timeline where threat peaks and valleys are graphed
 - A popup shows you the number of threat incidents on a given date
 - Varies to check/uncheck **All**, **Web threats**, **Viruses & Spyware** to filter the **Threat History** graph by your choices
3. Use the **Period** popup menu in the upper right-hand corner to designate the period the report will cover.
4. Check **Show this report monthly** to display the report on a monthly basis at the first of each month. You'll be notified when the report is ready.
5. Select the **View** popup to show log details for that type of threat by **Date/Time**, **Affected Files**, **Threat**, **Source**, and **Response**.

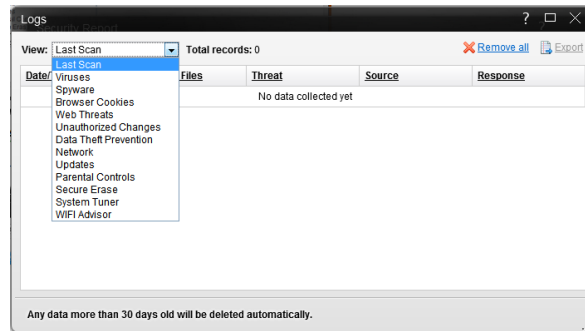


Figure 48. Logs

- Double-click an item in the table to view details on the specific threat.

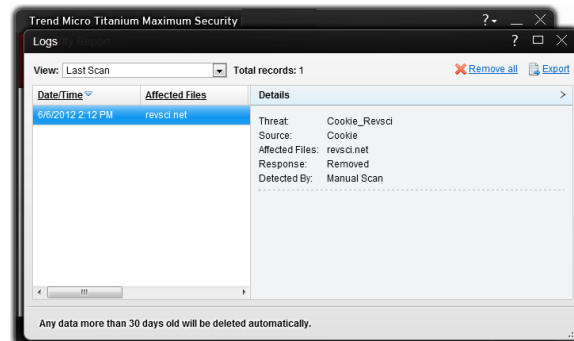


Figure 49. Logs > Item Details

- Click **Remove all** to remove the items from the table.
- Click **Export** in the upper right-hand corner to export the logs in .CSV or .TXT format.

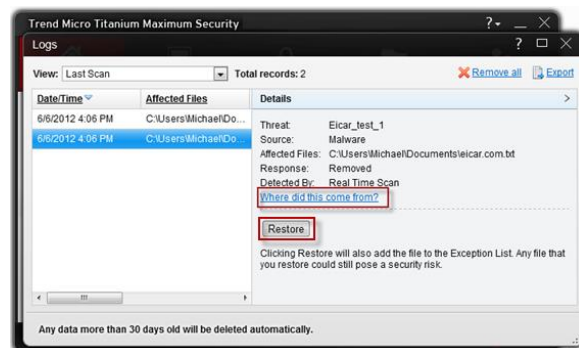


Figure 50. Where Did This Come From? | Restore

- Click **Restore** to restore to add the file to the **Exception List**. Any file that you restore could still pose a security risk.
- When an item in a log warrants a deeper look, Titanium will provide a link to show more details on the source of the infection. Click **Where did this come from?** to generate a

Root Cause Analysis Report. A dialog appears, showing you the progress while generating the report.

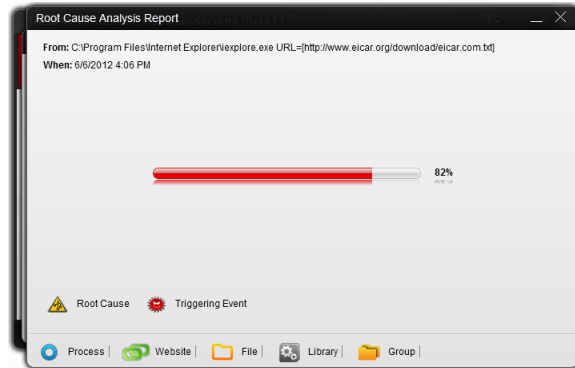


Figure 51. Generating the Root Cause Analysis Report

11. When the report generates, it displays in graphic format.



Figure 52. Root Cause Analysis Report

12. The **Root Cause Analysis Report** maps the root cause and triggering event(s) graphically, using **Process**, **Website**, **File**, **Library**, and **Group** icons to show you items involved in the infection chain. Use the **Root Cause Analysis Report** to analyze the source of infections, so you can help prevent them in the future.

Chapter 4: Trend Micro Titanium Antivirus+

Protection Overview

Trend Micro™ Titanium™ Antivirus+ 2013 provides essential protection for customers against viruses, spyware, web threats, and other malware threats, as shown in the **Safety Summary** section of the Trend Micro **Titanium Console** below.

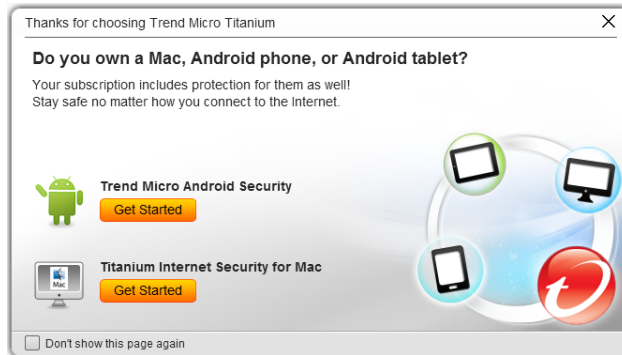


Figure 53. Trend Micro Titanium Antivirus+ Welcome Page

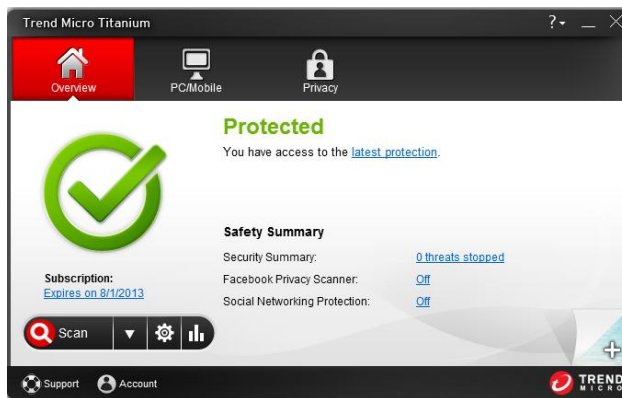


Figure 54. Trend Micro Titanium Antivirus+ Console



Figure 55. PC/Mobile > PC & Internet Security | Rescue Disk



Figure 56. Privacy > Facebook Privacy Scanner | Social Networking Protection

Note: Titanium Antivirus+ Console Features: PC & Internet Security, Rescue Disk, Facebook Privacy Scanner, Social Networking Protection. Additional Offerings: Free Trial - Android Security; 3-device Option - Titanium for Mac

KEY MALWARE PROTECTIONS FOR TITANIUM ANTIVIRUS+

Antivirus and Antispyware

Titanium Antivirus+ provides essential protection against viruses; that is, any malicious program that can replicate itself and infect your computer. Titanium also protects you from a broad range of other malware, including worms, Trojans, bots, and rootkits. It also provides protection from spyware; that is, any program that installs itself in the background and gathers information about you or your computer without your knowledge. Since browser cookies can act like spyware, Titanium will delete cookies as well.

Rescue Disk

Rootkit-based malware is especially difficult to remove from user's computers. Titanium provides a Rescue Disk, which lets you create a USB/CD/DVD disk to remove rootkits and other malware. Rescue Disk reboots your computer into a Linux kernel, scans your computer for rootkits and other malware and removes them, then reboots back to Windows.

Windows Firewall Booster and Wi-Fi Protection

Activation of the Windows Firewall Booster provides additional network-level protections, including a Network Virus Scan and Anti-Botnet feature. Users can opt to activate the booster for increased network security. Titanium Antivirus+ 2013 also provides authentication for Wi-Fi networks.

Anti-Spam

Titanium Antivirus+ 2013 adds anti-spam to its list of feature. Users of POP3 e-mail can be protected from spammers, stopping unsolicited advertisements and other unwanted bulk email. Titanium's anti-spam function taps into the email reputation services of the Smart Protection Network.

Unauthorized Change Prevention

Titanium includes behavior monitoring in its list of security protections. Unauthorized changes to system settings and other suspicious behavior can be blocked, as well as autorun programs on portable drives.

Web Threat Protection

The majority of threats nowadays come from the web, when you're simply browsing the Internet or visiting a site. However, attacks may also begin with a phishing email that uses social engineering techniques to coax you to click a URL link in the email. You then may be taken to a website that secretly harbors malicious threats, which either steals your personal data or infects you with malware.

Titanium Antivirus+ proactively protects you from a variety of these web threats, so that they never touch your computer. To provide thorough protection from and rapid response times to emerging threats, Titanium uses the Trend Micro Smart Protection Network cloud-client security infrastructure along with a combination of cloud-based web, file, and email reputation services. It also employs real-time scans of what's in memory and on disks.

Titanium Antivirus+ 2013 now also blocks malicious links and image spam in emails, as well as malicious links in instant messaging software. Additionally, the Trend Micro Toolbar adds a rate links on mouseover feature to its URL ratings and a Facebook Privacy Scanner that checks security concerns in Facebook.

Note: Since Trend Micro Toolbar is turned off by default in Titanium Antivirus+, you must turn on the toolbar to enable these functions.

Facebook Privacy Scanner

Titanium's Facebook Privacy Scanner lets you scan your Facebook security settings on-demand. When it's done, you're given a recommendation to change all vulnerable settings that don't meet your preferred security levels.

Social Networking Security

Social Networking Protection keeps you safe from security risks when visiting the most popular social networking sites including Facebook, Google+, LinkedIn, Mixi, MySpace, Pinterest, Twitter, and Weibo.

Android Security

Trend Micro™ Mobile Security for Android filters sites, calls, and apps for full security protection for your Android mobile devices. Start a Free Trial.

Titanium Security for Mac

Protect your Mac from viruses, spyware, and unsafe websites with Titanium Internet Security for Mac. Available in a 3-device version.

Getting Started > Additional Protections

When you first load Titanium, a **Welcome Page** appears, showing additional security options for your Android Mobile and Mac devices. You can start a free trial of Android Security using the download link. Titanium for Mac is included as a fully operable download option in a 3-device version.

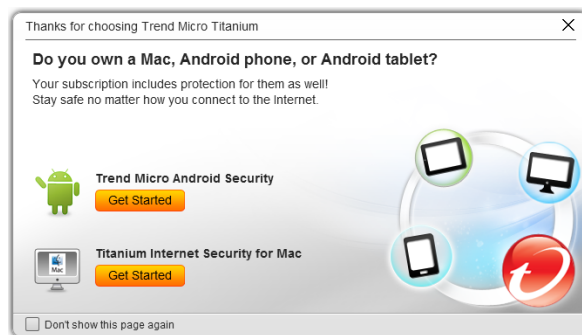


Figure 57. Welcome to Trend Micro Titanium

These are also available from the PC/Mobile tab.



Figure 58. PC/Mobile | Android Security | Titanium for Mac

To download the programs:

1. In the **Welcome** screen, click **Get Started** with **Trend Micro Android Security**, or **Titanium Internet Security for Mac** to download the software.
2. Similarly, in the **PC/Mobile** screen, click **Start a Free Trial** or **Get Started** to get started with the respective software.

3. Your browser launches and takes you to the respective download webpage; for example, Titanium for Mac.

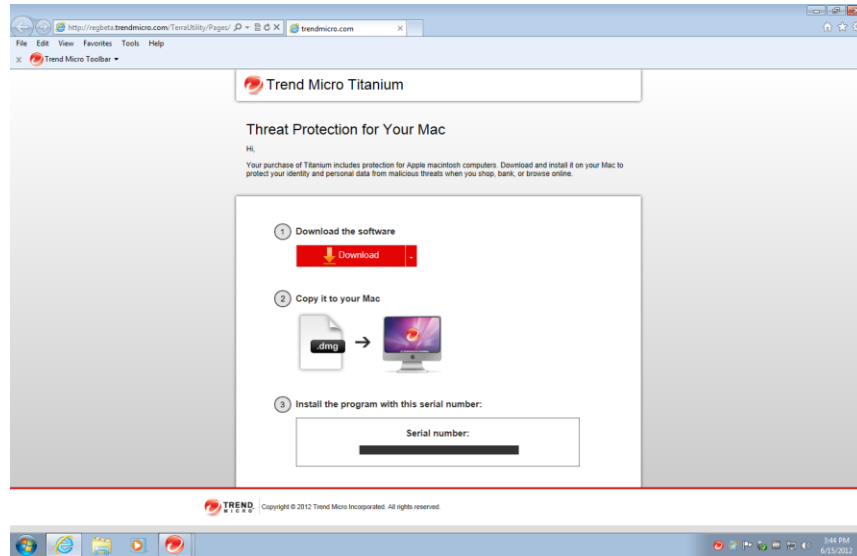


Figure 59. Titanium Download Webpage

4. Click **Download** to download the software, then follow the instructions to install it. Make sure you copy the serial number and save it in a secure place. You'll need it to activate the software.
5. If you don't wish to download the software now, simply close the **Welcome Page** by clicking the close box in the upper right-hand corner.

Virus & Spyware Controls: Scan Preferences

Upon install, Titanium chooses a group of default settings to immediately protect the user. However, users can modify settings as they wish. Titanium keeps its controls simple and suitable for the everyday user.

To modify Virus & Spyware Controls settings:

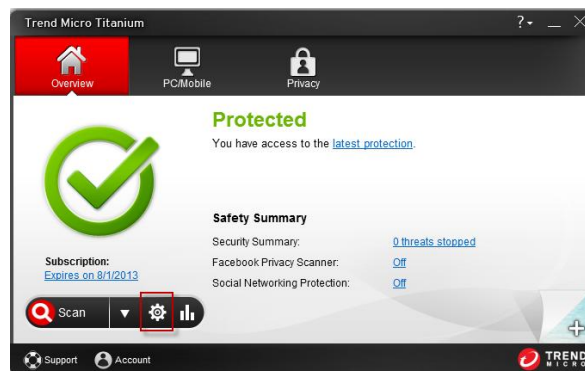


Figure 60. Titanium Console > Protection Settings Tool

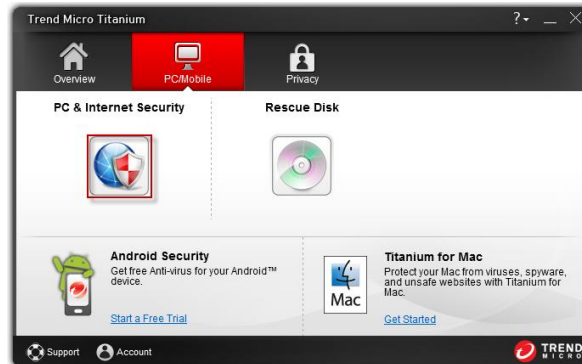


Figure 61. Titanium Console > PC/Mobile > PC & Internet Security

1. Click the **Protection Settings** tool in the **Overview** tab of the **Titanium Console**; or click the **PC/Mobile** tab, then **PC & Internet Security**. The **Protection Settings** screen appears, with **Virus & Spyware Controls** > **Scan Preferences** selected by default in the **Command Menu**.

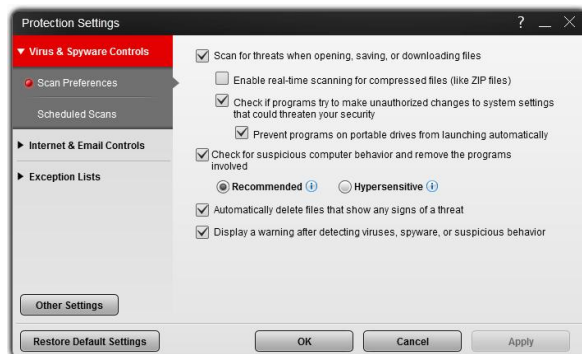


Figure 62. Windows 7: Virus & Spyware Controls > Scan Preferences

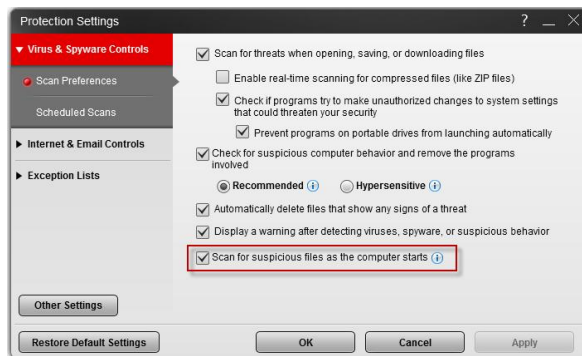


Figure 63. Windows 8: Scan During Start

2. The following **Scan Preferences** are displayed. Unchecked items can be checked and applied.

- **Scan for threats when opening, saving, or downloading files.** This is the real-time scan that protects you at all times when you're using your computer. This is enabled by default.
 - **Enable real-time scanning check compressed files (like ZIP files).** This is disabled by default. Checking the checkbox enables the item, but the deeper scan uses more CPU cycles.
 - **Check if programs try to make unauthorized changes to system settings that could threaten your security.** This is enabled by default.
 - **Prevent programs on portable drives from launching automatically.** This is enabled by default.
 - **Check for suspicious computer behavior and remove the programs involved.** This behavior monitoring function is enabled by default at the recommended level, but you can change the setting by clicking the radio buttons.
 - **Recommended** - Detects and stops security threats based on clearly risky behavior.
 - **Hypersensitive** - Aggressively eliminates programs even if they only pose a small risk of bad behavior.
 - **Automatically delete files that show any signs of a threat.** This is disabled by default. Check the item to automatically delete threatened files.
 - **Display a warning after detecting viruses, spyware, or suspicious behavior.** This is enabled by default. Titanium is selective when using pop-ups; it's never overly intrusive.
 - **Windows 8 Only: Scan for suspicious files as the computer starts.** Key security component begin working even before Microsoft Windows 8 has finished loading, before threats have a chance to attack.
3. Click **Apply** to apply your changes, then **OK** to close the **Protection Settings** window.

Virus & Spyware Controls: Schedule Scans

To modify Scheduled Scan preferences:

1. Click **Virus & Spyware Controls > Scheduled Scans**. The schedule options panel displays.

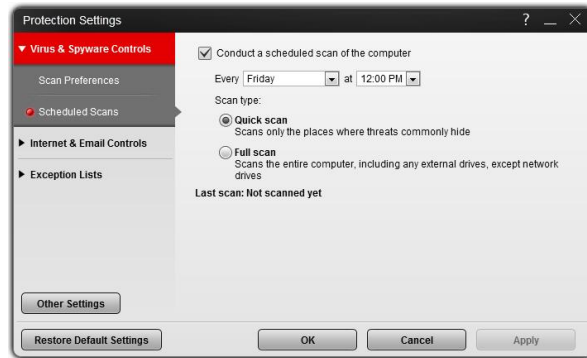


Figure 64. Virus & Spyware Controls > Scheduled Scans

2. Choose among the following options:
 - **Conduct a scheduled scan of the computer.** This is enabled by default. “Friday at 12:00 PM” is chosen by default as the day and time to conduct the scheduled scan. Use the popup menus to change the day and time the scheduled scan will be conducted.

TIP: Scheduled scans are best conducted when the computer is on but not in use, as they take up a portion of Memory, CPU, and Disk processes.

- **Scan Type.** Quick Scan is selected by default.
 - Select **Quick Scan** to scan only the places where threats commonly hide.
 - Select **Full Scan** to scan the entire computer, including any external drives, except network drives.
3. Click **Restore Default Settings** to restore default settings to their factory condition.
 4. Click **Apply** to apply any changes, then **OK** to close the **Protection Settings** window.

Internet & Email Controls: Web Threats | Trend Micro Toolbar

To modify the Internet & Email Controls > Web Threats settings:

1. Click **Internet & Email Controls**. The **Web Threats** panel appears by default.

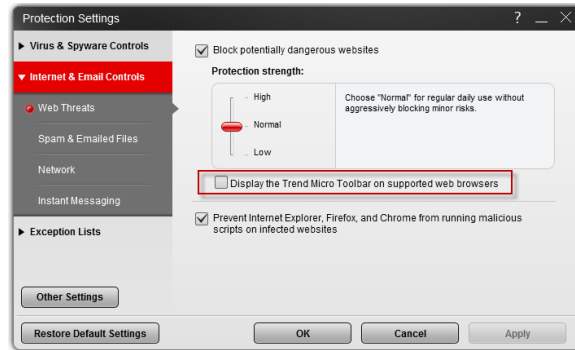


Figure 65. Internet & Email Controls > Web Threats

2. **Block potentially dangerous websites** is checked by default.
3. For **Protection strength**, use the slider to select the strength. More aggressive blocking blocks more websites, some of which you may not wish to be blocked.
 - **High** - Choose “High” to block threats in sites that show *any* signs of fraud or malicious software.
 - **Normal** - Choose “Normal for regular daily use without aggressively blocking minor risks. This is the default setting.
 - **Low** - Choose “Low” to block only websites confirmed as fraudulent or dangerous.
 - **Display the Trend Micro Toolbar on supported web browsers** - The Trend Micro Toolbar rates links on webpages and mouse-over, and also lets you check your Facebook Privacy settings.

Note: The Trend Micro Toolbar is currently disabled by default in Titanium Antivirus+ and Titanium Internet Security. *You must enable the toolbar to enable all three functions mentioned above, including the two new Titanium 2013 features of URL mouse-over on-demand ratings and Facebook Privacy scanning.*

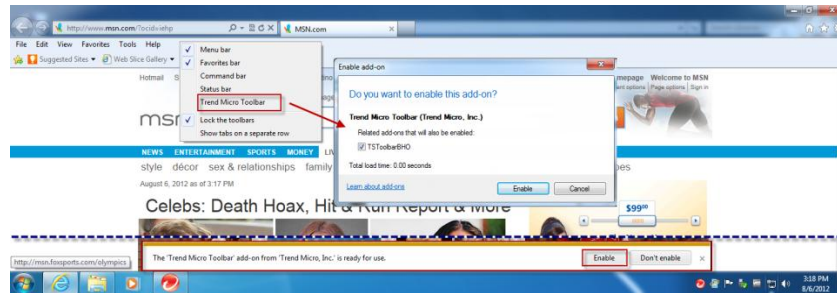


Figure 66. Enable Trend Micro Toolbar

4. Once you check it, Internet Explorer lets you finishing enabling the **Trend Micro Toolbar** by either right-clicking the IE option menu to show it and select it, which brings up an **Enable** add-on popup, where you click the **Enable** button to enable it; or by clicking the **Enable** button in the popup at the bottom of the browser. This completes the enablement of the toolbar.
5. **Prevent Microsoft Internet Explorer and Mozilla Firefox from running malicious scripts on infected websites** is checked by default.
6. Click **Apply** to apply your changes, then **OK** to close the **Protection Settings** window.

Internet & Email Controls: Spam & Emailed Files

To modify the Internet & Email Controls > Spam & Emailed Files setting:

1. Click **Internet & Email Controls > Spam & Emailed Files** to open the panel. The panel opens with the setting unchecked by default.



Figure 67. Internet & Email Controls > Spam & Emailed Files

2. Check **Filter out unsolicited advertisements and other unwanted email messages** if you wish to stop spam and other unsought messages.
3. Check the checkbox **Check for threats in files attached to email messages** to scan all POP3 email messages for malicious attachments and remove them.
4. Click **Apply** to apply any changes, then **OK** to close the **Protection Settings** window.

5. Trend Micro Anti-Spam (TMAS) support for OS Platform and Mail Client is given in the table below.

Table 5. TMAS OS Platform and Mail Client Support

OS Platform	Mail Client
Windows XP	Outlook Express
Windows Vista (32 and 64 bit)	Windows Mail, Windows Live Mail 2011
Windows 7 (32 and 64 bit)	Windows Live Mail 2011
Windows 8 (32 and 64 bit)	Windows Live Mail 2011
All	Outlook 2003(32bit), 2007(32bit), 2010(32bit), Windows Live Mail 2009

Internet & Email Controls: Network | Firewall Booster and Wi-Fi Protection

To modify the Wi-Fi Protection Settings:

1. Click the **Protection Settings** tool in the Titanium Console. The **Protection Settings** screen appears, with **Virus & Spyware Controls** selected by default.
2. Click **Internet & Email Controls > Network** in the Command menu. The **Network** screen appears.

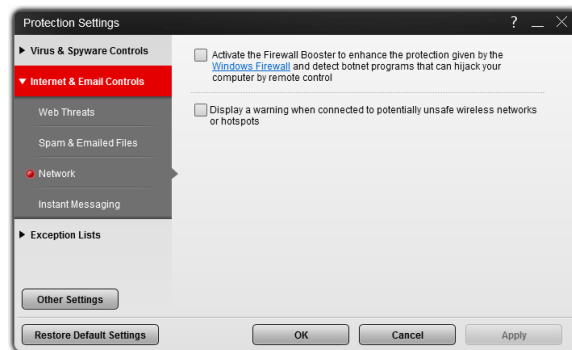


Figure 68. Internet & Email Controls > Network

3. Check **Activate the Firewall Booster** checkbox to enhance the protection given by the Windows Firewall and to detect botnet programs that can hijack your computer by remote control.
4. Check **Display a warning when connected to potentially unsafe wireless networks or hotspots** to enable the feature.
5. Click **OK** to save your changes.

Note: The Exception List for Wi-Fi Protection allows users to add unprotected home networks to an exception list, so that users are not subject to frequent warnings for networks they know to be safe. See the Exception Lists section for more details.

Internet & Email Controls: Instant Messaging

Titanium Antivirus+ adds an additional layer of protection for instant messaging, checking for security risks in links to websites received via IM programs. With IM protection, if you click a link to a bad website, you're instantly and proactively blocked at the exposure layer by the SPN in-the-cloud URL reputation service and given a warning. You never get the chance to be infected.

To install the IM protection, you first need to install the IM program(s) you'll be using. The installation button for the installed IM program(s) will then become active in the Titanium user interface.

Titanium supports the following instant messaging programs/versions:

- Windows Live™ Messenger 8.1, 9.0, 2009, 2010, and 2011
- Yahoo!® Messenger 8.0, 8.1, 9.0, and 10.0
- AOL® Instant Messenger™ (AIM®) 6.8, and 6.9
- Skype™ 3.6, 3.8, 4.0, and 4.2

Note: In the example below, Yahoo! Messenger has been previously installed.

To install IM protection:

1. In the **Protection Settings** screen, click **Internet & Email Controls > Instant Messaging**. The **Instant Messaging** protection screen appears.

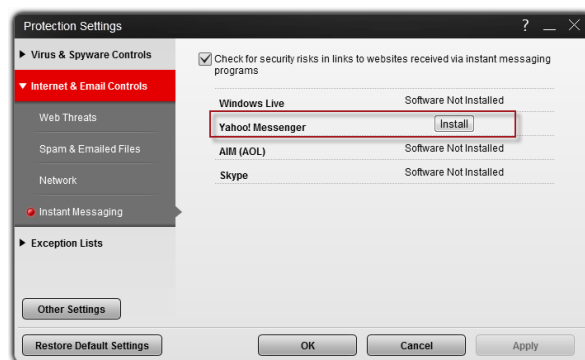


Figure 69. Internet & Email Controls > Instant Messaging

2. In the Yahoo! Messenger section, click **Install**. A pop-up appears, indicating that IM protection for the installation has completed.

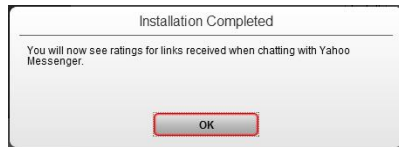


Figure 70. IM Protection Installation Completed

3. The IM protection is enabled by default. You will now see ratings for links received when chatting with Yahoo Messenger. Click **OK** to close the pop-up.

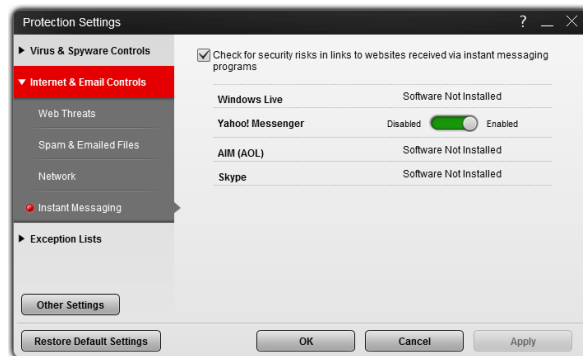


Figure 71. Enable / Disable IM Protection

4. Click **OK** again to close the Titanium **Protection Settings** window.
5. Return to this window to disable the protection at any time. Simply move the slider to **Disabled**, then click **OK** to save your changes.

Exception Lists: Programs/Folders

To add items to Exception Lists Programs/Folders:

Titanium lets you add programs, folders, or websites to exception lists so that scans will ignore them. Adding programs or folders to exception lists can increase performance during scans, while adding frequently-accessed websites can prevent unwanted blockage. Users are advised to use exception lists wisely, as it may open computers up to more threats.

1. To add items to exception lists, click **Exception Lists**. **Programs/folders** appears by default.

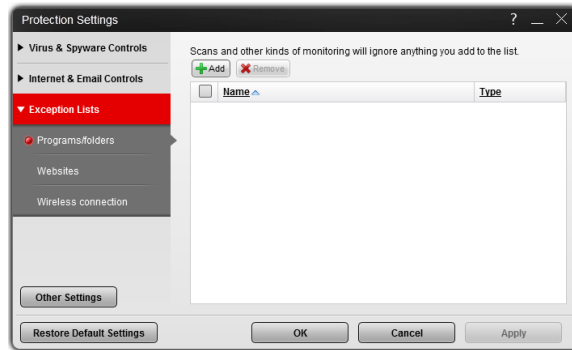


Figure 72. Exception Lists > Programs/folders

- Click **+Add** to add a program or folder to the exception list. A dialog appears, letting you **Add an Item**.

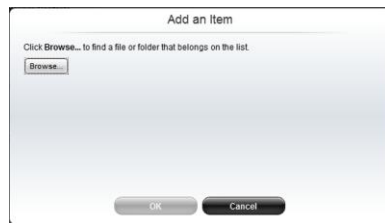


Figure 73. Add an Item

- Click **Browse** to browse to the file or folder you wish to add. An **Open** dialog appears.

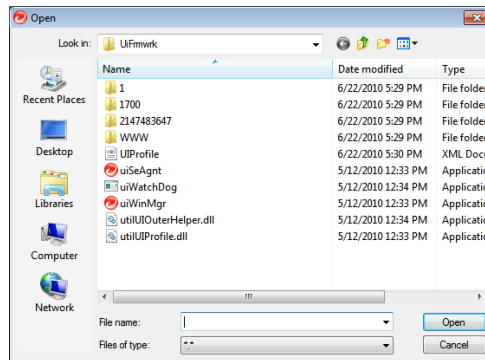


Figure 74. Open Dialog

- Select the item you wish to add, then click **Open**. This adds the item to the **Add an Item** dialog.



Figure 75. Add an Item (item added)

- Click **OK** in the **Add an Item** dialog. The item is added to the exception list.

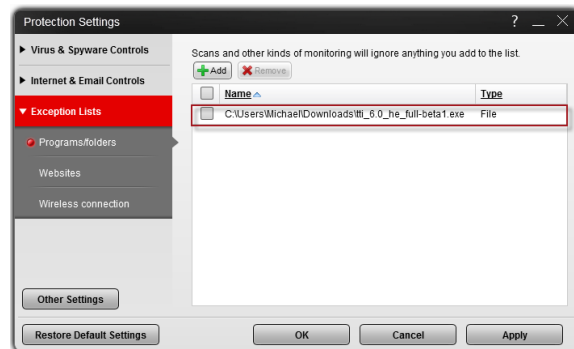


Figure 76. Item Added to Exception List

- To remove an item, check it, and then click the **X Remove** button.
- Click **Apply** to save any changes, then **OK** to close the Titanium Console.

Exception Lists: Websites

To add websites to an exception list:

- In a similar way, to add or remove a website from its exception list, click **Exception Lists > Websites** in the **Command Menu**. The **Websites** exception list appears.

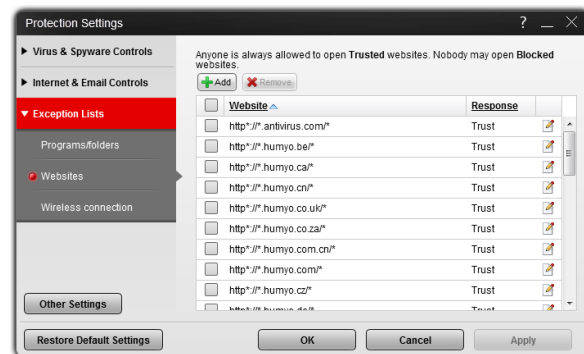


Figure 77. Exception Lists > Websites

- Click **Add** to add a website. A dialog appears, letting you **Add** or **Edit an Item**.
- Choose among the following options:

- a. Type in the URL you wish to add in the edit field.



Figure 78. Add or Edit an Item

- b. Or select **Import addresses (URLs) from your Internet Explorer “Favorites”**.

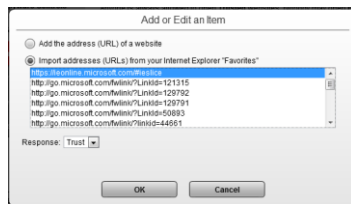


Figure 79. Import URLs from IE

- c. Choose **Block** or **Trust** from the **Response** pop-up (for either option).
 - d. Click **OK** to save the option.
4. Click **Apply** to save your changes, then **OK** again to close the Titanium Console.

Exception Lists: Wireless Connection

Titanium Maximum Security allows you to add access points to the **Wireless Connections Exception List** that Titanium may consider risky or dangerous. Wi-Fi hotspots added to the list are considered trusted access points.

To add and remove a Wireless connection to the Exception List:

1. When you attempt to log onto an access point, Titanium may give you a pop-up warning that the network connection is risky or dangerous.



Figure 80. Risky Network Connection

2. If you know this access point probably isn't risky, you may wish to add this network to the Wireless Connections Exception List. To do so, simply click **Trust this network despite the risk** and the site will be added to the list.
3. Later, you may wish to delete this from the Exception List. To do so, click the **Settings** tool to open the **Protection Settings** screen. The **Virus & Spyware Controls** screen opens by default.
4. Click **Exception Lists > Wireless connection** in the Command menu. The Exception List for **Wireless connections** appears.

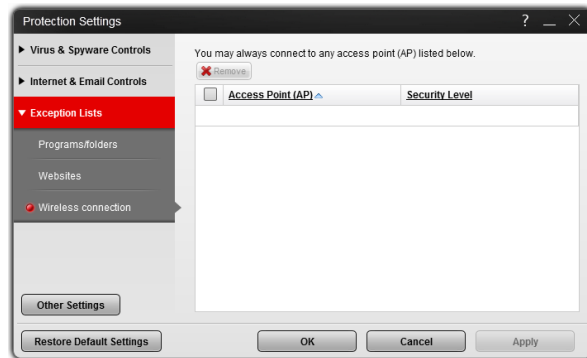


Figure 81. Exception Lists > Wireless connection

5. Select the access point in the list and click **Remove**. Titanium deletes it from the list.
6. Click **Apply** to save your changes.

Other Settings: System Startup

By default, Titanium chooses the optimal settings when starting your computer. You can change these settings.

To modify Other Settings > System Startup:

1. Click **Other Settings** in the Command Menu. The **System Startup** screen appears by default, with **Balanced Protection** chosen by default (the screen below shows an alternate choice).



Figure 82. Other Settings > System Startup

2. Select among the following options:
 - **Extra Security** - Security software drivers will load as soon as the computer starts, which makes the operating system launch more slowly.
 - **Balanced Protection** - This is the default setting. Only some security software drivers will load when the computer starts to reduce delays. Others will be loaded later.
 - **Extra Performance** - Security software drivers will load only after the computer has started to help the operating system launch more quickly.
3. Click **Apply** to save your changes, then **OK** to close the **Protection Settings** window.
4. Restart the computer to apply the changes to your system.

Other Settings: Network Settings

To modify **Other Settings > Proxy Settings**:

1. Click **Other Settings > Proxy Settings** in the Command Menu. **Proxy Settings** appears, with **Use a proxy server** and **Use Internet Explorer Proxy Settings** chosen by default.

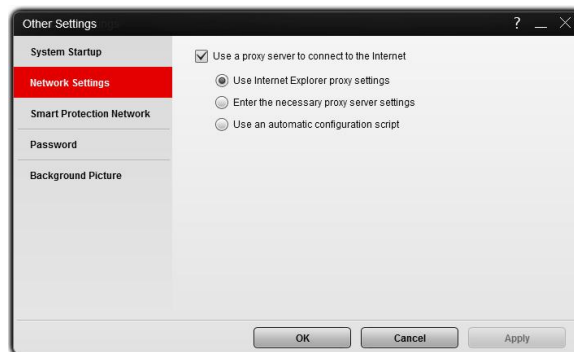


Figure 83. Other Settings > Proxy Settings

2. Select **Enter the necessary proxy server settings** to manually enter a proxy server's name, port, and credentials (if required).

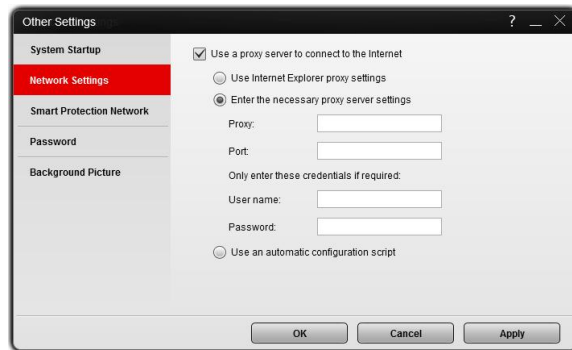


Figure 84. Other Settings > Proxy Settings > Enter Settings

3. Or select **Use an automatic configuration script** and enter the script in the **Address** field provided.
4. Click **Apply** to save your changes, then **OK** to close the **Protection Settings** window.

Other Settings: Smart Protection Network

To share/not share feedback with the Smart Protection Network:

Titanium can provide feedback to the Smart Protection Network (SPN), to automatically correlate and analyze information about threats found on your computer (and millions of others), for better protection. By opting into the SPN feedback process, you improve yours and others' threat protection, since threats sent from your computer are immediately added to the threat analysis/detection/prevention process, but the choice is yours to opt in or out.

1. Select **Other Settings > Smart Protection Network** from the Command Menu. The threat information feedback panel appears.

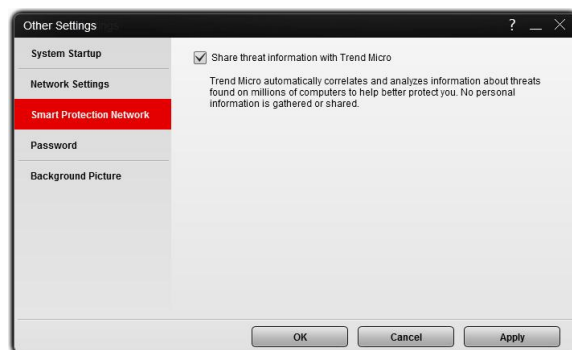


Figure 85. Other Settings > Smart Protection Network

2. Check/Uncheck **Share threat information with Trend Micro** to opt in or out of the feedback process. (This will be checked or unchecked depending upon the choice you made to participate or not participate when you installed Titanium.)
3. Click **Apply** to save your changes, then **OK** to close the **Protection Settings** window.

Other Settings: Password

To add or change your password:

Titanium allows you to add a password to protect your overall program settings, so only those who know the password can make changes. For Titanium Internet Security (TIS) and Maximum Security (MS), the password enables other functions, such as **Parental Controls** in IS and MS and **Trend Micro Vault** in MS. See the two following chapters for details.

1. Select **Other Settings > Password** from the Command Menu. The **Password** screen appears.

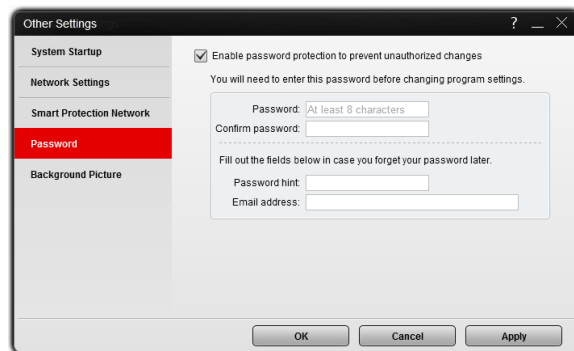


Figure 86. Other Settings > Password

2. Check **Enable password protection to prevent unauthorized changes**.
3. Enter your email address, a password, and the password again to confirm it. Titanium gives you feedback on your password strength.
4. Fill out the **Password Hint** and **Email Address** fields in case you forget your password later.
5. Click **Apply** to save the password changes, then **OK** to close the **Protection Setting** window.

Other Settings: Background Picture

Titanium allows you to change the background picture of the **Titanium Console**. You can use backgrounds provided by Trend Micro, or customize the background using your own pictures.

To change your Titanium interface:

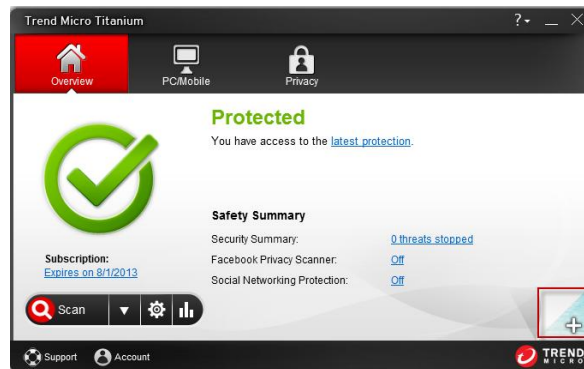


Figure 87. Tear Page

1. Using the upturned tear page, simply click it and drag it to the left to change the background picture to another one provided by Trend Micro.



Figure 88. Alternate Background

2. Alternately in the **Overview** screen of the **Titanium Console**, click the + icon in the lower-right hand corner; or in **Other Settings**, select the **Background Picture** menu item. The **Background Picture** editor appears.

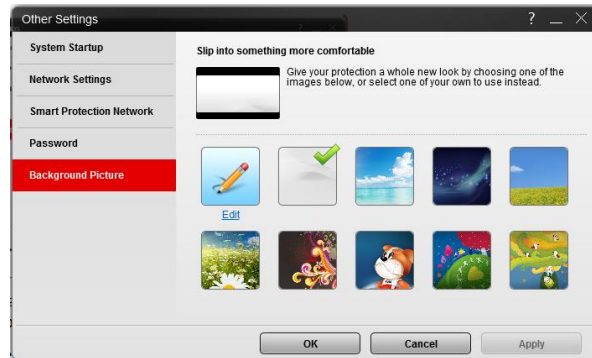


Figure 89. Background Picture Editor

3. Select any background picture provided and click **Apply** to save the new background, or add a picture from your computer.
4. For the second option, click the **Edit** button to edit your user interface. The **Select a Picture** dialog displays.



Figure 90. Select a Picture

5. Click **Browse** to select a picture, then navigate to a folder containing your pictures.



Figure 91. Browse to Picture

6. Select your picture and click **Open**. The picture is loaded into the editor.

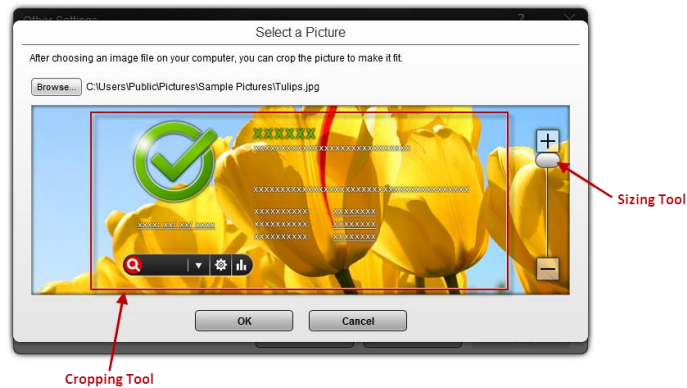


Figure 92. Cropping and Sizing

7. Use the **Cropping** tool to move the picture in the cropping area to the place in the picture that you wish to display.
8. Use the **Sizing** tool to make your image larger or smaller. Click the (+) or (-), or drag the slider.
9. When you're done, click **OK** to close the editor.
10. Click **Apply** to save your UI change, the **OK** to close the **Background Picture** tab. Your new background picture appears in the Titanium Console.



Figure 93. Titanium Console with New Skin

11. You can return to the classic Titanium background at any time by clicking its icon in the editor and clicking **Apply**, then **OK**.

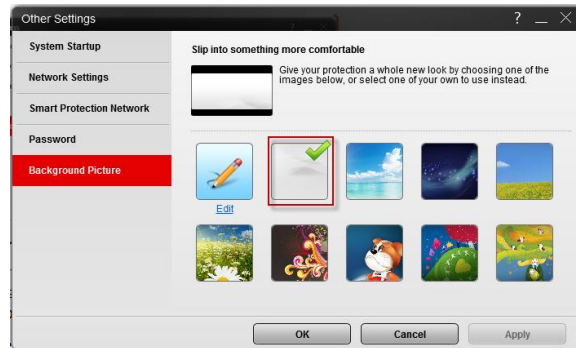


Figure 94. Classic Titanium Background

12. Click the **Close** box to close the **Titanium Console**.

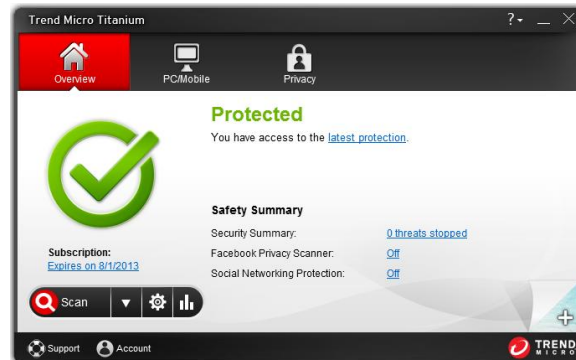


Figure 95. Titanium Console

PC/Mobile: Rescue Disk

As noted in the installation section of this Product Guide, Titanium also provides the ability to create a **Rescue Disk** for severe malware removal, either on a CD/DVD or a USB drive. **Rescue Disk** boots to a Linux kernel, scans your computer for malware and rootkits, cleaning them from your system, then reboots to Windows. Accessible through the scan result window when needed through a hotlink, **Rescue Disk** is also available through the **Computer** tab in the **Titanium Console**.

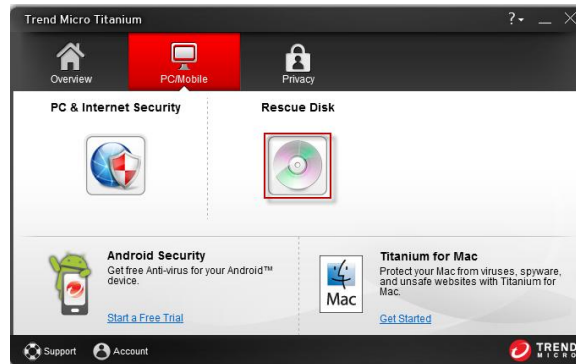


Figure 96. Computer > Rescue Disk

See [Using Rescue Disk for Rootkit and Malware Removal](#) in Chapter 3 for details on how to use this tool.

Privacy: Facebook Privacy Scanner

The **Facebook Privacy Scanner** is turned off by default in Titanium Antivirus+ and Titanium Internet Security and turned on by default in Titanium Maximum Security. If you haven't previously turned on the **Trend Micro Toolbar** (see the *Internet & Email Controls: Web Threats | Trend Micro Toolbar* section above), which is necessary to use the **Facebook Privacy Scanner**, follow the process below and it will be enabled when you turn on the scanner.

To turn on the Facebook Privacy Scanner:

1. Double-click the Titanium shortcut on the desktop to open the **Titanium Console**. The **Titanium Console** appears.
2. Do one of two things:

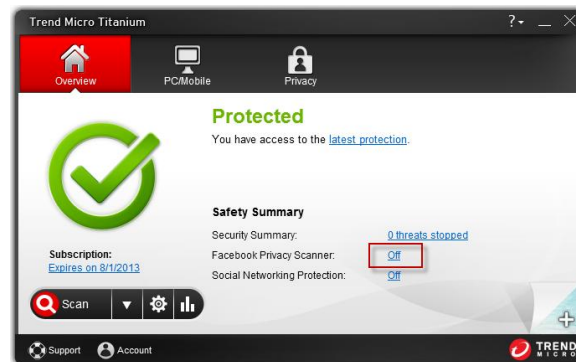


Figure 97. Titanium Console | Facebook Privacy Scanner

> In the main Console window, click the **Facebook Privacy Scanner Off** link.

OR



Figure 98. Privacy > Facebook Privacy Scanner

> Click the **Privacy** tab, then click the **Facebook Privacy Scanner** icon.

3. The **Facebook Privacy Scanner** window appears.

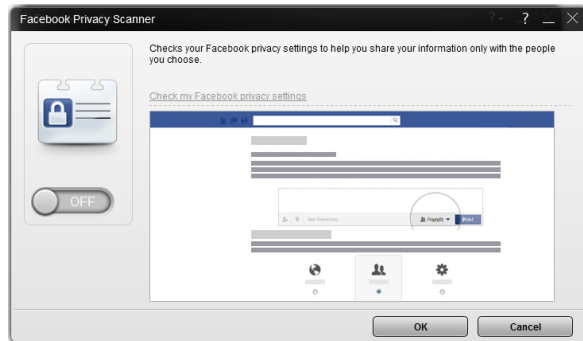


Figure 99. Facebook Privacy Scanner window

4. Click the slider from **Off** to **On**. A dialog appears, indicating that switching the feature on will enable the **Trend Micro Toolbar**, which will appear when you re-start your browser.



Figure 100. Turn On Trend Micro Toolbar

5. Click **Yes** to turn on Trend Micro Toolbar.
6. Click **OK** to close the **Facebook Privacy Scanner** window.

To use the Facebook Privacy Scanner:

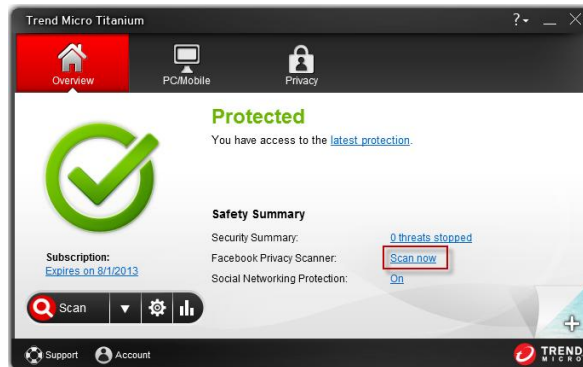


Figure 101. Facebook Privacy Scanner: Scan Now

1. In the **Titanium Console** main screen, click **Scan Now**. Titanium automatically loads your browser and takes you to the Facebook login website.

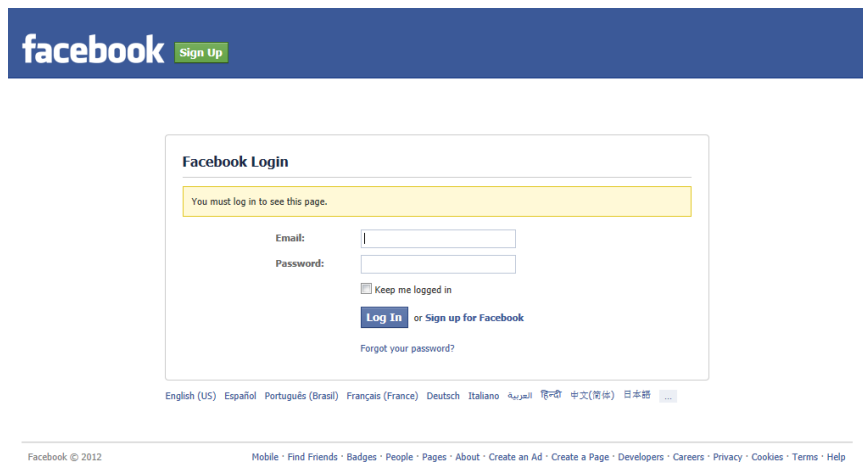


Figure 102. Facebook Login Webpage

2. If you're using Internet Explorer, a dialog appears at the bottom of your window, asking you to **Choose add ons**. Click the close box in the dialog to close it.



Figure 103. Enable Trend Micro Toolbar

3. A second dialog appears behind the first, telling you **The 'Trend Micro Toolbar' add on from 'Trend Micro Inc.' is ready for use**. Click **Enable** to enable the toolbar.



4. Log in to your Facebook account. The **Facebook News Feed** page displays, showing Titanium's **Facebook Privacy Scanner**.

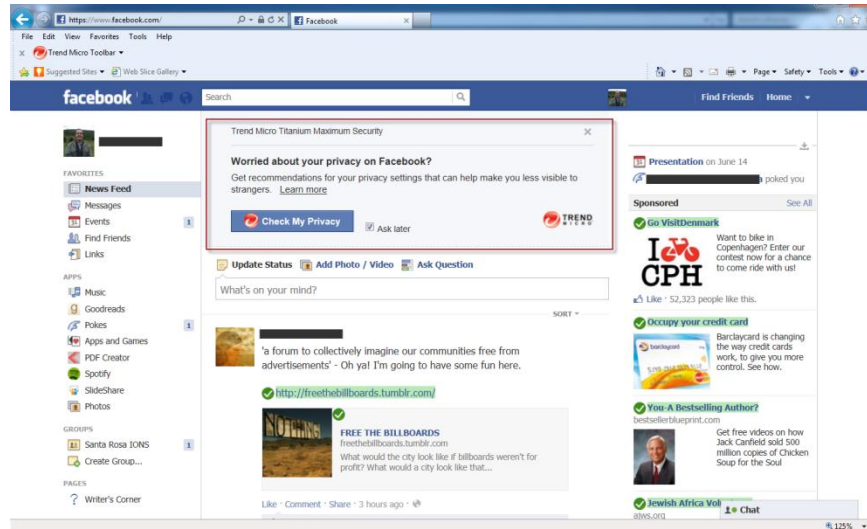


Figure 104. Facebook > Check My Privacy

5. Click **Check My Privacy**. Facebook returns the results, indicating when you have privacy concerns.

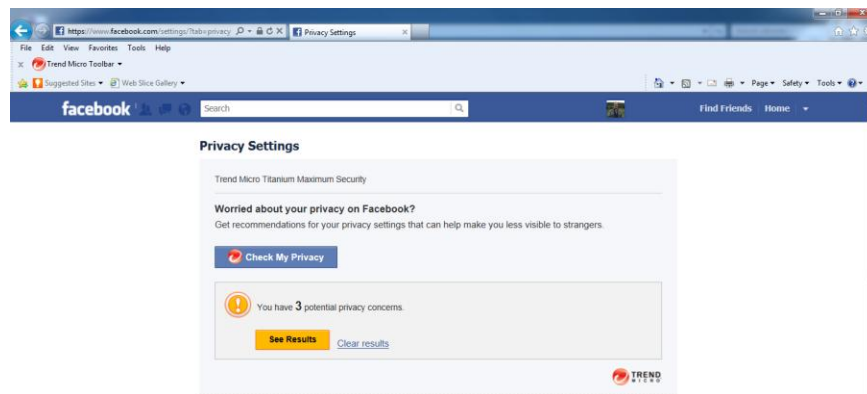


Figure 105. Facebook > See Results

6. Click **See Results**. Your Facebook page scrolls down, highlighting the areas where Titanium indicates potential security concerns.

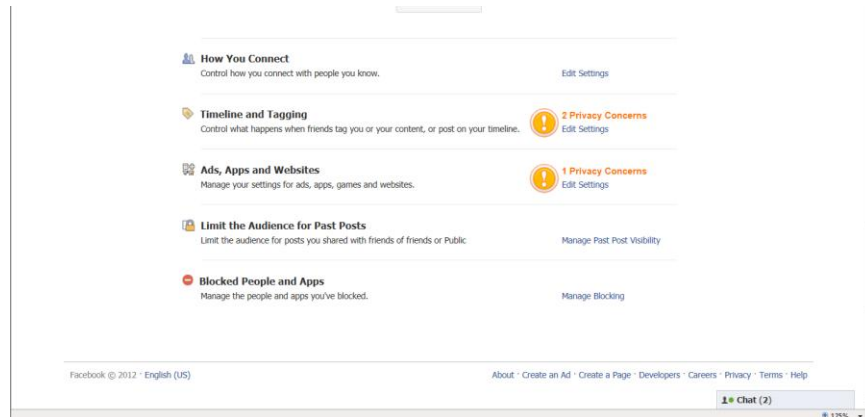


Figure 106. Facebook Privacy Concerns

7. Click **Edit Settings** for the setting with **Privacy Concerns**. The **Facebook Setting Editor** appears, letting you edit the settings.

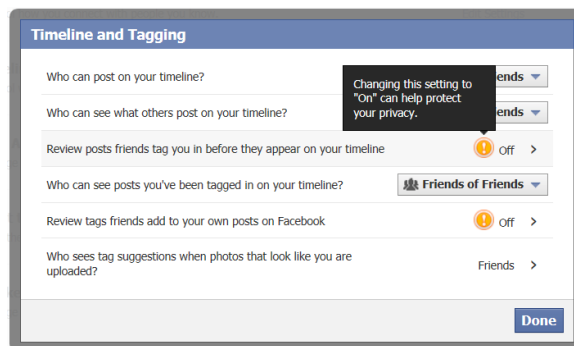


Figure 107. Titanium Advice

8. Click the right-arrows to edit the particular settings with warnings. The **Setting Editor** opens, allowing you to make your changes.

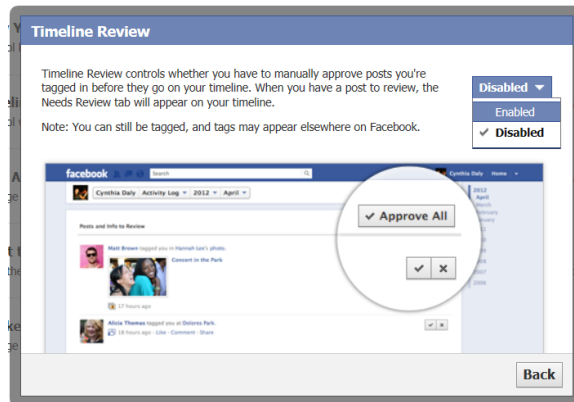


Figure 108. Facebook Change Setting

9. In this example, we've enabled the **Timeline Review** setting. Click **Back** to change more settings.
10. Scroll down the Facebook page to see more privacy concerns highlighted by Titanium, then edit the settings that need editing.

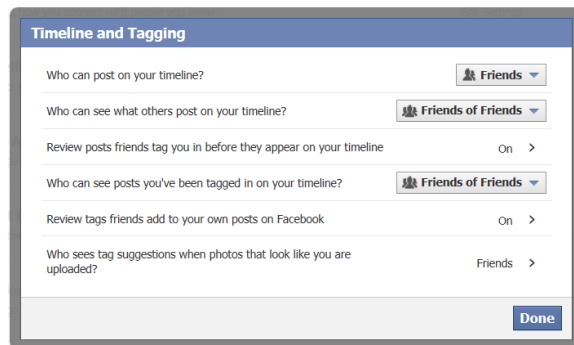


Figure 109. Facebook Settings Editor > Done

11. When you're finished making your changes, click **Done** to close the Facebook Settings editor.
12. Titanium provides ongoing protection for Facebook. At any time, you can run another **Facebook Privacy Scan** on your Facebook page to check your Facebook security settings.

Privacy: Social Networking Protection

Titanium Antivirus+ 2013 includes Social Networking Protection that keeps you safe from security risks when visiting the most popular social networking sites including Facebook, Google+, LinkedIn, Mixi, MySpace, Pinterest, Twitter, and Weibo. In Facebook, you can also warn a friend when a link is dangerous. The scanner is turned off by default in Titanium Antivirus+ and Internet Security, but on in Titanium Maximum Security.

To enable Social Networking Protection:

1. Double-click the Titanium shortcut on the desktop. The **Titanium Console** appears.
2. Do one of two things:

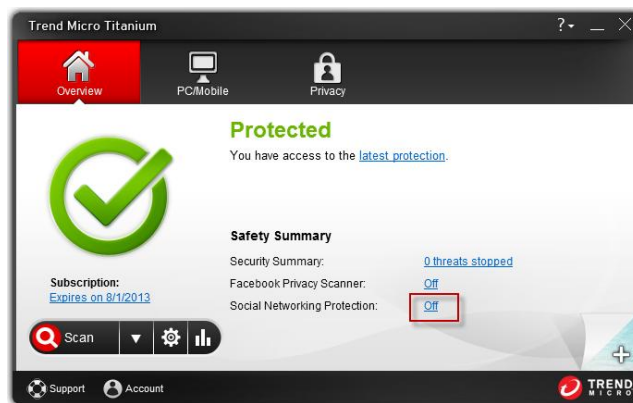


Figure 110. Social Networking Protection

> In the **Titanium Console**, click the **Social Networking Protection Off** link.



Figure 111. Privacy > Social Networking Protection

OR

> Click the **Privacy** tab, then **Social Networking Protection**.

3. The **Social Networking Protection** screen appears.

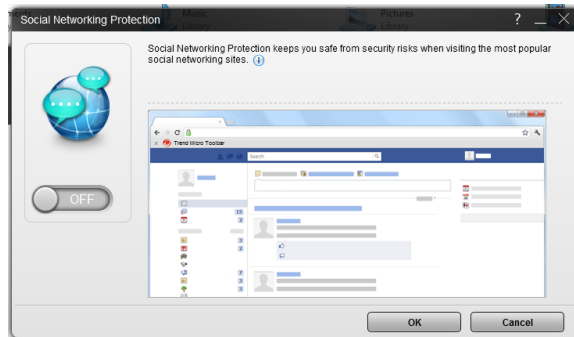


Figure 112. Social Networking Protection > Off

- Click the slider from **Off** to **On** to enable the function.

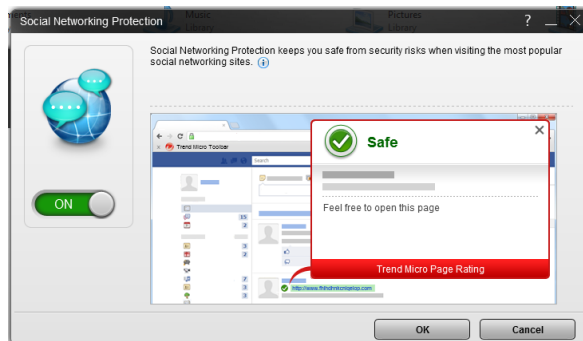


Figure 113. Social Networking Protection > On

- Click **OK** to save your changes. A dialog appears, asking if you're **Ready to Turn On the Trend Micro Toolbar**.



Figure 114. Ready to Turn On the Trend Micro Toolbar

- Click **Yes** to turn on the **Trend Micro Toolbar**. The toolbar will appear once you restart the web browser. In Internet Explorer, a popup appears at the bottom of your browser, letting you enable the plugin.

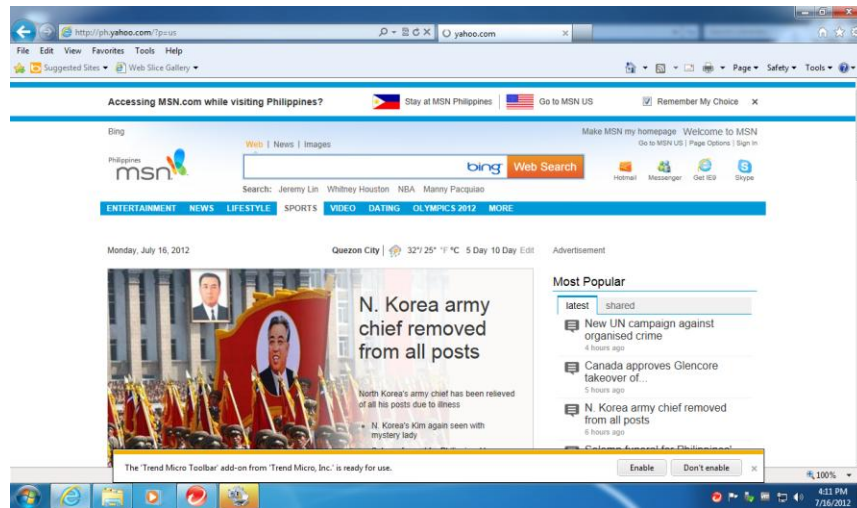


Figure 115. Enable Trend Micro Toolbar

7. Click **Enable** to enable the Trend Micro Toolbar add-on.



Figure 116. Toolbar Menu Items

8. Select **Rate links on web pages** (selected by default), or **Rate links on mouseover** to enable the features. For the latter, an additional pop-up appears in IE.

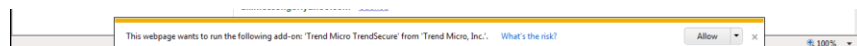


Figure 117. Trend Micro TrendSecure

9. Click **Allow** to enable the **Trend Micro TrendSecure** add-on. Now, when you mouse-over a link, Titanium will scan it in real-time and provide you with a rating.

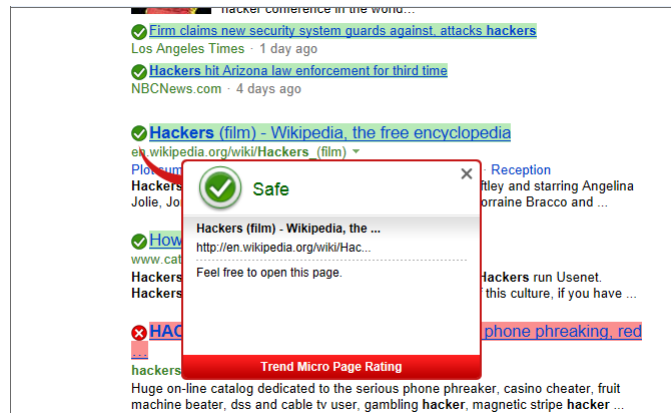


Figure 118. Safe Trend Micro Page Rating

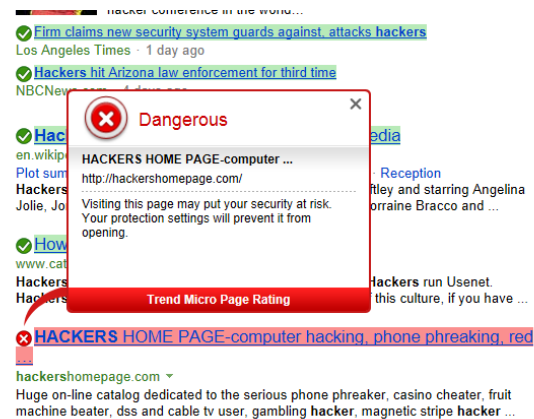


Figure 119. Dangerous Trend Micro Page Rating

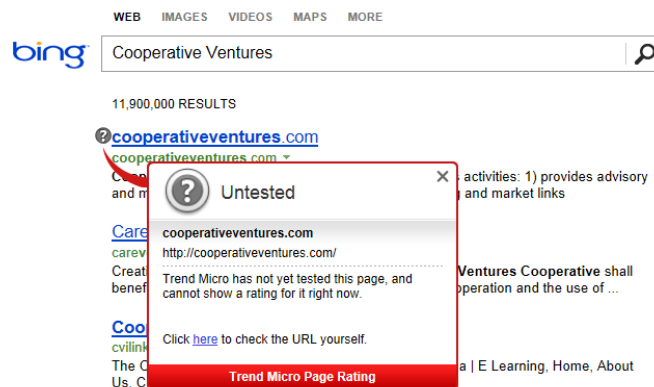


Figure 120. Untested Trend Micro Page Rating

10. Simply position your mouse over the checkmark to view details about the rating.

11. Note too, that when a URL posted on Facebook is rated as dangerous by Titanium, you can warn your friend about it.

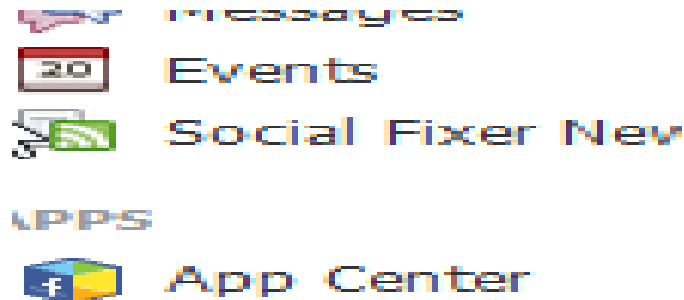


Figure 121. Dangerous URL on Facebook Detected by Titanium

12. Below the dangerous URL, click the link **Warn your friend about this post**. Titanium adds the warning to the comment field.



Figure 122. Warn a Friend About the Dangerous URL

13. Click **Enter** to post the warning. Titanium posts the warning along with a **Welcome** link from Trend Micro. The user is advised to remove the dangerous link and to scan their computer for security threats.

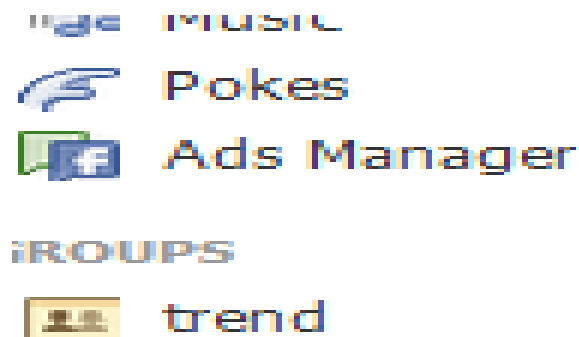


Figure 123. Dangerous URL Warning Posted on Facebook

Chapter 5: Trend Micro Titanium Internet Security

Protection Overview

Trend Micro Titanium Internet Security provides everything included in Trend Titanium Antivirus+, but adds some significant protections and tools, outlined below. To enable all functions, you need a paid version of Titanium Internet Security.



Figure 124. Titanium Internet Security Welcome Screen



Figure 125. Trend Micro Titanium Internet Security Console



Figure 126. PC/Mobile > System Tuner



Figure 127. Data > Data Theft Prevention | Secure Erase | DirectPass

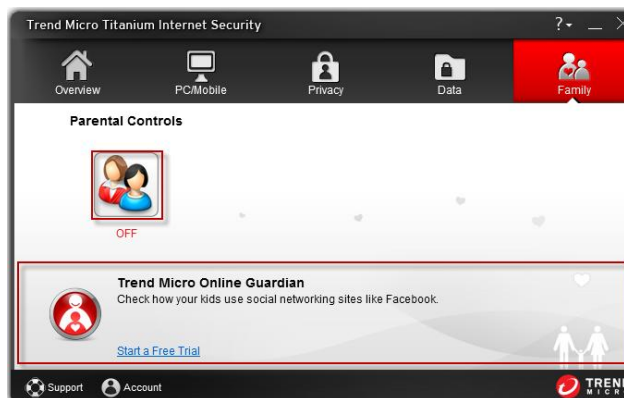


Figure 128. Family > Parental Controls | Online Guardian

Note: Titanium Internet Security Additional Features: System Tuner, Data Theft Prevention, Secure Erase, Parental Controls. Additional Offerings: DirectPass, Online Guardian; Free Trial - Android Security; 3-device Option - Titanium for Mac

ADDITIONAL TOOLS FOR TITANIUM INTERNET SECURITY PAID VERSION

System Tuner

Titanium Internet Security adds the **System Tuner**, which can improve PC performance by cleaning up temporary files, registries, and the Start-up Manager.

Data Theft Prevention

With its **Data Theft Prevention** feature, Titanium Internet Security allows you to prevent data leakage (from email and instant messaging tools) or data theft (from tools such as keyloggers).

Secure Erase

Titanium Internet Security also adds **Secure Erase**, which shreds computer files that have sensitive information, making it impossible for an unauthorized person to recover them.

Parental Controls

Titanium Internet Security allows parents to restrict access to websites by users, rule sets, and categories. **Parental Controls** also gives parents the ability to limit the amount of time their child is allowed to use the Internet. Titanium's Parental Controls tap into Windows User Accounts, assigning each rule set to a specific user.

DirectPass

Titanium Internet Security provides a free 5-account version of Trend Micro DirectPass, a password manager that helps you to manage all your online credentials. Titanium Internet Security users can buy the full version for unlimited password management.

Online Guardian

Titanium Internet Security users are also provided easy access to a 30-Day Free Trial version of Trend Micro Online Guardian for Families. Online Guardian lets parents manage and monitor their kids internet usage and includes a full monitoring system for social networking sites.

PC/Mobile: System Tuner

Titanium Internet Security (and Maximum Security) provides a **System Tuner** that can help you recover disk space, make Microsoft Windows start faster, clean up your instant messaging history, and optimize your computer's performance. You can also plan scheduled tune-ups that can automatically keep everything running smoothly.

To perform a System Tune-up:

1. Click **PC/Mobile > System Tuner** in the Console.

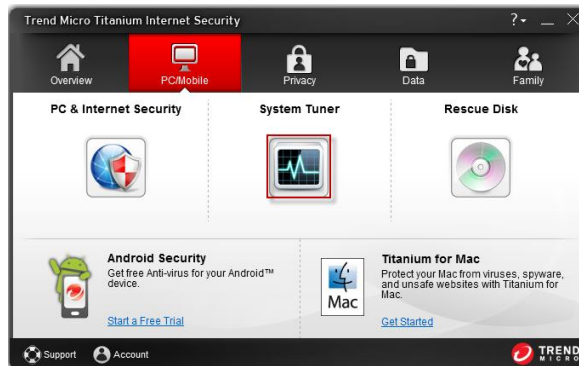


Figure 129. PC/Mobile > System Tuner

2. The **System Tuner** introduction appears.

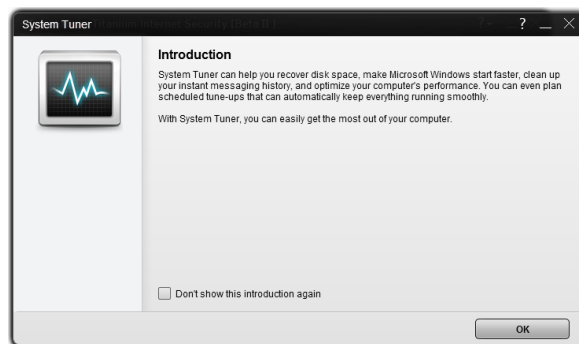


Figure 130. System Tuner Introduction

3. Click **OK** to close the window. The **System Tuner** settings screen appears.

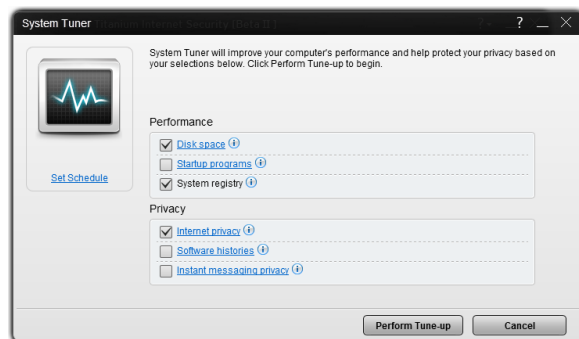


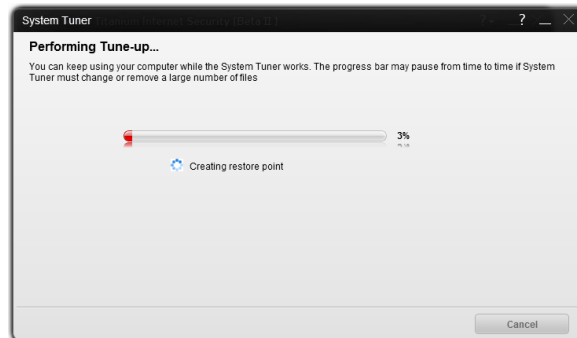
Figure 131. System Tuner Performance / Privacy Settings

4. You can define how System Tuner works by checking a **Performance** or **Privacy** item and modifying the settings for the following options:

Table 6. System Tuner Options

Performance Options	Description
Disk Space	You can regain disk space by removing Windows, Internet, and Update Temporary files and Recycle Bin contents.
Startup Programs	Remove Startup Programs or Processes.
System Registry	Remove unused, broken or invalid entries from the Registry that can affect the computer's stability and performance.
Privacy Options	Description
Internet Privacy	Delete history of websites visited, AutoComplete records, Google toolbar search history, and website cookies.
Software Histories	Delete the list of files opened by Microsoft Windows Search, Windows, Office, Media Players; also the list of programs and files recently opened or from the Windows Start Menu list.
Instant Messaging Privacy	Remove chat histories, recent screen names, transaction logs, and user profiles from instant messengers.

- Click **Perform Tune-up**. The Tune-up process begins first by creating a **System Restore Point**; it then performs the Tune-up.

**Figure 132. System Tuner Performing Tune-up / Creating Restore Point**

- When the System Tuner has completed its tasks, it indicates that the **Tune-up Completed**, providing a list of what it did (depending upon what you selected).

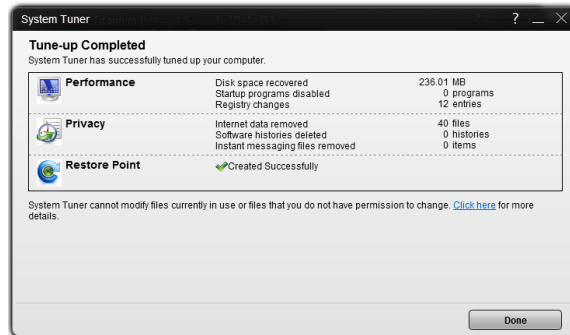


Figure 133. Tune-up Completed

7. During the system tune-up process, a dialog will ask if you wish to create a tune-up schedule.

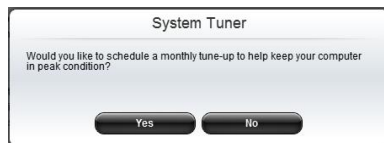


Figure 134. System Tuner Dialog

8. Click **Yes** to set up a schedule. However, you can also set up a System Tuner schedule by clicking **Set Schedule** in the System Tuner panel in the main Titanium Console.

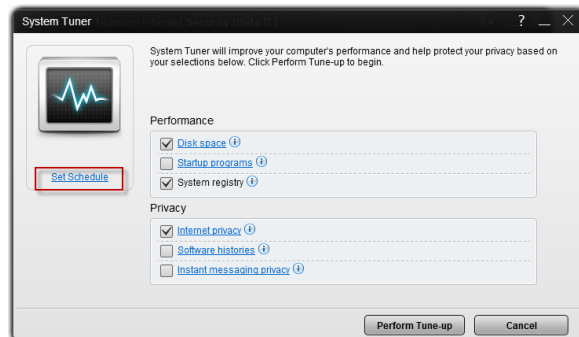


Figure 135. System Tuner > Set Schedule

Either way, the scheduler appears, with the toggle set to **On**.

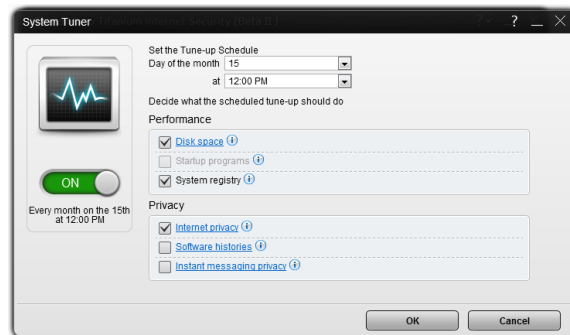


Figure 136. System Tuner Schedule On

9. Select the **Day** and **Time** you wish to perform the automatic tune-up using the pop-up menus. The default day and time is the 15th of the month at 12:00PM.
10. Click **Performance** and **Privacy** links to select subcomponent options. The subcomponents list appears.



Figure 137. System Tuner Subcomponents (Disk Space Options)

11. Check the checkbox of component(s) to include them in the tune-up. (See figure above.)
12. Click **OK** to save your changes.
13. Titanium creates a **System Restore Point** before it makes any changes to your system, enabling you to go back to a previous restore point at any time.

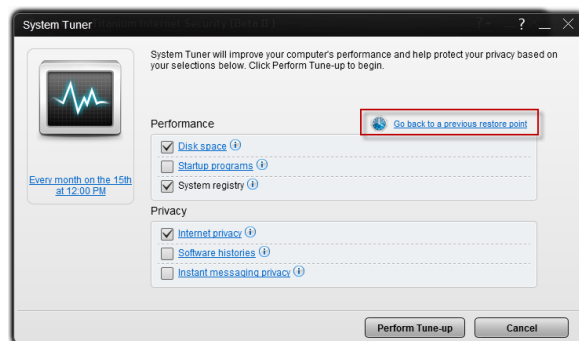


Figure 138. Go back to a previous restore point

14. Click **Go back to a previous restore point** to restore the computer to its previous state. The **Choose a Restore Point** window appears.

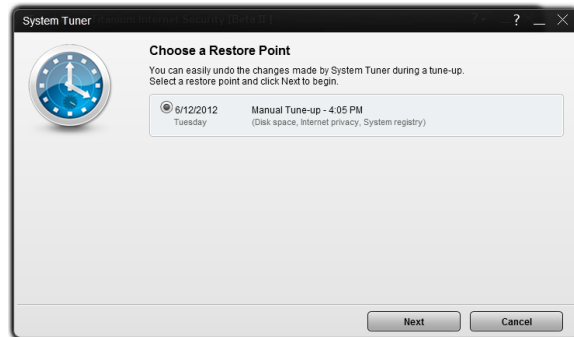


Figure 139. Choose a Restore Point

15. Select a date using the radio buttons and click **Next**. The **Confirm Restore Point** window appears.

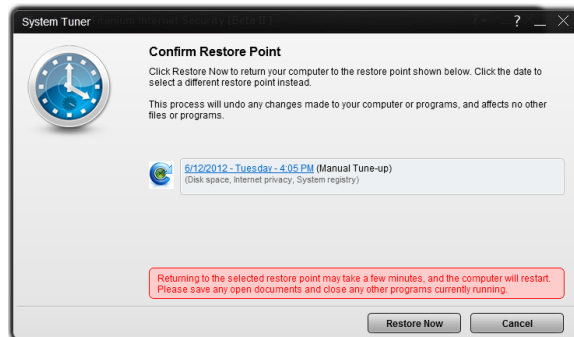


Figure 140. Confirm Restore Point

16. Click **Restore Now** to restore to the chosen Restore Point.
17. Restoring to the selected restore point may take a few minutes and the computer will restart. Save any open documents and close any programs before restoring to the Restore Point.

Security Report: System Tuner

Once you have conducted one or more system tune-ups, you can view a System Tuner Security Report.

To view a System Tuner Security Report:

1. Open the **Titanium Console**.



Figure 141. Security Report Tool

2. Click the **Security Report** tool. The **Security Report** appears, with **Threats** selected by default.
3. Select the **System Tuner** icon in the left-hand Command Menu. The **System Tuner Security Report** appears.

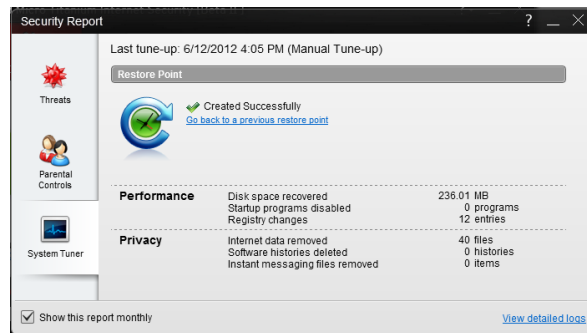


Figure 142. System Tuner Security Report

4. Depending upon which System Tuner jobs have been conducted, the System Tuner Security Report will provide a summary and details.
5. Click **Go back to a previous restore point** to perform a restore.
6. Note that **Show this report monthly** is preselected to show it monthly on the first of each month. You'll be notified when the report is ready.
7. Click **View detailed logs** to see the detailed logs for **System Tuner**.

Date/Time	Item	Results
6/12/2012 4:05 PM	Internet privacy	Successfully removed
6/12/2012 4:05 PM	System Registry	Successfully removed
6/12/2012 4:05 PM	Windows Update download temp file	Successfully removed
6/12/2012 4:05 PM	Temporary Files	Successfully removed
6/12/2012 4:05 PM	Temporary Internet Files	Successfully removed
6/12/2012 4:05 PM	Temporary Files	Unable to remove
6/12/2012 4:05 PM	Temporary Internet Files	Unable to remove
6/12/2012 4:05 PM	Restore Point	Successfully created

Any data more than 30 days old will be deleted automatically.

Figure 143. System Tuner Logs

8. Click **Remove all** to remove the logs.
9. Click **Export** to export the log in .CSV or .TXT format.

Data: Data Theft Prevention

Data Theft Prevention prevents hackers and spyware from stealing sensitive data like credit card numbers, passwords, and email addresses. It can also stop children from accidentally sending out personal information through email, via instant messaging, or to untrustworthy websites.

To activate **Data Theft Prevention** in Titanium Internet Security (or Maximum Security) you first have to enter an email address and password. See the previous section for **Titanium Antivirus+** to obtain instructions on doing this.

To activate Data Theft Prevention:

1. Click **Data** tab in the Console. The **Privacy** screen appears, showing the tools available.



Figure 144. Data Theft Prevention

Note: This screen also presents an offering for Trend Micro DirectPass, our secure password manager that lets you manage all your online credentials using a single master password. Click *Start a Free Trial* to get started with a five-password version of DirectPass.

- Click the **Data Theft Prevention** button. Titanium provides you with an introduction to Data Theft Prevention.

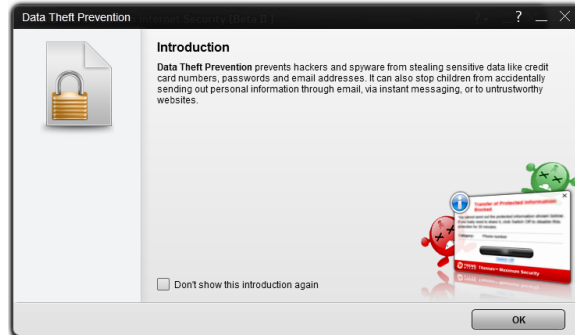


Figure 145. Data Theft Prevention Introduction

- Click **OK** to close the introduction. The **Password** screen appears.



Figure 146. Select a Password

- Enter your password and confirm it. Fill out the **Password hint** and **Email address**, in case you forget your password later. This will enable Trend Micro to send you a new password. Then click **Create**. The **Data Theft Prevention** settings screen appears, with the toggle set to **Off** by default.



Figure 147. Data Theft Prevention On

- Click the slider to **On** to enable **Data Theft Protection**.

6. Titanium Internet Security provides you with some suggested categories such as **Email address, Phone number, Credit card**. You can edit any category name by typing over it.
7. In the **What to Protect** column, type the actual data you wish to protect; for example, in the Email address field you might type john.doe@yahoo.com.
8. Click **+New Category** to add a new category.
9. Click the trashcan in the right-hand column of **What to Protect** to delete any category.
10. Click **Ok** to save your changes/additions.

DTP Limitations

- Data Theft Prevention won't protect the receiving data via POP3 traffic.
- Data Theft Prevention monitors HTTP traffic (ports 80, 81, 8080, and any proxy server port you configure in your Microsoft® Internet Explorer® settings), but not HTTPS traffic (i.e., encrypted information cannot be filtered, such as webmail).
- Data Theft Prevention uses SMTP on TCP port 25/587 and is blocked as spec. TLS and SSL encryption authentication don't block as spec. Most free webmail programs provide TLS and SSL encryption authentication such as Hotmail, Gmail, and Yahoo! Mail.
- Data Theft Prevention doesn't monitor "IMAP" traffic as spec. An IMAP server is generally used with programs such as Microsoft Exchange Server, Hotmail, Gmail, AOL Mail.
- Data Theft Prevention can protect a maximum of 20 entries that have different data and categories.

Data: Secure Erase

Deleting a file just removes the directory information used to find it, not the actual data. The **Secure Erase** function first provided in Titanium Internet Security (an also in Maximum Security) overwrites the unwanted file with data, so no one can retrieve the contents; while **Permanent Erase** overwrites the unwanted files making seven passes (overwriting the files 21 times, meeting US Government Security Standards).

To enable Secure Erase / Permanent Erase:

1. Click **Data > Secure Erase**.



Figure 148. Privacy > Secure Erase

2. The **Secure Erase Introduction** window appears.

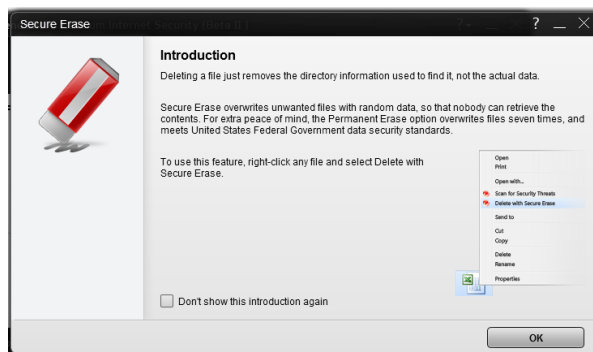


Figure 149. Secure Erase Introduction

3. Click **OK** to close the **Introduction** window. The **Type of Erase** window appears, with **Quick Erase** selected by default.

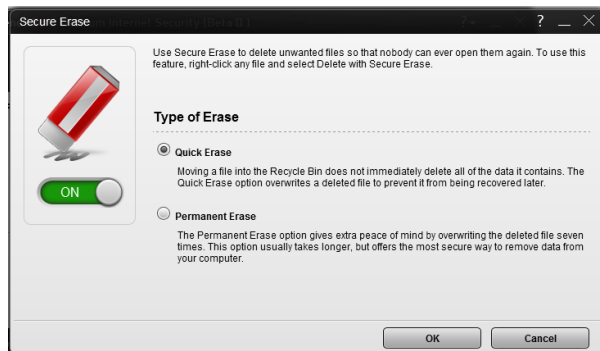


Figure 150. Type of Erase

4. Move the slider to **On** to enable the function.
5. Keep **Quick Erase** or select the **Permanent Erase** button.
6. Click **OK** to save your changes.

To Secure/Permanent Erase a file:

1. Right-click a folder or file to perform a Quick/Permanent Erase. A file processing popup appears.

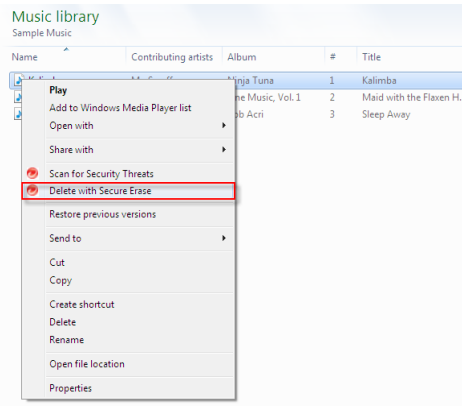


Figure 151. Right-click File for Secure Erase

2. Select **Delete with Secure Erase / Permanent Erase**.
3. The folder or file is securely deleted.

Family: Parental Controls

The **Parental Controls** tool in Titanium Internet Security (and Maximum Security) lets you protect your children from inappropriate websites, limit their time on the internet, and see detailed reports about what they do online, without having to look over their shoulders.

To enable **Parental Controls** in Titanium Internet Security you first have to enter an email address and password. See the previous section on **Data Theft Prevention** to obtain instructions on doing this.

To enable Parental Controls:

1. Click the **Family** tab in the Titanium Console. The **Family** screen appears.

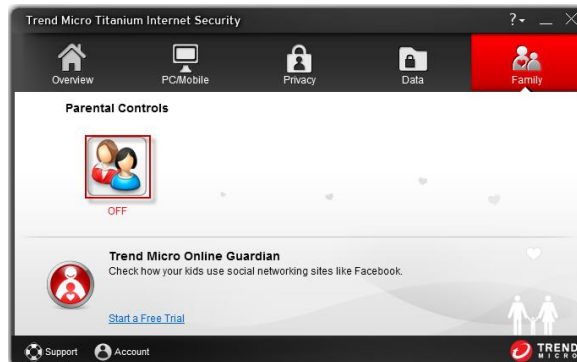


Figure 152. Family > Parental Controls

Note: This screen will also display a Free Trial message about Trend Micro Online Guardian, which provides enhanced controls for monitoring family internet usage. Click *Start a Free Trial* to get started with a 30-Day Free Trial of Online Guardian.

- Click the **Parental Controls** button in the **Family** screen. The **Parental Controls** Introduction screen appears.

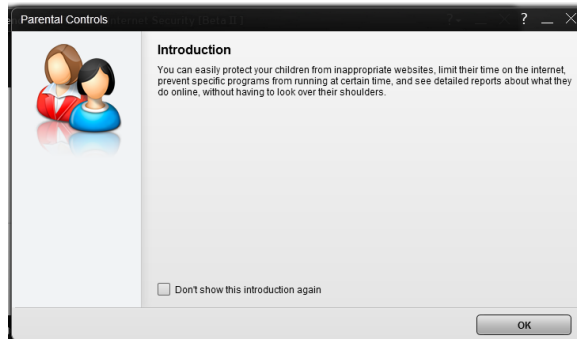


Figure 153. Parental Controls Introduction

- Read the instructions and click **OK** to continue. A screen appears for you to enter your Password.

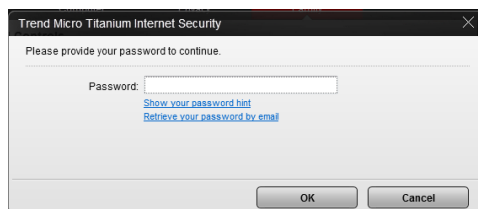


Figure 154. Enter Password

- Enter your Password and click **OK**. The **Parental Controls Get Started** screen appears.

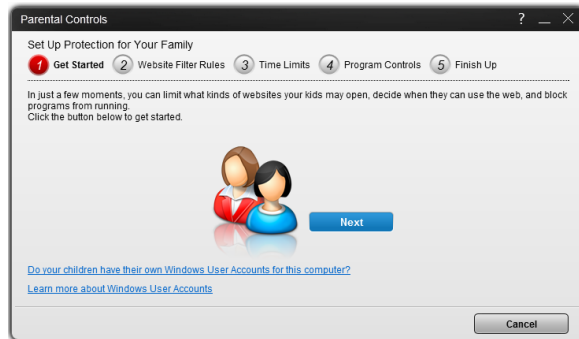


Figure 155. Parental Controls Get Started

5. **Important note:** the screen asks **Do your children have their own Windows User Accounts for this computer?** If they don't, click the link on the question to create them, so your various settings can be assigned to the proper child. The **Parental Controls > Add Windows Account** screen appears.

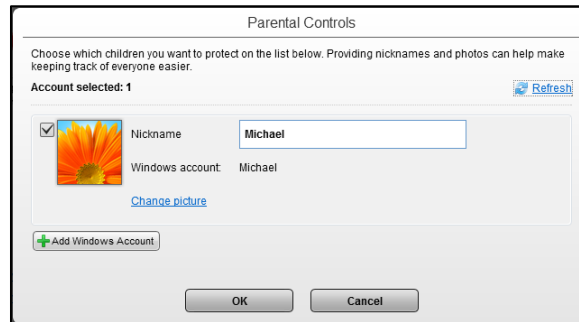


Figure 156. Parental Controls

6. In the lower left-hand corner, click **Add Windows Account**. The **Windows User Accounts** Control Panel appears.

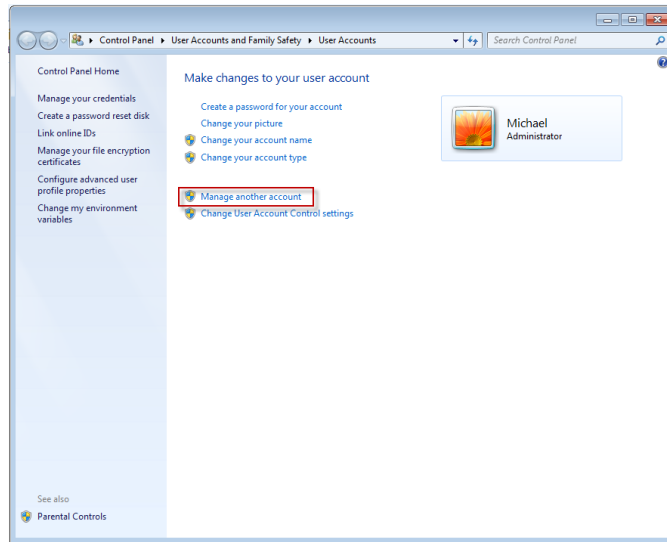


Figure 157. Windows User Accounts

7. Click **Manage another account**. The **Manage Accounts** screen appears.

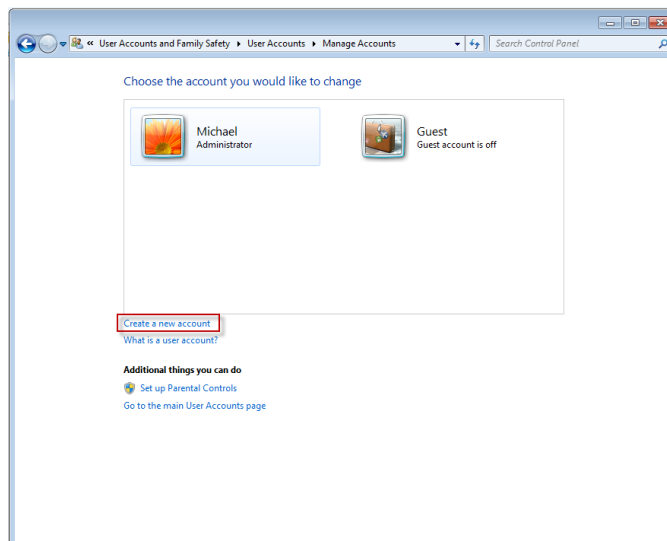


Figure 158. Windows Manage Accounts

8. Click **Create a new account**. A window to create an account appears.

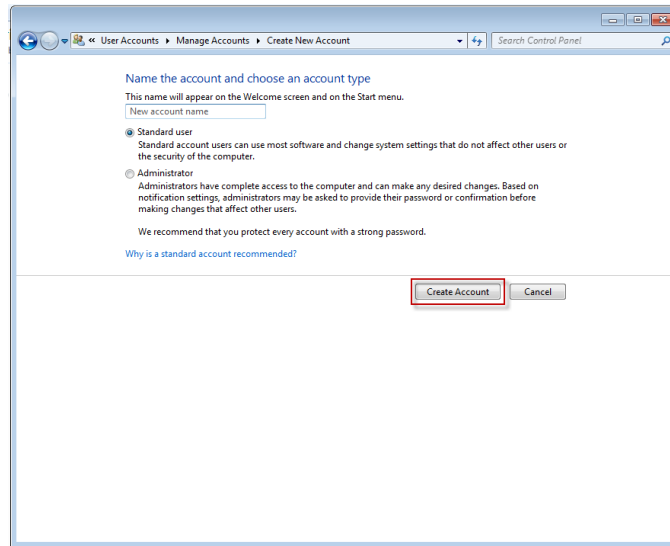


Figure 159. Name the Account

9. Type a name for the account (e.g., John), leave the default **Standard user** selected, and click **Create Account**. This creates the standard user account named **John**.

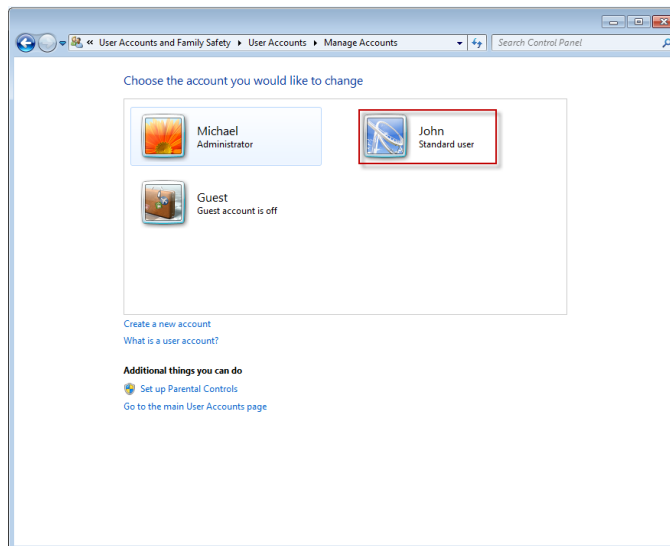


Figure 160. Standard Account - John

10. Click the **Close** box to close the **Manage Accounts** window.
11. Back in the **Select Kids to Protect** window, click the **Refresh** link if the new account is not showing. The **John** account now appears in the list.

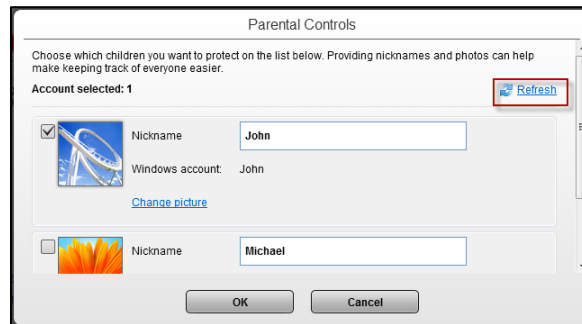


Figure 161. Guest Account Listed

12. Uncheck the account you're logged on to, check the **John** account, and click **OK**. A popup appears, telling you "You have not set the rules for one or more users. Let's set it up now."



Figure 162. Set Up Rules Popup

13. Click **Ok**. The **Step 2 - Website Filter Rules** page appears.

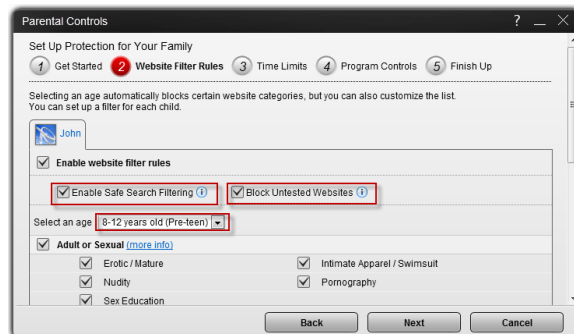


Figure 163. Step 2: Website Filter Rules

14. In the **Select An Age** popup, choose the age the filter will apply to from the **Select an age** pop-up. For example, choose **Ages 8-12 (Pre-teen)**. (You can also define a **Custom** age bracket.)
15. A subset of the general categories is selected by default; for example, all of **Adult or Sexual**. Other subcategories in Communications or Media, Controversial, and Shopping and Entertainment are checked. Scroll down to see the full category/subcategory listings.

You can check or uncheck a category or subcategory to redefine the filter. You can also obtain more information on a category by clicking the **more info** link; a definition list will pop up.

16. Check **Enable Safe Search Filtering** and **Block Untested Websites**. These options will increase your child's security when searching or browsing the Internet.
17. Click **Next** to define the **Time Limits**. The **Time Limits** page appears.

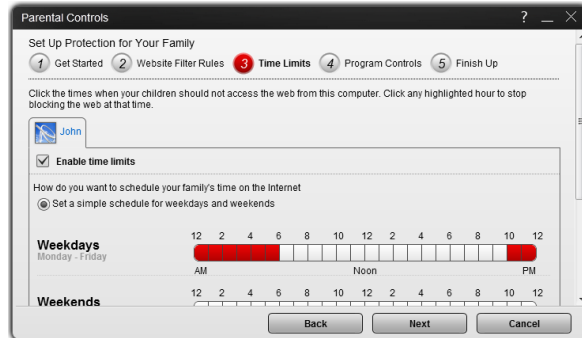


Figure 164. Time Limits

18. Using your mouse pointer, select the weekday and weekend hours you kids **should not** access the web by holding your mouse down and stroking across the hours, then scroll down and indicate the number of hours your children may use this computer.

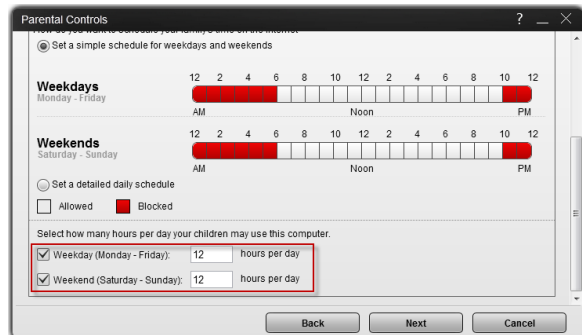


Figure 165. Allowed Hours on Computer

19. You may also click **Set a detailed daily schedule** to do so. The daily schedule panel appears.

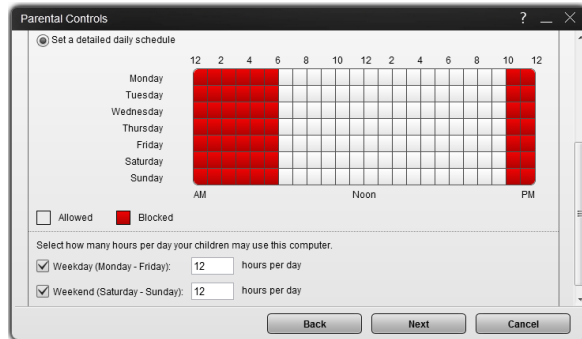


Figure 166. Detailed Daily Schedule

20. Adjust the daily schedule for each day as you see fit. Click **Next**. A screen appears, letting you set the child's program controls.

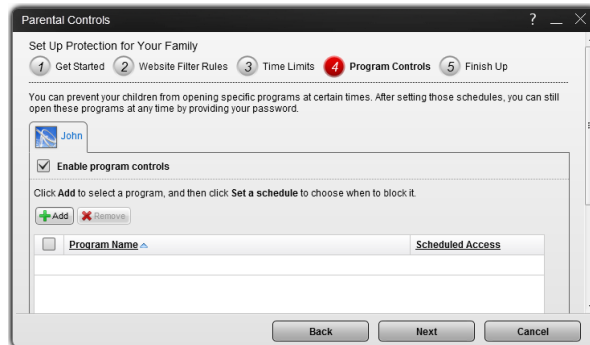


Figure 167. Program Controls

21. Click **Enable program controls**, then click **Add** to add the program you want to control the usage of.

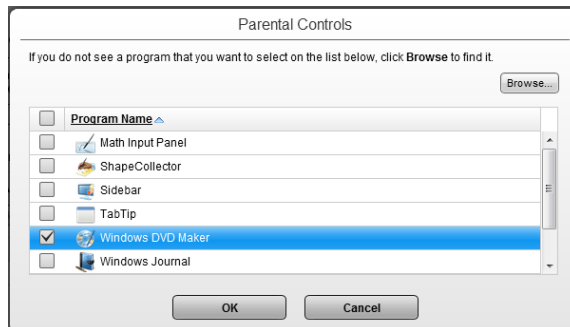


Figure 168. Program List

22. Select the program you want to control from the list, or click **Browse** to find it.

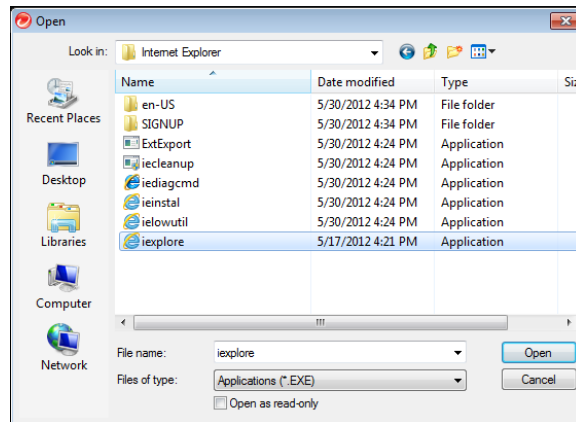


Figure 169. Browsing for Programs to Add to Program Controls

23. Navigate to the program, select it and click **Open**. Titanium adds it to the list.

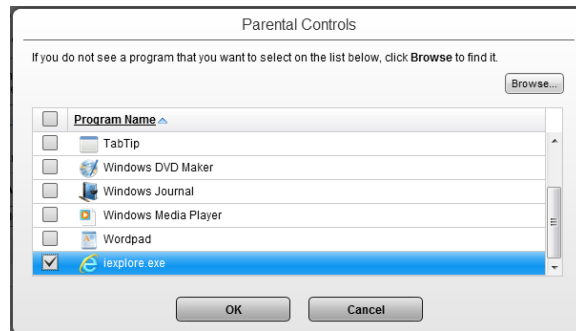


Figure 170. Programs in List | IE Added

24. Check the program checkbox and click **OK**.

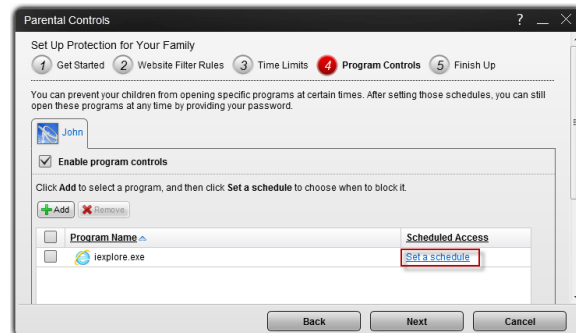


Figure 171. Set a Schedule

25. The program is added to the **Parental Controls** window. Click **Set a Schedule** in the **Scheduled Access** field. The schedule appears.

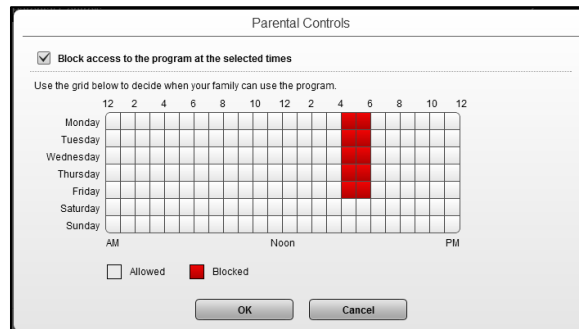


Figure 172. Access Schedule

26. Check **Block access to the program at the selected times**, then select the hours in the week the child will be prohibited use of the program, then click **OK**. When the wizard window appears, click **Next**.
27. A screen appears, indicating that protection has been activated for **John**, applying the **Pre-teen Website Filter**, giving the **Time Limits** and **Program Controls**.



Figure 173. "John" Protection Criteria

28. Click **Done** to finish adding the parental control for this child. The main **Parental Controls** window reappears.

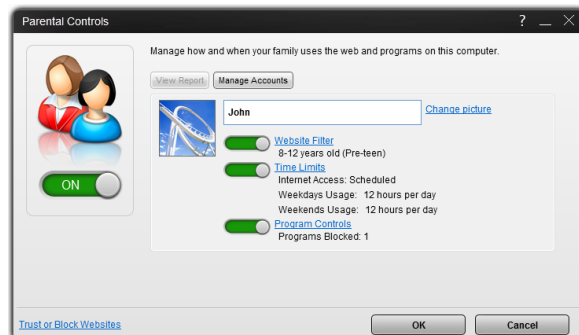


Figure 174. Slider is "On"

29. In **Parental Controls** the slider button should be **On**. If not, slide it to **On**, then click **OK**. The rule set is now applied to the **John** account.

30. Note that the link **Trust or Block Websites** allows you to set exceptions to your rules. This function was covered in the previous **Titanium Antivirus+** section. Go to [Exception Lists: Websites](#) for details.
31. Note also that you can turn the **Website Filter**, **Time Limits**, and **Program Controls** functions on or off by using the appropriate slider. You can also edit the functions by clicking the hotlinks and making your changes in the respective editor.
32. Click **OK** to close the **Parental Controls** window, note that **Parental Control** status is now **ON** in the **Tools** popup, then click the respective **Close** boxes to close the **Tools** pop-up and the **Titanium Console**.
33. Log off the **Administrator's** account (or switch users) and log on using the **John** account.
34. Using your browser, attempt to go to a website at a time prohibited by the account rules. Titanium will block access to the web and provide a **No Web Surfing Allowed** notification, indicating the user cannot use the web at this time.

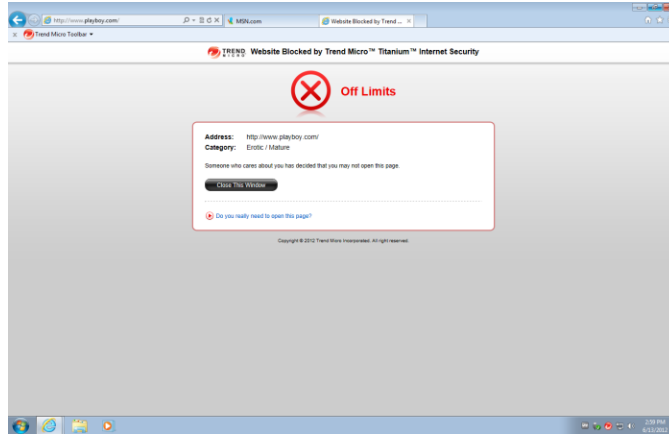


Figure 175. No Web Surfing Allowed Notification

35. During the hours allowed for surfing, if the user attempts to browse to a site not permitted by the rules, Titanium will block access to the site and provide an **Off Limits** notification for the user in the browser.

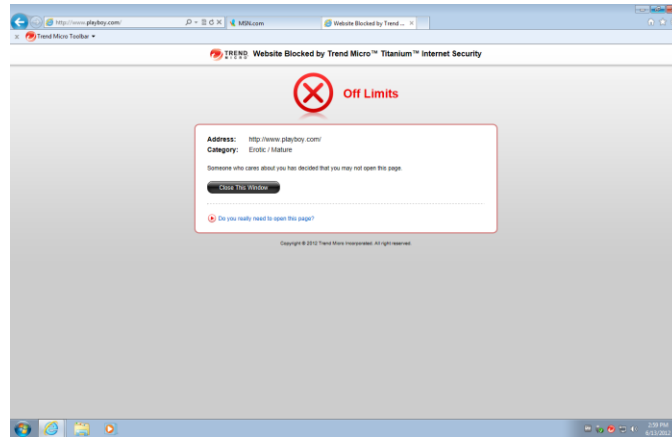


Figure 176. Titanium Off Limits Notification in Browser

Security Report: Parental Controls

Once you've enabled Parental Controls, Titanium Internet Security provides a security report that can give you basic information about how many times your kids have attempted to access prohibited sites and the kinds of website violations they are.

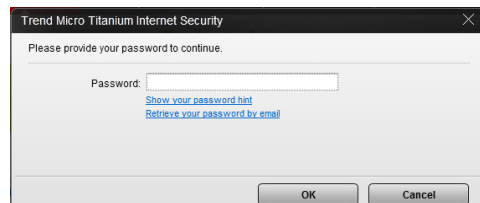
To view the Parental Controls Security Report:

1. Open the Titanium Console.



Figure 177. Console > Reports

2. Click the **Reports** icon. The **Password** screen appears.



3. Enter your password and click **OK**. The **Security Report** window appears.

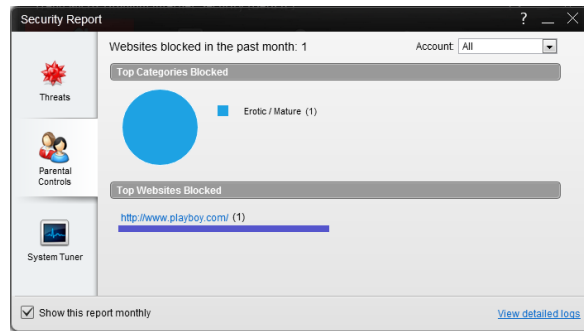


Figure 178. Parental Controls

4. Click the **Parental Controls** tab in the left-hand column to show the **Parental Controls Security Report**. The report will show the **Top Categories** and **Websites Blocked**. Use the Account pop-up to show the report for **All users**, or for a specific user account; e.g., "John."
5. Check **Show this report monthly** to show it on the first of each month. You'll be notified when the report is ready.
6. Click **View Detailed logs**, then **Parental Controls** in the **View** dropdown menu to display the **Parental Controls** logs.

The screenshot shows the 'Logs' window with a dropdown menu set to 'Parental Controls' and 'Total records: 2'. It includes 'Remove all' and 'Export' buttons. The table below displays the log entries.

Date/Time	Blocked Websites	User Name
6/13/2012 3:01 PM	http://www.msn.com/?ocid=iehp	John
6/13/2012 2:59 PM	http://www.playboy.com/	John

Any data more than 30 days old will be deleted automatically.

Figure 179. Parental Controls Logs

7. Click **Remove all** to delete the logs
8. Click **Export** to export the Parental Controls log in .CSV or .TXT format.

Chapter 6: Trend Micro Titanium Maximum and Premium Security

Protection Overview

Trend Micro Titanium Maximum is functionally the most robust version of Titanium, providing everything previously described in the Titanium Antivirus+ and Internet Security chapters, but adding additional protections and tools. To enable all functions, you need a paid version of Titanium Maximum Security.

Titanium Premium Security is an enhanced package for Titanium Maximum Security, providing more sync/backup space (25GB) in the cloud.



Figure 180. Titanium Maximum Security Welcome Screen

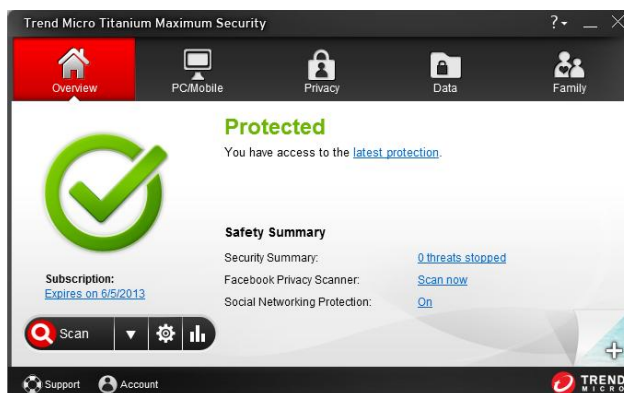


Figure 181. Titanium Maximum Security Console Overview



Figure 182. Privacy | Facebook Privacy Scanner



Figure 183. Data > Trend Micro Vault, DirectPass, SafeSync

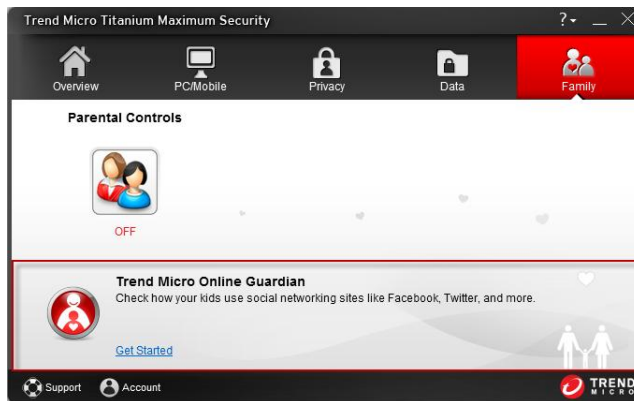


Figure 184. Trend Micro Online Guardian

Note: Titanium Maximum Security Additional Features: Facebook Privacy Scanner, Trend Micro Vault. Additional Offerings: 5GB of SafeSync.

Note also that full paid versions of Mobile Security for Android, DirectPass, and Online Guardian are included in your purchase of Titanium Maximum Security.

ADDITIONAL TOOLS FOR TITANIUM MAXIMUM SECURITY PAID VERSION

Trend Micro Vault

Users can enable a password-protected folder that can safeguard sensitive files. If the computer is lost or stolen, the vault can be sealed shut by remote control until the computer is return to its rightful owner.

SafeSync

Titanium Maximum Security users are provided with 5GB of cloud storage for backup and sync using Trend Micro SafeSync. Titanium Premium Security users can boost their SafeSync storage space to 25GB. SafeSync keeps all your files in sync across all platforms that have it installed.

Data: Trend Micro Vault

Trend Micro Vault is a password-protected folder that can safeguard your sensitive files. Using a password, files inside the vault are kept invisible until you enter the password. If your computer is stolen, Trend Micro Vault can also seal itself shut by remote control, so that even using the password you cannot open the vault—that is, until the computer is returned to its rightful owner.

To set up Trend Micro Vault:

1. In the Titanium Console, click **Data > Trend Micro Vault**.



Figure 185. Data > Trend Micro Vault

2. The Introduction to **Trend Micro Vault** appears.

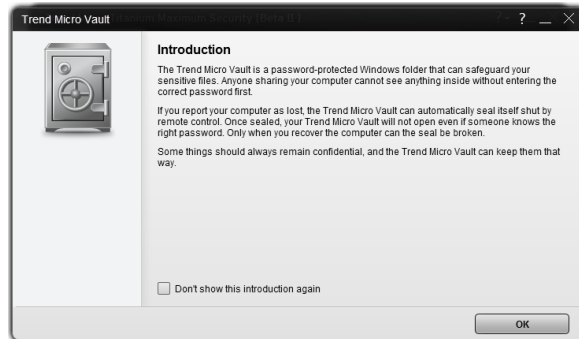


Figure 186. Trend Micro Vault Introduction

3. Click **OK** to close the introduction. The **Password** entry screen appears.

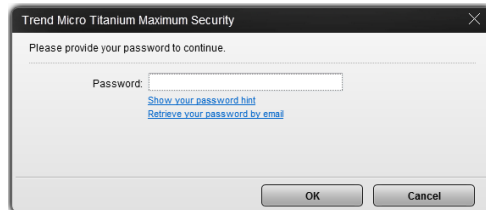


Figure 187. Enter Password

4. Enter your **Password** and click **OK**. An activation dialog appears, indicating to trial users that their upgrade to a paid version of Titanium Maximum Security lets them initialize the Trend Micro Vault.



Figure 188. Trend Micro Vault Initialized

5. Click **OK**. The **Trend Micro Vault** window appears.

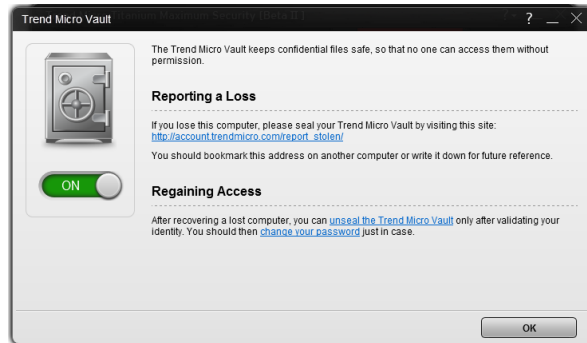


Figure 189. Trend Micro Vault

- The **Trend Micro Vault** desktop icon also appears on your desktop.



Figure 190. Trend Micro Vault Desktop Icon

- You can now use Trend Micro Vault to protect your sensitive files, to seal the vault if your computer is stolen or misplaced, and to regain access to the vault if you've turned it off.
- To open the Trend Micro Vault, double-click the desktop icon. The password window appears.

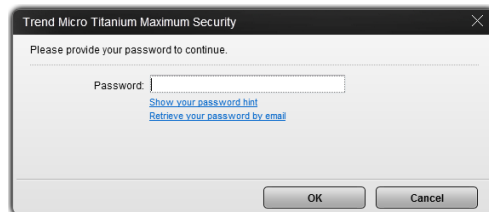


Figure 191. Trend Micro Vault > Password Protection

- Enter your password and click **OK**. This opens the **Trend Micro Vault**.

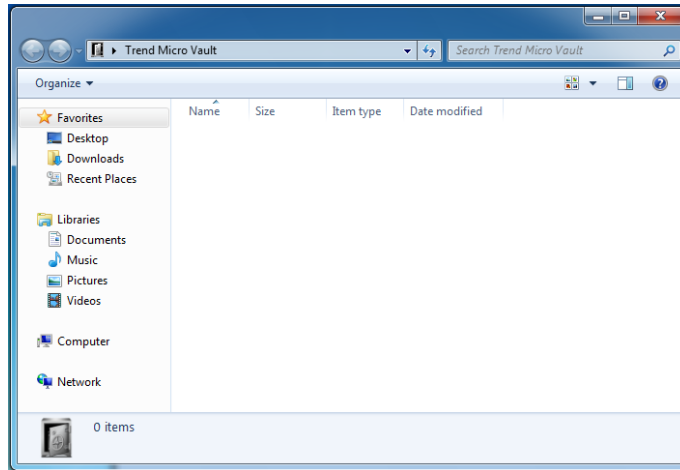


Figure 192. Trend Micro Vault

10. Drag files and folders you wish to protect into the **Trend Micro Vault**, then close it.

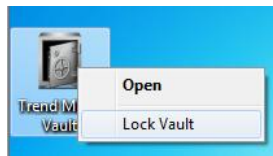


Figure 193. Lock Vault Menu Item

11. Right-click the Vault and select **Lock Vault** to lock it. A dialog appears, warning you to that locking the vault does not automatically block access to files currently open. Make sure you close all files that need protection before you lock the Vault.

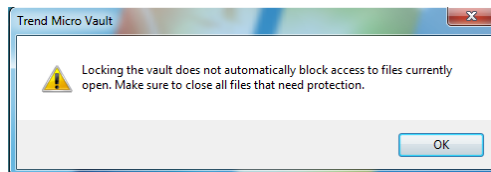


Figure 194. Trend Micro Vault Warning

12. Click ok to close the dialog.
13. In the Trend Micro Vault window, note the link http://account.trendmicro.com/report_stolen/ for reporting a loss.

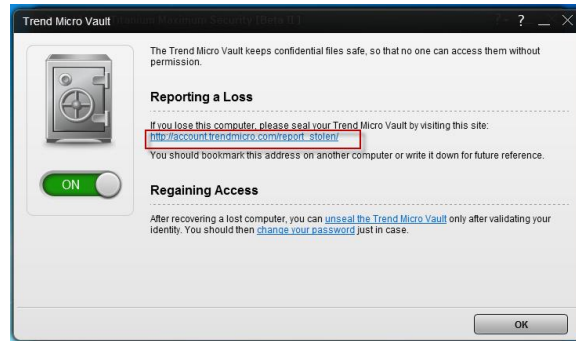


Figure 195. Reporting a Loss

14. You should bookmark this address on another computer or write it down for future reference. Clicking it takes you to the Trend Micro Vault **Report Stolen** webpage, where you can report the loss.

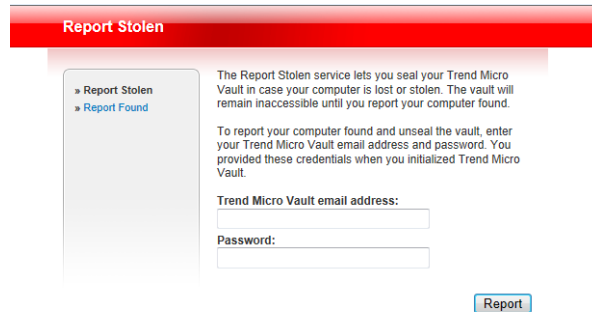


Figure 196. Report Stolen Service

15. Enter your Trend Micro Vault email address and password and click **Report** to seal the vault. Once you do, your Vault-protected folders and files cannot be opened, even if they knew your email address and password.
16. Once you recover the computer, return to the Trend Micro Vault console and click the link **Unseal the Trend Micro Vault**.

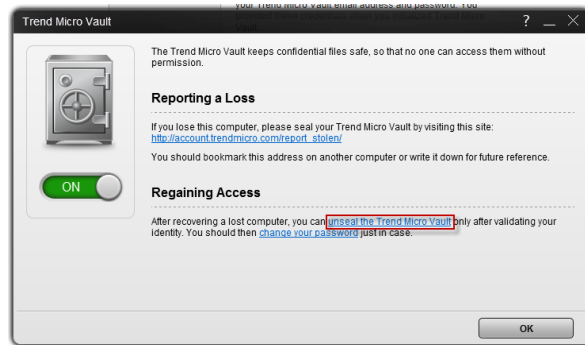


Figure 197. Regaining Access

17. This takes you to the Trend Micro Vault Report **Report Found** webpage, where you can unseal the Vault.

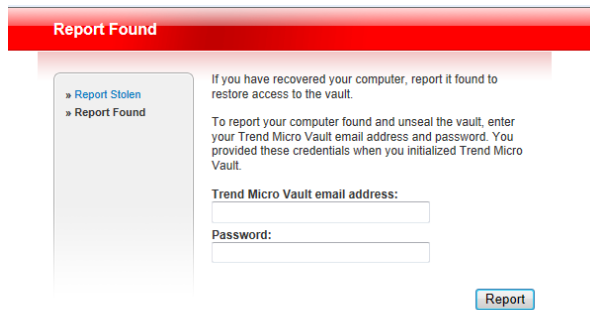


Figure 198. Report Found

18. Enter the **Trend Micro Vault email address** and **Password** and click **Report**. This unseals the Vault and you're notified by Titanium.
19. For your safety, you should now change your Titanium password.

Chapter 7: Titanium Help and Support

All Titanium editions provide **Help** in the form of a popup menu and a **Support** hotlink in the Console.

To access Help and Support:

1. Open the Titanium Console.



Figure 199. Titanium Console

2. Note the ? (**Help**) menu in the upper right-hand and the **Support** hotlink in the lower left-hand corners of the console.
3. Click the **Support** link to take you directly to the Trend Micro Support webpage.

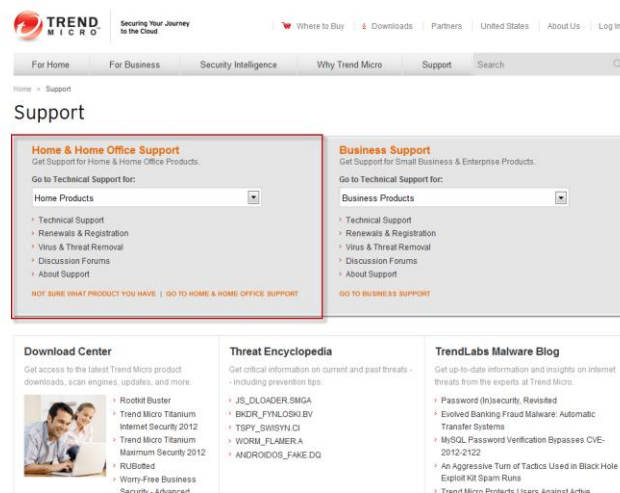


Figure 200. Trend Micro Support

4. Select the ? (**Help**) menu to display the submenus.

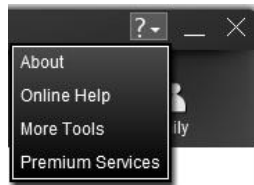


Figure 201. ? (Help) Menu

5. Select **About** to initiate a manual program update and to display details about your edition, version, type, serial number, and expiration date.

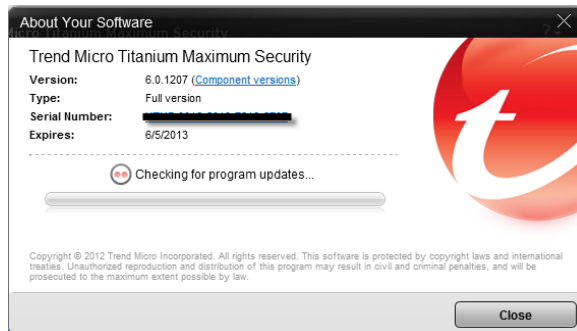


Figure 202. About Screen

6. You can click the **Component versions** hotlink to get information about your component versions.

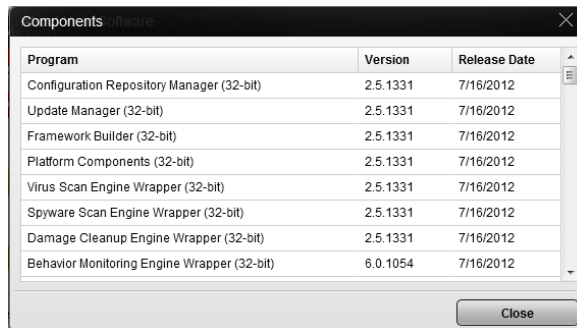


Figure 203. Component Versions

7. You can click the **Serial Number** hotlink to view and change your serial number.



Figure 204. Enter the Serial Number

8. Select **Online Help** to display the **Online Help** webpage. Navigate through **Online Help** using the menus and hotlinks; conduct a search using keywords.

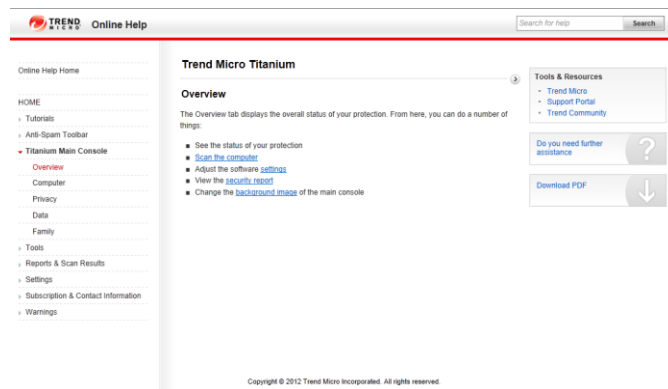


Figure 205. Titanium 2012 Online Help

9. Select **More Tools** to take you to a webpage to obtain more tools in the **Free Tools Center**.

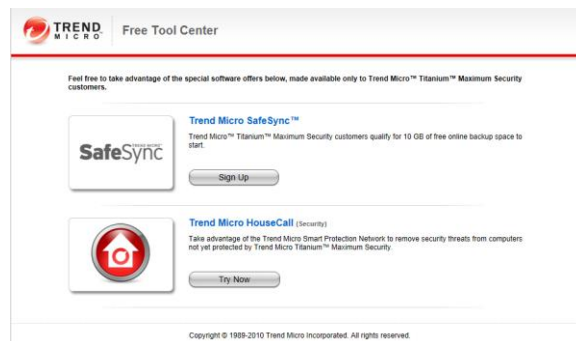


Figure 206. Free Tools Center

10. Select **Premium Services** to access a webpage for everything you need to know about **Premium Services for Home Users**.

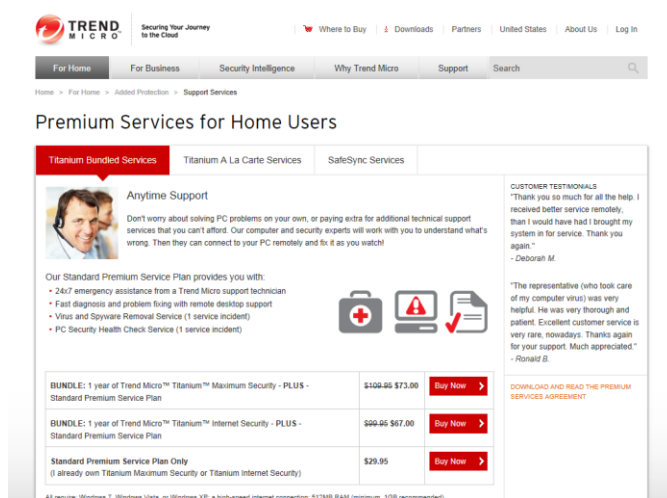


Figure 207. Trend Micro Products and Services

11. Select the **Account** button in the lower left-hand corner of the Titanium Console to access the **Trend Micro Account** webpage.

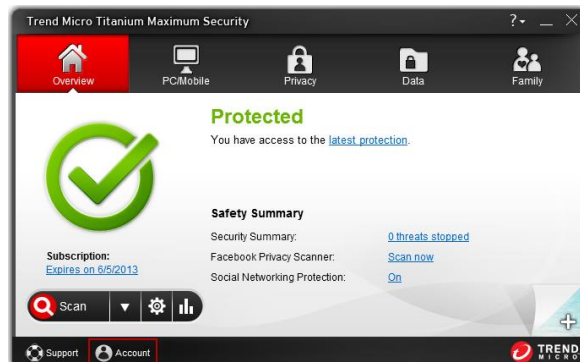
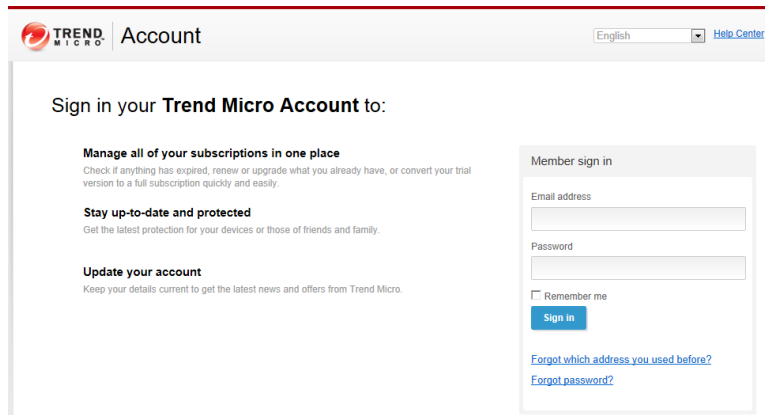


Figure 208. Titanium Console > Account



The screenshot displays the Trend Micro Account Webpage. At the top, the Trend Micro logo is on the left, followed by the word "Account". On the right, there is a language dropdown menu set to "English" and a "Help Center" link. The main content area is titled "Sign in your Trend Micro Account to:". Below this title, there are three sections of text: "Manage all of your subscriptions in one place" (with a subtext about checking expiration and upgrading), "Stay up-to-date and protected" (with a subtext about getting the latest protection), and "Update your account" (with a subtext about keeping details current). To the right of these sections is a "Member sign in" box. This box contains input fields for "Email address" and "Password", a "Remember me" checkbox, and a blue "Sign in" button. Below the button are two links: "Forgot which address you used before?" and "Forgot password?".

Figure 209. Trend Micro Account Webpage

12. In the **Trend Micro Account Webpage**, you can sign in to your account if you've already purchased Trend Micro products or services, manage all of your subscriptions in one place, stay up-to-date and protected by getting the latest protection for your devices or those of friends and family, and you can update your account.

Chapter 8: Applications Bundled with Titanium

Introduction

Trend Micro™ Titanium is bundled with additional applications to expand your protection. The programs provided depend upon your edition of Titanium.

Table 7. Titanium Bundled Programs

Tool	Titanium Antivirus+	Titanium Internet Security	Titanium Maximum Security	Titanium Premium Security
Mobile Security for Android	√*	√*	√	√
Titanium for Mac	√**	√	√	√
Online Guardian			√	√
DirectPass		√ (5 Accts)	√ (No limit)	√ (No limit)
SafeSync			√ (5GB)	√ (25GB)
Security Center	√	√	√	√
SafeGuard Browser (W8)	√	√	√	√
Go Everywhere (W8)			√	√

*Lite Edition | **With 3-device subscription to Titanium

To get access to the bundled applications:

These applications are variously available from the **Titanium Welcome** screen or the category tabs in the **Titanium Console**, depending on your version of Titanium, as indicated above and in the previous chapters.

1. Simply click the **icon** or **hotlink** in the Welcome Page or Titanium Console tab to access the webpage where you can download the applications.
2. For detailed instructions on how to use these applications, go to www.trendmicro.com to download the relevant Product Guides:
 - *Trend Micro™ Mobile Security 2.2 - Product Guide*
 - *Trend Micro™ Titanium™ Internet Security for Mac 2.0 - Product Guide*
 - *Trend Micro™ DirectPass™ 1.2 - Product Guide*
 - *Trend Micro™ Online Guardian for Families 1.5 - Product Guide*
 - *Trend Micro™ SafeSync™ for Consumer 5.0 - Product Guide*
 - *Trend Micro™ SafeSync™ for Business 5.0 – Product Guide*

Mobile Security

Trend Micro™ Mobile Security protects your Android™ device from loss, malicious apps, and web threats. It's provided with all editions of Titanium.

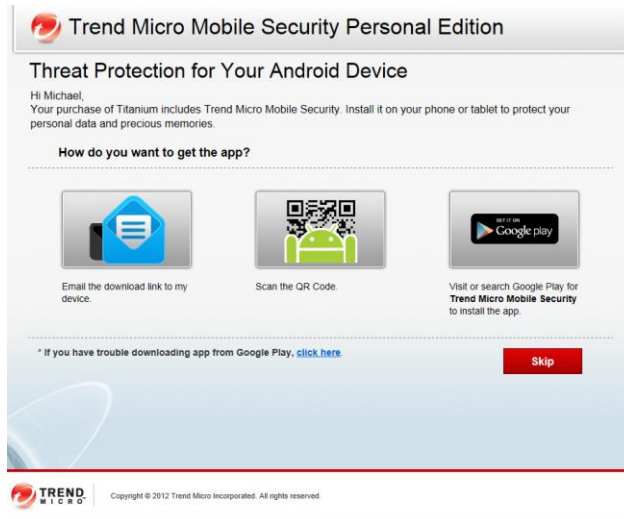


Figure 210. Trend Micro Mobile Security Personal Edition

Mobile Security protections include the following:

Trend Micro Mobile Security for Android

- Locate, lock and remotely erase data if your device is lost or stolen
- Block unwanted calls and texts
- Scan apps for viruses and other threats
- Enable parental controls to keep kids safe

Trend Micro SmartSurfing for iOS

- The first iPhone application to provide a secure web browsing environment is now also available for iPad/iPad2
- Protects against malicious web sites
- Blocks access to known phishing sites
- Blocks access to sites with malicious intentions such as drive-by downloads, malware, spyware
- Powered by the Smart Protection Network
- Uses Trend Micro web reputation

Trend Micro Mobile Security for Symbian (Nokia) and Windows Platforms

- Supports Symbian 3rd and 5th Editions, Windows Mobile v6.5
- Remote Wipe
- SIM Card Protection
- Web Threat Protection
- SMS Anti-spam

- WAP Push Protection
- Parental Controls
- Antivirus
- Firewall
- Automatic Updates

Titanium Internet Security for Mac

Trend Micro™ Titanium™ Internet Security for Mac protects your identity and personal data from malicious threats when you shop, bank, or browse online. In the Maximum and Premium versions of Titanium, you have the flexibility to allocate this protection on your Macintosh devices

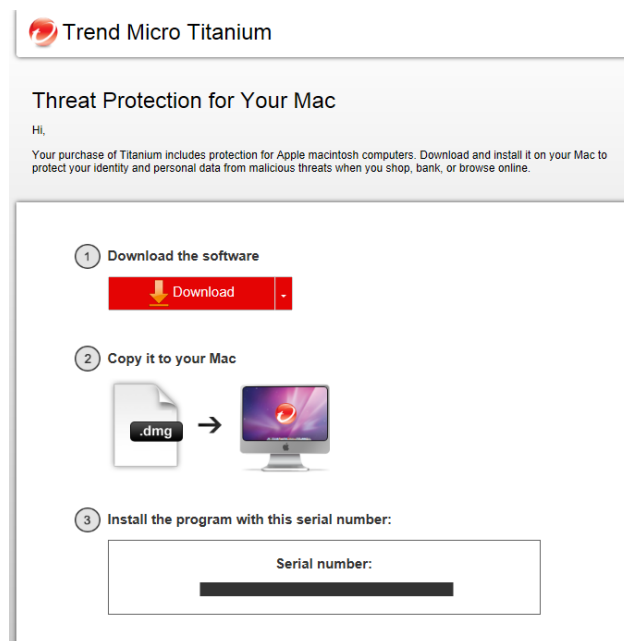


Figure 211. Trend Micro Titanium Internet Security for Mac

Titanium Internet Security for Mac protections include the following:

Essential Protections

- Defends against viruses, worms, Trojan horse programs, and other everyday security threats
- Guards against spyware and other malicious software
- Includes free automatic updates so your protection stays current against new threats

Web Protections

- Blocks IM and email links that lead to dangerous websites
- Protects against phishing scams that can trick you into revealing confidential information
- Prevents websites from installing dangerous software on your Mac

Parental Controls

- Restricts Internet access by content categories
- Controls access to chat and IM sites
- Allows you to block specific websites

Online Guardian

Trend Micro™ Online Guardian for Families helps you protect your children against Internet dangers, including cyberbullying and online predators. It lets you monitor your kids' Internet activity 24x7 from anywhere and take action to keep them safe. In one easy-to-read report, you'll get a clear view of what your kids are doing online. Online Guardian shows web browsing history, wall postings, messages, photos, and chats.

With Internet monitoring and filtering, Online Guardian helps you safeguard your children and prevent damage to their online reputations. Also, it lets you set age appropriate rules for your kids' Internet activities that include filtering out adult content and limiting their time online.

Online Guardian is available with the Titanium Maximum and Premium versions.

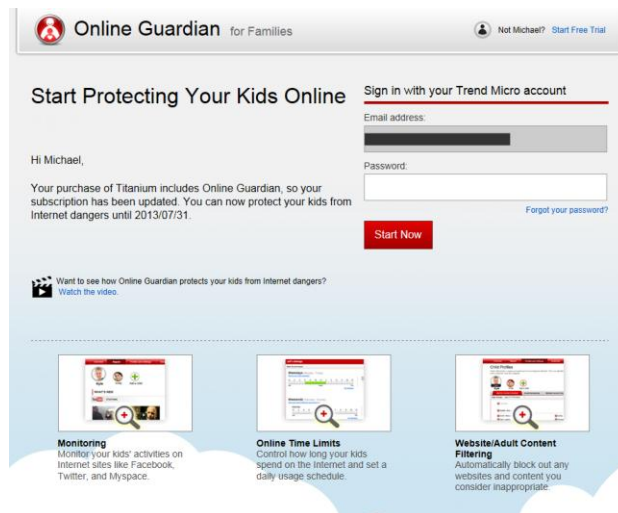


Figure 212. Trend Micro Online Guardian for Families

Key features include:

- Centralized online management console to manage and report events
- Social networking monitoring, protection and reporting (ex: Facebook, MySpace, Twitter, etc.)
- URL filtering and time management
- Instant messaging/chat monitoring with Data Loss Protection
- Password override capabilities
- Report on use of online medias (ex: Flickr and YouTube, etc.)

- Support installation for Windows OS
- Keyword search monitoring and reporting
- Common Sense Media forum integration
- Web crawler (generate report on social medias used)

DirectPass

Trend Micro™ DirectPass™ helps you manage and secure all your online credentials, ensuring an easy and safe online experience, while offering a faster, more secure, and convenient way to access web sites. Using a single Master Password, DirectPass users have instant access to all their login credentials, no matter where they're located or what device they're using.

DirectPass is provided with Titanium Maximum and Premium versions.

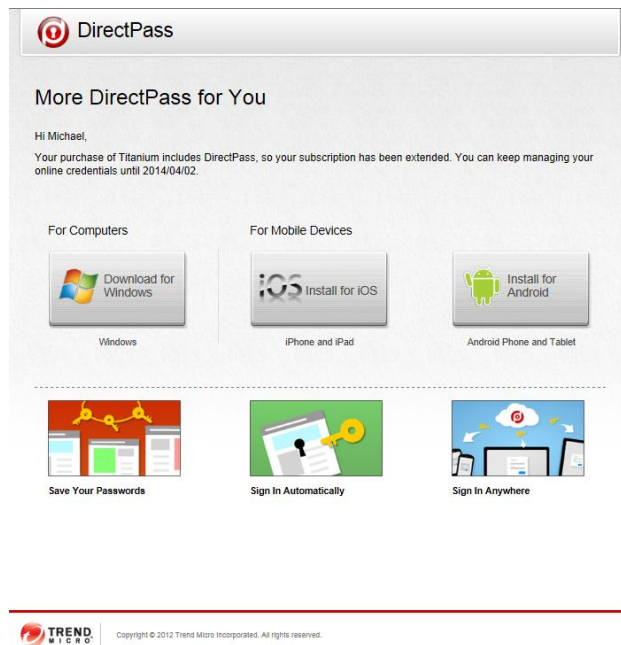


Figure 213. Trend Micro DirectPass

DirectPass features include:

- **URL and Password Management** - Automatically capture your websites and password login credentials in a complete secure environment
- **Cloud Storage and Synchronization** - Credentials are available across all devices where DirectPass is installed
- **Password Generator** - Automatically generate strong passwords with custom criteria for increased login security
- **Secure Notes Management** - Store and manage Secure Notes regarding your accounts, logins, and procedures.

- **Keystroke and Data Encryption** - All keystrokes are encrypted. AES 256-bit Encryption ensures the highest security for your data.
- **Secure Browser** - Use the Secure Browser to ensure complete security and privacy for online financial transactions.
- **Profile for Auto-Form Filling** - Create a Profile to enable auto-form filling when filling out online forms.
- **Mobile Support** - iOS and Android smartphones and tablet devices are fully supported.

SafeSync

Trend Micro™ SafeSync™ works where you want it to, backing up and syncing files between your computers and mobile devices. You can stream music and video to your smartphone, share photos with friends on your tablet, or just play it safe and keep secure backups of your most important memories on all your devices.

SafeSync is featured with the Titanium Maximum (5GB) and Premium (25GB) editions. Users with multi-seat subscriptions can allocate a seat (or seats) to SafeSync.

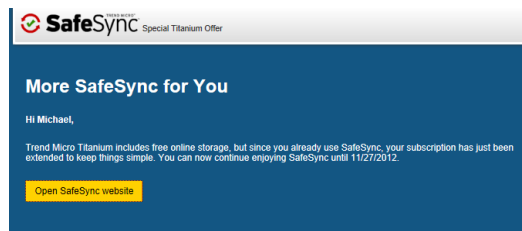


Figure 214. More SafeSync for You



Figure 215. Trend Micro SafeSync

SafeSync is provided in two versions: SafeSync for Consumer and SafeSync for Business. SafeSync for Consumer features include:

Synchronized Backup and Sharing

- SafeSync works quietly in the background, securely backing up your digital content to the cloud
- SafeSync keeps your files synchronized. When you make a change it filters down to your other SafeSync enabled computers
- Your files are at your fingertips, so you can access them anytime and anywhere from any computer or mobile device
- You can invite your Facebook, Hotmail, or Gmail contacts to view your shared albums, or send links directly to family and friends.
- SafeSync synchronizes your PC and Mac, as well as your Android or iOS smartphone or tablet

SafeSync Security

- Trend Micro cannot see your files without your authorization
- Data is transferred using the same 256-bit AES encryption used by financial institutions for security
- You have the ability to share or revoke access to your shared files at any time
- Trend Micro firewalls defend equipment from cyber attack
- Trend Micro's network and server security systems use industry best practice secure permission structure to safeguard file access
- Load balancers ensure constant availability of online backup and file restoration, even in the event of an equipment failure
- Each file is secured on multiple independent storage clusters with continuous backup; network partitioning ensures backup storage clusters cannot be accessed from the Internet
- Redundant servers ensure you can always access your data

Chapter 9: Windows 8 Applications

Titanium 2013 provides three security applications specifically designed for Windows 8 RT, all available through the Windows Apps Store. You launch a Windows 8 RT application by clicking the icon on a PC or by tapping it on a mobile device.

- **Micro™ SafeGuard** is a secure browser for Windows 8 that has security technology built right in. It provides you with a safer browsing experience by including safe search results ratings, social networking security, and more. Browse the web without worry with Trend Micro SafeGuard.
- **Trend Micro™ Security Center** delivers current information about malware outbreaks in your area, offering insights into dangerous websites and malicious file downloads to avoid near you. For Trend Micro™ Titanium™ customers, it also provides up-to date information about your protection status. Surf the web knowing your protection is current and what sites to avoid with Trend Micro Security Center.
- **Trend Micro™ Go Everywhere** protects your Windows 8 tablet from loss or theft. Locate your tablet if lost or stolen with just one click. You can find your missing device on a worldwide Google map or sound a 1-minute alarm. Wherever you misplaced your tablet, Trend Micro Go Everywhere has got you covered.

The examples below use a Windows 8 PC.

SafeGuard Browser

To use the SafeGuard browser:



Figure 216. SafeGuard

1. Click the **SafeGuard** icon. The **SafeGuard** license agreement appears.



Figure 217. SafeGuard License Agreement

2. Read the license agreement. If you agree to the terms of the agreement, click **Agree**. The **SafeGuard** splash screen appears.

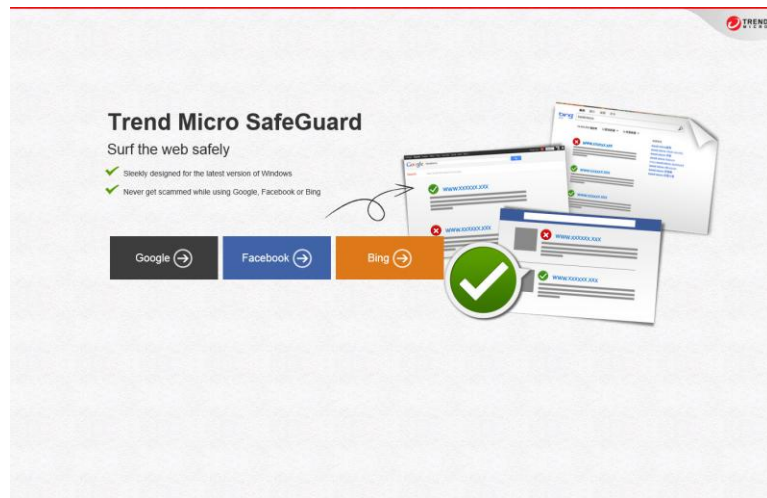


Figure 218. SafeGuard Splash Screen

3. Activate the **SafeGuard** menus by positioning your mouse near the top of the screen. When a hand appears, **right-click**; or use the **Windows-Z** hotkey. The **SafeGuard** menus appear.

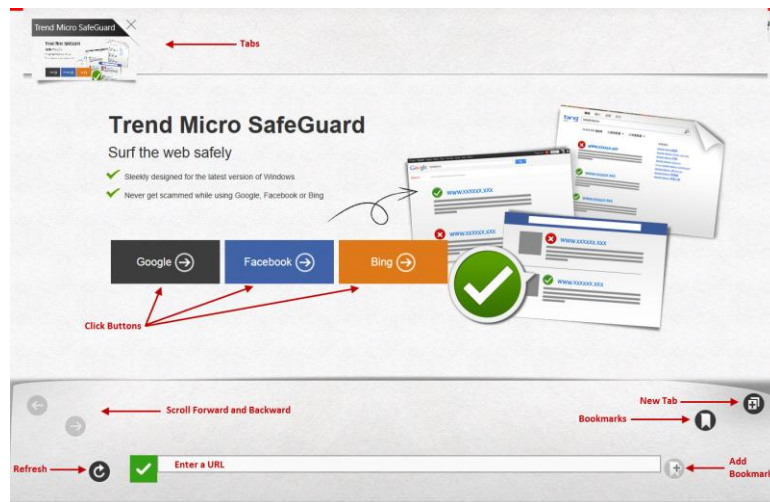


Figure 219. SafeGuard Menus

4. SafeGuard's simple functions include the following:
 - **Tabs**, which accumulate across the top menu as you browse. Click the **New Tab** icon to create a new tab.
 - **Splash** buttons for **Google**, **Facebook**, and **Bing**
 - **Forward** and **Backward** scroll buttons when browsing
 - A **Refresh** button to refresh the browser display
 - A **Bookmarks** icon, to navigate to the bookmarks page
 - An **Add Bookmarks** icon, to add bookmarks for key webpages you'd like to have easy access to.
5. Click on Google to do a search; for example, using the term "hacker." View the safe search results.

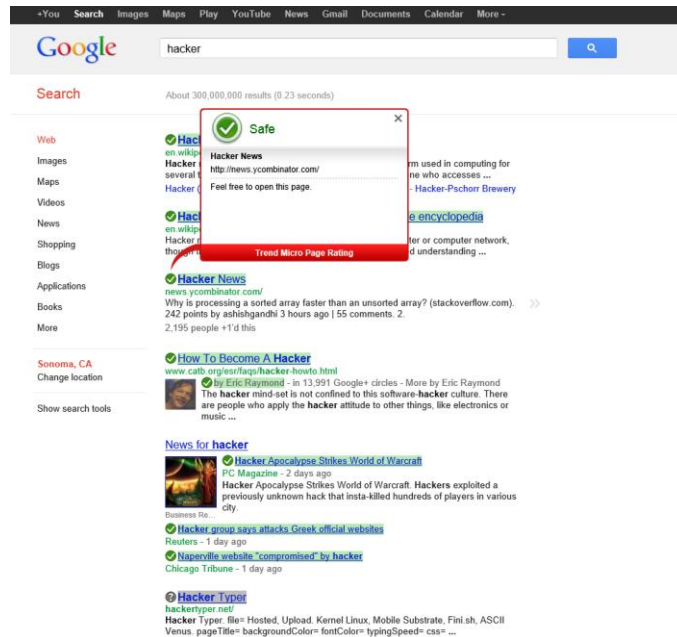


Figure 220. SafeGuard Safe Search / Link Ratings Results

- Similarly, click on Facebook link in the main page, then log into Facebook to view SafeGuard's safe link functions for social networking.



Figure 221. Link Ratings in Facebook

To add / delete a bookmark:

- Show the **SafeGuard** search field by typing **Windows-Z** on your keyboard. The search field displays in the lower menu.
- Type the URL of a site you wish to bookmark and hit **Enter** on your keyboard. The webpage displays.

3. Open the SafeGuard menus again by retyping **Windows-Z** on your keyboard.
4. Click the **Add Bookmark** icon. The **Bookmark Added!** popup appears.

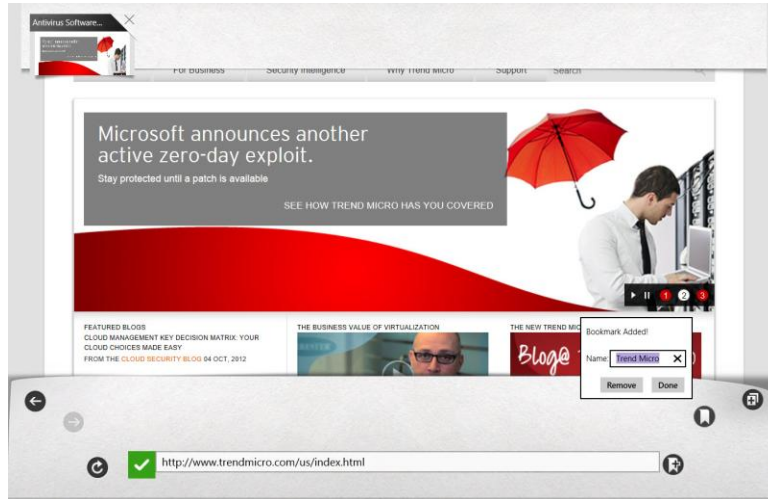


Figure 222. Adding a Bookmark

5. Use the default name, or type an alternate name you wish to give the bookmark and click **Done**. The bookmark is added to the **Bookmarks** page.
6. Click the **Bookmarks** icon to show the **Bookmarks** page and the bookmark you've added will be shown in the list.

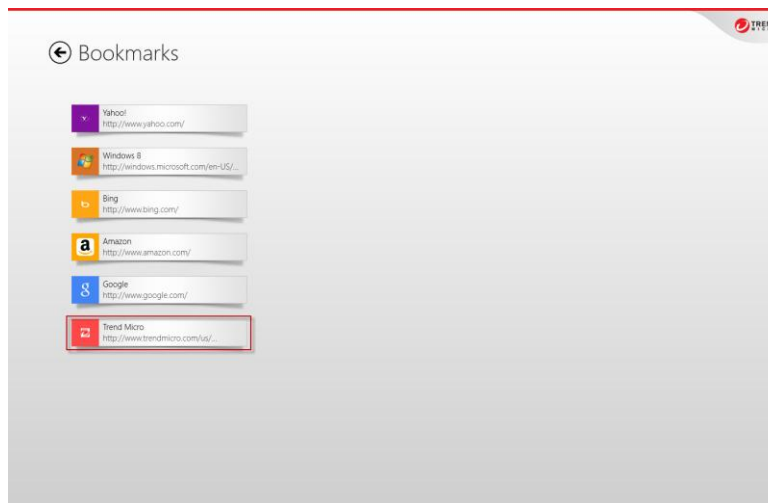


Figure 223. Bookmark Added

7. Right-click a bookmark to delete it; or click several bookmarks to delete them as a group. The **Trashcan** appears in the lower left-hand corner of the window.

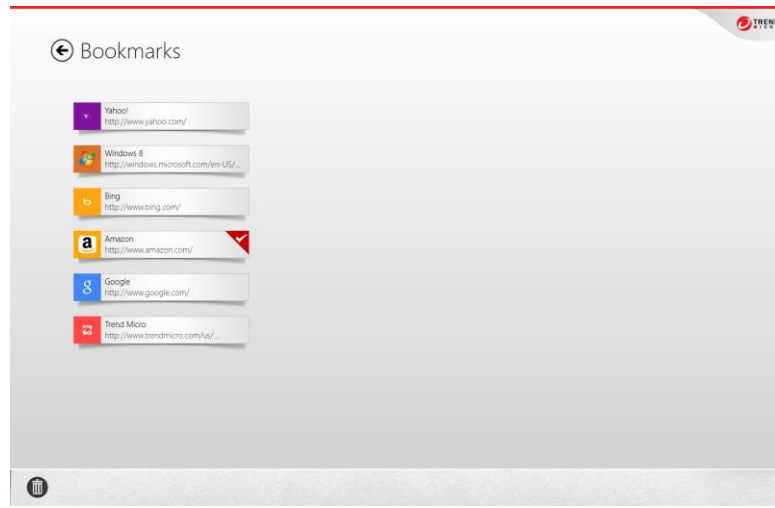


Figure 224. Deleting a Bookmark

8. Click the **Trashcan** to delete the bookmark(s).
9. Click the **Bookmarks** back-arrow to return to the main browser window.

To browse using Tabs:

1. After browsing successive websites, type **Windows-Z** on your keyboard to display the menus. Your **Tabs** display in the upper menu.
2. Click a **Tab** to display a website.

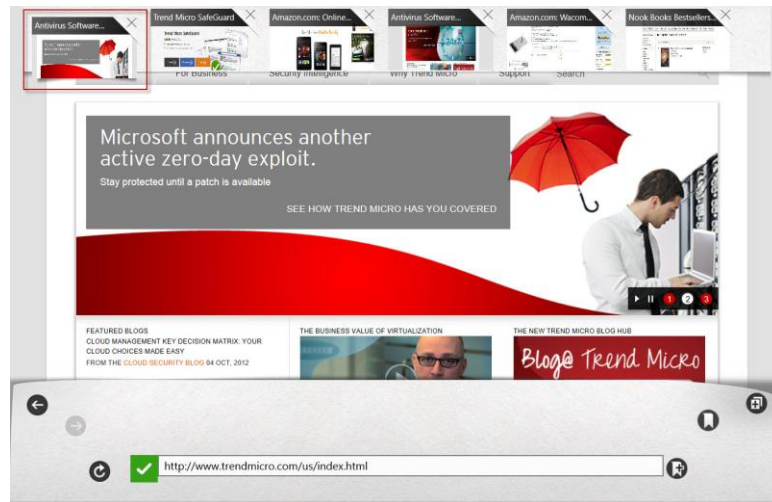


Figure 225. Using Tabs to Browse

3. Click the **Closebox (X)** in a **Tab** to delete it from the **Tabs** menu.

Security Center

To use the Security Center:



Figure 226. Security Center

7. Click/Tap the **Security Center** icon. The **Security Center** license agreement appears.



Figure 227. Security Center License Agreement

8. Read the license agreement. If you agree to the terms of the agreement, click **Agree**. The **Trend Micro Security Center** screen appears, with a popup asking **Do you want to turn on location services and allow Trend Micro Security Center to use your location?**

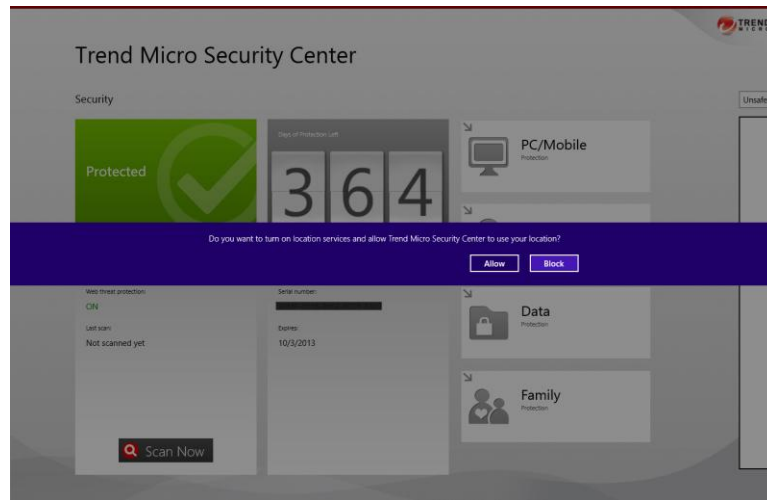


Figure 228. Security Center with Location Popup

9. If you do, click Allow. The **Trend Micro Security Center** main screen appears.



Figure 229. Protection, License, Titanium Settings

10. The first three panels of the **Security Center** provide essential data and tools:
 - **Protection Panel.** This panel shows the status of your protection and includes information on the **Real-time Scan**, your **Web Threat Protection**, the date of your **Last Scan**, and a **Scan Now** button, which launches Titanium and executes a **Quick Scan**.
 - **License Information.** The counter shows you how many days left you have on your subscription, the Serial Number for your License, and the Expiration Date.
 - **Titanium Console Tabs/Settings.** The **PC/Mobile**, **Privacy**, **Data**, and **Family** launch panels provide easy access into the **Titanium Console** settings. Clicking/tapping a

panel launches the Titanium Console and takes you to the category you've clicked, so you can edit the relevant settings.

11. For example, click **Scan Now** in the **Security Center**. A popup appears, asking **Did you mean to switch apps?**

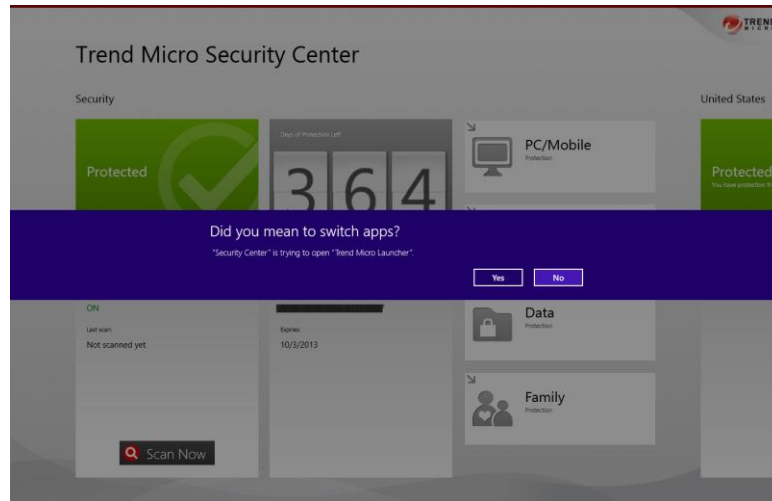


Figure 230. Did You Mean to Switch Apps?

12. Click **Yes**. Titanium launches and conducts a **Quick Scan**.



Figure 231. Quick Scan

13. Using another example, click **PC/Mobile** in the third panel of the **Security Center** to launch it in the Titanium Console.
14. Click **Yes** again when the popup asks you **Did you mean to switch apps?** The **Titanium Console** appears, with the **PC/Mobile** tab selected.



Figure 232. PC/Mobile Tab Selected (Titanium Maximum Security)

15. Click the relevant Settings icon for your edition of Titanium, to edit those settings. (Some icons shown above are only available in Titanium Maximum Security.)
16. Back in the **Security Center**, scroll the right to view the central panels. These provide data on the 10 most unsafe websites and 10 most active malicious files.

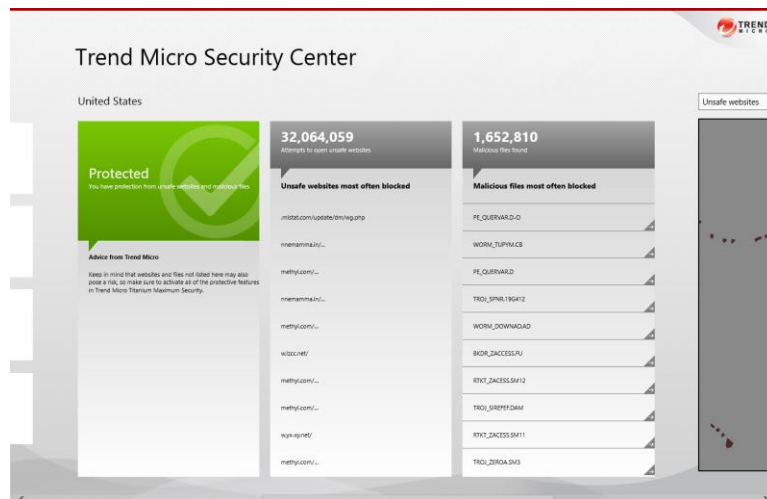


Figure 233. Unsafe Websites, Malicious Files

17. Click a right-arrow of a malicious file in the list to load your browser and find out more details about the malware in the **Trend Micro Threat Encyclopedia**.

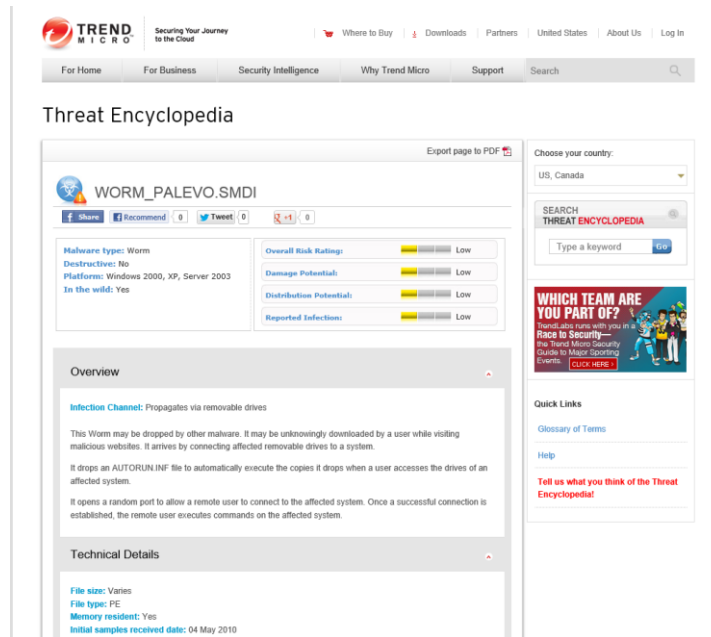


Figure 234. Trend Micro Threat Encyclopedia

18. Back in the **Security Center**, scroll to the right to see the right-hand panel of the Security, which provides a Regional Map of **Safe**, **Risky**, and **Not Checked** websites and files.

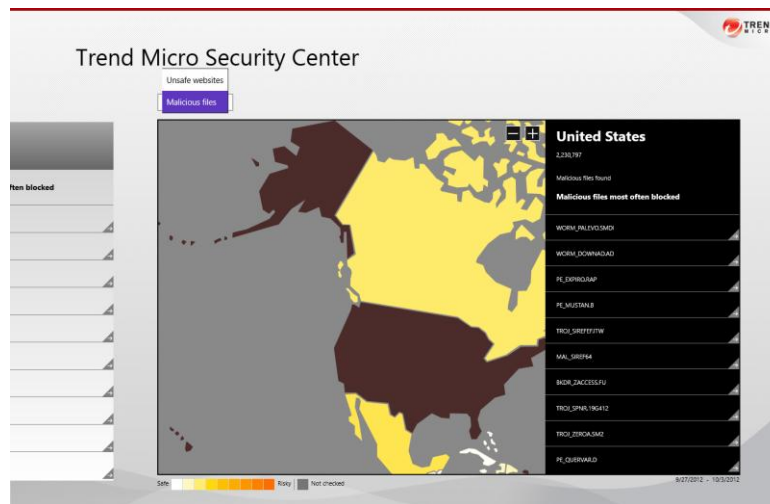


Figure 235. Unsafe Websites, Malicious Files, Regional Map

19. Select a subregion or country in the map to view the frequency of the unsafe website or malicious file in that location.
20. Use the popup menu to toggle the Regional Map between **Unsafe Websites** and **Malicious Files** in the **Security Center**.

Go Everywhere

To use Go Everywhere:



Figure 236. Go Everywhere

1. Click the **Go Everywhere** icon to launch it. The Trend Micro Go Everywhere **Sign In** screen appears.

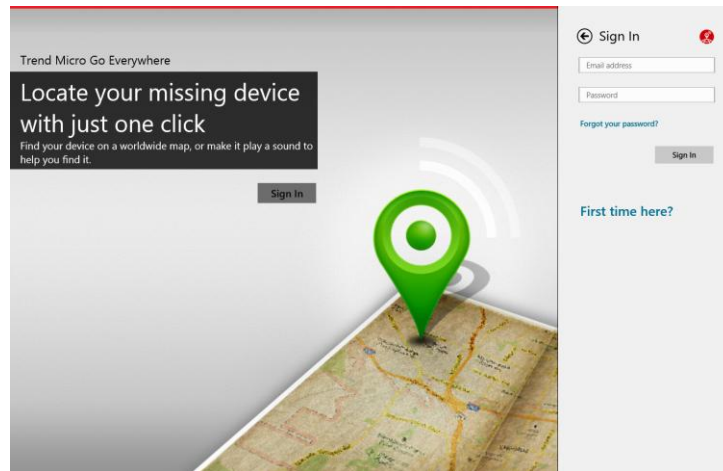


Figure 237. Sign In

2. You have two options to sign in:
 - If you already have a Trend Micro account, enter the email address and password you used to create your account and click **Sign In**.
 - If you don't already have a Trend Micro account, click **First Time Here** and in the panel that appears, enter your credentials, then click **Create Account** to create a Trend Micro account.

Trend Micro Go Everywhere

Locate your missing device
with just one click

Find your device on a worldwide map, or make it play a sound to help you find it.

Sign In

Create an account

First name Last name

E-mail address

Password

Re-type password

United States

☒ Receive the latest news and offers from Trend Micro

Create Account

Sign in

Figure 238. Create an Account

3. The **Trend Micro Go Everywhere License Agreement** appears.

Trend Micro Go Everywhere

Lost Device Protection

License Agreement

TREND MICRO INCORPORATED
STANDARD APPLICATION LICENSE TERMS

These license terms are an agreement between you and Trend Micro. Please read them. They apply to the software application you download from the Windows Store, including any updates or supplements for the application, unless the application comes with separate terms, in which case those terms apply.

BY DOWNLOADING OR USING THE APPLICATION, OR ATTEMPTING TO DO ANY OF THESE, YOU ACCEPT THESE TERMS. IF YOU DO NOT ACCEPT THEM, YOU HAVE NO RIGHT TO AND MUST NOT DOWNLOAD OR USE THE APPLICATION.

Trend Micro means the entity licensing the application to you, as identified in the Windows Store.

Agree Disagree

Figure 239. License Agreement

4. Read the **License Agreement**. If you agree, click **Agree**. A popup appears, asking if you wish to **Let Trend Micro Go Everywhere run in the background?**

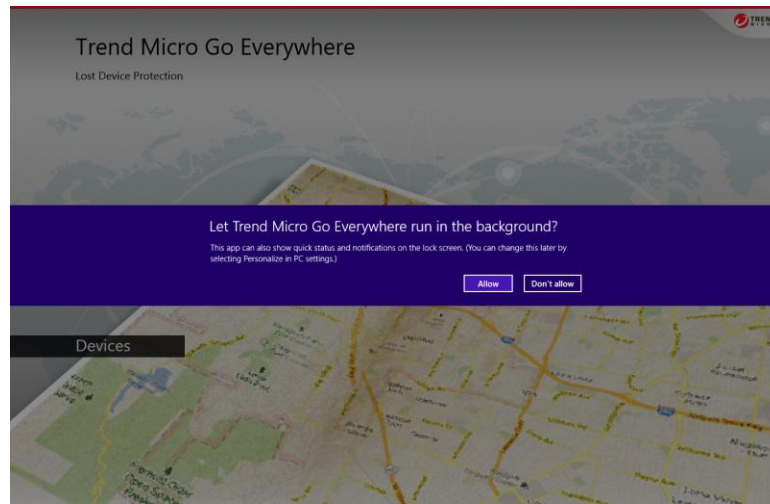


Figure 240. Run In The Background?

5. If you agree, click **Allow**. Another popup appears, asking **Can Trend Micro Go Everywhere Use Your Location?**

Note: For tablets and smart phones, Go Everywhere uses GPS. For laptops and desktops, Go Everywhere uses the nearest access point and IP Address, which is less accurate.

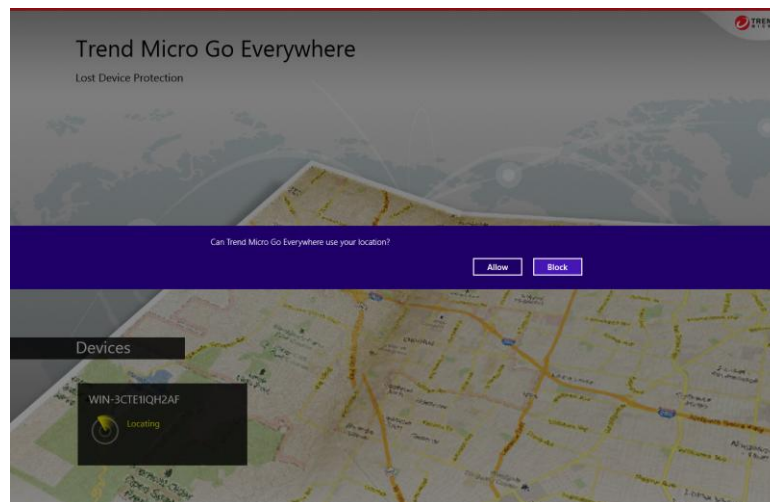


Figure 241. Use Your Location?

6. If you agree, click **Allow**. **Go Everywhere** lists the devices you've registered with the application.

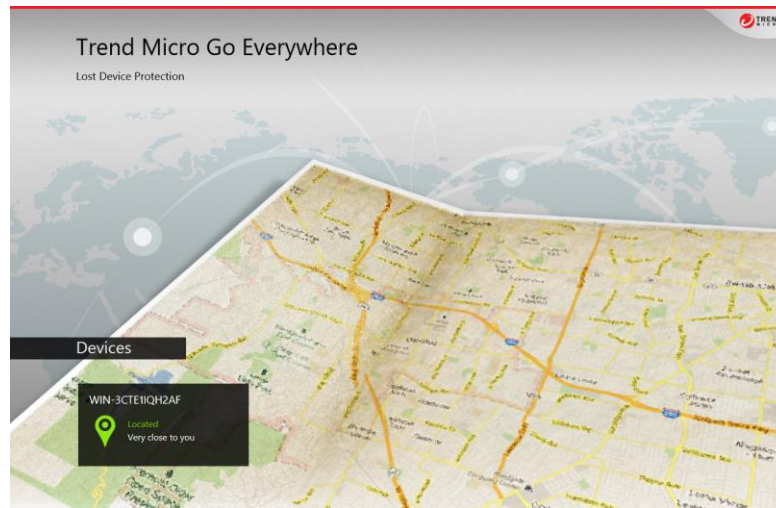


Figure 242. Devices

7. Click the icon of a **Device** for which you wish to obtain more location details. The **Go Everywhere** Google map appears, showing the most recent location of your device.

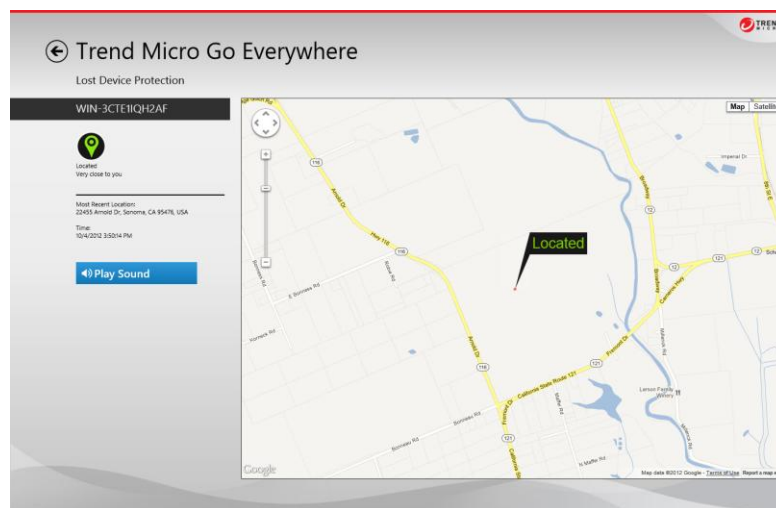


Figure 243. Device Located (Map)

8. Use the **Zoom** tools to zoom in or out of the map, or position your cursor (or finger) on the map to drag the map to a different position in the window.
9. Toggle to **Satellite** view by clicking the **Satellite** icon in the upper right-hand corner of the map. Toggle back to **Map** view by clicking its icon.

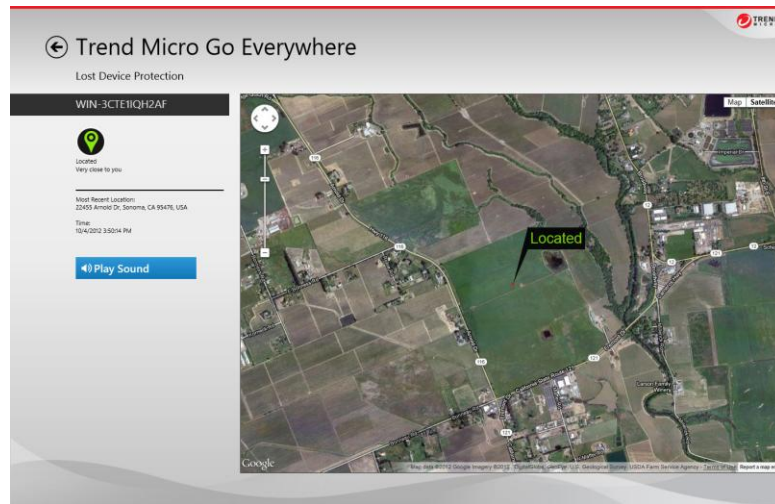


Figure 244. Device Located (Satellite)

10. Click **Play Sound** to sound the **Lost Device Protection Alert**. The alert sounds, showing a popup and helping you to locate your device or to alert others nearby if it has been picked up or stolen.

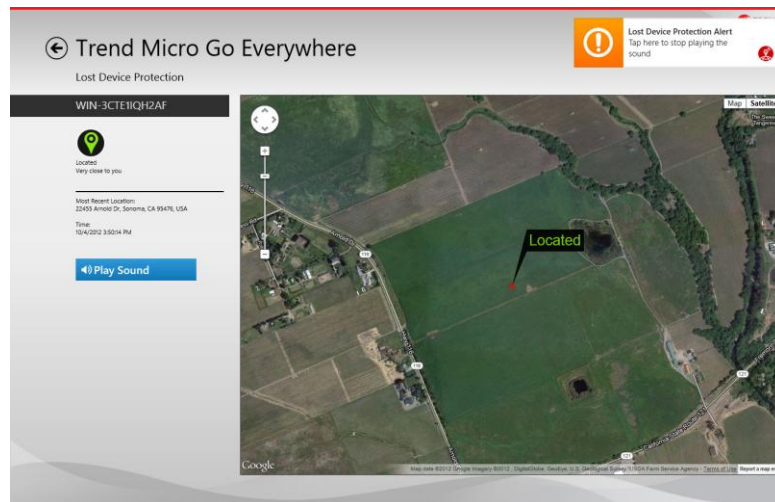


Figure 245. Lost Device Protection Alert

11. Click the **Lost Device Protection Alert** popup badge to turn off the sound.

About Trend Micro

Trend Micro Incorporated, a global leader in Internet content security, focuses on securing the exchange of digital information for businesses and consumers. A pioneer and industry vanguard, Trend Micro is advancing integrated threat management technology to protect operational continuity, personal information, and property from malware, spam, data leaks, and the newest web threats.

Visit TrendWatch at <http://www.trendmicro.com/go/trendwatch> to learn more about the threats and Trend Micro™ Smart Protection Network™ infrastructure. Trend Micro's flexible solutions, available in multiple form factors, are supported 24/7 by threat intelligence experts around the globe. A transnational company, with headquarters in Tokyo, Trend Micro's trusted security solutions are sold through its business partners worldwide. Please visit <http://www.trendmicro.com>.

Copyright © 2012 by Trend Micro Incorporated. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the prior written consent of Trend Micro Incorporated. Trend Micro, the t-ball logo, and Titanium are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice.

Legal Notice: Trend Micro licenses this product in accordance with terms and conditions set forth in the License Agreement inside this package. If you wish to review the License Agreement prior to purchase, visit: www.trendmicro.com/license. If you (or the company you represent) do not agree to these terms and conditions, promptly return the product and package to your place of purchase for a full refund.

Protected by United States Patent No. 5,951,698.