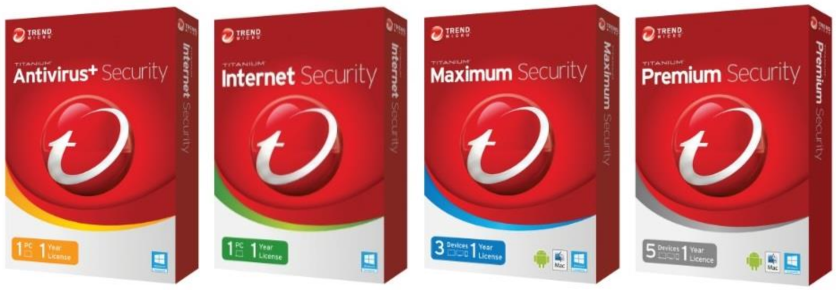
Trend Micro™

Titanium™ Security 2014

Product Guide



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

Trend Micro™ Titanium Security™ 2014 - Product Guide provides help for analysts, reviewers, and customers who are evaluating, reviewing, or using Trend Micro™ Titanium Security™ Antivirus+ Security; Trend Micro™ Titanium Security™ Internet Security; Trend Micro™ Titanium Security™ Maximum Security; or Trend Micro™ Titanium Security™ Premium 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 Security™ Internet Security for Mac 2014 - Product Guide*
- *Trend Micro™ Mobile Security 3.0 - Product Guide*
- *Trend Micro™ DirectPass™ 1.8 - 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*

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 provide feedback at docs@trendmicro.com.

DOCUMENT PROFILE:

Product: Trend Micro™ Titanium Security™ 2014 (7.0)

Document Title: Trend Micro™ Titanium Security™ 2014 - Product Guide

Document Filename: PG - Titanium for PC 2014 - Product Guide GL v1.4

Document Release Date: August 26, 2013

Team: Consumer Technical Product Marketing

Table of Contents

Chapter 1: Introduction to Titanium Security

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.

The Titanium Security Family

The family of **Trend Micro™ Titanium Security™** products includes the following:

- **Trend Micro™ Titanium Security™ Antivirus+**. Our entry-level product provides all the essential protection you need while surfing the web or opening, saving, or downloading files. It provides coverage for netbooks, laptops, and entry level computers, unlike free options, which leave you exposed in key areas.
- **Trend Micro™ Titanium Security™ Internet Security**. Our mid-range product provides advanced protection with maximum performance, adding our unique privacy scanner and the broadest web threat protections available for social networking. It also provides basic parental controls to restrict or filter online access for kids.
- **Trend Micro™ Titanium Security™ Maximum Security**. Our high-end product provides the complete security solution for protecting your PC, Mac, or mobile devices and up to 3 users or devices. It includes a complimentary copy of DirectPass™, Trend Micro's password manager; Online Guardian for Families; Mobile Security for Android; and 5GB of secure online Trend Micro SafeSync™ storage.
- **Trend Micro™ Titanium Security™ Premium Security** has all of the same features as Titanium Security™ Maximum Security, for up to 5 users or devices, but SafeSync storage is expanded to 25GB.
- **Trend Micro™ Titanium Security™ Internet Security for Mac.** This is our Titanium Security offering specifically designed for the Macintosh and is bundled with Titanium Security™ Maximum Security and Premium Security editions, or can be purchased separately.

Titanium Security leverages the expertise Trend Micro has gained over 25 years and delivers:

- The fastest protection against new web threats*
- The best phishing detection rates, guarding against identity theft*
- Unique cloud-based protection, SafeSurfinging our customers from 250+ million threats per day.

*NSS Labs 2013

Titanium Security: Comprehensive Protection

Titanium Security is equipped with special protections and is bundled with companion products to address specific needs:

Privacy Protection and Social Networking Security

Titanium 2014 continues its leadership role in social networking security (SNS):

- **Enhanced! Privacy Protection for Facebook, Twitter, and Google +.** Titanium Security features an exclusive Privacy Scanner for social media, which identifies privacy settings that may leave your personal information publicly available and vulnerable to identity theft. Privacy protection is now extended beyond Facebook to Twitter and Google+.
- **Social Networking Security (SNS) Protection.** Titanium Security provides protection from threats you may encounter from malicious links in Facebook, Twitter, Google+, MySpace, LinkedIn, Pinterest, Mixi, and Sina Weibo—the broadest and most effective SNS protection available on the market for consumers today.
- **Clear Warning.** Our SNS proactively warns you when a link is bad by highlighting it in red. When it's a safe link, it's highlighted in green. You can also mouse over a link to get real-time details about its safety from our Web Threat Protection servers.
- **Warn a Friend.** Titanium Security even allows you to easily and quickly inform your Facebook friends when it identifies a malicious link, so they can delete it from their Facebook page.

Data Theft Prevention

- **Data Theft Prevention (DTP).** DTP lets you stop specific data, such as email accounts or credit card numbers, from being shared in outward bound email or online forms.
- **Secure Erase** lets you overwrite and delete data from your disk, so it can't be recovered.
- **Vault** lets you encrypt data on your hard drive and remotely lock it up if your laptop lost or stolen; when the device is found you can then unlock that data.
- **Trend Micro™ DirectPass™** is a standalone product bundled with Titanium™ Maximum™ Security and Titanium Premium Security that lets you protect and manage all your logins and passwords safely. It uses a single master password and works across Windows and Mac desktops and laptops, as well as Android and iOS tablets and smartphones. DirectPass also provides a **Secure Browser**, for use with online banking and financial websites, which encrypts all your keystrokes, so they can't be stolen by keyloggers.
- **Trend Micro™ SafeSync™** is a standalone product bundled with Titanium Maximum Security and Titanium Premium Security that lets you back up and sync all your data to a secure cloud, to ensure you have it should your hard drive crash. It also provides the ability to access it across Windows and Mac desktops and laptops, as well as Android and iOS tablets.

Family Protection

- **Parental Controls** let you restrict your kids' usage of the Internet and prevent them from visiting inappropriate websites. Functions include program restrictions, which can be set by schedule; safe search filtering, which helps prevent adult content from appearing in search results; and blocking of untested websites, to increase security when browsing.
- **Online Guardian.** For parents who want to know exactly what their children are doing online, there's **Trend Micro™ Online Guardian** - a standalone product bundled with Titanium Maximum Security and Titanium Premium Security. Online Guardian is a complete monitoring and reporting solution adding deeper oversight and visibility into specific social networking sites, as well as instant messaging programs, beyond simple parental controls.

Other Highlights

- **New! Screen Reader –** Screen Reader support is now available for visually-impaired users.
- **New! Intensive Scan Switch** – Automatically increases the protection level only when you need it – for intensive scans when your computer is infected.
- **Search Results Rating –** When you conduct a search on the internet the search results give you a list of URLs, proactively highlighted.
- **Manual URL/Link Scanner –** As with SNS, when you hover your mouse over a link in search results, the manual link scanner rates the safety and reputation of any links on the web page.
- **Enhanced Malware Cleanup -** Titanium Security has always been tops in preventing infections, but now it has been enhanced to help repair and clean up computers that have already been infected, prior to installation. Both its normal scan and its severe malware removal tools such as Rootkit Buster, Anti-Theft Tool Kit / Clean Boot, and Rescue Disk have expanded anti-malware features. Anti-Ransomware 3.0 USB tool is also available for Windows XP, Vista, and 7 users.
- **Mobile Security for Android** – Titanium Security Maximum Security and Titanium Security Premium Security include Trend Micro Mobile Security for protection of your Android devices.
- **Windows 8 compatibility -** Titanium Security 2014 is fully compatible with Microsoft's Windows 8 RT and Pro operating systems. Trend Micro SafeSurfing, Security Center, and Go Everywhere are apps specifically designed for Windows 8 desktop and tablets users, available for free on the Windows app store. (See below.)
- **Mountain Lion OS compatibility -** Titanium Internet Security for Mac 3.0 is fully compatible with Apple's Mountain Lion MacOS, version 10.8.

Available from the Windows App Store

- **Trend Micro™ SafeSurfing** 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 SafeSurfing.
- **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 Security™ 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 Security 2014

Table 1. Titanium Security 2014 - Key Features

TITANIUM 2014 – Key Features	Titanium Internet Security for Mac	Titanium Antivirus+ Security	Titanium Internet Security	Titanium Maximum Security	Titanium Premium Security
Licensing (Multi-license subscriptions can be activated on PC, Mac, and Android devices.)	1 user Mac only	1 user PC only	3 users PC only	3 users PC, Mac & Mobile	5 users PC, Mac & Mobile
Pricing	$39.95 yr	$39.95 yr	$79.95 yr	$89.95 yr	$99.95 yr
Essential Protection					
Virus and Spyware Protection	✓	✓	✓	✓	✓
Rootkit Detection and Removal		✓	✓	✓	✓
Rescue Disk		✓	✓	✓	✓
Web Threat Protection	✓	✓	✓	✓	✓
Anti-Spam	✓	✓	✓	✓	✓
Anti-Phishing	✓	✓	✓	✓	✓
Auto Intensive-level Protection Scan Switch		✓	✓	✓	✓
Authenticate Wi-Fi Networks and Hotspots		✓	✓	✓	✓
Windows Firewall Booster		✓	✓	✓	✓
Block Malicious Links in Email and IM	✓	✓*	✓	✓	✓
Search Results Ratings	✓		✓	✓	✓
Social Networking Security	✓		✓	✓	✓
Data Protection & Privacy					
Privacy Scanner for Facebook, Twitter, Google+	✓		✓	✓	✓
Data Theft Prevention			✓	✓	✓
Secure Erase			✓	✓	✓
System Tuner			✓	✓	✓
Vault with Remote File Lock				✓	✓
DirectPass**	✓			✓	✓
SafeSync**	✓			5GB	25GB
*Email=Yes, IM=No **Bundled with Titanium Maximum and Premium Security, separate purchase for Mac					

Table 2. Titanium Security 2014 – Key Features (Continued)

TITANIUM 2014 – Key Features	Titanium Internet Security for Mac	Titanium Antivirus+ Security	Titanium Internet Security	Titanium Maximum Security	Titanium Premium Security
Family Protection					
Parental Controls	✓		✓	✓	✓
Online Guardian				✓	✓
Platform Protection					
Trend Micro SafeSurfing for Window 8*		✓	✓	✓	✓
Trend Micro Security Center for Windows 8*		✓	✓	✓	✓
Trend Micro Go Everywhere		✓	✓	✓	✓
Android				✓	✓
MacOS**	✓				
*Available for free from the Windows App Store **Bundled with Titanium Maximum and Premium Security					

System Requirements

Table 3. Titanium Antivirus+, Internet Security, Maximum Security, Premium Security

Operating System	CPU	Memory	Disk Space
Windows 8, (32 or 64- bit)	1 GHz	1 GB (32-bit) 2 GB (64-bit)	500 MB (600 MB recommended)
Windows® 7 Family and Service Pack 1, (32 or 64- bit)	800MHz (1GHz recommended)	1 GB	
Windows ® Vista Family, (32 or 64-bit) Service Pack 2	800MHz (1GHz recommended)	512 MB (1 GB recommended)	
Windows® XP Family, (32- bit only) Service Pack 2 or above	350MHz (800 MHz recommended)	256 MB (512 MB recommended)	
Other Requirements			
Web browser	Microsoft® Internet Explorer® 7.0, 8.0, 9.0, 10.0, or 11.0 Mozilla Firefox® latest version Google Chrome™ latest version		
Display	High-color display with a resolution of 800x480 pixels or above (Desktop), 1024x768 or above (Windows Store), 1366x768 or above (Snap View)		

Table 4. Titanium Internet Security for Mac

Operating System	CPU	Memory	Disk Space
Mac OS® X version 10.8 "Mountain Lion"	Apple Macintosh computer with an Intel® Core™ Processor	2GB	1.5GB
Mac OS® X version 10.7 "Lion" (10.7 or higher)			
Other Requirements			
Web Browser	Apple® Safari® 5.1 or higher Mozilla® Firefox® 22.0 or previous versions still supported by Mozilla Google Chrome™ 28 or previous versions still supported by Google		

Table 5. Trend Micro Mobile Security Personal Edition

Operating System	Storage Space	Memory Usage	Other
Android OS 2.2 and above	7.5MB minimum	9MB for phone 15MB for tablet	Internet Connection

Global Availability

September 3, 2013

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 offers free phone, email, and chat support. For more info, 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 Security

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

- Trend Micro™ Titanium Security™ Antivirus+ Security
- Trend Micro™ Titanium Security™ Internet Security
- Trend Micro™ Titanium Security™ Maximum Security
- Trend Micro™ Titanium Security™ Premium Security simply extends Maximum Security by increasing your sync and backup storage capacity.
- Trend Micro™ Titanium Security™ Internet Security for Macintosh

(See our separate Product Guide for instructions on installing and using Trend Micro™ Titanium Security™ Internet Security for Macintosh.)

In the examples below we install Titanium Maximum Security on Windows 8, but each version of Titanium has a nearly identical installation and activation process on the various versions of Windows and Macintosh.

Installing Titanium Security

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

Note: **For users of Windows 8 on touch screen laptops, tablets, or smartphones, "click" instructions below should be read as "tap."**

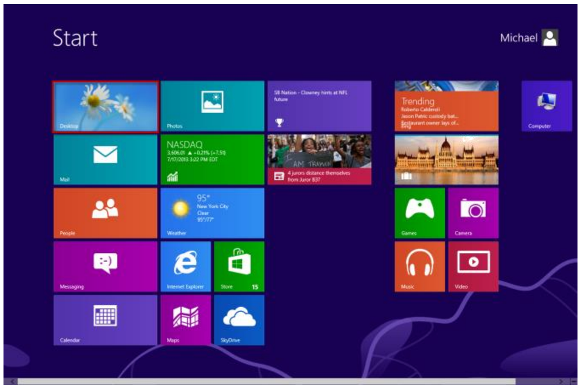


Figure 1. Windows 8 Modern UI

By Download:

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

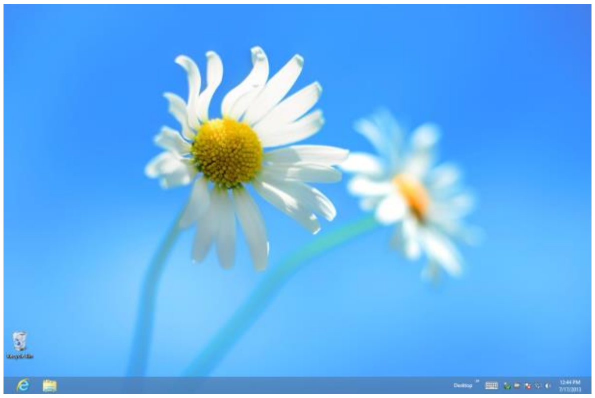


Figure 2. Windows 8 Desktop

Note: **Once you're in the Windows 8 Desktop, the installation process for the core Titanium program is nearly identical for Windows 7. The main exceptions appear when you install the Windows 8 Modern UI options after the main program installation.**

2. Go to http://www.trendmicro.com/us/home/products/titanium/index.html to download Titanium 2014.

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**.

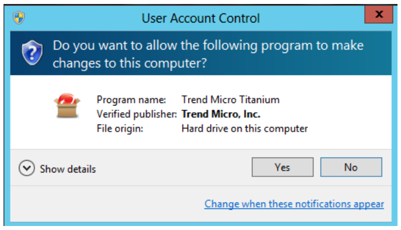
6. When the download completes, click **Open Folder** (in IE), then double-click the **Downloader**.

By CD:

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

Note: **From this point on, the CD install process is the same as the download process.**

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

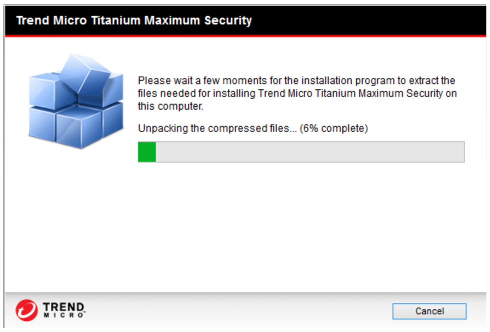

User Account Control

Do you want to allow the following program to make changes to this computer?

Program name: Trend Micro Titanium
Verified publisher: **Trend Micro, Inc.**
File origin: Hard drive on this computer

Figure 3. 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.

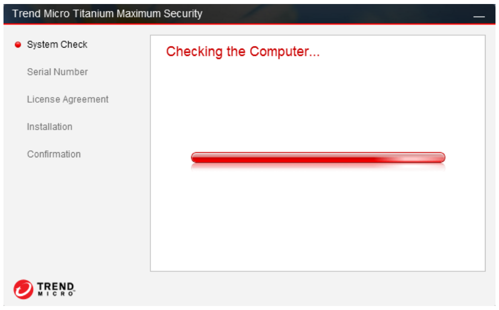

Trend Micro Titanium Maximum Security

Please wait a few moments for the installation program to extract the files needed for installing Trend Micro Titanium Maximum Security on this computer.

Unpacking the compressed files... (6% complete)

Figure 4. Unpacking Files

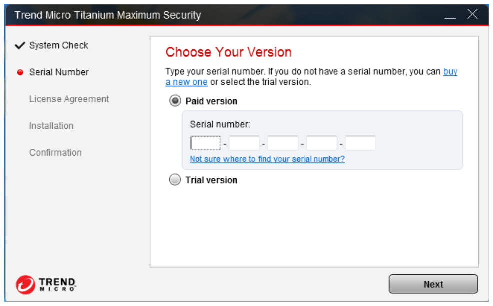
10. Titanium will then check if your computer meets the minimum system requirements and will conduct a quick malware scan.


Trend Micro Titanium Maximum Security

Checking the Computer...

Figure 5. Checking the Computer

11. When the process completes, a screen appears asking you to **Choose Your Version.**



Trend Micro Titanium Maximum Security

Choose Your Version

Type your serial number. If you do not have a serial number, you can buy a new one or select the trial version.

● Paid version

Serial number: ____ - ____ - ____ - ____ - ____

Not sure where to find your serial number?

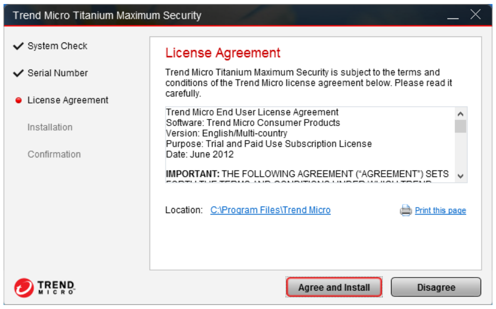
○ Trial version

Figure 6. Choose Your Version

12. If you’re installing a **paid version**, enter the **serial number** provided by Trend Micro on your retail box or in your confirmation email, then **click** Next.

13. If you’re installing a **trial version**, click the **trial version** button, then click **Next**.

14. The **License Agreement** appears.



Trend Micro Titanium Maximum Security

License Agreement

Trend Micro Titanium Maximum Security is subject to the terms and conditions of the Trend Micro license agreement below. Please read it carefully.

Trend Micro End User License Agreement
Software: Trend Micro Consumer Products
Version: English/Multi-country
Purpose: Trial and Paid Use Subscription License
Date: June 2012

IMPORTANT: THE FOLLOWING AGREEMENT (“AGREEMENT”) SETS

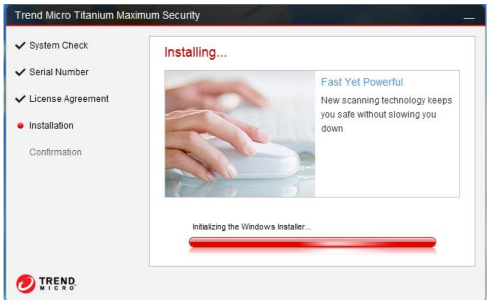
Location: C:\Program Files\Trend Micro

Figure 7. License Agreement

15. Titanium chooses a default location for the installation. You can change this by clicking the link and browsing to another location. (Trend Micro recommends you use the default.)

16. Read the **License Agreement**. (Click **Print this page** to print it out.) If you agree with the License Agreement, click **Agree and Install**.

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



Installing...

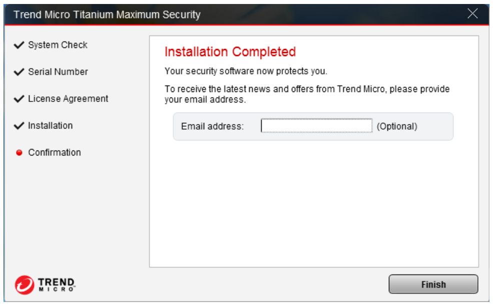
Fast Yet Powerful

New scanning technology keeps you safe without slowing you down

Initializing the Windows Installer...

Figure 8. Progress Indicator

18. If you have installed a Trial version, when the installation is completed, the wizard will indicate **Installation Completed**.



Installation Completed

Your security software now protects you.

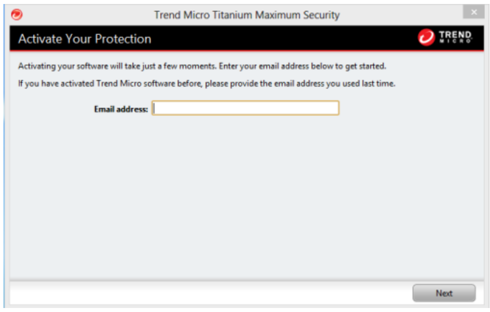
To receive the latest news and offers from Trend Micro, please provide your email address.

Email address: (Optional)

Figure 9. Installation Completed

19. To receive the latest news and offers from Trend Micro, enter your email address and click **Finish**.

20. If you have installed a Paid version, a dialog appears, asking you to enter your email address to activate your protection.



Activate Your Protection

Activating your software will take just a few moments. Enter your email address below to get started.

If you have activated Trend Micro software before, please provide the email address you used last time.

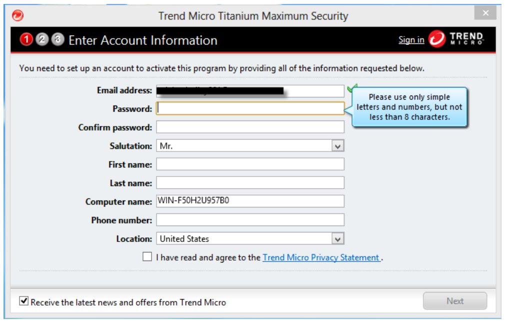
Email address:

Figure 10. Activate Your Protection

21. One of two alternate processes will now occur:

    - If you have activated Trend Micro software before, simply enter the email you used before and click **Next**. The program activates and the installation is complete.

    - If you have not activated Trend Micro software before, enter your preferred email address and click **Next**. A dialog appears, asking you to **Enter Account Information.**


Trend Micro Titanium Maximum Security
1 2 3 Enter Account Information
Sign in
TREND MICRO
Next

You need to set up an account to activate this program by providing all of the information requested below.

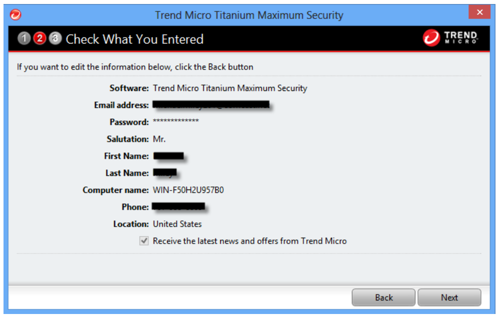
Email address: [redacted]
Password:
Confirm password:
Salutation: Mr.
First name:
Last name:
Computer name: WIN-F50H2U957B0
Phone number:
Location: United States

Please use only simple letters and numbers, but not less than 8 characters.

□ I have read and agree to the Trend Micro Privacy Statement .

☑ Receive the latest news and offers from Trend Micro

Figure 11. Enter Account Information

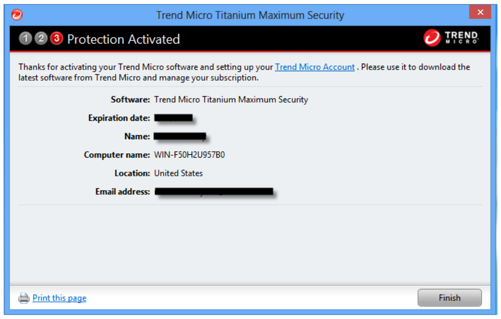

Trend Micro Titanium Maximum Security
1 2 3 Check What You Entered
TREND MICRO
Back
Next

If you want to edit the information below, click the Back button

Software: Trend Micro Titanium Maximum Security
Email address: [redacted]
Password: *************
Salutation: Mr.
First Name: [redacted]
Last Name: [redacted]
Computer name: WIN-F50H2U957B0
Phone: [redacted]
Location: United States
☑ Receive the latest news and offers from Trend Micro

Figure 12. Check What You Entered

22. If your entries are accurate, click **Next**. A dialog indicates **Protection Activated.** You may print this page.

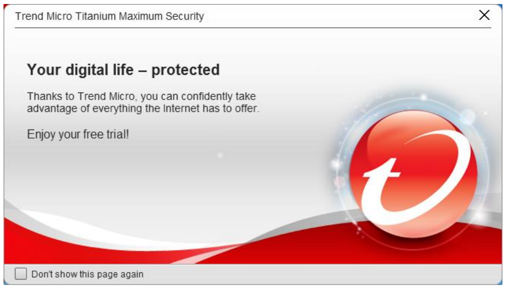

Trend Micro Titanium Maximum Security
1 2 3 Protection Activated
TREND MICRO
Print this page
Finish

Thanks for activating your Trend Micro software and setting up your Trend Micro Account . Please use it to download the latest software from Trend Micro and manage your subscription.

Software: Trend Micro Titanium Maximum Security
Expiration date: [redacted]
Name: [redacted]
Computer name: WIN-F50H2U957B0
Location: United States
Email address: [redacted]

Figure 13. Protection Activated

23. Click **Finish**. The **Welcome** screen displays. Its content depends on whether you've installed the Free or Paid version.



Trend Micro Titanium Maximum Security

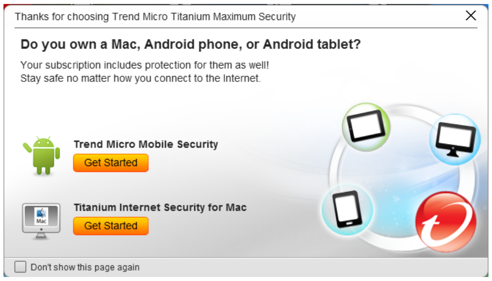
Your digital life – protected

Thanks to Trend Micro, you can confidently take advantage of everything the Internet has to offer.

Enjoy your free trial!

☐ Don't show this page again

Figure 14. Titanium Maximum Security Welcome (Free Version)



Thanks for choosing Trend Micro Titanium Maximum Security

Do you own a Mac, Android phone, or Android tablet?

Your subscription includes protection for them as well!
Stay safe no matter how you connect to the Internet.

Trend Micro Mobile Security

Titanium Internet Security for Mac

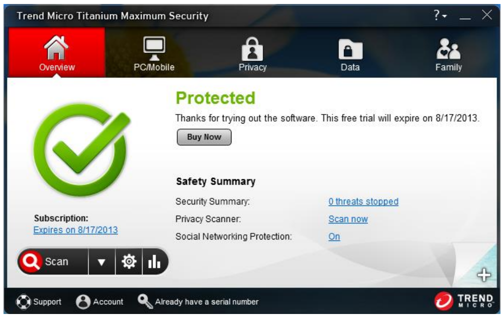
☐ Don't show this page again

Figure 15. Titanium Maximum Security Welcome (Paid Version)

24. For the Paid version, click the **Get Started** buttons to get started with the products bundled with Titanium Maximum Security. (You can always come back to the Welcome screen later simply by opening the Titanium Console. This 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 you can mix and match to suite your needs. To see how many seats you have been allocated and to what device, please visit MyAccount.**

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



Protected

Thanks for trying out the software. This free trial will expire on 8/17/2013.

Safety Summary

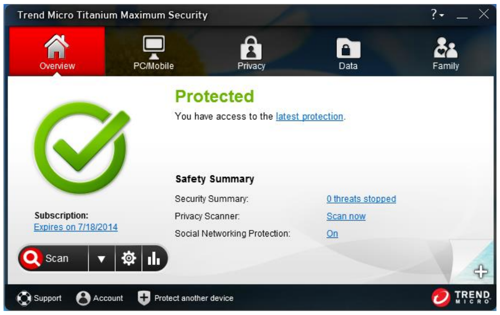
Security Summary: 0 threats stopped

Privacy Scanner: Scan now

Social Networking Protection: On

Subscription:
Expires on 8/17/2013

Figure 16. Titanium Maximum Security Console (Free Version)



Protected

You have access to the latest protection.

Safety Summary

Security Summary: 0 threats stopped

Privacy Scanner: Scan now

Social Networking Protection: On

Subscription:
Expires on 7/18/2014

Figure 17. Titanium Maximum Security Console (Paid Version)

26. 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. You can also protect another device.

27. 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.

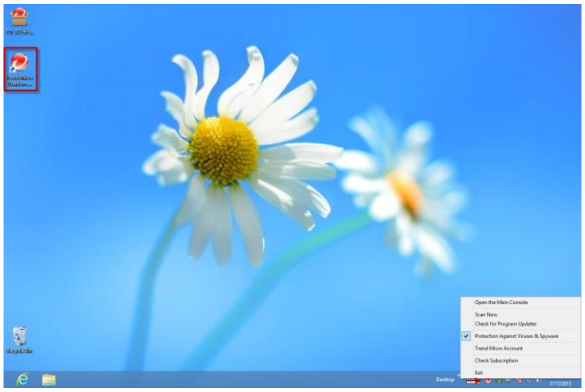


Figure 18. Windows 8 Desktop

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

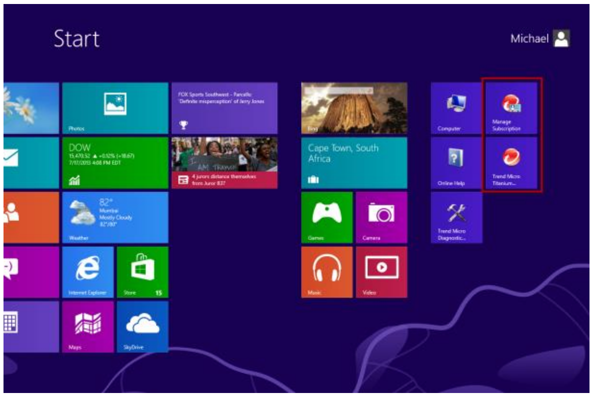
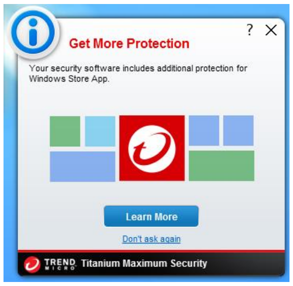


Figure 19. Windows 8

29. You can click the **Trend Micro Titanium** icon to access the **Titanium Console** right from the Modern UI. The action will toggle back to Windows 8 Desktop and launch the **Titanium Console**.

30. Once you've finished your installation, Titanium also provides a popup that says **Get More Protection** for Windows 8.

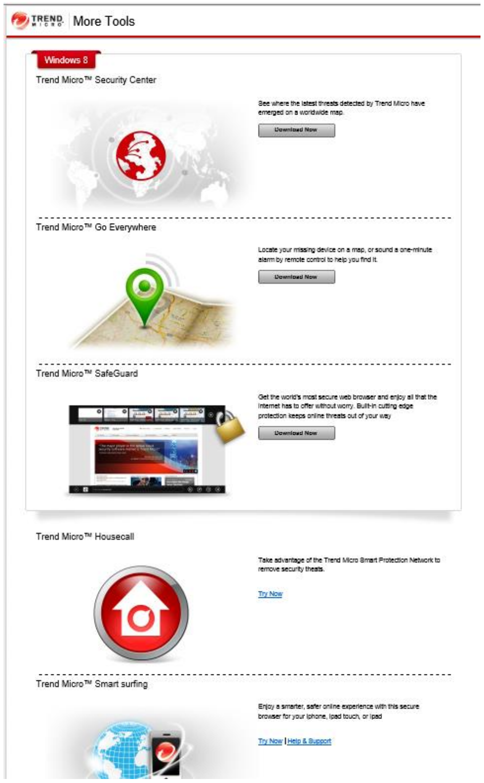

Get More Protection

Your security software includes additional protection for Windows Store App.

Figure 20. Get More Protection

31. Click **Learn More**. This launches your browser and takes you to the **More Tools** web page, which provides links (among others) to **SafeSurfing, Security Center,** and **Go Everywhere** in the Windows App Store.

32. 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.



More Tools

Windows 8

Trend Micro™ Security Center

See where the latest threats detected by Trend Micro have emerged on a worldwide map.

Download Now

Trend Micro™ Go Everywhere

Locate your missing device on a map, or sound a one-minute alarm by remote control to help you find it.

Download Now

Trend Micro™ SafeGuard

Get the world's most secure web browser and enjoy all that the internet has to offer without worry. Built-in cutting edge protection keeps online threats out of your way

Download Now

Trend Micro™ Housecall

Take advantage of the Trend Micro Smart Protection Network to remove security theats.

Try Now

Trend Micro™ Smart surfing

Enjoy a smarter, safer online experience with this secure browser for your iphone, ipad touch, or ipad

Try Now | Help & Support

Figure 21. More Tools Web Page

33. Click **Download Now** to try an additional tool, including Windows 8 Modern UI tools such as **Trend Micro™ Security Center, Trend Micro™ Go Everywhere,** and **Trend Micro™ SafeSurfing**.

    - **Security Center** provides top-level status on the security of your machine, and provides information on global and regional security.
    - **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.
    - **SafeSurfing** browser provides greater security when browsing in Windows 8, providing the cutting-edge protection Titanium users have come to enjoy in their browser.

34. Click **Try Now** to try **Trend Micro™ Housecall** to use the SPN to check for security threats or **Trend Micro™ Smart Surfing** to enjoy safer browsing on your iPhone, iPod Touch, or iPad.

Using Rescue Disk for Severe Malware Removal

Titanium's **Rescue Disk**, available for Titanium through the **Scan Results** dialog on an infected system 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:

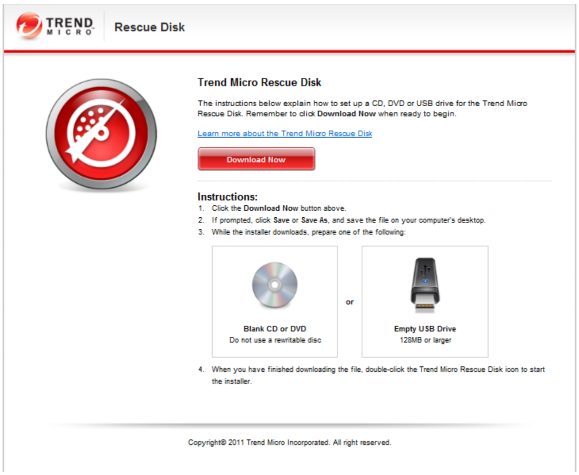
1. Choose between the following options:

    - If you just conducted a scan on an infected system and you receive the message in the scan result window "Additional Cleaning Needed," click the **Download Now** button to take you to the **Trend Micro Rescue Disk** web page.

      OR

    - In the **PC/Mobile** tab of your **Titanium Console**, click **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.



Trend Micro Rescue Disk

The instructions below explain how to set up a CD, DVD or USB drive for the Trend Micro Rescue Disk. Remember to click **Download Now** when ready to begin.

Learn more about the Trend Micro Rescue Disk

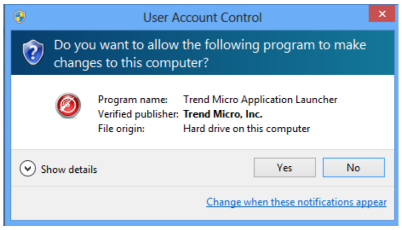
Instructions:
1. Click the **Download Now** button above.
2. If prompted, click **Save** or **Save As**, and save the file on your computer's desktop.
3. While the installer downloads, prepare one of the following:

4. When you have finished downloading the file, double-click the Trend Micro Rescue Disk icon to start the installer.

Copyright© 2011 Trend Micro Incorporated. All right reserved.

Figure 22. Trend Micro Rescue Disk Download

3. Once downloaded, double-click the **Rescue Disk** icon on your desktop. A **User Account Control** dialog appears, asking if you want to run this program.

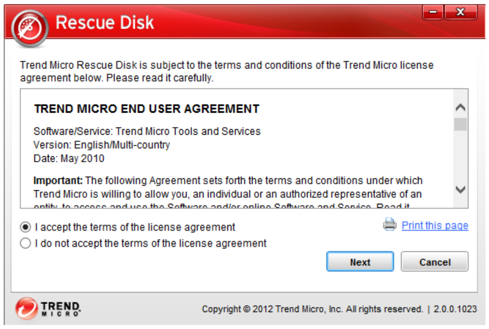


Do you want to allow the following program to make changes to this computer?

Program name: Trend Micro Application Launcher
Verified publisher: **Trend Micro, Inc.**
File origin: Hard drive on this computer

Figure 23. User Account Control

4. Click **Yes** to continue. The **Rescue Disk License Agreement** appears.



Trend Micro Rescue Disk is subject to the terms and conditions of the Trend Micro license agreement below. Please read it carefully.

TREND MICRO END USER AGREEMENT

Software/Service: Trend Micro Tools and Services
Version: English/Multi-country
Date: May 2010

Important: The following Agreement sets forth the terms and conditions under which Trend Micro is willing to allow you, an individual or an authorized representative of an entity, to access and use the Software and/or online Software and Service. Read it

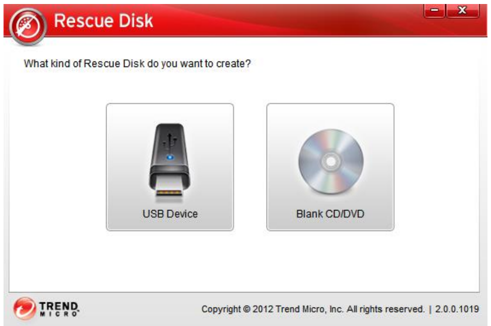
● I accept the terms of the license agreement
○ I do not accept the terms of the license agreement

Copyright © 2012 Trend Micro, Inc. All rights reserved. | 2.0.0.1023

Figure 24. Rescue Disk License Agreement

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

6. 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).

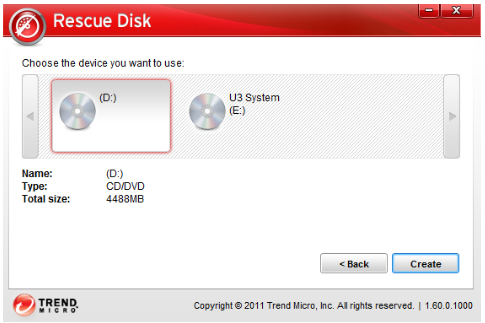


What kind of Rescue Disk do you want to create?

Copyright © 2012 Trend Micro, Inc. All rights reserved. | 2.0.0.1019

Figure 25. Rescue Disk Types

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



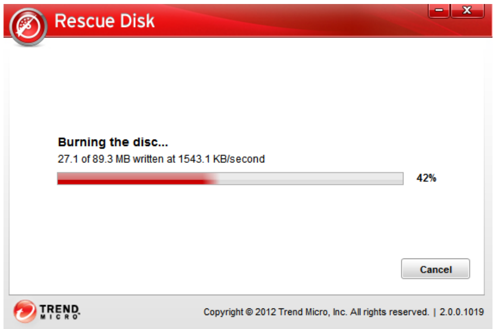
Choose the device you want to use:

Name: (D:)
Type: CD/DVD
Total size: 4488MB

Copyright © 2011 Trend Micro, Inc. All rights reserved. | 1.60.0.1000

Figure 26. Device Selector

8. 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.



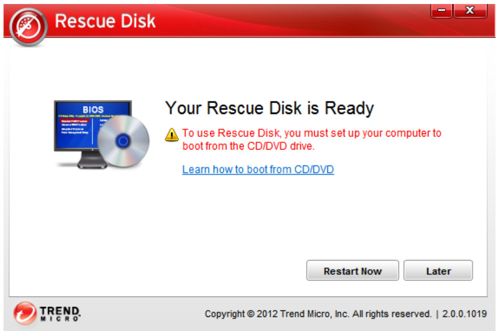
Burning the disc...

27.1 of 89.3 MB written at 1543.1 KB/second

Copyright © 2012 Trend Micro, Inc. All rights reserved. | 2.0.0.1019

Figure 27. Burning the Rescue Disk

9. Once the **Rescue Disk** has been created, you're notified that **Your Rescue Disk is Ready.**



Your Rescue Disk is Ready

To use Rescue Disk, you must set up your computer to boot from the CD/DVD drive.

Copyright © 2012 Trend Micro, Inc. All rights reserved. | 2.0.0.1019

Figure 28. 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.)

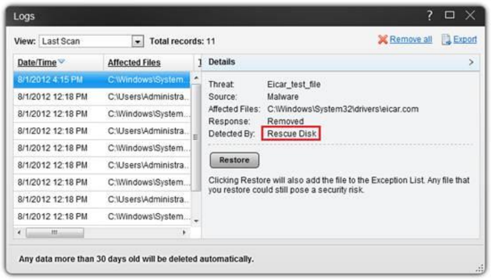
Note: **To use Rescue Disk, you must have previously set up your computer to boot from the CD/DVD Drive first. Most computers are already set to seek the CD/DVD first when booting.**

---

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 computer will reboot to the Windows Desktop.
18. Note that **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.



View: Last Scan

Total records: 11

Date/Time	Affected Files
8/1/2012 4:15 PM	C:\Windows\System...
8/1/2012 12:18 PM	C:\Users\Administra...
8/1/2012 12:18 PM	C:\Windows\System...
8/1/2012 12:18 PM	C:\Users\Administra...
8/1/2012 12:18 PM	C:\Windows\System...
8/1/2012 12:18 PM	C:\Users\Administra...
8/1/2012 12:18 PM	C:\Windows\System...
8/1/2012 12:18 PM	C:\Users\Administra...
8/1/2012 12:18 PM	C:\Windows\System...

Threat: Eicar_test_file
Source: Malware
Affected Files: C:\Windows\System32\drivers\eicar.com
Response: Removed
Detected By: Rescue Disk

Clicking Restore will also add the file to the Exception List. Any file that you restore could still pose a security risk.

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

Figure 29. Titanium Rescue Disk Log

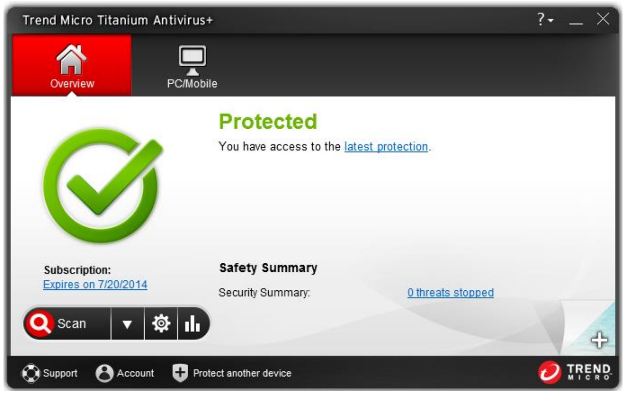
Chapter 3: Titanium Security Overview

In the following chapters, we'll walk through each edition of Titanium Security, explaining the key features provided in each. In this chapter, we'll give you a quick overview of some easy-to-use functions.

Note: **If you have a higher-end edition of Titanium, you should read the prior chapters devoted to the lower-end edition. The higher-end editions have all the features of their lower-end siblings, but provide additional "premium" features on top of the ones they share with the lower editions.**

Quick Start: The Titanium Console

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



Protected

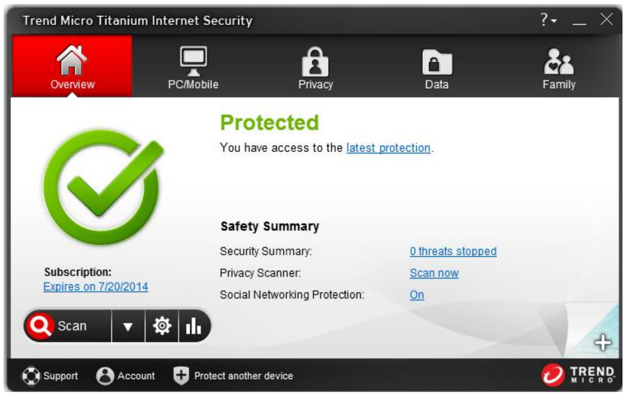
You have access to the latest protection.

Subscription: Expires on 7/20/2014

Safety Summary

Security Summary: 0 threats stopped

Figure 30. Titanium Antivirus+ Console



Protected

You have access to the latest protection.

Subscription: Expires on 7/20/2014

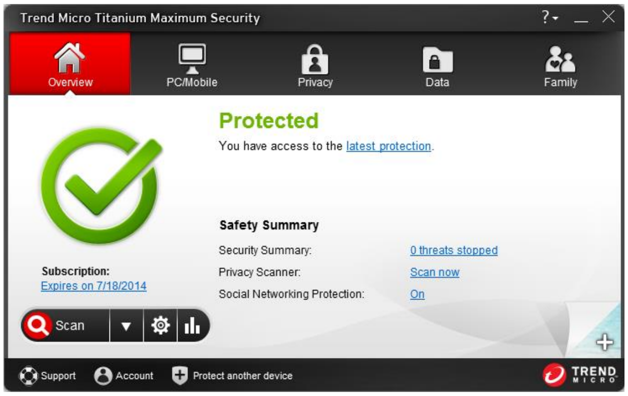
Safety Summary

Security Summary: 0 threats stopped

Privacy Scanner: Scan now

Social Networking Protection: On

Figure 31. Titanium Internet Security



Protected

You have access to the latest protection.

Safety Summary

Security Summary: 0 threats stopped

Privacy Scanner: Scan now

Social Networking Protection: On

Subscription: Expires on 7/18/2014

Figure 32. 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

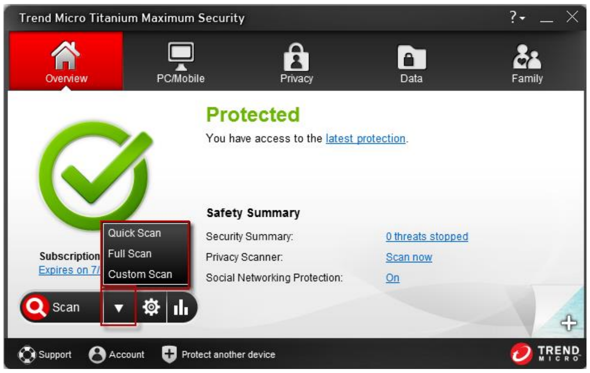
By default, Titanium activates a **real-time scan** when it is installed. This is always present in memory (unless disabled), to proactively protect you from real-time threats. Threats are caught as they try to enter memory or touch the hard drive, preventing infections.

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



Trend Micro Titanium Maximum Security

Protected

You have access to the latest protection.

Safety Summary

Security Summary: 0 threats stopped

Privacy Scanner: Scan now

Social Networking Protection: On

Subscription

Expires on 7/

Figure 33. Quick Scan | Scan Menu

To scan your computer disk:

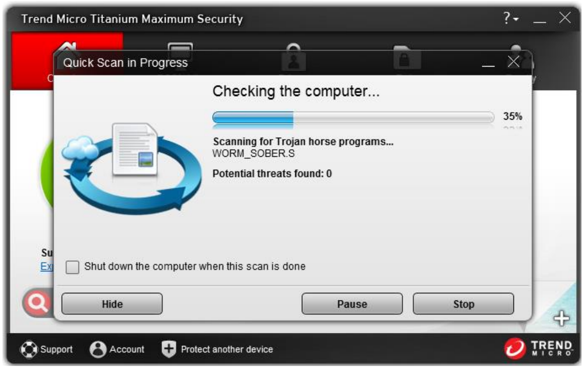
Titanium provides a **Scan** Tool on the console (shown above) which can be used in two ways:

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.



Checking the computer...

35%

Scanning for Trojan horse programs...
WORM_SOBER.S

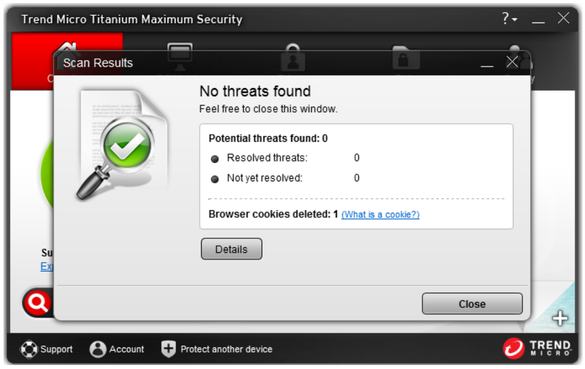
Potential threats found: 0

☐ Shut down the computer when this scan is done

Figure 34. 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.**



No threats found
Feel free to close this window.

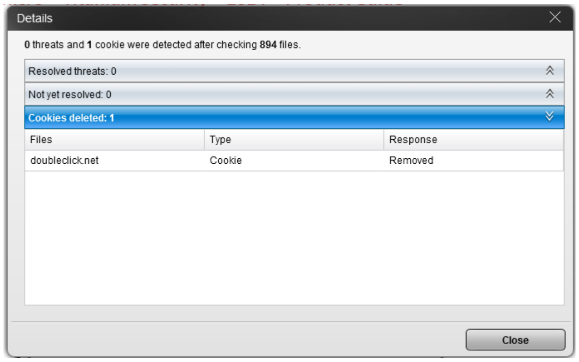
Potential threats found: 0
● Resolved threats: 0
● Not yet resolved: 0

Browser cookies deleted: 1 (What is a cookie?)

Figure 35. 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.



0 threats and 1 cookie were detected after checking 894 files.

Resolved threats: 0

Not yet resolved: 0

Cookies deleted: 1

Files	Type	Response
doubleclick.net	Cookie	Removed

Figure 36. Details

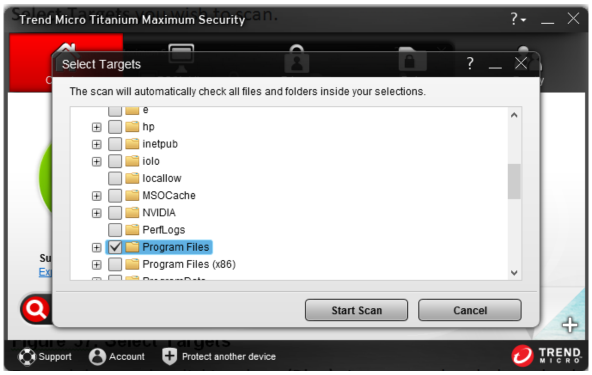
6. Click each of the collapsible panels in turn to show the **Details** tables, which include file names, types, and responses to the threats.

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.



The scan will automatically check all files and folders inside your selections.

- □ e
- ⊞ □ hp
- ⊞ □ inetpub
- ⊞ □ iolo
- □ locallow
- ⊞ □ MSOCache
- ⊞ □ NVIDIA
- □ PerfLogs
- ⊞ ☑ Program Files
- ⊞ □ Program Files (x86)

Figure 37. 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.

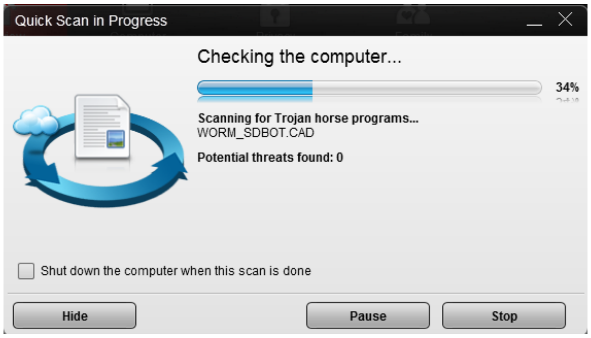
Intensive Scan

Titanium automatically 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.



Quick Scan in Progress

Checking the computer...

34%

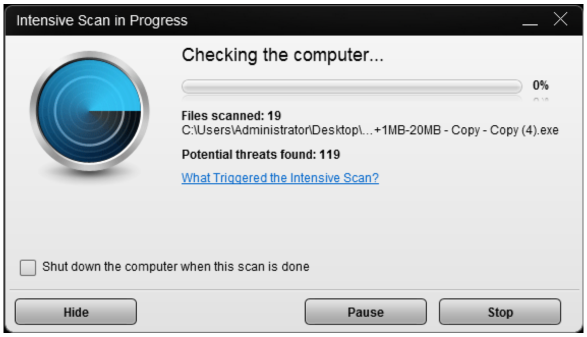
Scanning for Trojan horse programs...
WORM_SDBOT.CAD

Potential threats found: 0

☐ Shut down the computer when this scan is done

Figure 38. Quick Scan in Progress

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



Intensive Scan in Progress

Checking the computer...

0%

Files scanned: 19
C:\Users\Administrator\Desktop\...+1MB-20MB - Copy - Copy (4).exe

Potential threats found: 119

What Triggered the Intensive Scan?

☐ Shut down the computer when this scan is done

Figure 39. 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?**

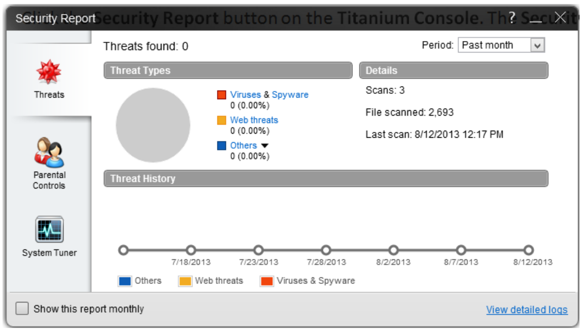
Quick Start: Viewing Threat Security Reports

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.



Security Report

Threats found: 0

Period: Past month

Threat Types

Viruses & Spyware
0 (0.00%)

Web threats
0 (0.00%)

Others
0 (0.00%)

Details

Scans: 3

File scanned: 2,693

Last scan: 8/12/2013 12:17 PM

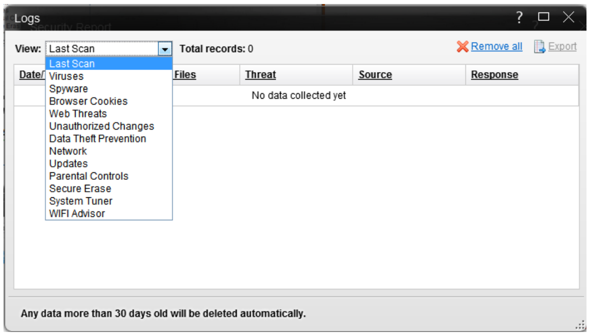
Threat History

□ Show this report monthly

View detailed logs

Figure 40. 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
     - Variously 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.**



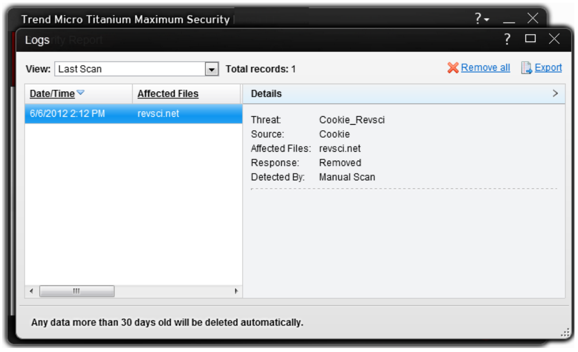
View: Last Scan Total records: 0

Date/	Files	Threat	Source	Response
		No data collected yet		

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

Figure 41. Logs

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



View: Last Scan Total records: 1

Date/Time	Affected Files
6/6/2012 2:12 PM	revsci.net

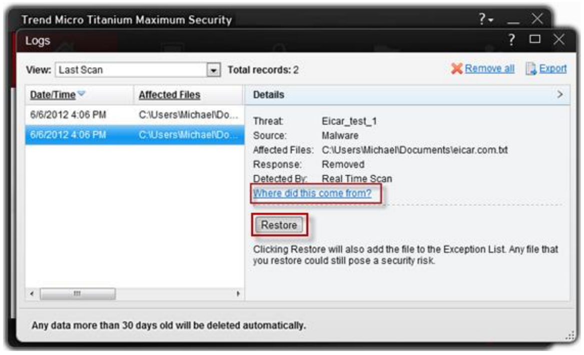
Threat: Cookie_Revsci
Source: Cookie
Affected Files: revsci.net
Response: Removed
Detected By: Manual Scan

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

Figure 42. Logs > Item Details

7. Click **Remove all** to remove the items from the table.

8. Click **Export** in the upper right-hand corner to export the logs in .CSV or .TXT format.


Trend Micro Titanium Maximum Security
Logs
Remove all
Export
Details
Where did this come from?
Restore

View: Last Scan Total records: 2

Date/Time	Affected Files
6/6/2012 4:06 PM	C:\Users\Michael\Do...
6/6/2012 4:06 PM	C:\Users\Michael\Do...

Threat: Eicar_test_1
Source: Malware
Affected Files: C:\Users\Michael\Documents\eicar.com.txt
Response: Removed
Detected By: Real Time Scan

Clicking Restore will also add the file to the Exception List. Any file that you restore could still pose a security risk.

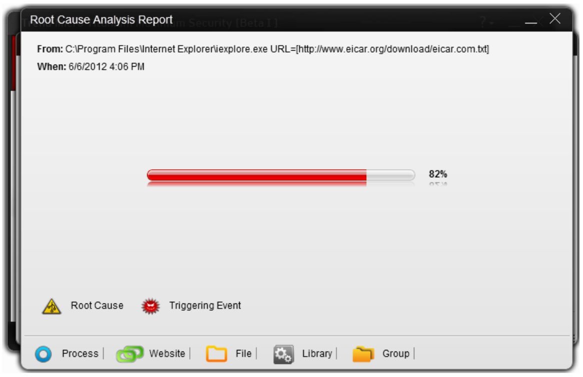
Any data more than 30 days old will be deleted automatically.

Figure 43. Where Did This Come From? | Restore

9. Click **Restore** to restore to add the file to the **Exception List**. Any file that you restore could still pose a security risk.

10. 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

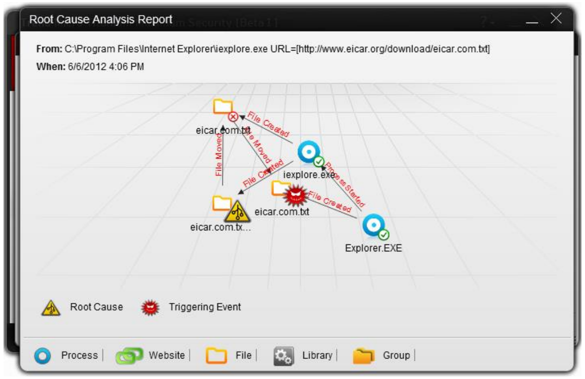
Root Cause Analysis Report. A dialog appears, showing you the progress while generating the report.



From: C:\Program Files\Internet Explorer\iexplore.exe URL=[http://www.eicar.org/download/eicar.com.txt]
When: 6/6/2012 4:06 PM

Figure 44. Generating the Root Cause Analysis Report

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



From: C:\Program Files\Internet Explorer\iexplore.exe URL=[http://www.eicar.org/download/eicar.com.txt]
When: 6/6/2012 4:06 PM

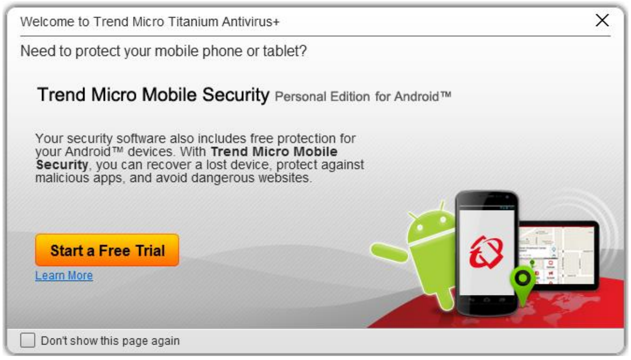
Figure 45. Root Cause Analysis Report

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+ 2014 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.



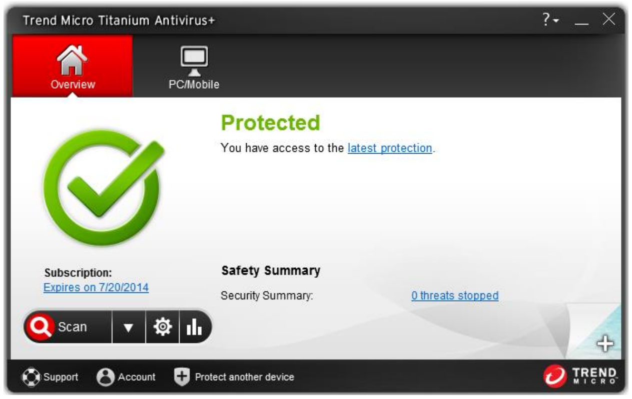
Welcome to Trend Micro Titanium Antivirus+

Need to protect your mobile phone or tablet?

Trend Micro Mobile Security Personal Edition for Android™

Your security software also includes free protection for your Android™ devices. With **Trend Micro Mobile Security**, you can recover a lost device, protect against malicious apps, and avoid dangerous websites.

Figure 46. Trend Micro Titanium Antivirus+ Welcome Page



Protected

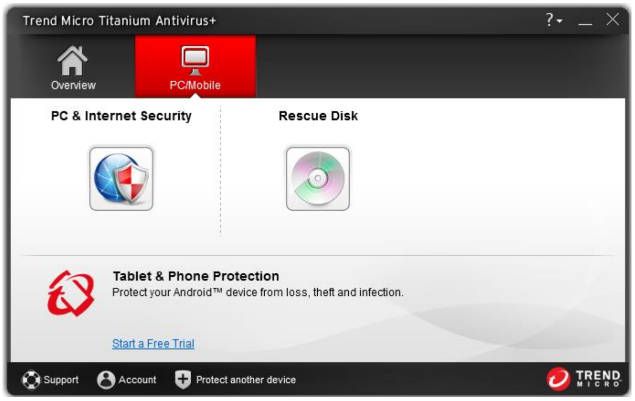
You have access to the latest protection.

Subscription:
Expires on 7/20/2014

Safety Summary

Security Summary: 0 threats stopped

Figure 47. Trend Micro Titanium Antivirus+ Console



Tablet & Phone Protection

Protect your Android™ device from loss, theft and infection.

Figure 48. PC/Mobile > PC & Internet Security | Rescue Disk

Note: **Titanium Antivirus+ Console Features: PC & Internet Security, Rescue Disk. Additional Offerings: Free 3-day Trial - Tablet & Phone Protection (Trend Micro Mobile Security for Android)**

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+ 2014 includes anti-spam in its list of features. 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. Titanium Antivirus+ also protects you from threats in files attached to email messages.

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. Finally, Titanium Antivirus+ 2014 now includes the ability to switch your protection level automatically, to aggressively eliminate programs that pose even a small risk of bad behavior.

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.

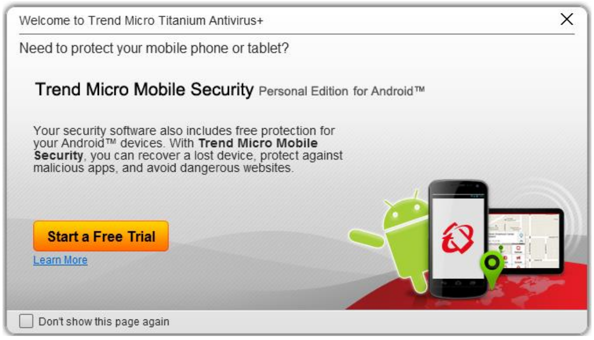
Titanium Antivirus+ proactively protects you from a variety of these web threats, so that they never touch your computer. To provide thorough protection from and rapid response times to emerging threats, Titanium uses the Trend Micro Smart Protection Network cloud-client security infrastructure along 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+ 2014 also blocks malicious links and image spam in emails

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.

Getting Started > Additional Protection For Android

When you first load Titanium, a **Welcome Page** appears, showing an additional security option for your Android Mobile device. You can **Start a Free Trial** of Trend Micro Mobile Security by simply clicking the button.



Welcome to Trend Micro Titanium Antivirus+

Need to protect your mobile phone or tablet?

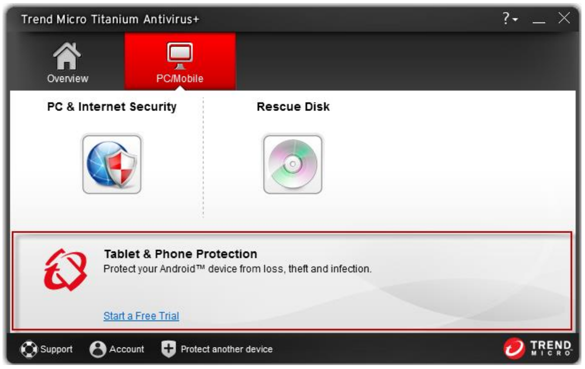
Trend Micro Mobile Security Personal Edition for Android™

Your security software also includes free protection for your Android™ devices. With **Trend Micro Mobile Security**, you can recover a lost device, protect against malicious apps, and avoid dangerous websites.

Figure 49. Welcome to Trend Micro Titanium

You can **Start a Free Trial** of Trend Micro Mobile Security by simply clicking the button.

This option is also available from the PC/Mobile tab.



Tablet & Phone Protection

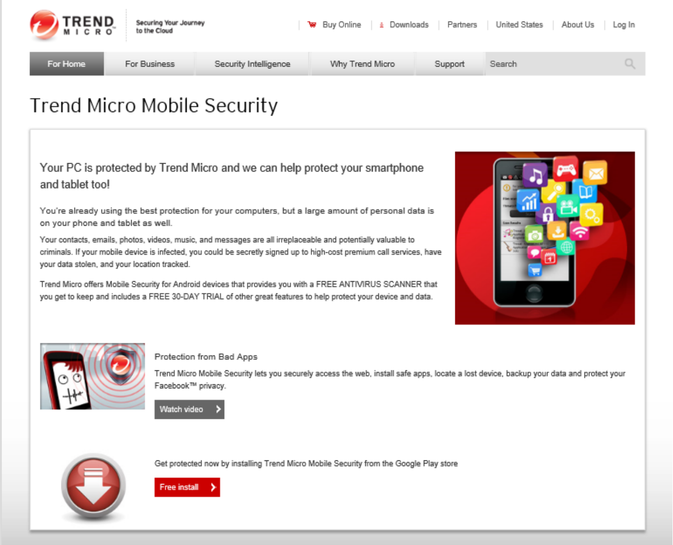
Protect your Android™ device from loss, theft and infection.

Start a Free Trial

Figure 50. PC/Mobile | Tablet & Phone Protection for Android

To download the program to your Android device:

1. In the **Welcome** or **PC/Mobile** screen, click **Start A Free Trial** to download the software.
2. Your browser launches and takes you to the Trend Micro Mobile Security download page.



Trend Micro Mobile Security

Your PC is protected by Trend Micro and we can help protect your smartphone and tablet too!

You're already using the best protection for your computers, but a large amount of personal data is on your phone and tablet as well.

Your contacts, emails, photos, videos, music, and messages are all irreplaceable and potentially valuable to criminals. If your mobile device is infected, you could be secretly signed up to high-cost premium call services, have your data stolen, and your location tracked.

Trend Micro offers Mobile Security for Android devices that provides you with a FREE ANTIVIRUS SCANNER that you get to keep and includes a FREE 30-DAY TRIAL of other great features to help protect your device and data.

Protection from Bad Apps

Trend Micro Mobile Security lets you securely access the web, install safe apps, locate a lost device, backup your data and protect your Facebook™ privacy.

Get protected now by installing Trend Micro Mobile Security from the Google Play store

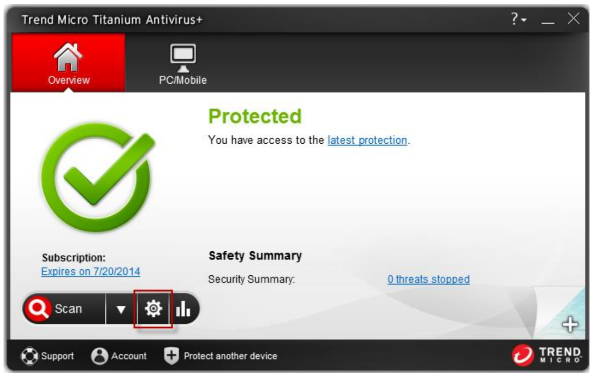
Figure 51. Trend Micro Mobile Security Download Webpage

3. Click **Free Install** to download the software, then follow the process to install it. If your device is already registered to your Google Play account, you can target that device for a remote install of a free 30-day trial.
4. 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:



Protected

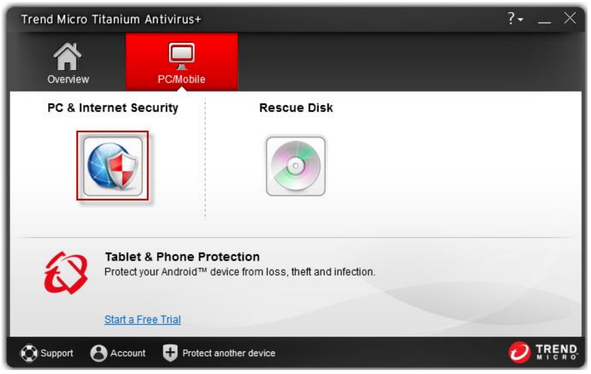
You have access to the latest protection.

Subscription:
Expires on 7/20/2014

Safety Summary

Security Summary: 0 threats stopped

Figure 52. Titanium Console > Protection Settings Tool

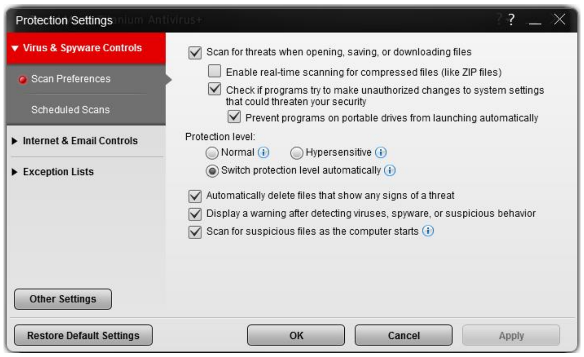


Tablet & Phone Protection

Protect your Android™ device from loss, theft and infection.

Figure 53. 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**.



☑ Scan for threats when opening, saving, or downloading files

□ Enable real-time scanning for compressed files (like ZIP files)

☑ Check if programs try to make unauthorized changes to system settings that could threaten your security

☑ Prevent programs on portable drives from launching automatically

Protection level:

○ Normal ○ Hypersensitive

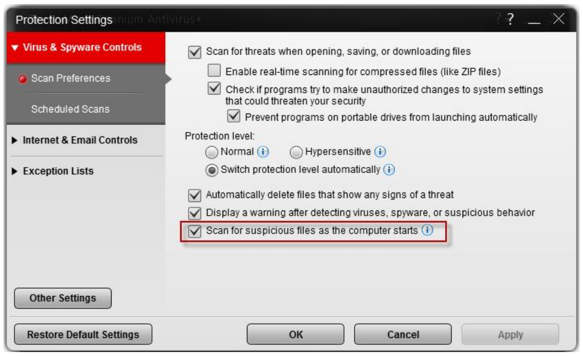
● Switch protection level automatically

☑ Automatically delete files that show any signs of a threat

☑ Display a warning after detecting viruses, spyware, or suspicious behavior

☑ Scan for suspicious files as the computer starts

Figure 54. Windows 7: Virus & Spyware Controls > Scan Preferences



☑ Scan for threats when opening, saving, or downloading files

□ Enable real-time scanning for compressed files (like ZIP files)

☑ Check if programs try to make unauthorized changes to system settings that could threaten your security

☑ Prevent programs on portable drives from launching automatically

Protection level:

○ Normal ○ Hypersensitive

● Switch protection level automatically

☑ Automatically delete files that show any signs of a threat

☑ Display a warning after detecting viruses, spyware, or suspicious behavior

☑ Scan for suspicious files as the computer starts

Figure 55. Windows 8: Scan During Start

2. The following **Scan Preferences** are displayed. Check or uncheck to change a setting.

- **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.
- **Protection Level**. This behavior monitoring function—the new automatic scan switch in Titanium 2014—is enabled by default to switch from Normal to Hypersensitive only when needed, but you can change this setting.
    - **Normal -** 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.

 - **Switch protection level automatically** - Increases the protection level only when you need it. The default setting.

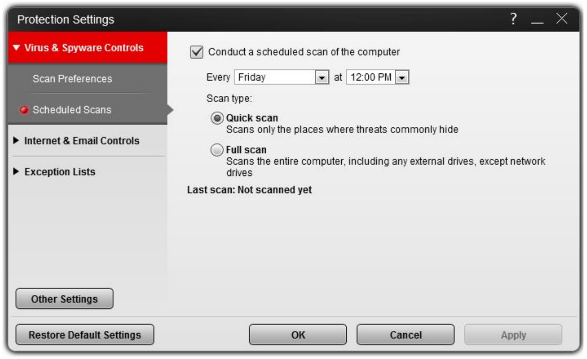
- **Automatically delete files that show any signs of a threat**. This is enabled by default, to automatically delete threatened files.
- **Display a warning after detecting viruses, spyware, or suspicious behavior.** This is enabled by default. Titanium is selective when using pop-ups; it's never overly intrusive.
- **Windows 8 Only: Scan for suspicious files as the computer starts.** Key security components 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.



☑ Conduct a scheduled scan of the computer

Every Friday at 12:00 PM

Scan type:

● **Quick scan**
Scans only the places where threats commonly hide

○ **Full scan**
Scans the entire computer, including any external drives, except network drives

Last scan: Not scanned yet

Figure 56. 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.

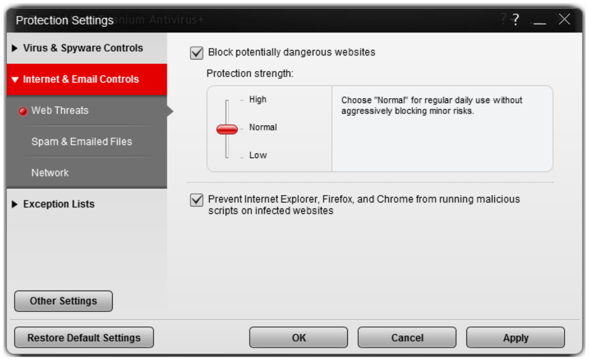
3. Click **Restore Default Settings** to restore default settings to their factory condition.

4. Click **Apply** to apply any changes, then **OK** to close the **Protection Settings** window.

Internet & Email Controls: Web Threats

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

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



☑ Block potentially dangerous websites

Protection strength:

High
Normal
Low

Choose "Normal" for regular daily use without aggressively blocking minor risks.

☑ Prevent Internet Explorer, Firefox, and Chrome from running malicious scripts on infected websites

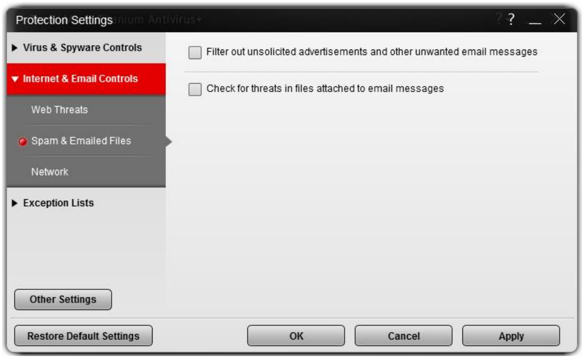
Figure 57. Internet & Email Controls > Web Threats

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.
4. **Prevent Microsoft Internet Explorer and Mozilla Firefox from running malicious scripts on infected websites** is enabled by default.
5. 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.



☐ Filter out unsolicited advertisements and other unwanted email messages

☐ Check for threats in files attached to email messages

Figure 58. Internet & Email Controls > Spam & Emailed Files

2. **Filter out unsolicited advertisements and other unwanted email messages** is disabled by default. Check this if you wish to stop spam and other unsought messages.
3. **Check for threats in files attached to email messages** is disabled by default. Check this 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 per OS Platform and Mail Client is given in the table below.

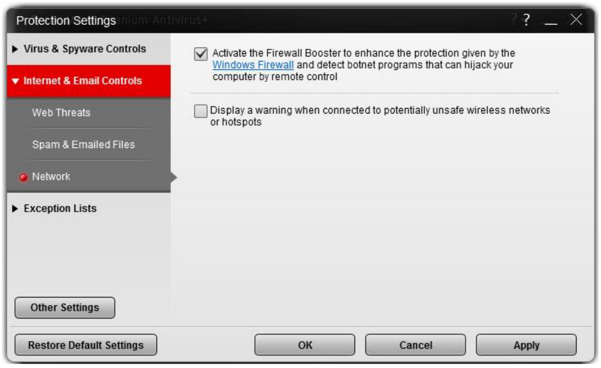
Table 6. TMAS OS Platform and Mail Client Support

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.



☑ Activate the Firewall Booster to enhance the protection given by the Windows Firewall and detect botnet programs that can hijack your computer by remote control

□ Display a warning when connected to potentially unsafe wireless networks or hotspots

Figure 59. Internet & Email Controls > Network

3. **Activate the Firewall Booster** is checked by default. This enhances the protection given by the Windows Firewall and detect botnets programs that can hijack your computer by remote control.

4. **Display a warning when connected to potentially unsafe wireless networks or hotspots** is disabled by default. Check this to enable the feature.

5. Click **OK** to save your changes.

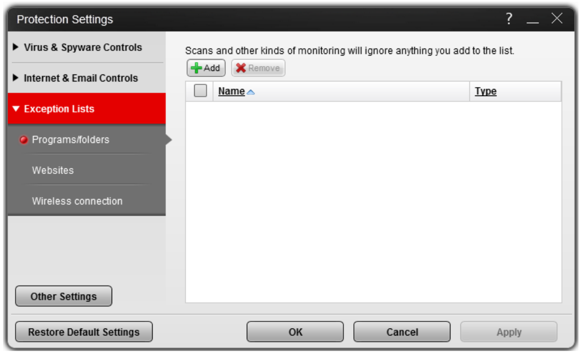
Note: The Exception List for Wi-Fi Protection allows users to add unprotected home networks to an exception list, so that users are not subject to frequent warnings for networks they know to be safe. See the Exception Lists section below for more details.

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.

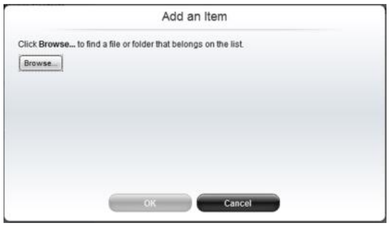
1. To add items to exception lists, click **Exception Lists**. **Programs/folders** appears by default.



Scans and other kinds of monitoring will ignore anything you add to the list.

Figure 60. Exception Lists > Programs/folders

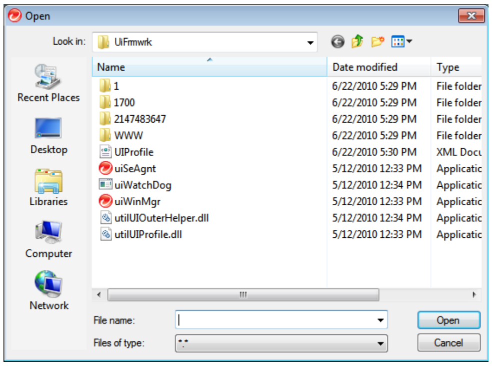
2. Click **+Add** to add a program or folder to the exception list. A dialog appears, letting you **Add an Item.**



Click **Browse...** to find a file or folder that belongs on the list.

Figure 61. Add an Item

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



Look in: UiFmwrk

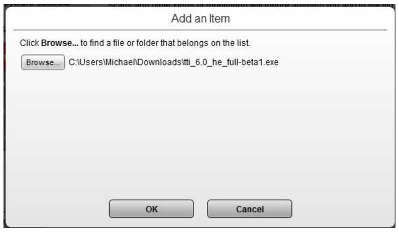
Name	Date modified	Type
1	6/22/2010 5:29 PM	File folder
1700	6/22/2010 5:29 PM	File folder
2147483647	6/22/2010 5:29 PM	File folder
WWW	6/22/2010 5:29 PM	File folder
UIProfile	6/22/2010 5:30 PM	XML Docu
uiSeAgnt	5/12/2010 12:33 PM	Applicatic
uiWatchDog	5/12/2010 12:34 PM	Applicatic
uiWinMgr	5/12/2010 12:33 PM	Applicatic
utilUIOuterHelper.dll	5/12/2010 12:34 PM	Applicatic
utilUIProfile.dll	5/12/2010 12:33 PM	Applicatic

File name:

Files of type: *.*

Figure 62. Open Dialog

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



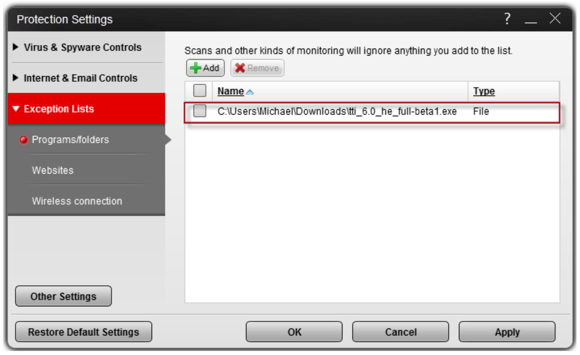
Add an Item

Click **Browse...** to find a file or folder that belongs on the list.

Browse... C:\Users\Michael\Downloads\tti_6.0_he_full-beta1.exe

Figure 63. Add an Item (item added)

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



Scans and other kinds of monitoring will ignore anything you add to the list.

Name	Type
C:\Users\Michael\Downloads\tti_6.0_he_full-beta1.exe	File

Figure 64. Item Added to Exception List

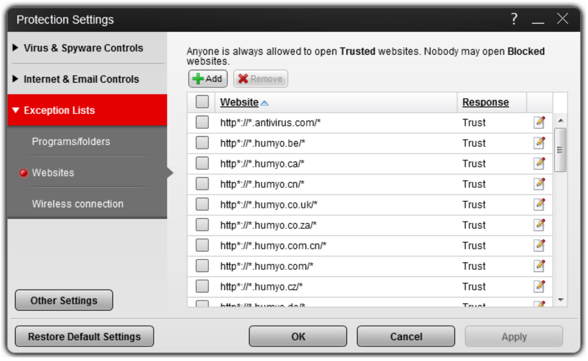
6. To remove an item, check it, and then click the **X Remove** button.

7. Click **Apply** to save any changes, then **OK** to close the Titanium Console.

Exception Lists: Websites

To add websites to an exception list:

1. 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.



Anyone is always allowed to open **Trusted** websites. Nobody may open **Blocked** websites.

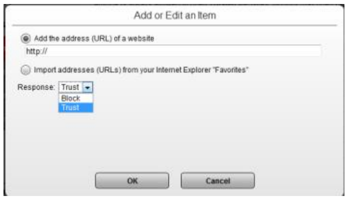
Website	Response
http*://*.antivirus.com/*	Trust
http*://*.humyo.be/*	Trust
http*://*.humyo.ca/*	Trust
http*://*.humyo.cn/*	Trust
http*://*.humyo.co.uk/*	Trust
http*://*.humyo.co.za/*	Trust
http*://*.humyo.com.cn/*	Trust
http*://*.humyo.com/*	Trust
http*://*.humyo.cz/*	Trust
http*://*.humyo.de/*	Trust

Figure 65. Exception Lists > Websites

2. Click **Add** to add a website. A dialog appears, letting you **Add** or **Edit an Item.**

3. Choose among the following options:

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



Add or Edit an Item

● Add the address (URL) of a website

http://

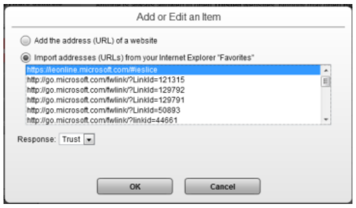
○ Import addresses (URLs) from your Internet Explorer "Favorites"

Response: Trust
Block
Trust

OK Cancel

Figure 66. Add or Edit an Item

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



Add or Edit an Item

○ Add the address (URL) of a website

● Import addresses (URLs) from your Internet Explorer "Favorites"

https://eonline.microsoft.com/#ieslice
http://go.microsoft.com/fwlink/?LinkId=121315
http://go.microsoft.com/fwlink/?LinkId=129792
http://go.microsoft.com/fwlink/?LinkId=129791
http://go.microsoft.com/fwlink/?LinkId=50893
http://go.microsoft.com/fwlink/?linkid=44661

Response: Trust

OK Cancel

Figure 67. Import URLs from IE

c. Choose **Block** or **Trust** from the **Response** pop-up (for either option).

d. Click **OK** to save the option.

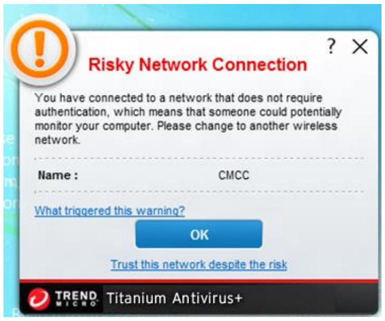
4. Click **Apply** to save your changes, then **OK** again to close the Titanium Console.

Exception Lists: Wireless Connection

Titanium 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.



Risky Network Connection

You have connected to a network that does not require authentication, which means that someone could potentially monitor your computer. Please change to another wireless network.

Name : CMCC

What triggered this warning?

OK

Trust this network despite the risk

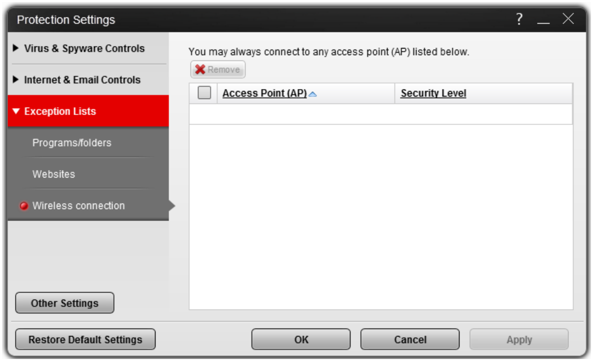
TREND MICRO Titanium Antivirus+

Figure 68. 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.



You may always connect to any access point (AP) listed below.

□	Access Point (AP)	Security Level

Figure 69. Exception Lists > Wireless connection

5. Select the access point in the list and click **Remove**. Titanium deletes it from the list.

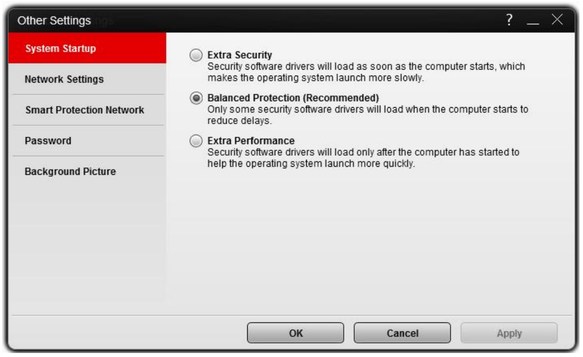
6. Click **Apply** to save your changes.

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).



○ **Extra Security**
Security software drivers will load as soon as the computer starts, which makes the operating system launch more slowly.

● **Balanced Protection (Recommended)**
Only some security software drivers will load when the computer starts to reduce delays.

○ **Extra Performance**
Security software drivers will load only after the computer has started to help the operating system launch more quickly.

Figure 70. Other Settings > System Startup

2. Select among the following options:

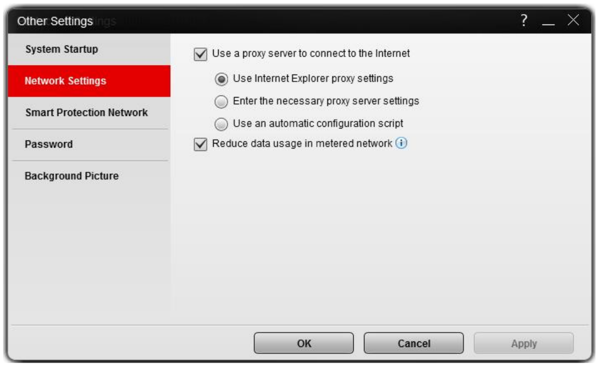
- **Extra Security -** Security software drivers will load as soon as the computer starts, which makes the operating system launch more slowly.
- **Balanced Protection -** This is the default setting. Only some security software drivers will load when the computer starts to reduce delays. Others will 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.



☑ Use a proxy server to connect to the Internet

● Use Internet Explorer proxy settings

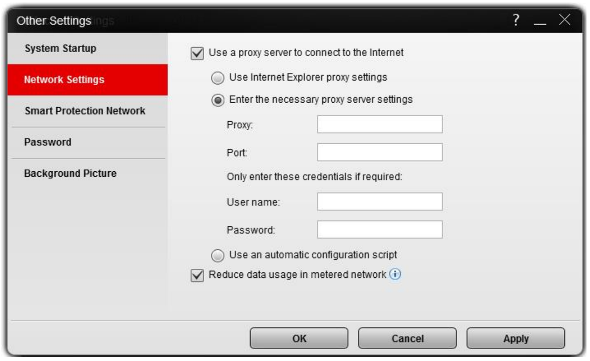
○ Enter the necessary proxy server settings

○ Use an automatic configuration script

☑ Reduce data usage in metered network

Figure 71. Other Settings > Proxy Settings

2. **Reduce data usage in metered network** is selected by default. The frequency of maintenance software updates will be less than on a non-metered network.
3. Select **Enter the necessary proxy server settings** to manually enter a proxy server's name, port, and credentials (if required).



☑ Use a proxy server to connect to the Internet

○ Use Internet Explorer proxy settings

● Enter the necessary proxy server settings

Proxy:

Port:

Only enter these credentials if required:

User name:

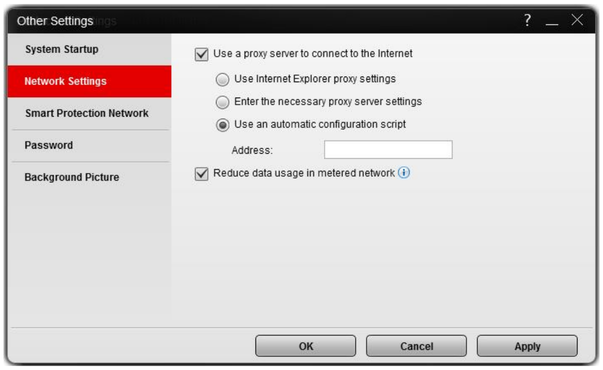
Password:

○ Use an automatic configuration script

☑ Reduce data usage in metered network ⓘ

Figure 72. Other Settings > Proxy Settings > Enter Settings

4. Or select **Use an automatic configuration script** and enter the script in the **Address** field provided.



☑ Use a proxy server to connect to the Internet

○ Use Internet Explorer proxy settings

○ Enter the necessary proxy server settings

● Use an automatic configuration script

Address:

☑ Reduce data usage in metered network ⓘ

Figure 73. Other Settings > Automatic Configuration Script

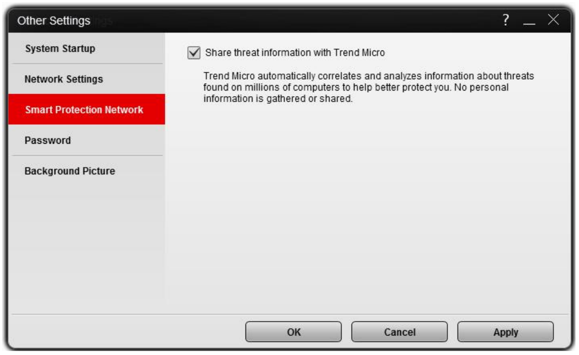
5. Click **Apply** to save your changes, then **OK** to close the **Protection Settings** window.

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.



☑ Share threat information with Trend Micro

Trend Micro automatically correlates and analyzes information about threats found on millions of computers to help better protect you. No personal information is gathered or shared.

Figure 74. 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.)

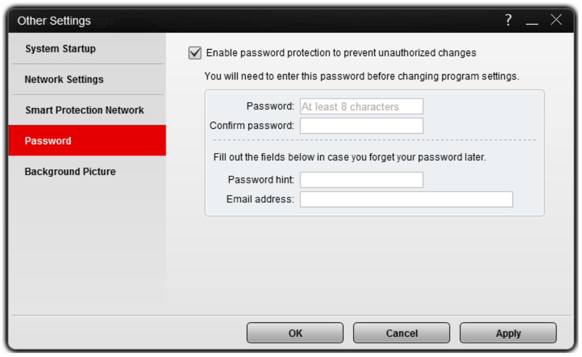
3. Click **Apply** to save your changes, then **OK** to close the **Protection Settings** window.

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.



☑ Enable password protection to prevent unauthorized changes

You will need to enter this password before changing program settings.

Password: At least 8 characters

Confirm password:

Fill out the fields below in case you forget your password later.

Password hint:

Email address:

Figure 75. 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.

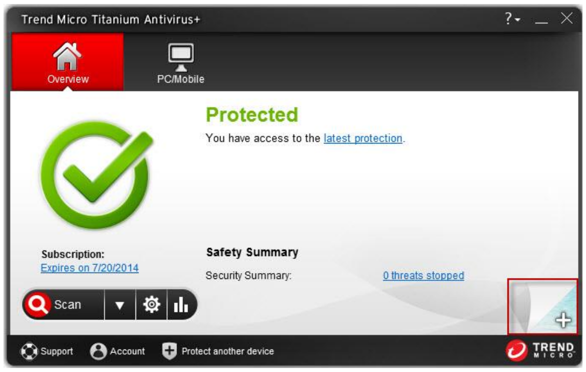
4. Fill out the **Password Hint** and **Email Address** fields in case you forget your password later.

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:

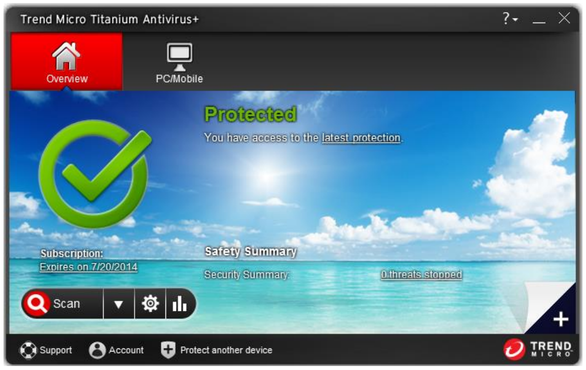


Protected

You have access to the latest protection.

Figure 76. 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.

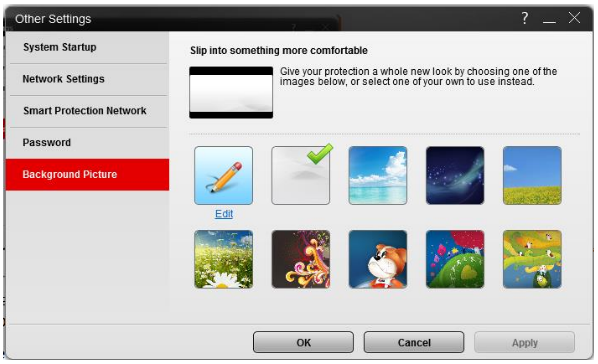


Protected

You have access to the latest protection.

Figure 77. 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.



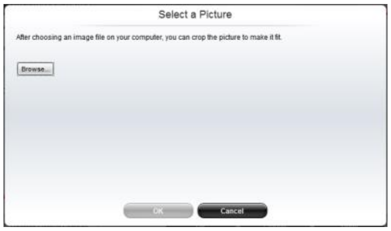
Slip into something more comfortable

Give your protection a whole new look by choosing one of the images below, or select one of your own to use instead.

Figure 78. Background Picture Editor

3. Select any background picture provided and click **Apply** to save the new background, or add a picture from your computer.

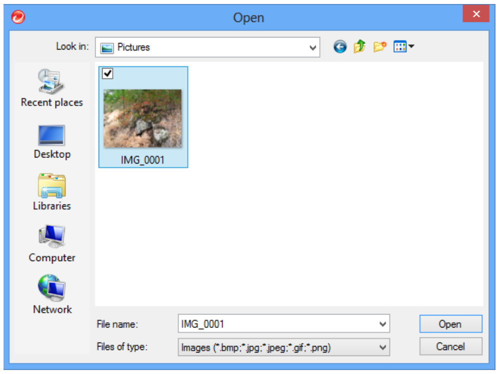
4. For the second option, click the **Edit** button to edit your user interface. The **Select a Picture** dialog displays.



After choosing an image file on your computer, you can crop the picture to make it fit.

Figure 79. Select a Picture

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



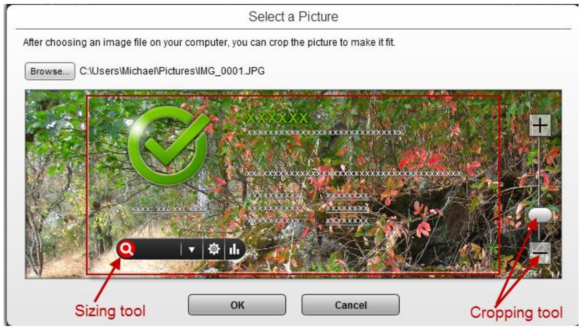
Look in: Pictures

File name: IMG_0001

Files of type: Images (*.bmp;*.jpg;*.jpeg;*.gif;*.png)

Figure 80. Browse to Picture

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



Select a Picture

After choosing an image file on your computer, you can crop the picture to make it fit.

Browse... C:\Users\Michael\Pictures\IMG_0001.JPG

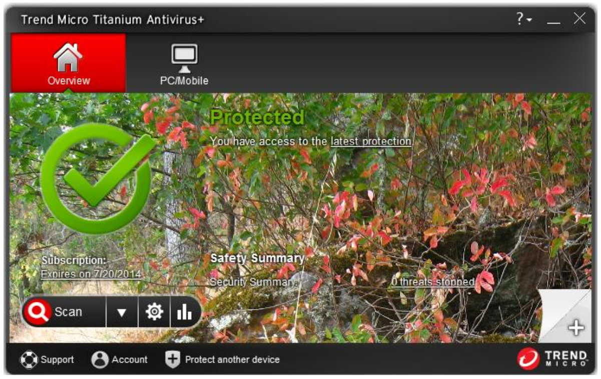
Figure 81. Cropping and Sizing

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.



Trend Micro Titanium Antivirus+

Protected

You have access to the latest protection

Subscription:
Expires on 7/20/2014

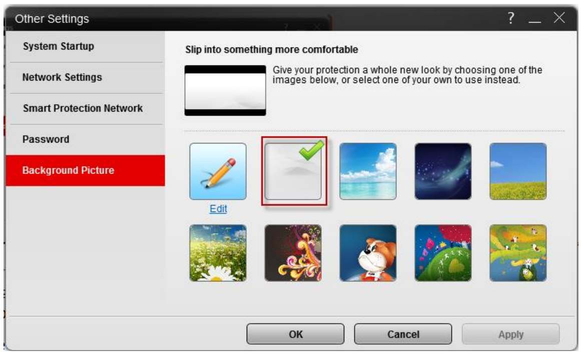
Safety Summary

Security Summary

0 threats stopped

Figure 82. 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**.

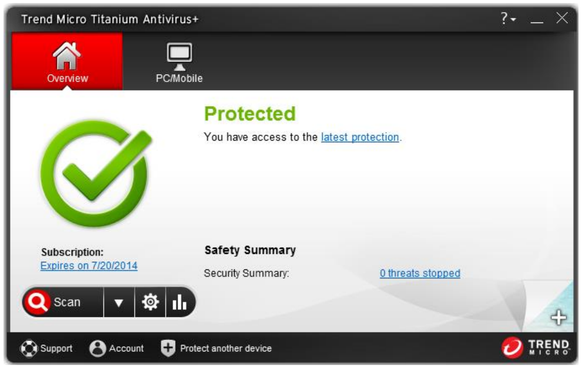


Slip into something more comfortable

Give your protection a whole new look by choosing one of the images below, or select one of your own to use instead.

Figure 83. Classic Titanium Background

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



Protected

You have access to the latest protection.

Subscription: Expires on 7/20/2014

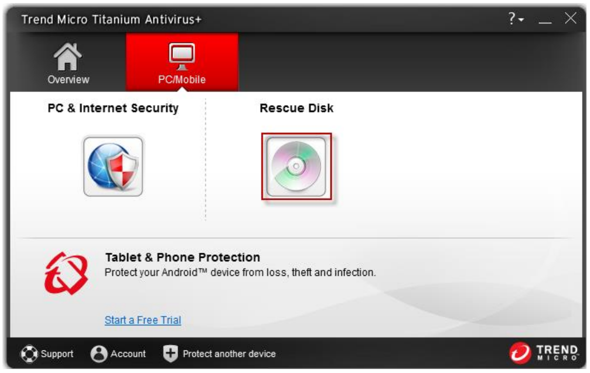
Safety Summary

Security Summary: 0 threats stopped

Figure 84. 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 **PC/Mobile** tab in the **Titanium Console.**



Trend Micro Titanium Antivirus+
Overview
PC/Mobile
PC & Internet Security
Rescue Disk
Tablet & Phone Protection
Protect your Android™ device from loss, theft and infection.
Start a Free Trial
Support
Account
Protect another device
TREND MICRO

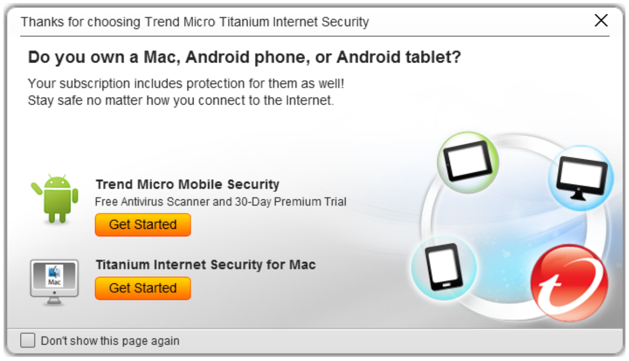
Figure 85. Computer > Rescue Disk

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

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.



Thanks for choosing Trend Micro Titanium Internet Security

Do you own a Mac, Android phone, or Android tablet?

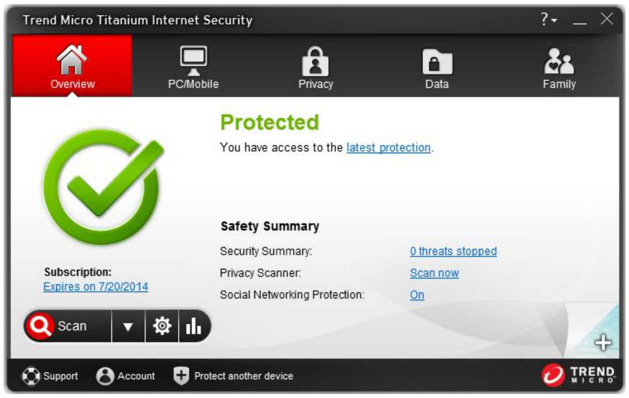
Your subscription includes protection for them as well!
Stay safe no matter how you connect to the Internet.

Trend Micro Mobile Security
Free Antivirus Scanner and 30-Day Premium Trial

Titanium Internet Security for Mac

□ Don't show this page again

Figure 86. Titanium Internet Security Welcome Screen



Trend Micro Titanium Internet Security

Protected

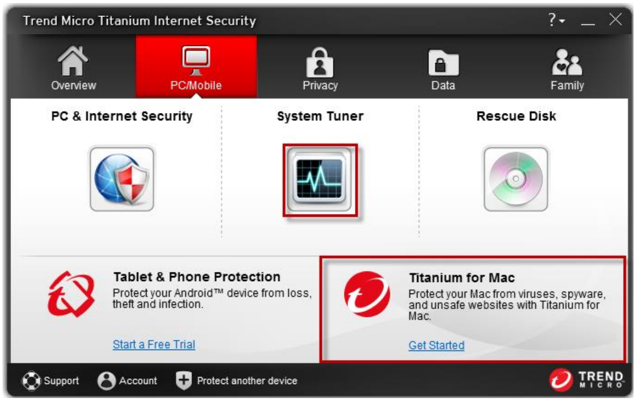
You have access to the latest protection.

Safety Summary

Security Summary: 0 threats stopped
Privacy Scanner: Scan now
Social Networking Protection: On

Subscription:
Expires on 7/20/2014

Figure 87. Trend Micro Titanium Internet Security Console



Protect your Android™ device from loss, theft and infection.

Protect your Mac from viruses, spyware, and unsafe websites with Titanium for Mac.

Figure 88. PC/Mobile > Tablet & Phone Protection

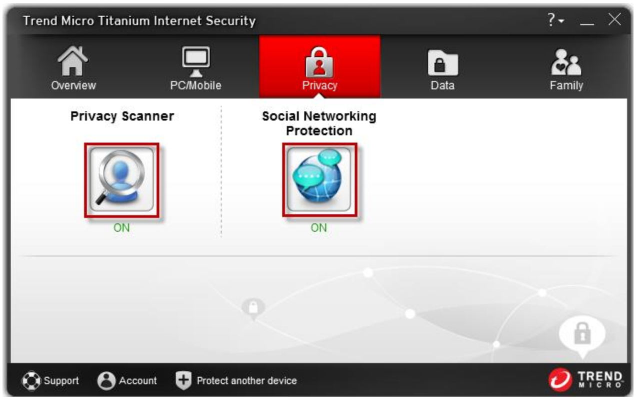
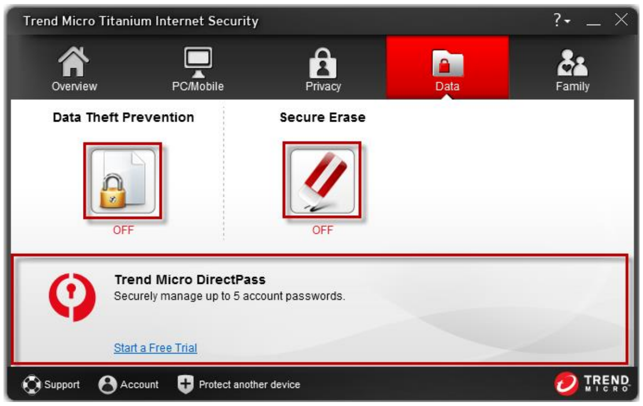
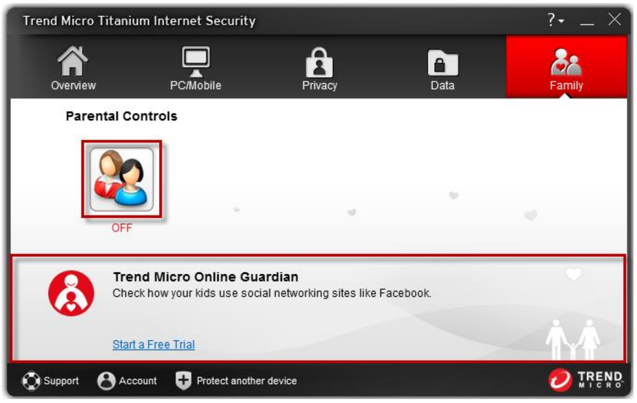


Figure 89. Privacy > Privacy Scanner | Social Networking Protection



Securely manage up to 5 account passwords.

Figure 90. Data > Trend Micro Vault | DirectPass | SafeSync



Parental Controls

OFF

Trend Micro Online Guardian

Check how your kids use social networking sites like Facebook.

Start a Free Trial

Figure 91. Family > Parental Controls | Online Guardian

Note: **Titanium Internet Security Additional Features beyond Titanium Antivirus +: Instant Messaging Protection, System Tuner, Privacy Scanner, Social Networking Protection, Data Theft Prevention, Secure Erase, Parental Controls. Additional Offerings: Free Trial of DirectPass and Online Guardian; 3-device Option - Titanium for Mac.**

ADDITIONAL TOOLS FOR TITANIUM INTERNET SECURITY PAID VERSION

Instant Messaging

Titanium Internet Security adds an additional layer of protection for instant messaging, checking for security risks in links to websites received via IM programs.

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.

Privacy Scanner

Titanium Internet Security adds the Privacy Scanner for Facebook, Twitter, and Google Plus, the latter two social networks new additions for 2014. The Privacy Scanner scans your privacy settings, alerts you to settings that expose you to potential identity theft, and lets you automatically change them.

Social Networking Protection

These protections in Titanium Internet Security extend web threat protection to social networking sites. See risk ratings for Facebook, Twitter, Google+, MySpace, LinkedIn, Pinterest, Mixi, and Sina Weibo. Mouse over URLs to get further details on the website. In Facebook, warn your friends of bad URLs on their pages, so they can delete them.

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.

Titanium for Mac

Titanium Internet Security's standard license allows you to protect up to three PCs. However, you may purchase a three-device option, which provides you with the ability to also protect a Macintosh

Internet & Email Controls: Instant Messaging

Titanium Internet Security 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.

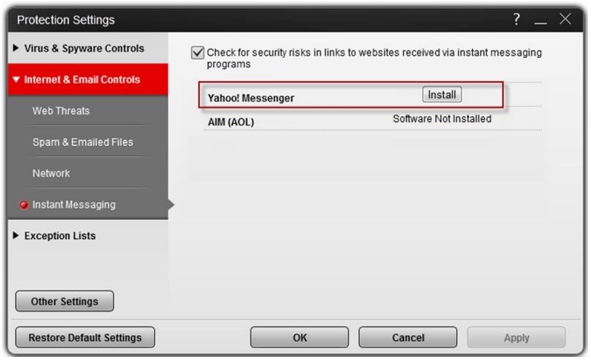
Titanium supports the following instant messaging programs/versions:

- Yahoo!® Messenger 8.0, 8.1, 9.0, 10.0, and 11.5
- AOL® Instant Messenger™ (AIM®) 6.8, and 6.9
- Facebook Chat
- Line

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.

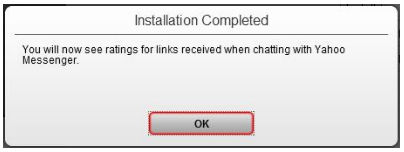


☑ Check for security risks in links to websites received via instant messaging programs

Yahoo! Messenger	Install
AIM (AOL)	Software Not Installed

Figure 92. Internet & Email Controls > Instant Messaging

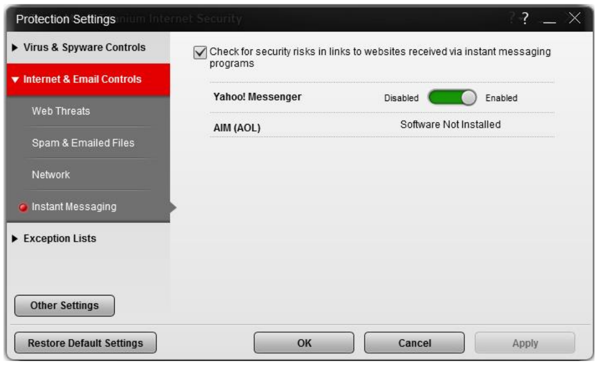
2. In the Yahoo! Messenger section, click **Install**. A pop-up appears, indicating that IM protection for the installation has completed.


Installation Completed

You will now see ratings for links received when chatting with Yahoo Messenger.

Figure 93. 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.



☑ Check for security risks in links to websites received via instant messaging programs

Yahoo! Messenger	Disabled Enabled
AIM (AOL)	Software Not Installed

Figure 94. Enable / Disable IM Protection

4. Click **OK** again to close the Titanium **Protection Settings** window.

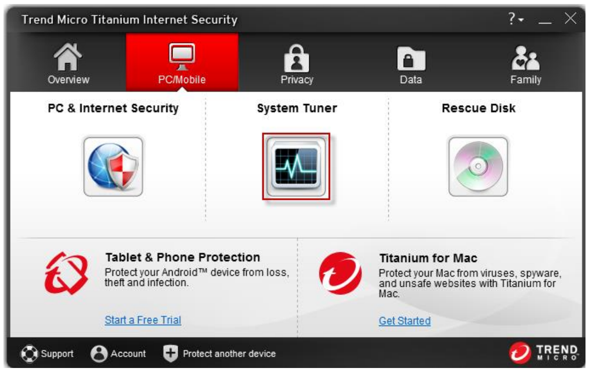
5. Return to this window to disable the protection at any time. Simply move the slider to **Disabled**, then click **OK** to save your changes.

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.

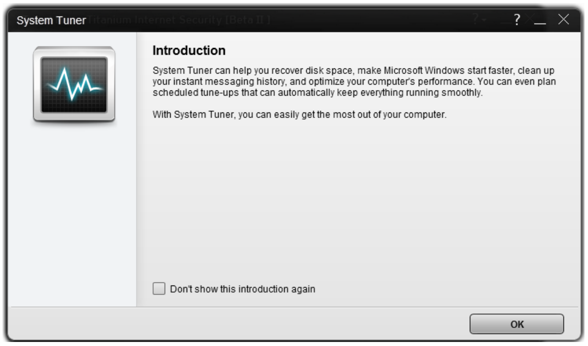


Tablet & Phone Protection
Protect your Android™ device from loss, theft and infection.
Start a Free Trial

Titanium for Mac
Protect your Mac from viruses, spyware, and unsafe websites with Titanium for Mac.
Get Started

Figure 95. PC/Mobile > System Tuner

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



Introduction

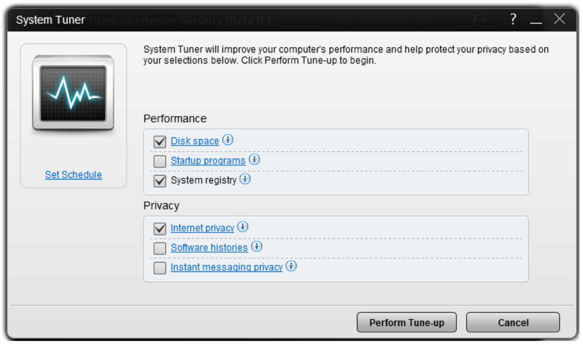
System Tuner can help you recover disk space, make Microsoft Windows start faster, clean up your instant messaging history, and optimize your computer's performance. You can even plan scheduled tune-ups that can automatically keep everything running smoothly.

With System Tuner, you can easily get the most out of your computer.

□ Don't show this introduction again

Figure 96. System Tuner Introduction

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



System Tuner will improve your computer's performance and help protect your privacy based on your selections below. Click Perform Tune-up to begin.

Performance

☑ Disk space

□ Startup programs

☑ System registry

Privacy

☑ Internet privacy

□ Software histories

□ Instant messaging privacy

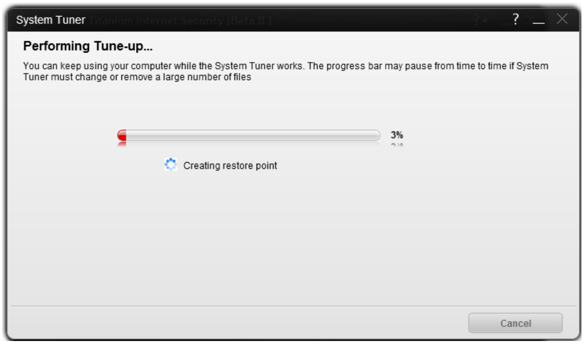
Figure 97. System Tuner Performance / Privacy Settings

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

Table 7. 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.

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



System Tuner

Performing Tune-up...

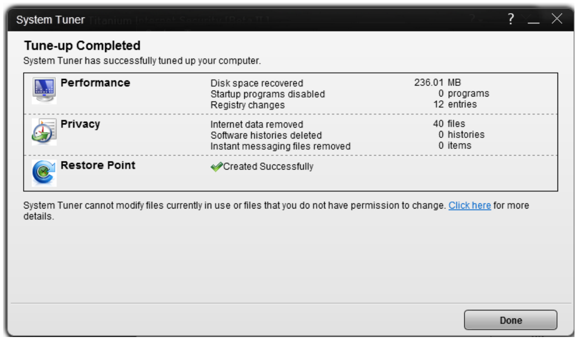
You can keep using your computer while the System Tuner works. The progress bar may pause from time to time if System Tuner must change or remove a large number of files

3%

Creating restore point

Figure 98. System Tuner Performing Tune-up / Creating Restore Point

6. 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).



System Tuner

Tune-up Completed

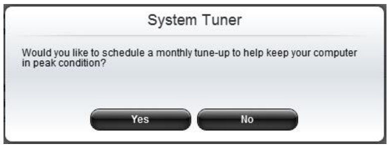
System Tuner has successfully tuned up your computer.

Performance	Disk space recovered Startup programs disabled Registry changes	236.01 MB 0 programs 12 entries
Privacy	Internet data removed Software histories deleted Instant messaging files removed	40 files 0 histories 0 items
Restore Point	✓Created Successfully	

System Tuner cannot modify files currently in use or files that you do not have permission to change. Click here for more details.

Figure 99. Tune-up Completed

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

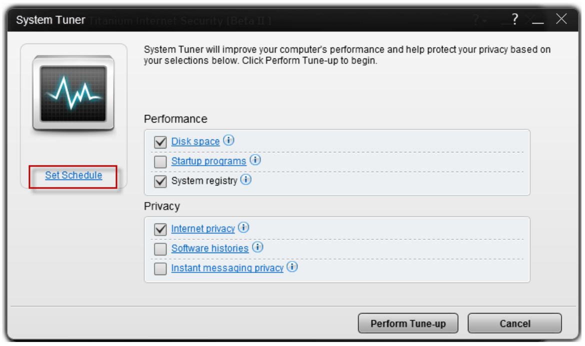


System Tuner

Would you like to schedule a monthly tune-up to help keep your computer in peak condition?

Figure 100. 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.



System Tuner

System Tuner will improve your computer's performance and help protect your privacy based on your selections below. Click Perform Tune-up to begin.

Performance

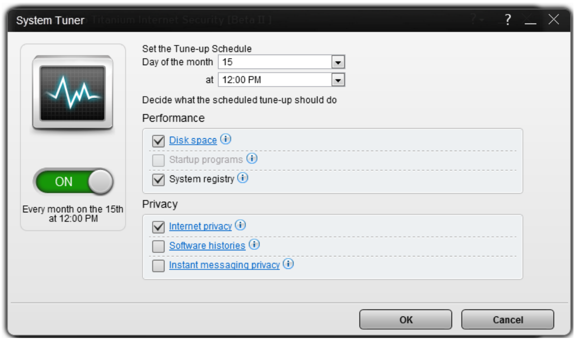
☑ Disk space
☐ Startup programs
☑ System registry

Privacy

☑ Internet privacy
☐ Software histories
☐ Instant messaging privacy

Figure 101. System Tuner > Set Schedule

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



System Tuner

Set the Tune-up Schedule
Day of the month 15
at 12:00 PM

Decide what the scheduled tune-up should do

Performance

☑ Disk space
☐ Startup programs
☑ System registry

Privacy

☑ Internet privacy
☐ Software histories
☐ Instant messaging privacy

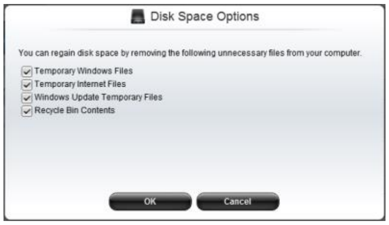
ON

Every month on the 15th at 12:00 PM

Figure 102. 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.



Disk Space Options

You can regain disk space by removing the following unnecessary files from your computer.

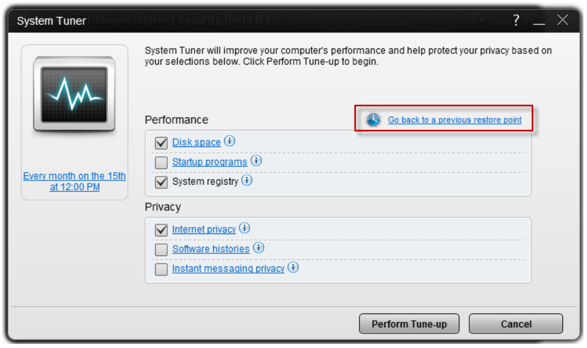
☑ Temporary Windows Files
☑ Temporary Internet Files
☑ Windows Update Temporary Files
☑ Recycle Bin Contents

Figure 103. 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.


System Tuner
?
Every month on the 15th at 12:00 PM
Go back to a previous restore point
Perform Tune-up
Cancel

System Tuner will improve your computer's performance and help protect your privacy based on your selections below. Click Perform Tune-up to begin.

Performance

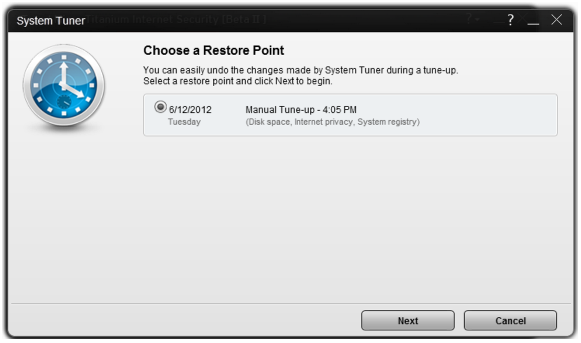
- ☑ Disk space
- □ Startup programs
- ☑ System registry

Privacy

- ☑ Internet privacy
- □ Software histories
- □ Instant messaging privacy

Figure 104. 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.



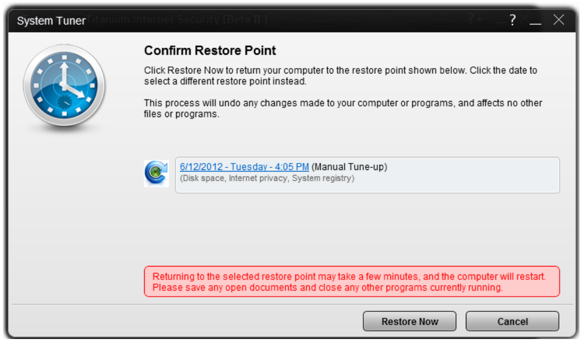
Choose a Restore Point

You can easily undo the changes made by System Tuner during a tune-up.
Select a restore point and click Next to begin.

● 6/12/2012 Tuesday — Manual Tune-up - 4:05 PM (Disk space, Internet privacy, System registry)

Figure 105. Choose a Restore Point

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



Confirm Restore Point

Click Restore Now to return your computer to the restore point shown below. Click the date to select a different restore point instead.

This process will undo any changes made to your computer or programs, and affects no other files or programs.

6/12/2012 - Tuesday - 4:05 PM (Manual Tune-up)
(Disk space, Internet privacy, System registry)

Returning to the selected restore point may take a few minutes, and the computer will restart. Please save any open documents and close any other programs currently running.

Figure 106. Confirm Restore Point

16. Click **Restore Now** to restore to the chosen Restore Point.

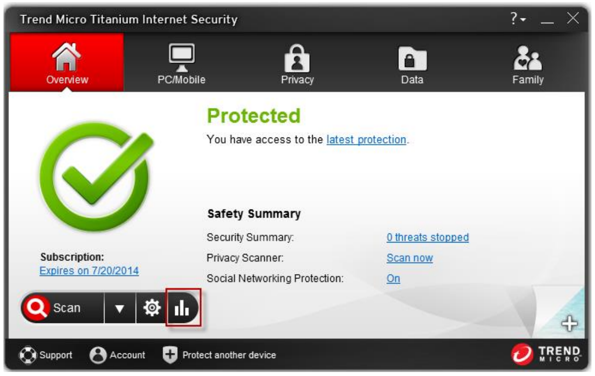
17. Restoring to the selected restore point may take a few minutes and the computer will restart. Save any open documents and close any programs before restoring to the Restore Point.

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.**



Protected

You have access to the latest protection.

Safety Summary

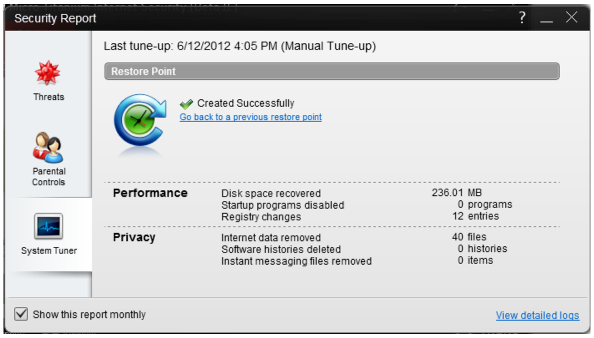
Security Summary: 0 threats stopped
Privacy Scanner: Scan now
Social Networking Protection: On

Subscription:
Expires on 7/20/2014

Figure 107. 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.



Last tune-up: 6/12/2012 4:05 PM (Manual Tune-up)

Created Successfully
Go back to a previous restore point

Performance	Disk space recovered	236.01 MB
	Startup programs disabled	0 programs
	Registry changes	12 entries
Privacy	Internet data removed	40 files
	Software histories deleted	0 histories
	Instant messaging files removed	0 items

☑ Show this report monthly

View detailed logs

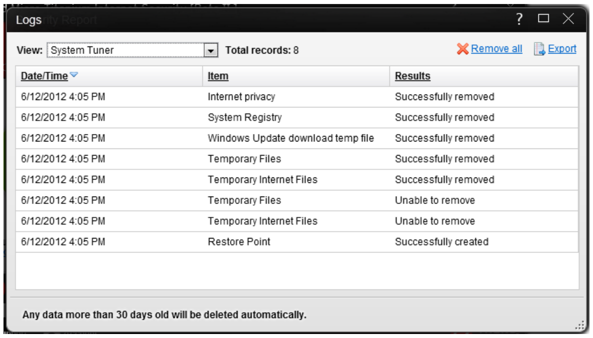
Figure 108. System Tuner Security Report

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**.



View: System Tuner Total records: 8

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 109. System Tuner Logs

8. Click **Remove all** to remove the logs.

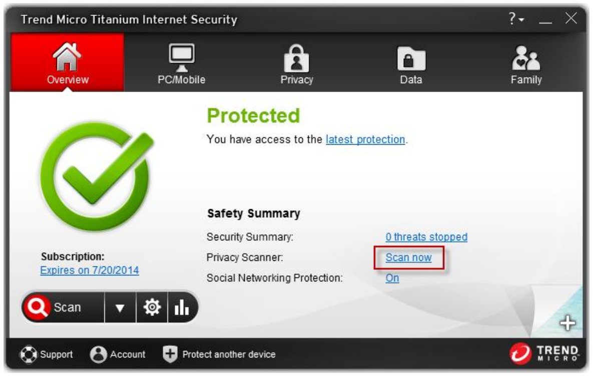
9. Click **Export** to export the log in .CSV or .TXT format.

Privacy: Privacy Scanner

The **Privacy Scanner** for Facebook, Twitter, and Google+ is turned on by default in Titanium Internet Security and Maximum Security; the default setting also turns on the Trend Micro Toolbar, which can be used to launch the Privacy Scanner.

To use the Privacy Scanner:

1. Double-click the Titanium shortcut on the desktop to open the **Titanium Console**. The **Titanium Console** appears.



Protected

You have access to the latest protection.

Safety Summary

Security Summary: 0 threats stopped

Privacy Scanner: Scan now

Social Networking Protection: On

Subscription:
Expires on 7/20/2014

Figure 110. Privacy Scanner > Scan Now

2. Do one of three things:

> In the main Console window, click the **Privacy Scanner Scan Now** link.

OR

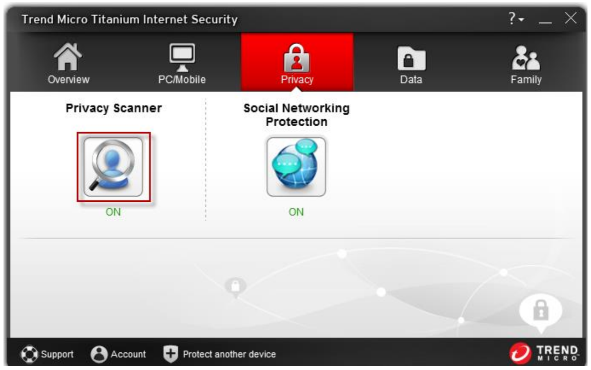
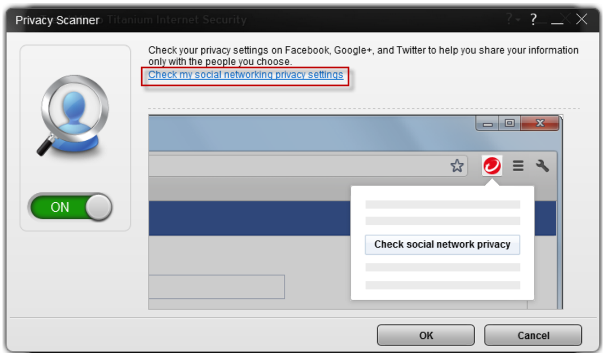


Figure 111. Privacy > Facebook Privacy Scanner

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

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



Check your privacy settings on Facebook, Google+, and Twitter to help you share your information only with the people you choose.

Check my social networking privacy settings

Figure 112. Privacy Scanner window

4. Click **Check my social networking privacy settings.**

OR

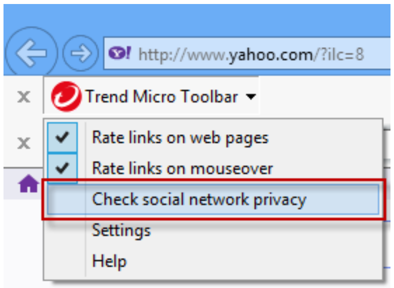
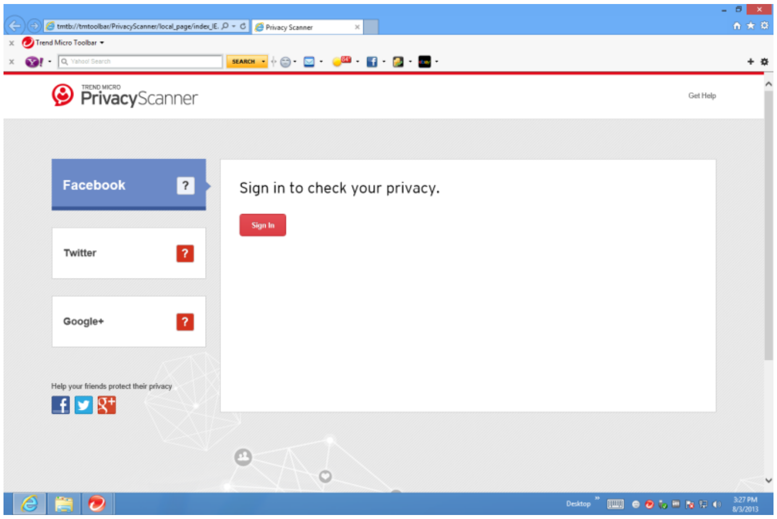


Figure 113. Check social network privacy

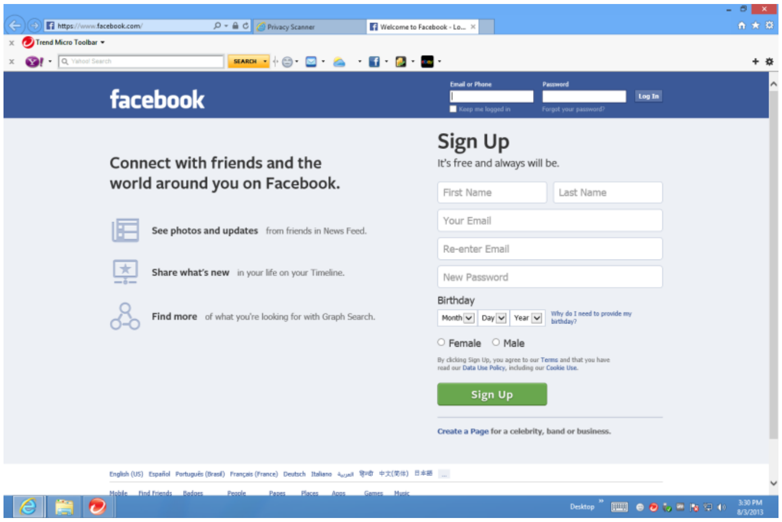
5. Select **Check social network privacy** in the Trend Micro Toolbar. Your browser launches and takes you to the **Trend Micro Privacy Scanner** page, with the **Facebook** sign in panel shown by default.


TREND MICRO PrivacyScanner
Get Help
Facebook
Twitter
Google+
Sign In
Help your friends protect their privacy

Sign in to check your privacy.

Figure 114. Trend Micro Privacy Scanner | Facebook

1. In the **Privacy Scanner** page, click **Sign In**. Titanium automatically takes you to the Facebook login website.



It's free and always will be.

Connect with friends and the world around you on Facebook.

See photos and updates from friends in News Feed.

Share what's new in your life on your Timeline.

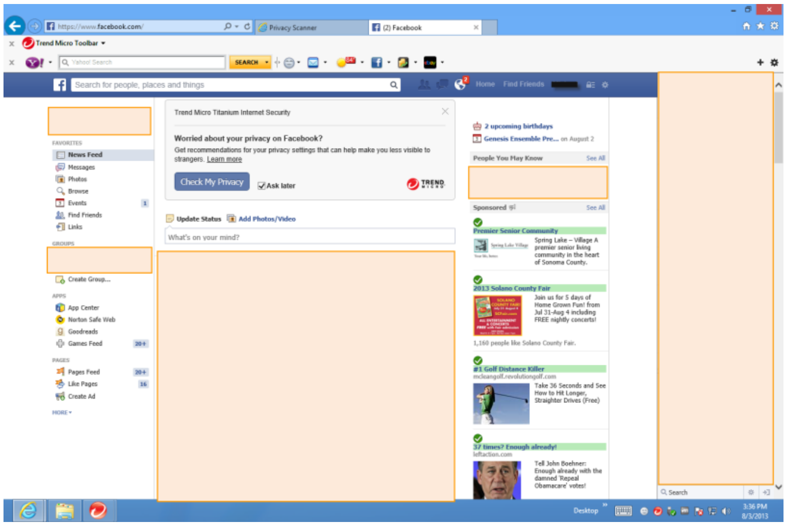
Find more of what you're looking for with Graph Search.

By clicking Sign Up, you agree to our Terms and that you have read our Data Use Policy, including our Cookie Use.

Create a Page for a celebrity, band or business.

Figure 115. Facebook Login Webpage

2. Sign in to your Facebook account. The **Facebook News Feed** page displays, showing Titanium's **Privacy Scanner for Facebook**.



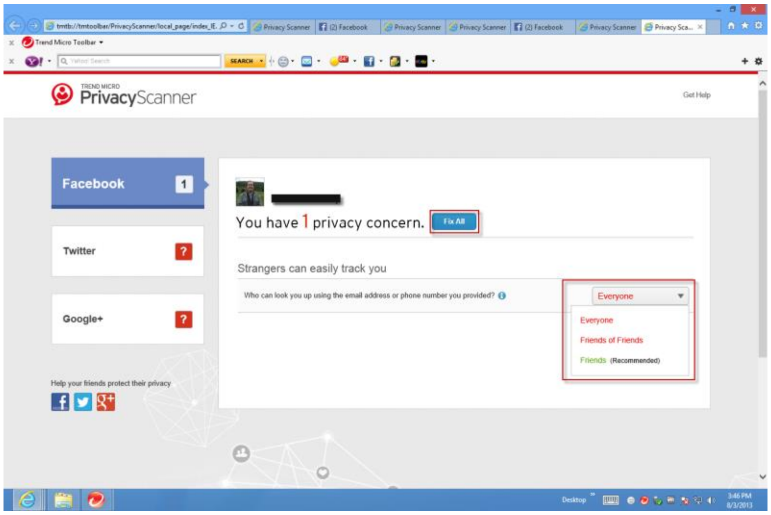
Trend Micro Titanium Internet Security

Worried about your privacy on Facebook?

Get recommendations for your privacy settings that can help make you less visible to strangers. Learn more

Figure 116. Facebook > Check My Privacy

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



[redacted]

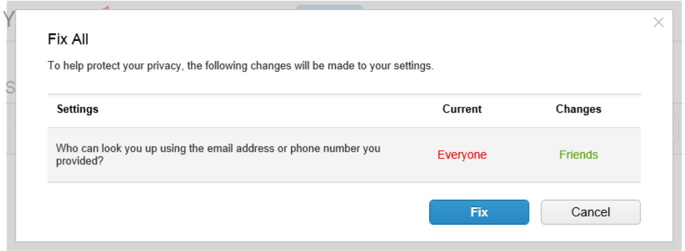
You have 1 privacy concern. Fix All

Strangers can easily track you

Who can look you up using the email address or phone number you provided? Everyone

Figure 117. Facebook Privacy Concerns

4. If you have concerns, click **Fix All** to fix all the concerns at once using the Titanium recommended privacy settings, or select the drop-down settings menu to fix them manually. In this example, we'll choose **Fix All**. The **Fix** popup appears.



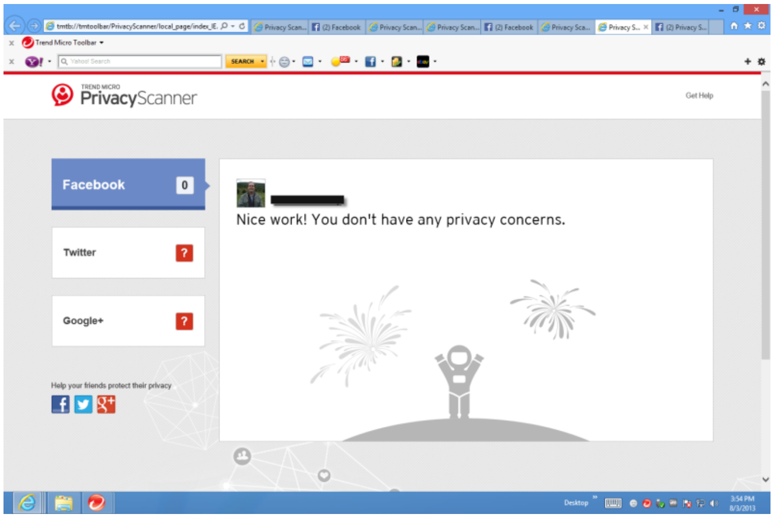
Fix All

To help protect your privacy, the following changes will be made to your settings.

Settings	Current	Changes
Who can look you up using the email address or phone number you provided?	Everyone	Friends

Figure 118. Fix All | Editor

5. Click **Fix** for the settings with Privacy Concerns. Titanium changes your settings and returns the result. In this case, since you accepted the default recommendations, it returned **Nice work! You don't have any privacy concerns.**



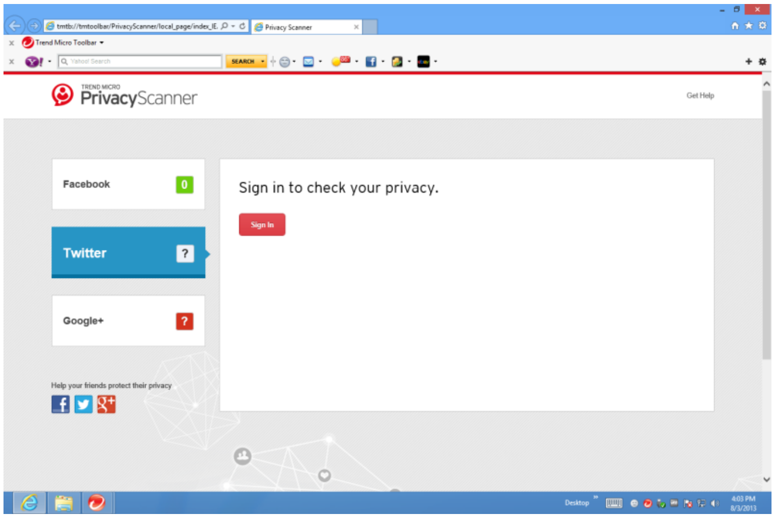
Trend Micro Toolbar
TREND MICRO PrivacyScanner
Get Help
Facebook 0
Twitter ?
Google+ ?
Help your friends protect their privacy
Desktop

[redacted]

Nice work! You don't have any privacy concerns.

Figure 119. Nice work!

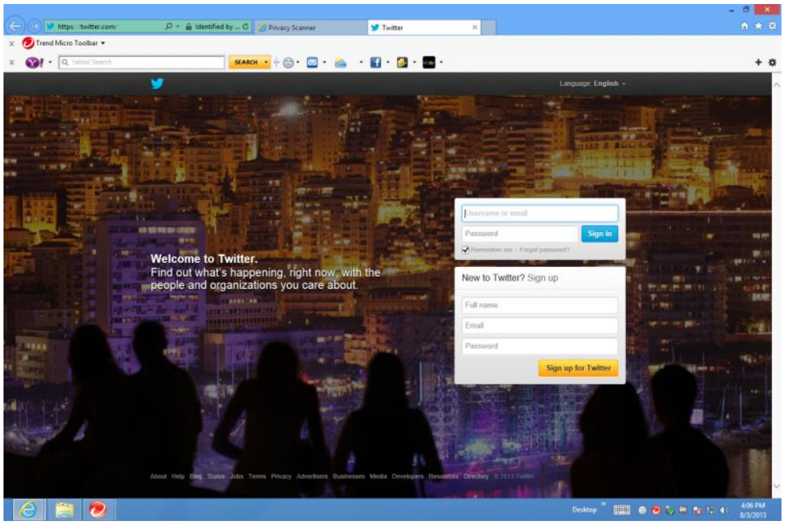
6. If you want to check your privacy settings in Twitter, click the **Twitter** tab. The **Twitter** sign in panel appears.


TREND MICRO PrivacyScanner
Get Help
Facebook 0
Twitter ?
Google+ ?
Sign In
Help your friends protect their privacy

Sign in to check your privacy.

Figure 120. Privacy Scanner | Twitter

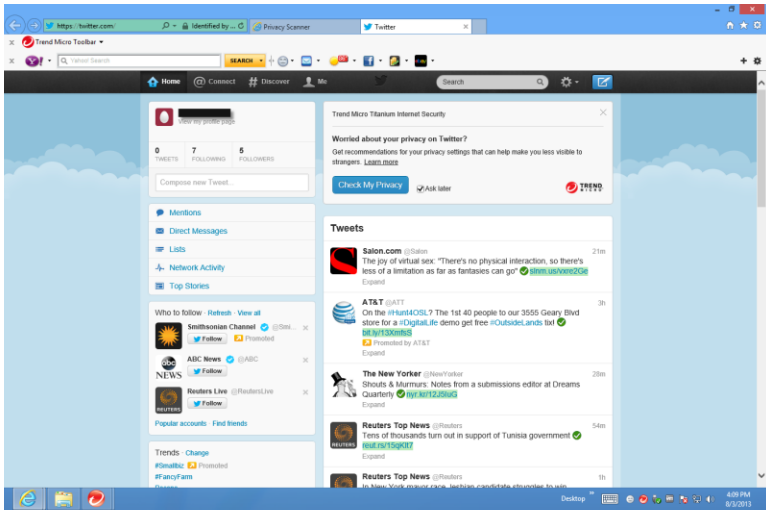
7. Click **Sign In.** The Twitter Welcome page appears.


Language: English
Username or email
Password
Sign in
Remember me · Forgot password?
New to Twitter? Sign up
Full name
Email
Password
Sign up for Twitter
About Help Blog Status Jobs Terms Privacy Advertisers Businesses Media Developers Resources Directory © 2013 Twitter

Welcome to Twitter.
Find out what's happening, right now, with the people and organizations you care about.

Figure 121. Welcome to Twitter

8. Sign in to your Twitter account. Your Twitter page appears.



[redacted]

Trend Micro Titanium Internet Security

Worried about your privacy on Twitter?

Get recommendations for your privacy settings that can help make you less visible to strangers. Learn more

☐ Check My Privacy ☑ Ask later

Tweets

Salon.com @Salon 21m
The joy of virtual sex: "There's no physical interaction, so there's less of a limitation as far as fantasies can go" slnm.us/vxre2Ge

AT&T @ATT 3h
On the #Hunt4OSL? The 1st 40 people to our 3555 Geary Blvd store for a #DigitalLife demo get free #OutsideLands tix! bit.ly/13XmfsS
Promoted by AT&T

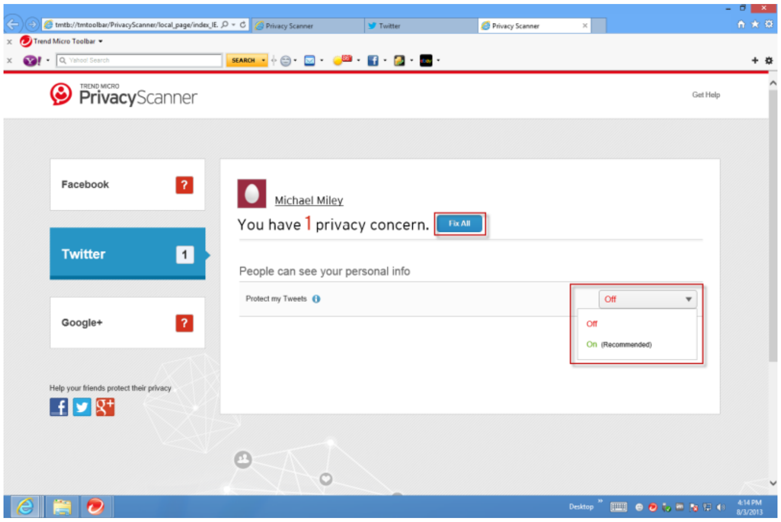
The New Yorker @NewYorker 28m
Shouts & Murmurs: Notes from a submissions editor at Dreams Quarterly nyr.kr/12J5luG

Reuters Top News @Reuters 54m
Tens of thousands turn out in support of Tunisia government reut.rs/15qKlt7

Reuters Top News @Reuters 1h
In New York mayor race, lesbian candidate struggles to win

Figure 122. Twitter > Check My Privacy

9. Click **Check My Privacy.** The Trend Micro Privacy Scanner returns the result.



TREND MICRO PrivacyScanner
Get Help
Facebook ?
Twitter 1
Google+ ?
Help your friends protect their privacy

Michael Miley

You have 1 privacy concern. Fix All

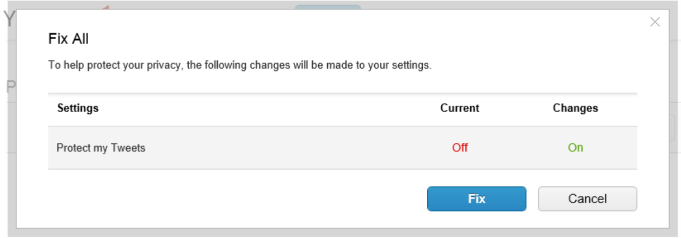
People can see your personal info

Protect my Tweets: Off

Off
On (Recommended)

Figure 123. Twitter Privacy Concern

10. As you did for Facebook, click **Fix All** or use the editor to edit specific settings. The editor appears.



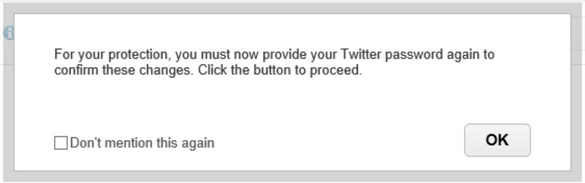
Fix All

To help protect your privacy, the following changes will be made to your settings.

Settings	Current	Changes
Protect my Tweets	Off	On

Figure 124. Fix All | Settings

11. Click **Fix** to fix your settings. Twitter requires that you enter your password to make changes to your account.

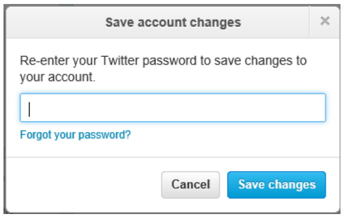


For your protection, you must now provide your Twitter password again to confirm these changes. Click the button to proceed.

□ Don't mention this again

Figure 125. Twitter Password Request

12. Click **OK** to proceed. The **Save account changes** dialog appears.

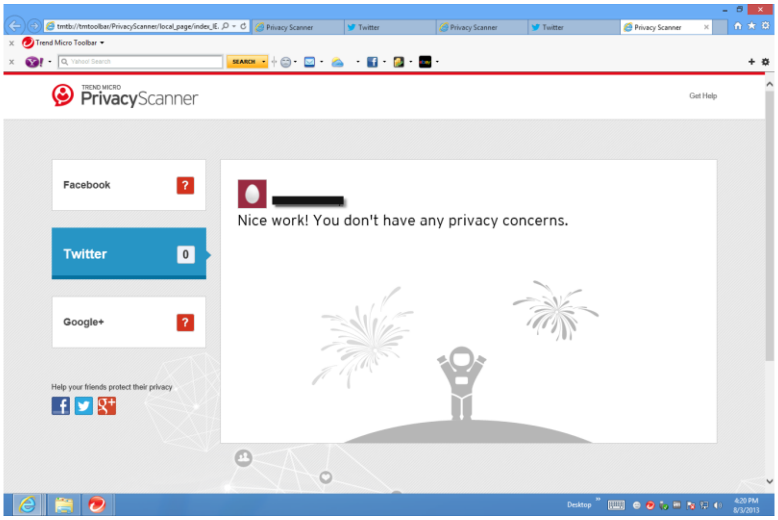


Save account changes

Re-enter your Twitter password to save changes to your account.

13. Re-enter your Twitter password and click **Save Changes.** Twitter saves the changes.

14. Return to your Twitter Home page and click **Check My Privacy** again to ensure you have no remaining privacy concerns. The **Privacy Scanner** returns the result.



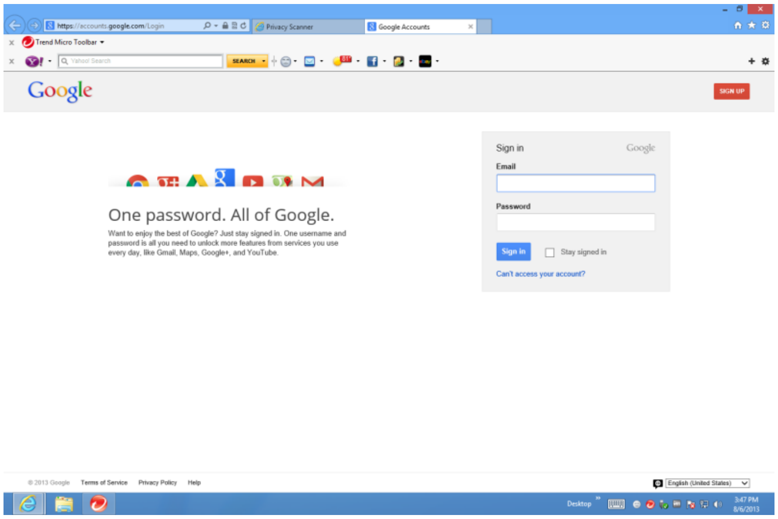
TREND MICRO PrivacyScanner
Get Help
Facebook ?
Twitter 0
Google+ ?
Help your friends protect their privacy

[redacted]

Nice work! You don't have any privacy concerns.

Figure 126. Privacy Scanner: No Privacy Concerns

15. Select the **Google+** tab if you have a **Google+** account. The Google+ sign in panel appears.



One password. All of Google.

Want to enjoy the best of Google? Just stay signed in. One username and password is all you need to unlock more features from services you use every day, like Gmail, Maps, Google+, and YouTube.

Sign in

Email

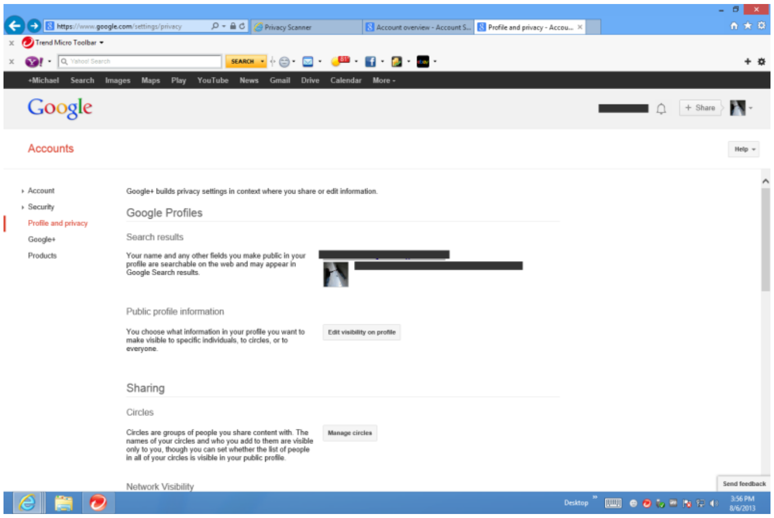
Password

Sign in □ Stay signed in

Can't access your account?

Figure 127. Google+ SIgn In

16. Sign in to your Google account. Titanium scans your privacy settings and automatically opens your privacy page for you to edit your settings if needed.



[redacted]

Google+ builds privacy settings in context where you share or edit information.

Google Profiles

Search results

Your name and any other fields you make public in your profile are searchable on the web and may appear in Google Search results.

[redacted]

Public profile information

You choose what information in your profile you want to make visible to specific individuals, to circles, or to everyone.

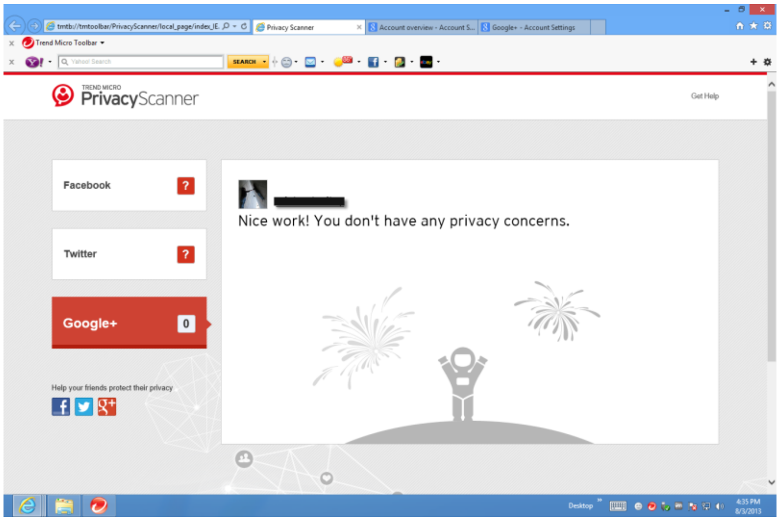
Sharing

Circles

Circles are groups of people you share content with. The names of your circles and who you add to them are visible only to you, though you can set whether the list of people in all of your circles is visible in your public profile.

Network Visibility

Figure 128. Google+ Privacy Settings


tmtb://tmtoolbar/PrivacyScanner/local_page/index_IE.
Privacy Scanner
Account overview - Account S...
Google+ - Account Settings
Trend Micro Toolbar
SEARCH
TREND MICRO
PrivacyScanner
Get Help
Facebook
?
Twitter
?
Google+
0
Help your friends protect their privacy
Desktop

[redacted]

Nice work! You don't have any privacy concerns.

Figure 129. Google+: No Privacy Concerns

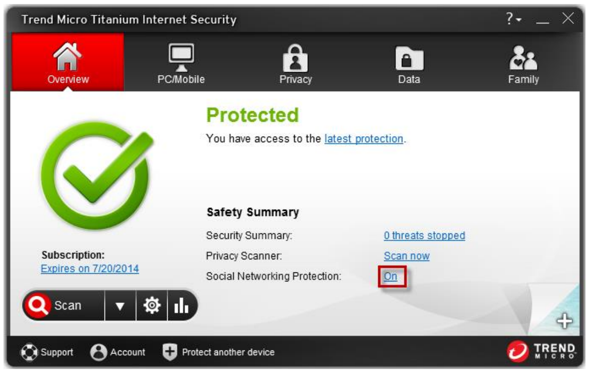
17. Titanium provides ongoing protection for Facebook, Twitter, and Google+. At any time, particularly when the social networking site changes any privacy policies, you can run another **Privacy Scan** on your social networking pages to check your privacy settings.

Privacy: Social Networking Protection

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

To use Social Networking Protection:

1. Double-click the Titanium shortcut on the desktop. The **Titanium Console** appears, with Social Networking Protection turned on.



Protected

You have access to the latest protection.

Safety Summary

Security Summary: 0 threats stopped

Privacy Scanner: Scan now

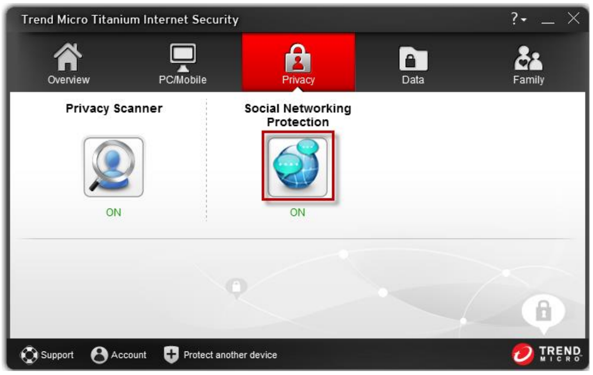
Social Networking Protection: On

Subscription: Expires on 7/20/2014

Figure 130. Social Networking Protection

2. To view the Social Networking toggle page, do one of two things:

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



Privacy Scanner: ON

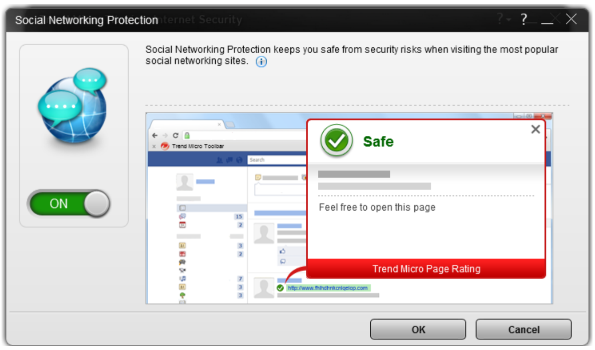
Social Networking Protection: ON

Figure 131. Privacy > Social Networking Protection

OR

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

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

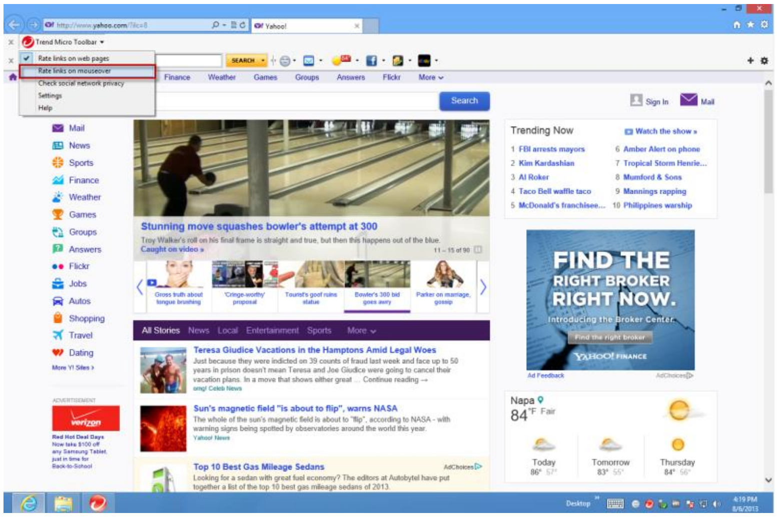


Social Networking Protection keeps you safe from security risks when visiting the most popular social networking sites.

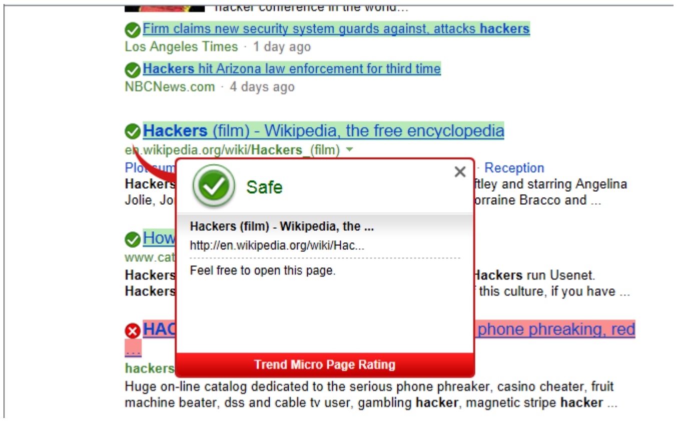
Figure 132. Social Networking Protection > On

4. If you wish, click the slider from **On** to **Off** to disable the function. Trend Micro does not recommend that you turn off the setting.

5. Open your browser, select the Trend Micro Toolbar, and note that **Rate links on web pages** is selected by default.



6. Select **Rate links on mouseover** to enable the feature. Now, when you mouse-over a link, Titanium will scan it in real-time and provide you with a rating and details about it.



hacker conference in the world...

✓ Firm claims new security system guards against, attacks hackers
Los Angeles Times · 1 day ago

✓ Hackers hit Arizona law enforcement for third time
NBCNews.com · 4 days ago

✓ Hackers (film) - Wikipedia, the free encyclopedia
en.wikipedia.org/wiki/Hackers_(film)

Safe

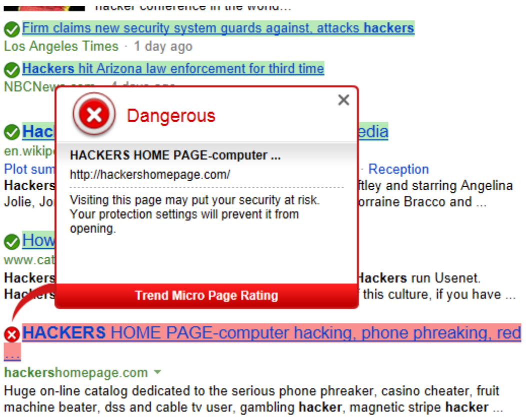
Hackers (film) - Wikipedia, the ...
http://en.wikipedia.org/wiki/Hac...

Feel free to open this page.

Trend Micro Page Rating

hackers
Huge on-line catalog dedicated to the serious phone phreaker, casino cheater, fruit machine beater, dss and cable tv user, gambling hacker, magnetic stripe hacker ...

Figure 133. Safe Trend Micro Page Rating



hacker conference in the world...

✓ Firm claims new security system guards against, attacks hackers
Los Angeles Times · 1 day ago

✓ Hackers hit Arizona law enforcement for third time

Dangerous

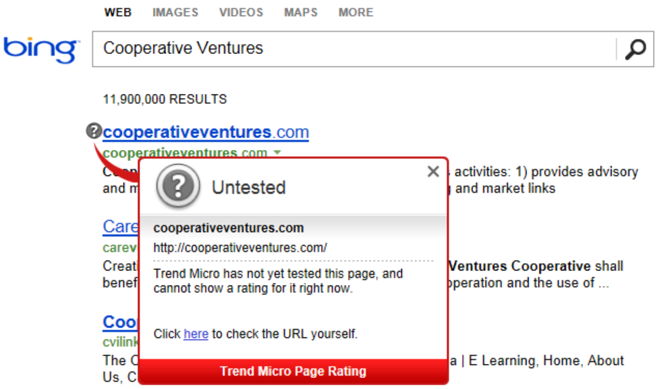
HACKERS HOME PAGE-computer ...
http://hackershomepage.com/

Visiting this page may put your security at risk. Your protection settings will prevent it from opening.

Trend Micro Page Rating

✗ HACKERS HOME PAGE-computer hacking, phone phreaking, red ...
hackershomepage.com
Huge on-line catalog dedicated to the serious phone phreaker, casino cheater, fruit machine beater, dss and cable tv user, gambling hacker, magnetic stripe hacker ...

Figure 134. Dangerous Trend Micro Page Rating



Cooperative Ventures

11,900,000 RESULTS

cooperativeventures.com
cooperativeventures.com

Untested

cooperativeventures.com
http://cooperativeventures.com/

Trend Micro has not yet tested this page, and cannot show a rating for it right now.

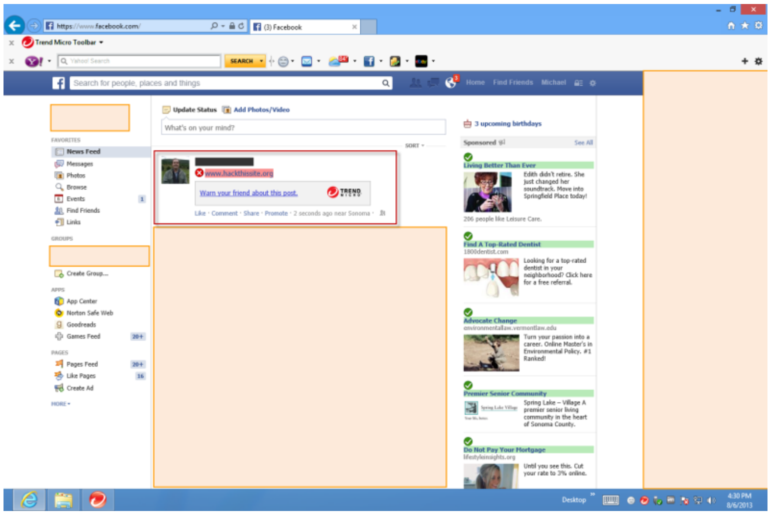
Click here to check the URL yourself.

Trend Micro Page Rating

Figure 135. Untested Trend Micro Page Rating

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

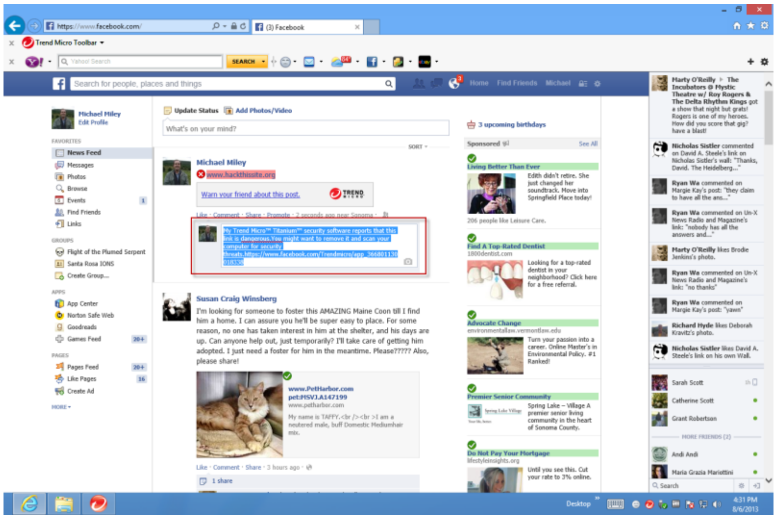
8. The same link ratings and mouse-over functions are available from within Titanium's supported social networking sites. Note too, that when a URL posted on Facebook is rated as dangerous by Titanium, you can warn your friend about it.



[redacted]
www.hackthissite.org
Warn your friend about this post.

Figure 136. Dangerous URL on Facebook Detected by Titanium

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

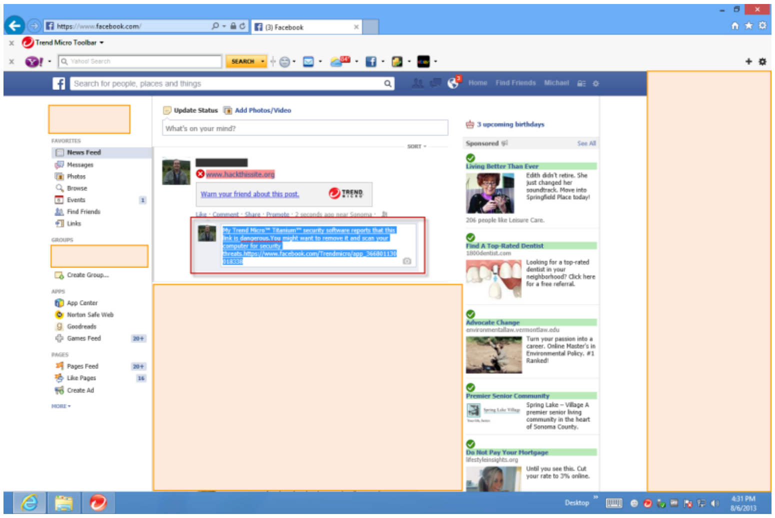


Michael Miley
www.hackthissite.org
Warn your friend about this post.

My Trend Micro™ Titanium™ security software reports that this link is dangerous.You might want to remove it and scan your computer for security threats.https://www.facebook.com/Trendmicro/app_366801130018338

Figure 137. Warn a Friend About the Dangerous URL

10. 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.



Update Status
Add Photos/Video
What's on your mind?
SORT
Warn your friend about this post.
Like · Comment · Share · Promote · 2 seconds ago near Sonoma

[redacted]

www.hackthissite.org

My Trend Micro™ Titanium™ security software reports that this link is dangerous.You might want to remove it and scan your computer for security threats.https://www.facebook.com/Trendmicro/app_366801130018338

Figure 138. Dangerous URL Warning Posted on Facebook

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 **Data** screen appears, showing the tools available.

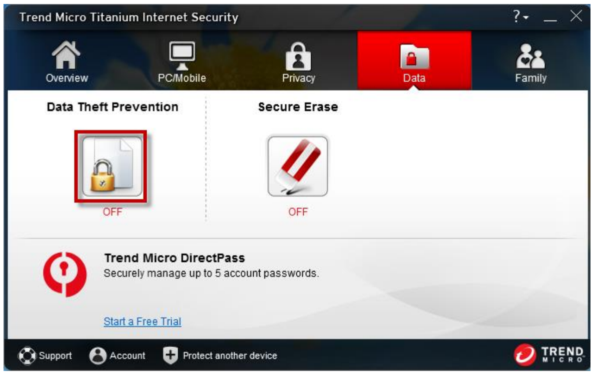
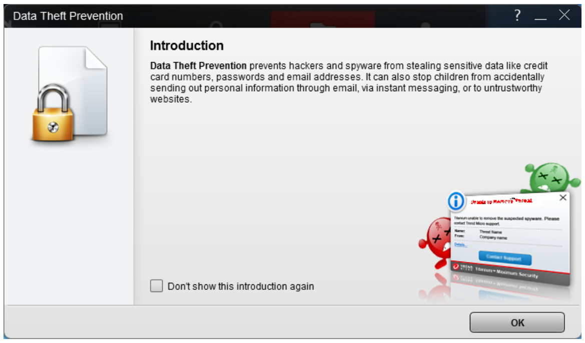


Figure 139. Data Theft Prevention

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.

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



Data Theft Prevention

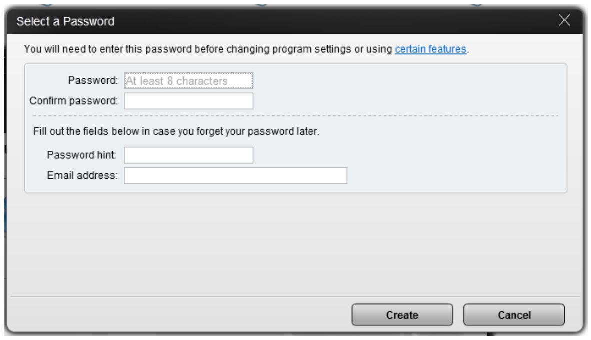
Introduction

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.

□ Don't show this introduction again

Figure 140. Data Theft Prevention Introduction

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



Select a Password

You will need to enter this password before changing program settings or using certain features.

Password: At least 8 characters

Confirm password:

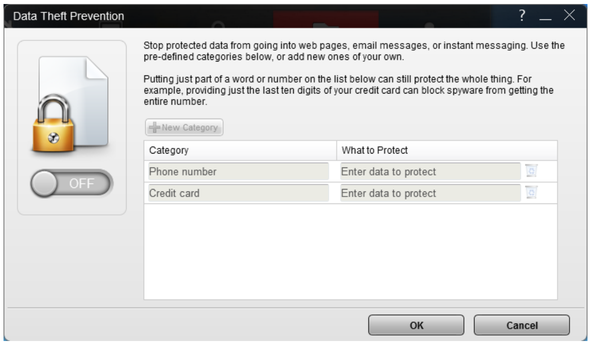
Fill out the fields below in case you forget your password later.

Password hint:

Email address:

Figure 141. Select a Password

4. 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.



Stop protected data from going into web pages, email messages, or instant messaging. Use the pre-defined categories below, or add new ones of your own.

Putting just part of a word or number on the list below can still protect the whole thing. For example, providing just the last ten digits of your credit card can block spyware from getting the entire number.

Category	What to Protect
Phone number	Enter data to protect
Credit card	Enter data to protect

Figure 142. Data Theft Prevention

5. Click the slider to **On** to enable **Data Theft Protection.**
6. Titanium Internet Security provides you with some suggested categories such as **Phone number** and **Credit card.** You can edit any existing 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 phone number field you might type 899-999-9899.
8. After you save it, Titanium hides it from view by using asterisks. Simply click in the field to make it visible.
9. Click **+New Category** to add a new category.
10. Click the trashcan in the right-hand column of **What to Protect** to delete any category.
11. Click **Ok** to save your changes.

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.

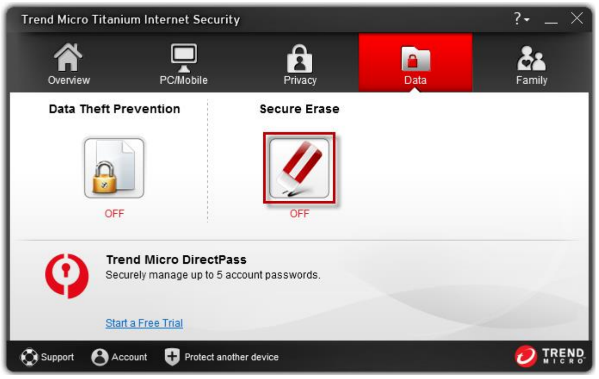
Data: Secure Erase

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:

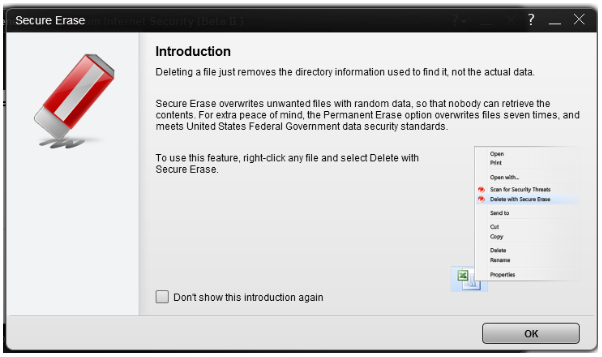
1. Click **Data > Secure Erase.**



Securely manage up to 5 account passwords.

Figure 143. Privacy > Secure Erase

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



Introduction

Deleting a file just removes the directory information used to find it, not the actual data.

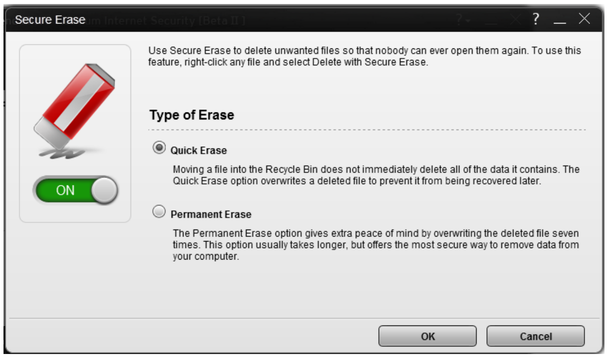
Secure Erase overwrites unwanted files with random data, so that nobody can retrieve the contents. For extra peace of mind, the Permanent Erase option overwrites files seven times, and meets United States Federal Government data security standards.

To use this feature, right-click any file and select Delete with Secure Erase.

□ Don't show this introduction again

Figure 144. Secure Erase Introduction

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



Secure Erase

Use Secure Erase to delete unwanted files so that nobody can ever open them again. To use this feature, right-click any file and select Delete with Secure Erase.

Type of Erase

● Quick Erase

Moving a file into the Recycle Bin does not immediately delete all of the data it contains. The Quick Erase option overwrites a deleted file to prevent it from being recovered later.

○ Permanent Erase

The Permanent Erase option gives extra peace of mind by overwriting the deleted file seven times. This option usually takes longer, but offers the most secure way to remove data from your computer.

Figure 145. 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.

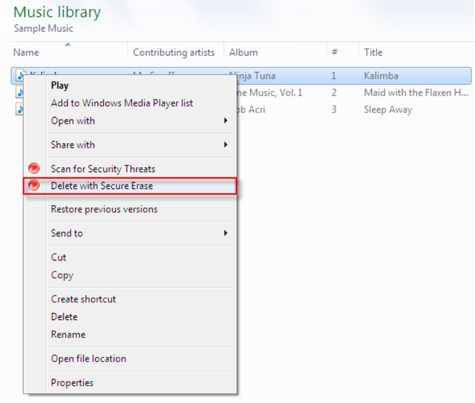


Figure 146. Right-click File for Secure Erase

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

Family: Parental Controls

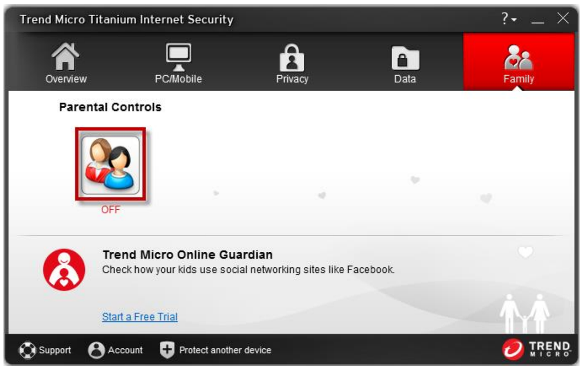
The **Parental Controls** tool in Titanium Internet Security (and Maximum Security) lets you protect your children from inappropriate websites, limit their time on the internet, and see detailed reports about what they do online.

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.

Note: The instructions below are tailored to Windows 8 users. The process for creating a new user account in Windows Vista or 7 is very similar, but not identical. Windows 8 flips you to the Modern UI – PC Settings when you create a new user.

To enable Parental Controls:

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

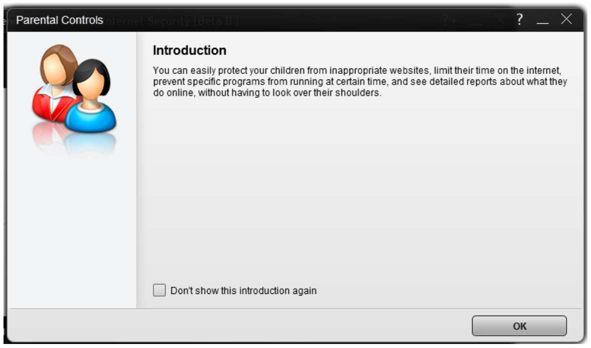


Check how your kids use social networking sites like Facebook.

Figure 147. Family > Parental Controls

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

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

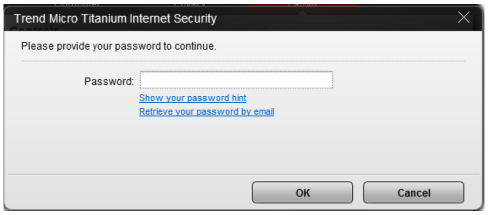


You can easily protect your children from inappropriate websites, limit their time on the internet, prevent specific programs from running at certain time, and see detailed reports about what they do online, without having to look over their shoulders.

□ Don't show this introduction again

Figure 148. Parental Controls Introduction

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



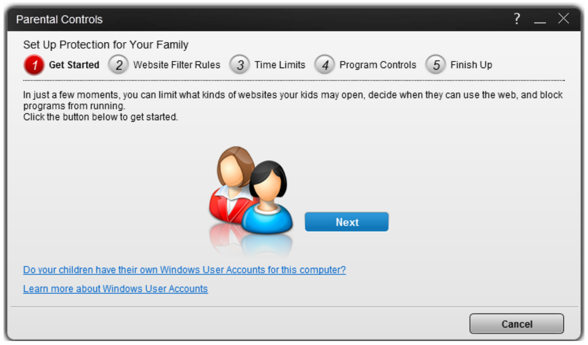
Trend Micro Titanium Internet Security

Please provide your password to continue.

Password:

Figure 149. Enter Password

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



Parental Controls

Set Up Protection for Your Family

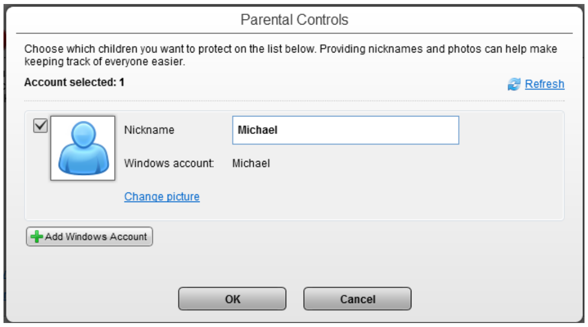
1 Get Started
2 Website Filter Rules
3 Time Limits
4 Program Controls
5 Finish Up

In just a few moments, you can limit what kinds of websites your kids may open, decide when they can use the web, and block programs from running.
Click the button below to get started.

Next
Do your children have their own Windows User Accounts for this computer?
Learn more about Windows User Accounts
Cancel

Figure 150. 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.



Parental Controls

Choose which children you want to protect on the list below. Providing nicknames and photos can help make keeping track of everyone easier.

Account selected: 1

☑ Nickname: Michael

Windows account: Michael

Figure 151. Parental Controls

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

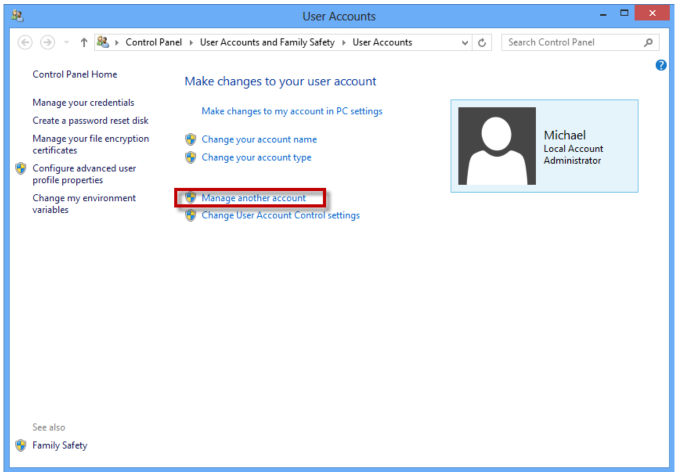

User Accounts
Control Panel › User Accounts and Family Safety › User Accounts
Search Control Panel
Control Panel Home
Manage your credentials
Create a password reset disk
Manage your file encryption certificates
Configure advanced user profile properties
Change my environment variables
Make changes to your user account
Make changes to my account in PC settings
Change your account name
Change your account type
Manage another account
Change User Account Control settings
Michael
Local Account
Administrator
See also
Family Safety

Figure 152. Windows User Accounts

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

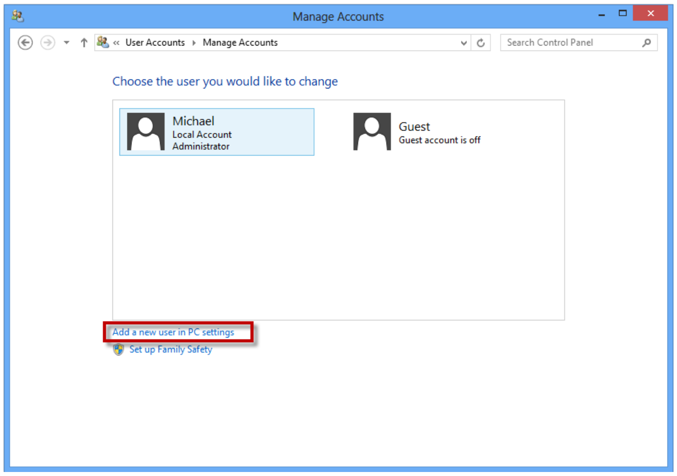
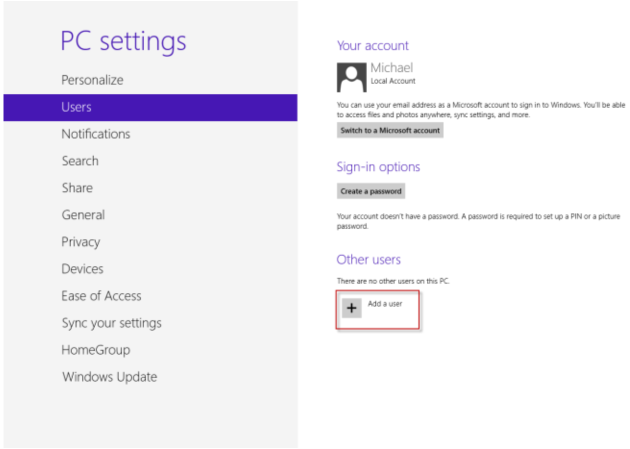


Figure 153. Windows Manage Accounts

8. Click **Add a new user in PC settings**. The Modern UI **PC Settings > Users** screen appears.



Your account

Michael
Local Account

You can use your email address as a Microsoft account to sign in to Windows. You'll be able to access files and photos anywhere, sync settings, and more.

Sign-in options

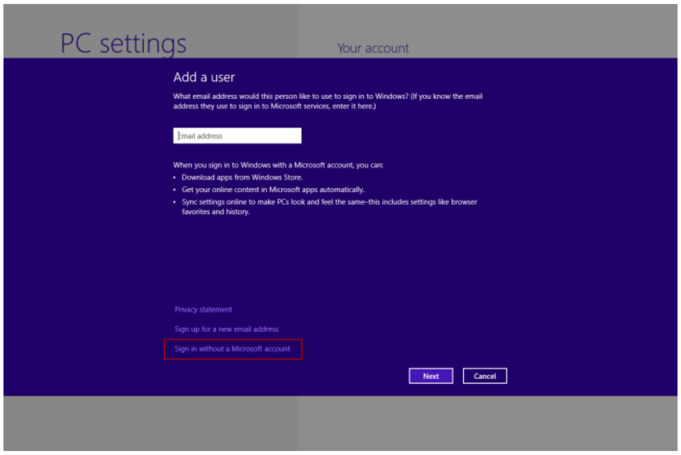
Your account doesn't have a password. A password is required to set up a PIN or a picture password.

Other users

There are no other users on this PC.

Figure 154. Name the Account

9. Click **Add a user**. The screen to **Add a user** appears, with the option to sign in to Windows using a Microsoft Account.



Add a user

What email address would this person like to use to sign in to Windows? (If you know the email address they use to sign in to Microsoft services, enter it here.)

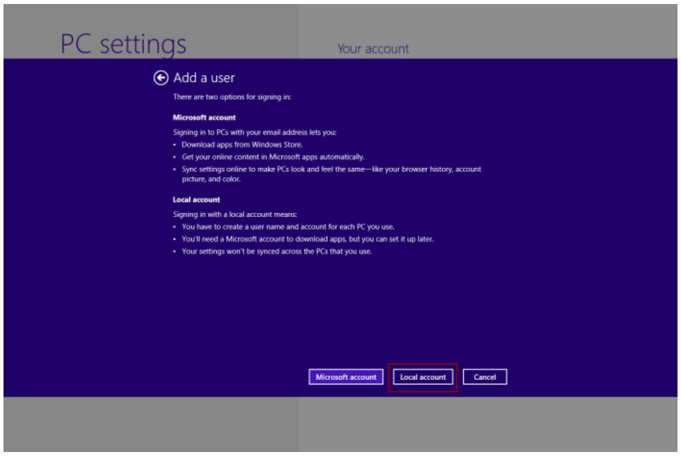
When you sign in to Windows with a Microsoft account, you can:

- Download apps from Windows Store.
- Get your online content in Microsoft apps automatically.
- Sync settings online to make PCs look and feel the same–this includes settings like browser favorites and history.

Privacy statement
Sign up for a new email address
Sign in without a Microsoft account
Next
Cancel

Figure 155. PC Settings (Windows 8)

10. Since you're monitoring your child's use of the internet, for this guide we'll start your child without a Microsoft Account, so click **Sign in without a Microsoft Account.** The second **Add a user** screen appears, emphasizing the difference between a **Microsoft Account** and a **Local Account.**



There are two options for signing in:

Microsoft account

Signing in to PCs with your email address lets you:

- Download apps from Windows Store.
- Get your online content in Microsoft apps automatically.
- Sync settings online to make PCs look and feel the same—like your browser history, account picture, and color.

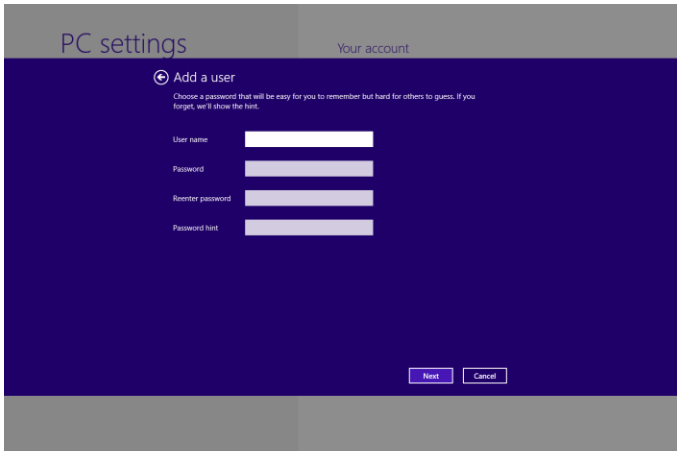
Local account

Signing in with a local account means:

- You have to create a user name and account for each PC you use.
- You'll need a Microsoft account to download apps, but you can set it up later.
- Your settings won't be synced across the PCs that you use.

Figure 156. PC Settings > Add a User

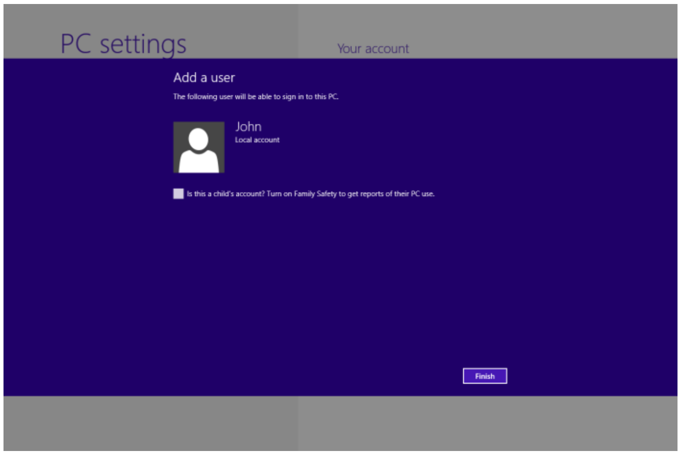
11. Click **Local Account.** The third **Add a user** screen appears.



Choose a password that will be easy for you to remember but hard for others to guess. If you forget, we'll show the hint.

Figure 157. PC Settings > Add a User

12. Type a name for the account (e.g., John), enter a password and confirm it, then provide a password hint and click **Next**. A screen appears, confirming the creation of the account for John.



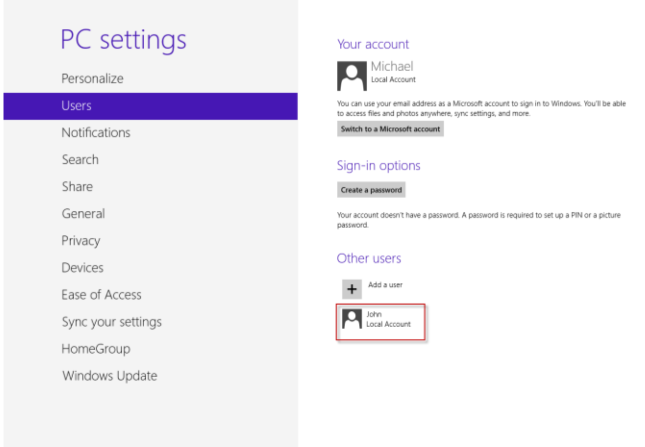
The following user will be able to sign in to this PC.

John
Local account

□ Is this a child's account? Turn on Family Safety to get reports of their PC use.

Figure 158. PC Settings > Add a User

13. Since you're using Titanium's Parental Controls to protect your kid, *do not check the checkbox for Family Safety,* and click **Finish**. This creates the local account named **John.**



Michael
Local Account

You can use your email address as a Microsoft account to sign in to Windows. You'll be able to access files and photos anywhere, sync settings, and more.

Your account doesn't have a password. A password is required to set up a PIN or a picture password.

John
Local Account

Figure 159. Local Account - John

14. Tap the Microsoft Menu key on your keyboard to return to the Modern UI.

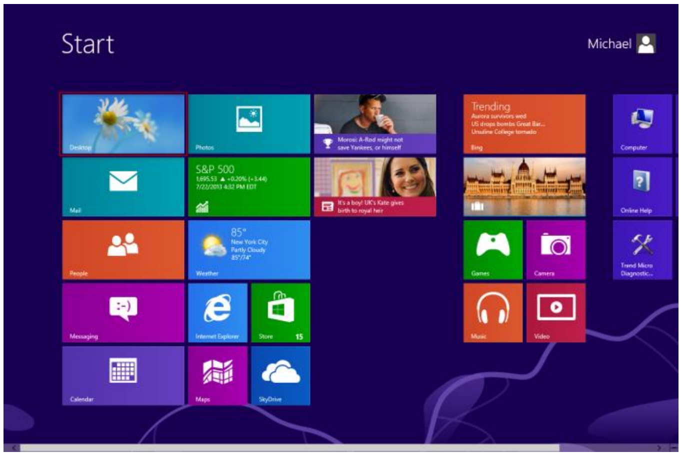
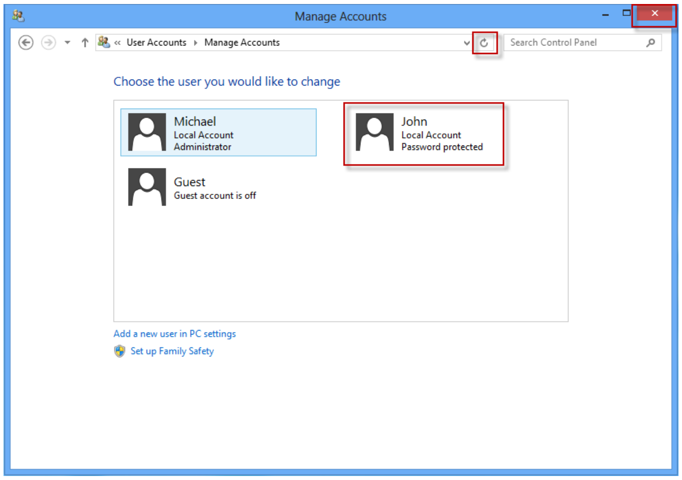


Figure 160. Modern UI - Windows 8

15. Click the **Desktop** icon to return to the Desktop, then click the **Refresh** button if the new account is not showing. The Local Account named John should appear.



Manage Accounts

« User Accounts › Manage Accounts

Search Control Panel

Choose the user you would like to change

Michael
Local Account
Administrator

John
Local Account
Password protected

Guest
Guest account is off

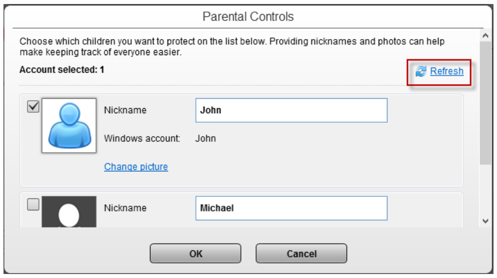
Add a new user in PC settings

Set up Family Safety

Figure 161. John Account

16. Click the **Close Box (X)** to close the window.

17. 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.



Parental Controls

Choose which children you want to protect on the list below. Providing nicknames and photos can help make keeping track of everyone easier.

Account selected: 1

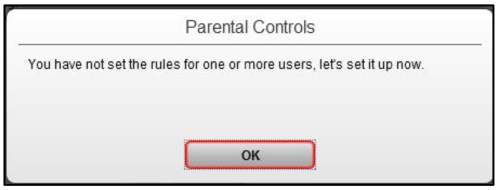
☑ Nickname: John

Windows account: John

□ Nickname: Michael

Figure 162. Guest Account Listed

18. 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."

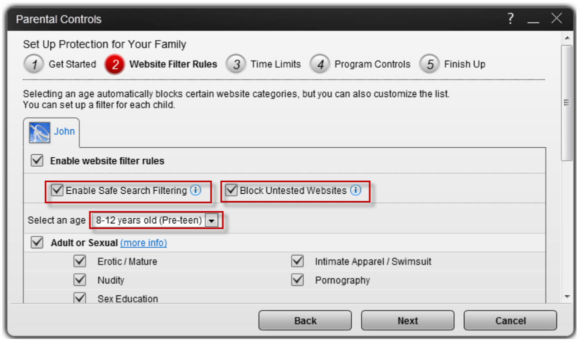


Parental Controls

You have not set the rules for one or more users, let's set it up now.

Figure 163. Set Up Rules Popup

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



Parental Controls

Set Up Protection for Your Family

Selecting an age automatically blocks certain website categories, but you can also customize the list. You can set up a filter for each child.

☑ Enable website filter rules

☑ Enable Safe Search Filtering ☑ Block Untested Websites

Select an age: 8-12 years old (Pre-teen)

☑ Adult or Sexual (more info)

☑ Erotic / Mature ☑ Intimate Apparel / Swimsuit

☑ Nudity ☑ Pornography

☑ Sex Education

Figure 164. Step 2: Website Filter Rules

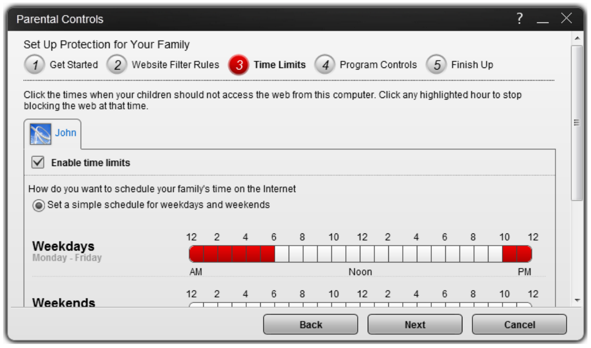
20. In the **Select An Age** popup, choose the age the filter will apply to from the **Select an age** pop-up. For example, choose **Ages 8-12 (Pre-teen).** (You can also define a **Custom** age bracket.)

21. 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.

22. Check **Enable Safe Search Filtering** and **Block Untested Websites.** These options will increase your child's security when searching or browsing the Internet.

23. Click **Next** to define the **Time Limits.** The **Time Limits** page appears.



Parental Controls

Set Up Protection for Your Family

1 Get Started 2 Website Filter Rules 3 Time Limits 4 Program Controls 5 Finish Up

Click the times when your children should not access the web from this computer. Click any highlighted hour to stop blocking the web at that time.

John

☑ Enable time limits

How do you want to schedule your family's time on the Internet

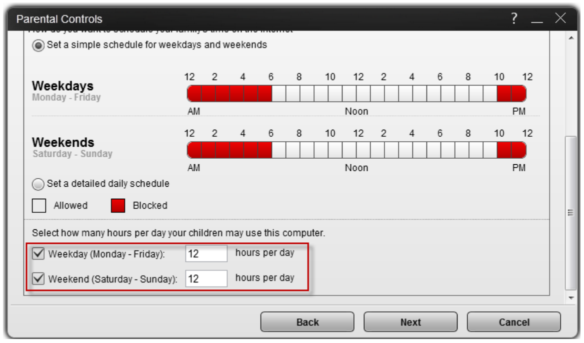
● Set a simple schedule for weekdays and weekends

Weekdays
Monday - Friday

Weekends

Figure 165. Time Limits

24. 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.



Parental Controls

● Set a simple schedule for weekdays and weekends

Weekdays
Monday - Friday

Weekends
Saturday - Sunday

○ Set a detailed daily schedule

□ Allowed 🟥 Blocked

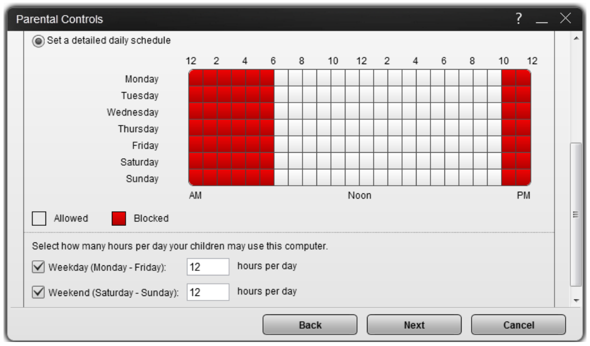
Select how many hours per day your children may use this computer.

☑ Weekday (Monday - Friday): 12 hours per day

☑ Weekend (Saturday - Sunday): 12 hours per day

Figure 166. Allowed Hours on Computer

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



Parental Controls

● Set a detailed daily schedule

□ Allowed 🟥 Blocked

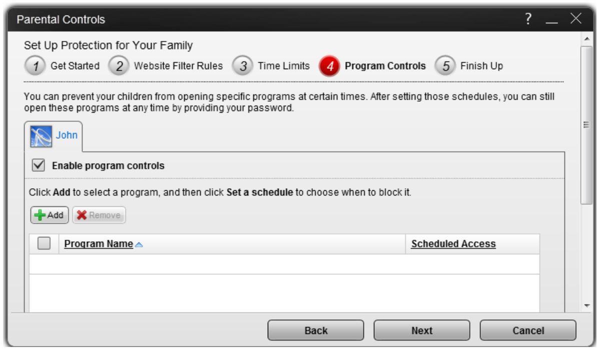
Select how many hours per day your children may use this computer.

☑ Weekday (Monday - Friday): 12 hours per day

☑ Weekend (Saturday - Sunday): 12 hours per day

Figure 167. Detailed Daily Schedule

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



Parental Controls

Set Up Protection for Your Family

You can prevent your children from opening specific programs at certain times. After setting those schedules, you can still open these programs at any time by providing your password.

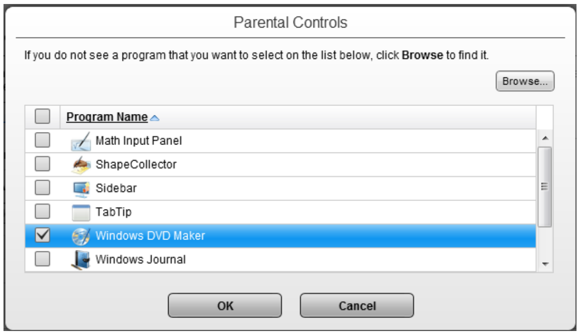
☑ Enable program controls

Click **Add** to select a program, and then click **Set a schedule** to choose when to block it.

□ Program Name	Scheduled Access

Figure 168. Program Controls

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



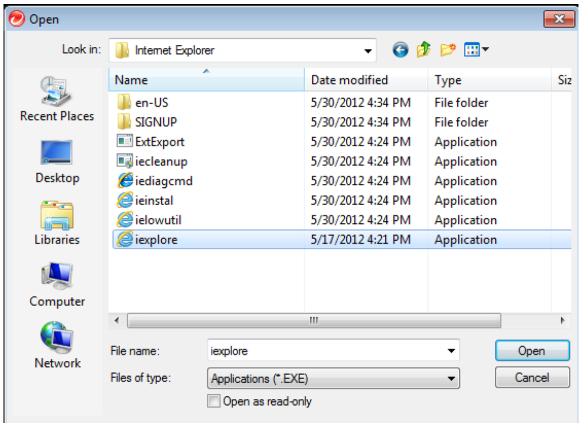
Parental Controls

If you do not see a program that you want to select on the list below, click **Browse** to find it.

□	Program Name
□	Math Input Panel
□	ShapeCollector
□	Sidebar
□	TabTip
☑	Windows DVD Maker
□	Windows Journal

Figure 169. Program List

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



Open

Look in: Internet Explorer

Name	Date modified	Type	Siz
en-US	5/30/2012 4:34 PM	File folder	
SIGNUP	5/30/2012 4:34 PM	File folder	
ExtExport	5/30/2012 4:24 PM	Application	
iecleanup	5/30/2012 4:24 PM	Application	
iediagcmd	5/30/2012 4:24 PM	Application	
ieinstal	5/30/2012 4:24 PM	Application	
ielowutil	5/30/2012 4:24 PM	Application	
iexplore	5/17/2012 4:21 PM	Application	

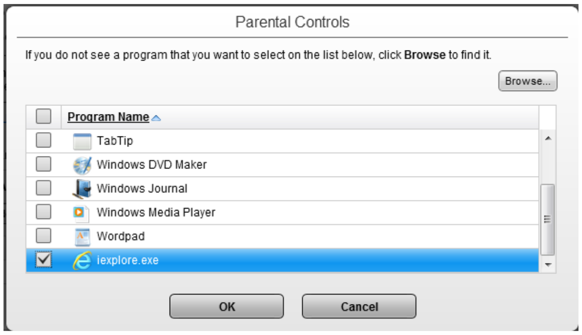
File name: iexplore

Files of type: Applications (*.EXE)

□ Open as read-only

Figure 170. Browsing for Programs to Add to Program Controls

29. Navigate to the program in the **Programs Folder**, select it from its own folder (e.g., Internet Explorer), and click **Open**. Titanium adds it to the list of controlled programs.



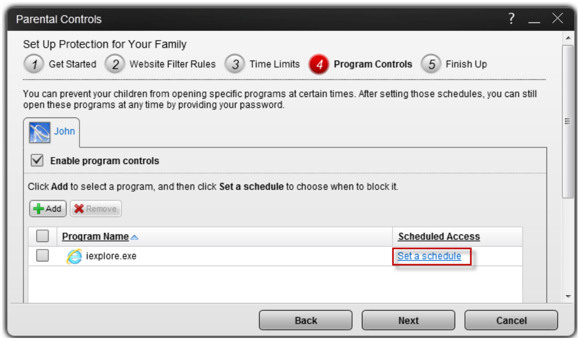
Parental Controls

If you do not see a program that you want to select on the list below, click **Browse** to find it.

	Program Name
□	TabTip
□	Windows DVD Maker
□	Windows Journal
□	Windows Media Player
□	Wordpad
☑	iexplore.exe

Figure 171. Programs in List | IE Added

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



Parental Controls

Set Up Protection for Your Family

You can prevent your children from opening specific programs at certain times. After setting those schedules, you can still open these programs at any time by providing your password.

John

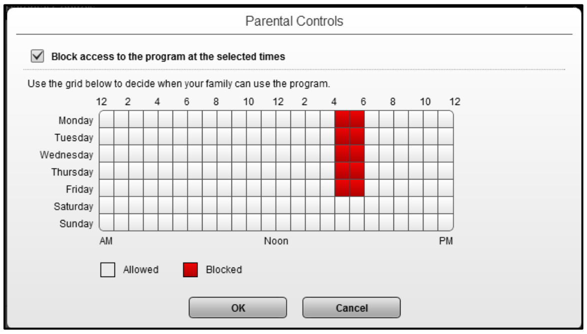
☑ Enable program controls

Click **Add** to select a program, and then click **Set a schedule** to choose when to block it.

	Program Name	Scheduled Access
□	iexplore.exe	Set a schedule

Figure 172. Set a Schedule

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



Parental Controls

☑ **Block access to the program at the selected times**

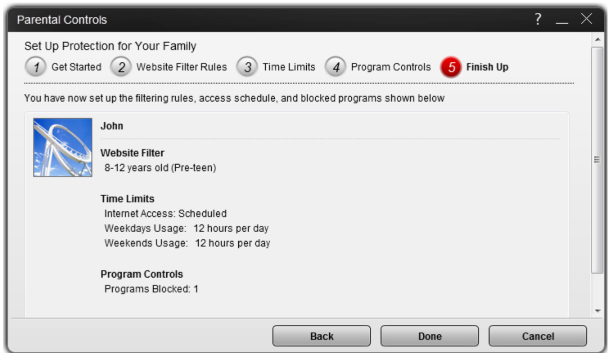
Use the grid below to decide when your family can use the program.

□ Allowed 🟥 Blocked

Figure 173. Access Schedule

32. 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**.

33. A screen appears, indicating that protection has been activated for **John**, applying the **Pre-teen Website Filter**, giving the **Time Limits** and **Program Controls**.



Parental Controls

Set Up Protection for Your Family

You have now set up the filtering rules, access schedule, and blocked programs shown below

John

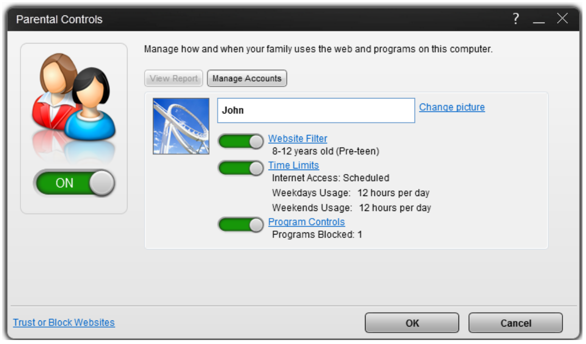
Website Filter
8-12 years old (Pre-teen)

Time Limits
Internet Access: Scheduled
Weekdays Usage: 12 hours per day
Weekends Usage: 12 hours per day

Program Controls
Programs Blocked: 1

Figure 174. "John" Protection Criteria

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



Parental Controls

Manage how and when your family uses the web and programs on this computer.

John

Website Filter
8-12 years old (Pre-teen)
Time Limits
Internet Access: Scheduled
Weekdays Usage: 12 hours per day
Weekends Usage: 12 hours per day
Program Controls
Programs Blocked: 1

Figure 175. Slider is "On"

35. 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.

36. 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.

37. 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.

38. 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.**

39. Log off the **Administrator's** account (or switch users) and sign on using the **John** account.

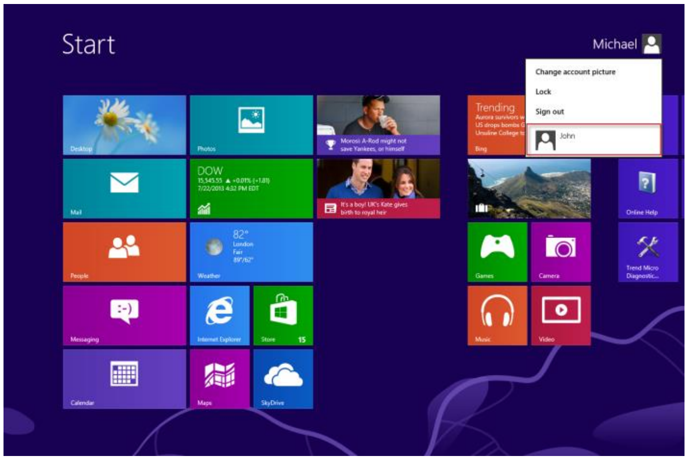
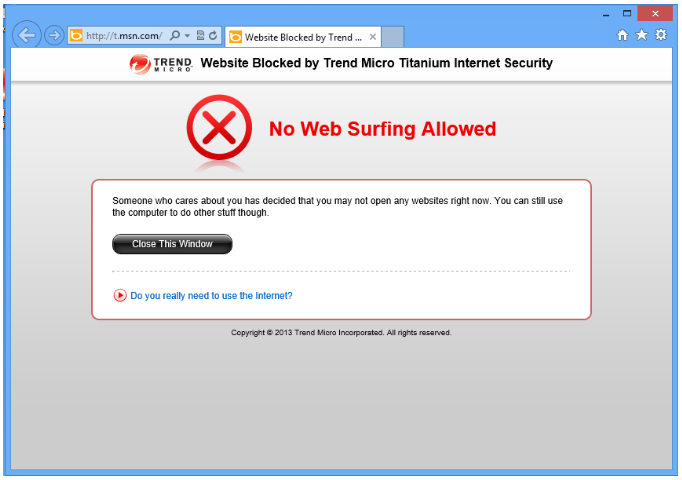


Figure 176. Switching to "John" Account

40. 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.



Website Blocked by Trend Micro Titanium Internet Security

No Web Surfing Allowed

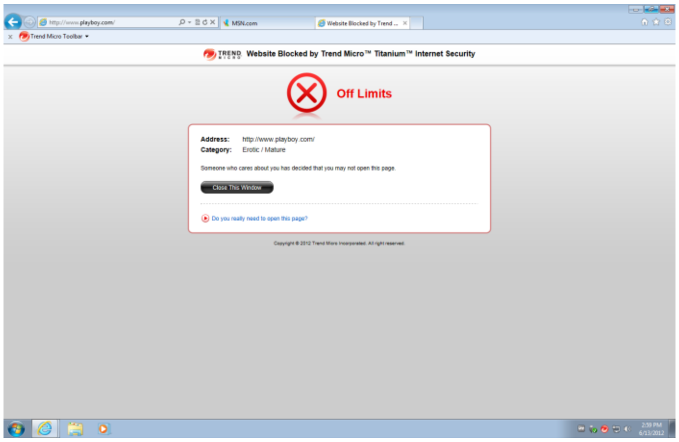
Someone who cares about you has decided that you may not open any websites right now. You can still use the computer to do other stuff though.

Do you really need to use the Internet?

Copyright © 2013 Trend Micro Incorporated. All rights reserved.

Figure 177. No Web Surfing Allowed

41. 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.



Website Blocked by Trend Micro™ Titanium™ Internet Security

Off Limits

Address: http://www.playboy.com/
Category: Erotic / Mature

Someone who cares about you has decided that you may not open this page.

Do you really need to open this page?

Copyright © 2012 Trend Micro Incorporated. All right reserved.

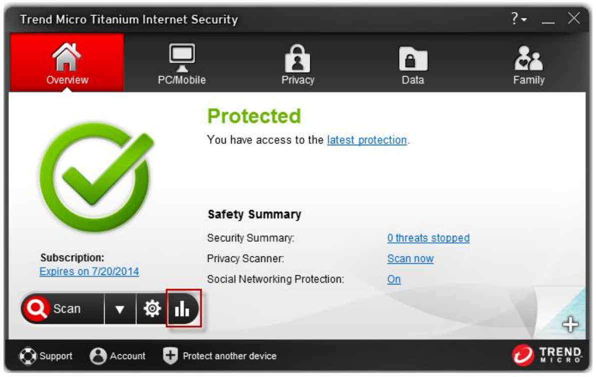
Figure 178. Titanium Off Limits Notification in Browser

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.



Protected

You have access to the latest protection.

Safety Summary

Security Summary: 0 threats stopped

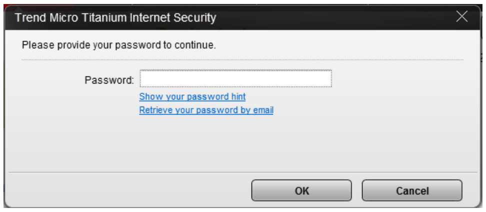
Privacy Scanner: Scan now

Social Networking Protection: On

Subscription: Expires on 7/20/2014

Figure 179. Console > Reports

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



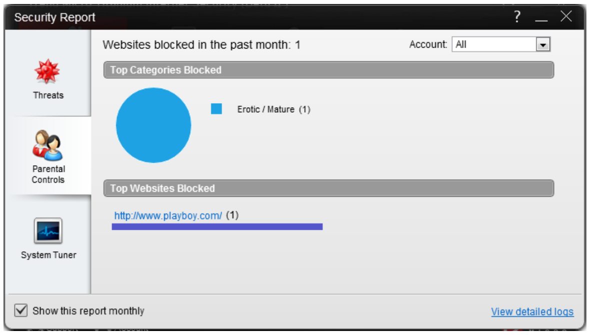
Please provide your password to continue.

Password:

Show your password hint

Retrieve your password by email

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



Websites blocked in the past month: 1

Account: All

■ Erotic / Mature (1)

http://www.playboy.com/ (1)

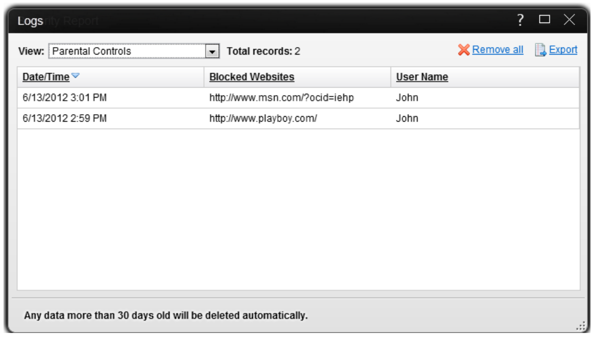
☑ Show this report monthly

Figure 180. 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.



View: Parental Controls Total records: 2

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 181. Parental Controls Logs

7. Click **Remove all** to delete the logs

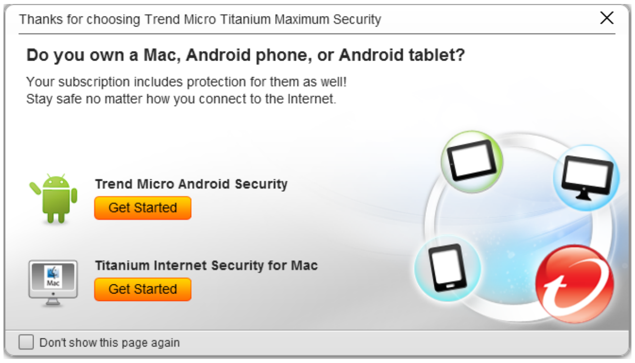
8. Click **Export** to export the Parental Controls log in .CSV or .TXT format.

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.



Thanks for choosing Trend Micro Titanium Maximum Security

Do you own a Mac, Android phone, or Android tablet?

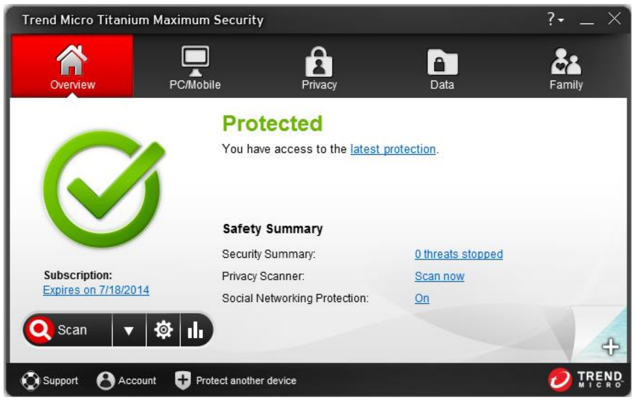
Your subscription includes protection for them as well!
Stay safe no matter how you connect to the Internet.

Trend Micro Android Security

Titanium Internet Security for Mac

☐ Don't show this page again

Figure 182. Titanium Maximum Security Welcome Screen



Trend Micro Titanium Maximum Security

Protected

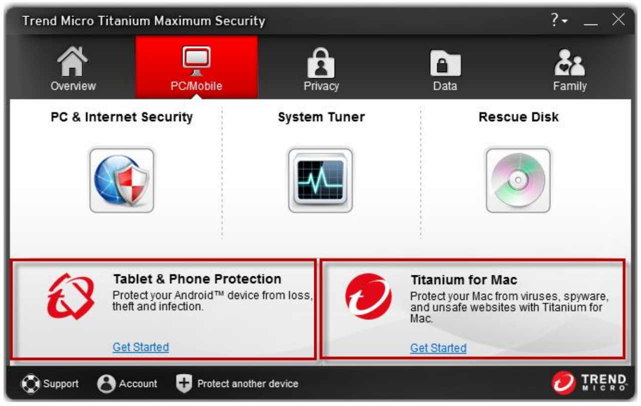
You have access to the latest protection.

Safety Summary

Security Summary: 0 threats stopped
Privacy Scanner: Scan now
Social Networking Protection: On

Subscription:
Expires on 7/18/2014

Figure 183. Titanium Maximum Security Console Overview



Protect your Android™ device from loss, theft and infection.

Protect your Mac from viruses, spyware, and unsafe websites with Titanium for Mac.

Figure 184. PC/Mobile > Tablet & Phone Protection

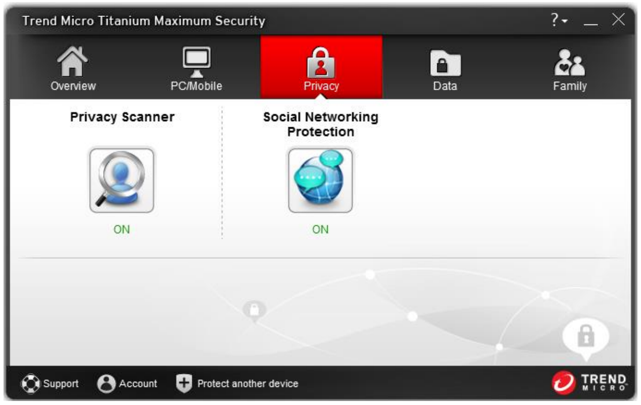
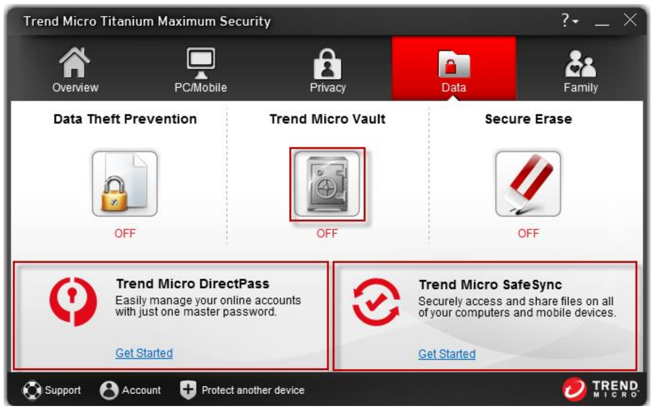


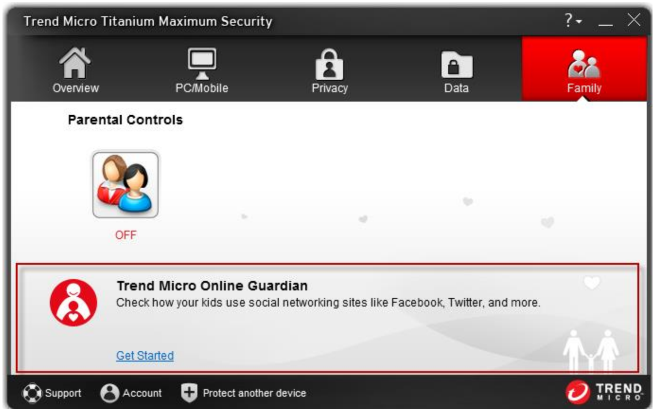
Figure 185. Privacy



Easily manage your online accounts with just one master password.

Securely access and share files on all of your computers and mobile devices.

Figure 186. Data > Trend Micro Vault, DirectPass, SafeSync



Trend Micro Online Guardian
Check how your kids use social networking sites like Facebook, Twitter, and more.

Figure 187. Trend Micro Online Guardian

Note: **Titanium Maximum Security Additional Features: Trend Micro Vault. Titanium Maximum users with a standard subscription can protect three devices, including Mac and Mobile.**

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

ADDITIONAL TOOLS FOR TITANIUM MAXIMUM SECURITY PAID VERSION

Trend Micro Vault

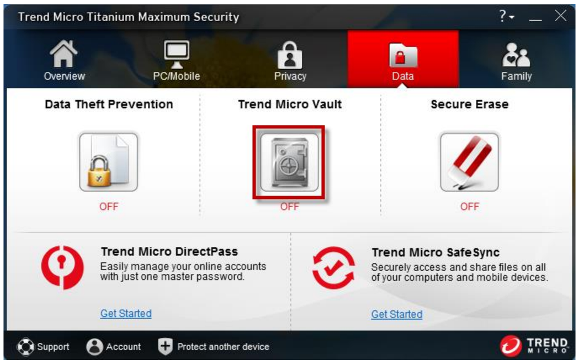
Users can enable a password-protected folder that can SafeSurfing sensitive files. If the computer is lost or stolen, the vault can be sealed shut by remote control until the computer is return to its rightful owner.

Data: Trend Micro Vault

Trend Micro Vault is a password-protected folder that can SafeSurfing 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, who then must report that the computer is found.

To set up Trend Micro Vault:

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

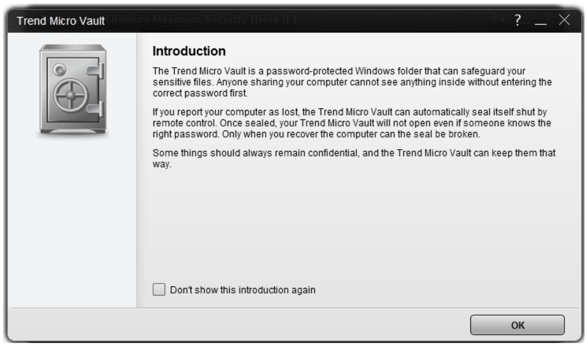


Trend Micro DirectPass
Easily manage your online accounts with just one master password.
Get Started

Trend Micro SafeSync
Securely access and share files on all of your computers and mobile devices.
Get Started

Figure 188. Data > Trend Micro Vault

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



Introduction

The Trend Micro Vault is a password-protected Windows folder that can safeguard your sensitive files. Anyone sharing your computer cannot see anything inside without entering the correct password first.

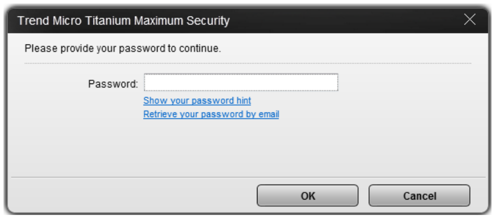
If you report your computer as lost, the Trend Micro Vault can automatically seal itself shut by remote control. Once sealed, your Trend Micro Vault will not open even if someone knows the right password. Only when you recover the computer can the seal be broken.

Some things should always remain confidential, and the Trend Micro Vault can keep them that way.

☐ Don't show this introduction again

Figure 189. Trend Micro Vault Introduction

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



Please provide your password to continue.

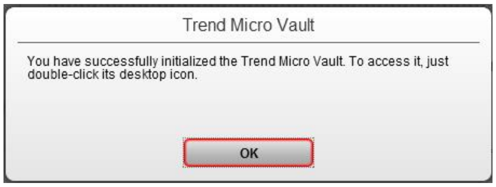
Password:

Show your password hint

Retrieve your password by email

Figure 190. Enter Password

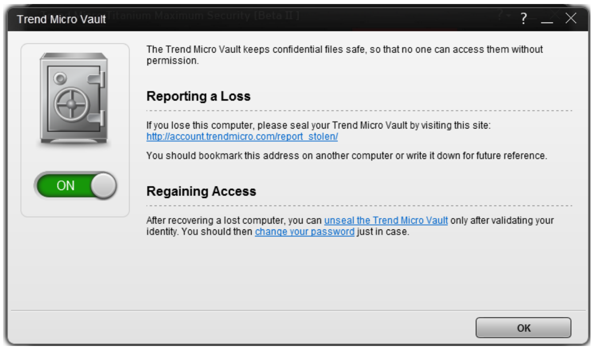
4. Enter your **Password** and click **OK**. An initialization dialog appears, instructing the user how to access the vault by double-clicking its desktop icon.



You have successfully initialized the Trend Micro Vault. To access it, just double-click its desktop icon.

Figure 191. Trend Micro Vault Initialized

5. Click **OK** to close the dialog. The **Trend Micro Vault** window appears.



The Trend Micro Vault keeps confidential files safe, so that no one can access them without permission.

Reporting a Loss

If you lose this computer, please seal your Trend Micro Vault by visiting this site: http://account.trendmicro.com/report_stolen/

You should bookmark this address on another computer or write it down for future reference.

Regaining Access

After recovering a lost computer, you can unseal the Trend Micro Vault only after validating your identity. You should then change your password just in case.

Figure 192. Trend Micro Vault

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

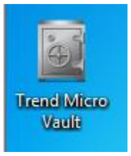
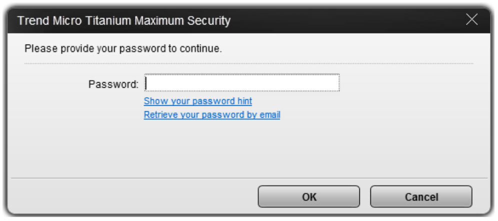


Figure 193. Trend Micro Vault Desktop Icon

7. 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.

8. To open the Trend Micro Vault, double-click the desktop icon. The password window appears.



Please provide your password to continue.

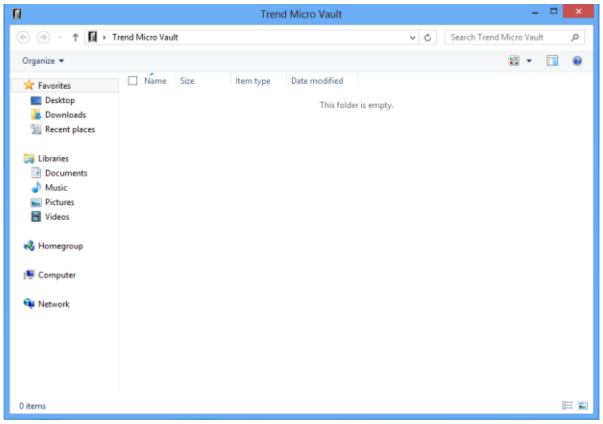
Password:

Show your password hint

Retrieve your password by email

Figure 194. Trend Micro Vault > Password Protection

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



This folder is empty.

Figure 195. Trend Micro Vault

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

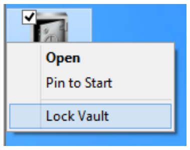
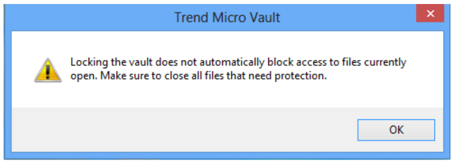


Figure 196. Lock Vault Menu Item

11. Right-click the Vault and select **Lock Vault** to lock it. A dialog appears, warning you 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.

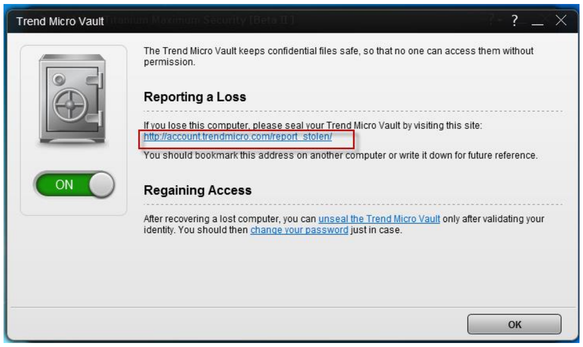


Locking the vault does not automatically block access to files currently open. Make sure to close all files that need protection.

Figure 197. 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.



Trend Micro Vault

The Trend Micro Vault keeps confidential files safe, so that no one can access them without permission.

Reporting a Loss

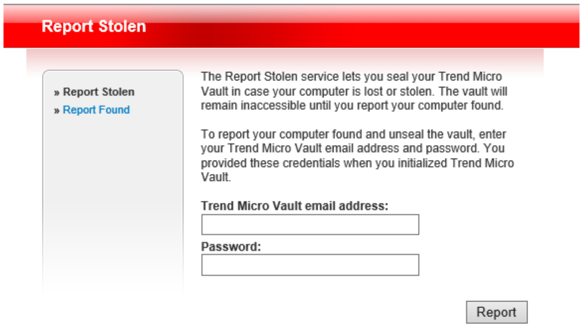
If you lose this computer, please seal your Trend Micro Vault by visiting this site:
http://account.trendmicro.com/report_stolen/
You should bookmark this address on another computer or write it down for future reference.

Regaining Access

After recovering a lost computer, you can unseal the Trend Micro Vault only after validating your identity. You should then change your password just in case.

Figure 198. Reporting a Loss

14. You should bookmark this link 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.



Report Stolen

» Report Stolen
» Report Found

The Report Stolen service lets you seal your Trend Micro Vault in case your computer is lost or stolen. The vault will remain inaccessible until you report your computer found.

To report your computer found and unseal the vault, enter your Trend Micro Vault email address and password. You provided these credentials when you initialized Trend Micro Vault.

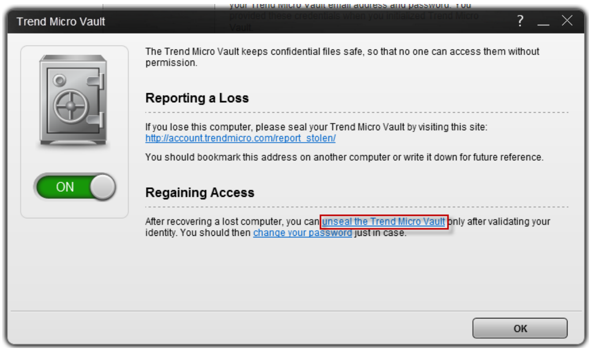
Trend Micro Vault email address:

Password:

Figure 199. Report Stolen Service

15. In the **Report Stolen** webpage, 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.

16. Once you recover the computer, open the Titanium console, click **Data > Trend Micro Vault**, re-enter your password, then click the link **Unseal the Trend Micro Vault** in the **Regaining Access** paragraph.



Trend Micro Vault

The Trend Micro Vault keeps confidential files safe, so that no one can access them without permission.

Reporting a Loss

If you lose this computer, please seal your Trend Micro Vault by visiting this site: http://account.trendmicro.com/report_stolen/

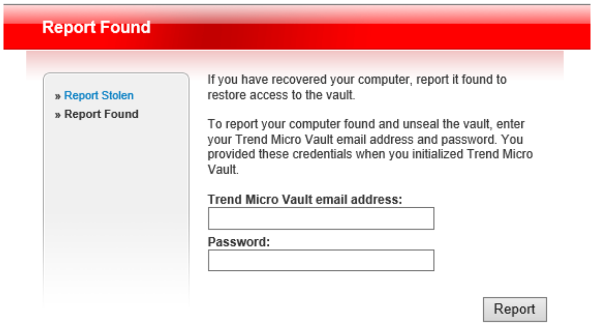
You should bookmark this address on another computer or write it down for future reference.

Regaining Access

After recovering a lost computer, you can unseal the Trend Micro Vault only after validating your identity. You should then change your password just in case.

Figure 200. Regaining Access

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



Report Found

If you have recovered your computer, report it found to restore access to the vault.

To report your computer found and unseal the vault, enter your Trend Micro Vault email address and password. You provided these credentials when you initialized Trend Micro Vault.

Trend Micro Vault email address:

Password:

Figure 201. 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.

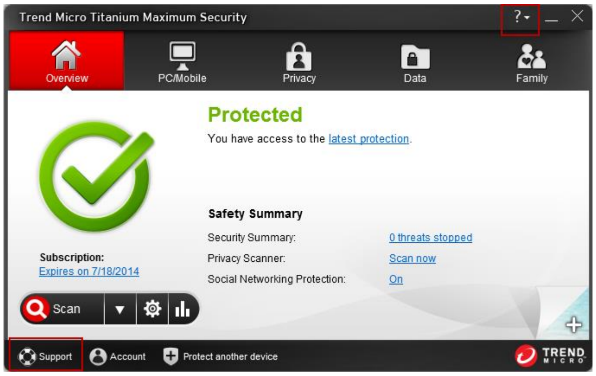
19. For your safety, you should now change your Titanium password.

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.



Protected

You have access to the latest protection.

Safety Summary

Security Summary: 0 threats stopped

Privacy Scanner: Scan now

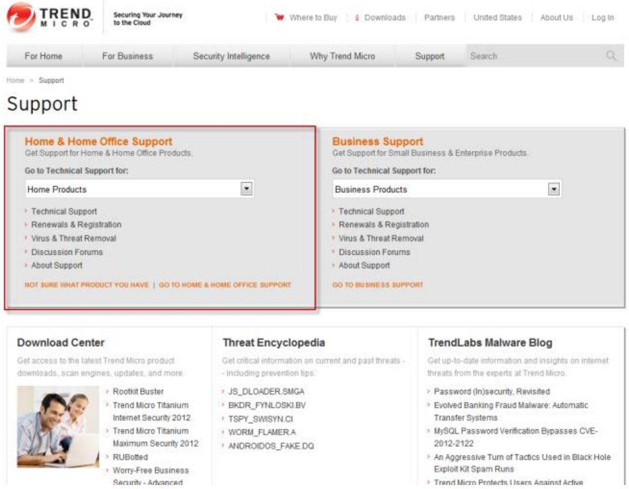
Social Networking Protection: On

Subscription: Expires on 7/18/2014

Figure 202. 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.



Support

Home & Home Office Support

Get Support for Home & Home Office Products.

Go to Technical Support for: Home Products

- Technical Support
- Renewals & Registration
- Virus & Threat Removal
- Discussion Forums
- About Support

NOT SURE WHAT PRODUCT YOU HAVE | GO TO HOME & HOME OFFICE SUPPORT

Business Support

Get Support for Small Business & Enterprise Products.

Go to Technical Support for: Business Products

- Technical Support
- Renewals & Registration
- Virus & Threat Removal
- Discussion Forums
- About Support

GO TO BUSINESS SUPPORT

Download Center

Get access to the latest Trend Micro product downloads, scan engines, updates, and more.

- Rootkit Buster
- Trend Micro Titanium Internet Security 2012
- Trend Micro Titanium Maximum Security 2012
- RUBotted
- Worry-Free Business Security - Advanced

Threat Encyclopedia

Get critical information on current and past threats - - including prevention tips.

- JS_DLOADER.SMGA
- BKDR_FYNLOSKI.BV
- TSPY_SWISYN.CI
- WORM_FLAMER.A
- ANDROIDOS_FAKE.DQ

TrendLabs Malware Blog

Get up-to-date information and insights on internet threats from the experts at Trend Micro.

- Password (In)security, Revisited
- Evolved Banking Fraud Malware: Automatic Transfer Systems
- MySQL Password Verification Bypasses CVE-2012-2122
- An Aggressive Turn of Tactics Used in Black Hole Exploit Kit Spam Runs
- Trend Micro Protects Users Against Active

Figure 203. Trend Micro Support

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

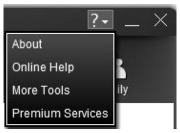
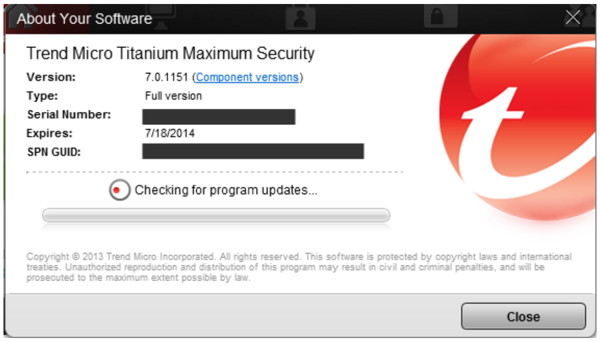


Figure 204. ? (Help) Menu

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



About Your Software

Trend Micro Titanium Maximum Security

Version: 7.0.1151 (Component versions)

Type: Full version

Serial Number: [redacted]

Expires: 7/18/2014

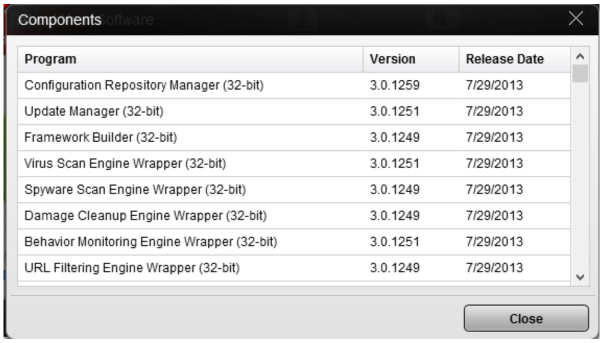
SPN GUID: [redacted]

Checking for program updates...

Copyright © 2013 Trend Micro Incorporated. All rights reserved. This software is protected by copyright laws and international treaties. Unauthorized reproduction and distribution of this program may result in civil and criminal penalties, and will be prosecuted to the maximum extent possible by law.

Figure 205. About Screen

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

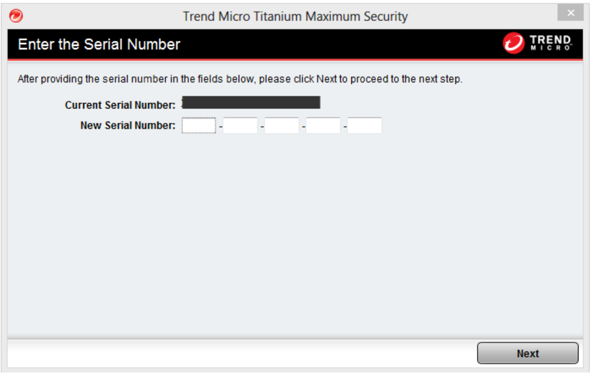


Components

Program	Version	Release Date
Configuration Repository Manager (32-bit)	3.0.1259	7/29/2013
Update Manager (32-bit)	3.0.1251	7/29/2013
Framework Builder (32-bit)	3.0.1249	7/29/2013
Virus Scan Engine Wrapper (32-bit)	3.0.1251	7/29/2013
Spyware Scan Engine Wrapper (32-bit)	3.0.1249	7/29/2013
Damage Cleanup Engine Wrapper (32-bit)	3.0.1249	7/29/2013
Behavior Monitoring Engine Wrapper (32-bit)	3.0.1251	7/29/2013
URL Filtering Engine Wrapper (32-bit)	3.0.1249	7/29/2013

Figure 206. Component Versions

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



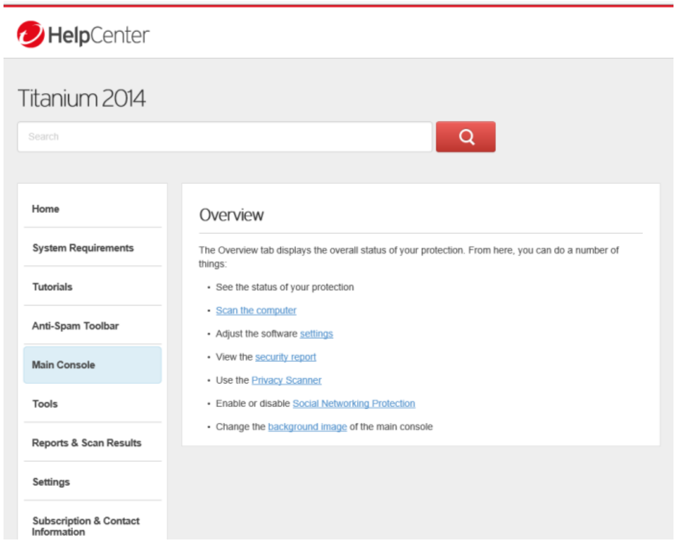
After providing the serial number in the fields below, please click Next to proceed to the next step.

Current Serial Number: [redacted]

New Serial Number: - - - -

Figure 207. Enter the Serial Number

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



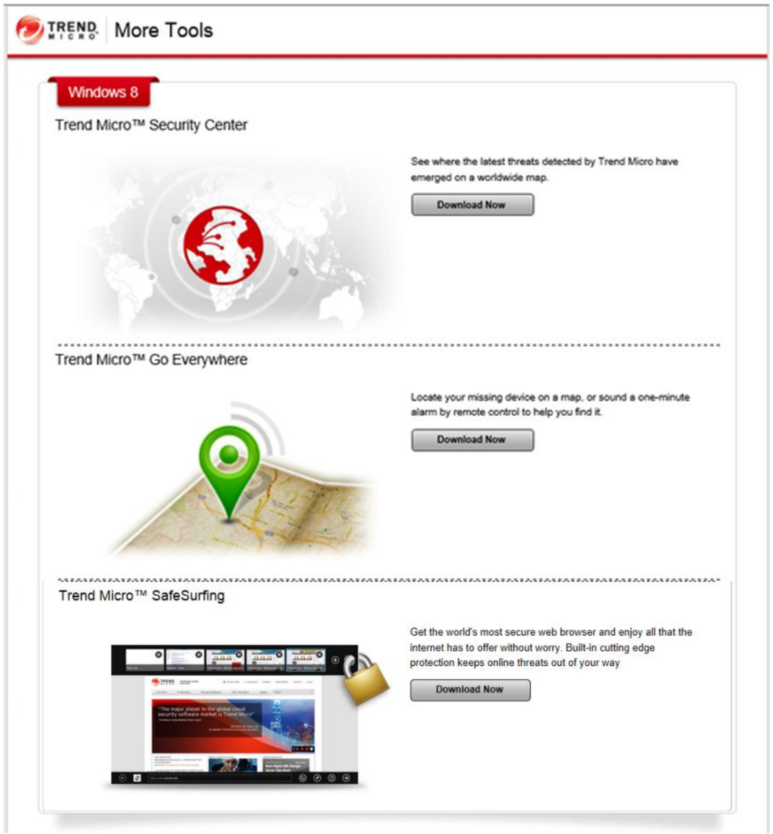
Overview

The Overview tab displays the overall status of your protection. From here, you can do a number of things:

- See the status of your protection
- Scan the computer
- Adjust the software settings
- View the security report
- Use the Privacy Scanner
- Enable or disable Social Networking Protection
- Change the background image of the main console

Figure 208. Titanium 2012 Online Help

9. Select **More Tools** to take you to the **More Tools** webpage, where you can download other tools, including apps for Windows 8.



More Tools

Windows 8

Trend Micro™ Security Center

See where the latest threats detected by Trend Micro have emerged on a worldwide map.

Download Now

Trend Micro™ Go Everywhere

Locate your missing device on a map, or sound a one-minute alarm by remote control to help you find it.

Download Now

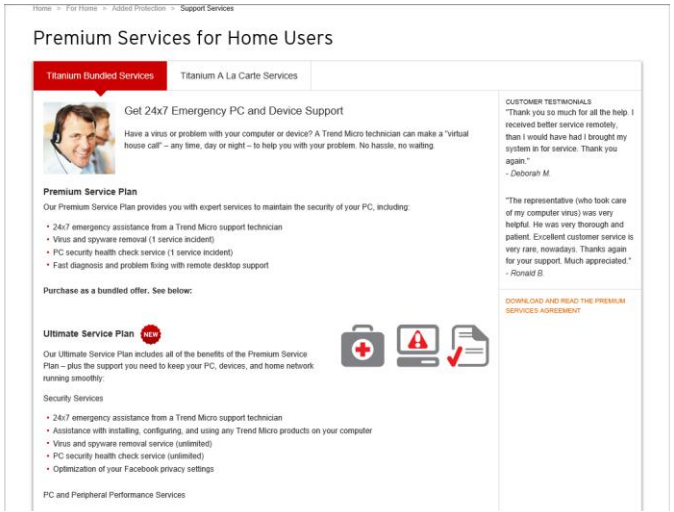
Trend Micro™ SafeSurfing

Get the world's most secure web browser and enjoy all that the internet has to offer without worry. Built-in cutting edge protection keeps online threats out of your way

Download Now

Figure 209. More Tools

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



Home > For Home > Added Protection > Support Services

Premium Services for Home Users

Titanium Bundled Services | Titanium A La Carte Services

Get 24x7 Emergency PC and Device Support

Have a virus or problem with your computer or device? A Trend Micro technician can make a "virtual house call" – any time, day or night – to help you with your problem. No hassle, no waiting.

Premium Service Plan

Our Premium Service Plan provides you with expert services to maintain the security of your PC, including:

- 24x7 emergency assistance from a Trend Micro support technician
- Virus and spyware removal (1 service incident)
- PC security health check service (1 service incident)
- Fast diagnosis and problem fixing with remote desktop support

Purchase as a bundled offer. See below:

Ultimate Service Plan NEW

Our Ultimate Service Plan includes all of the benefits of the Premium Service Plan – plus the support you need to keep your PC, devices, and home network running smoothly:

Security Services

- 24x7 emergency assistance from a Trend Micro support technician
- Assistance with installing, configuring, and using any Trend Micro products on your computer
- Virus and spyware removal service (unlimited)
- PC security health check service (unlimited)
- Optimization of your Facebook privacy settings

PC and Peripheral Performance Services

CUSTOMER TESTIMONIALS

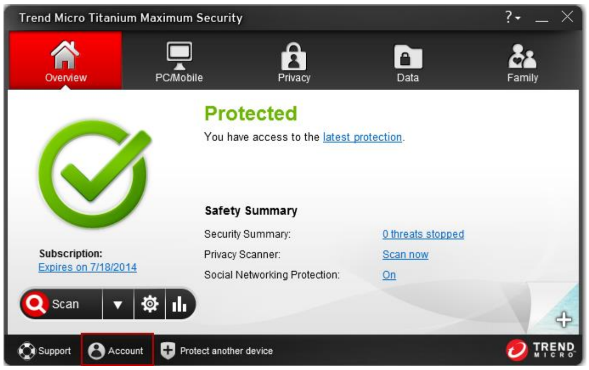
"Thank you so much for all the help. I received better service remotely, than I would have had I brought my system in for service. Thank you again."
- *Deborah M.*

"The representative (who took care of my computer virus) was very helpful. He was very thorough and patient. Excellent customer service is very rare, nowadays. Thanks again for your support. Much appreciated."
- *Ronald B.*

DOWNLOAD AND READ THE PREMIUM SERVICES AGREEMENT

Figure 210. 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.



Protected

You have access to the latest protection.

Safety Summary

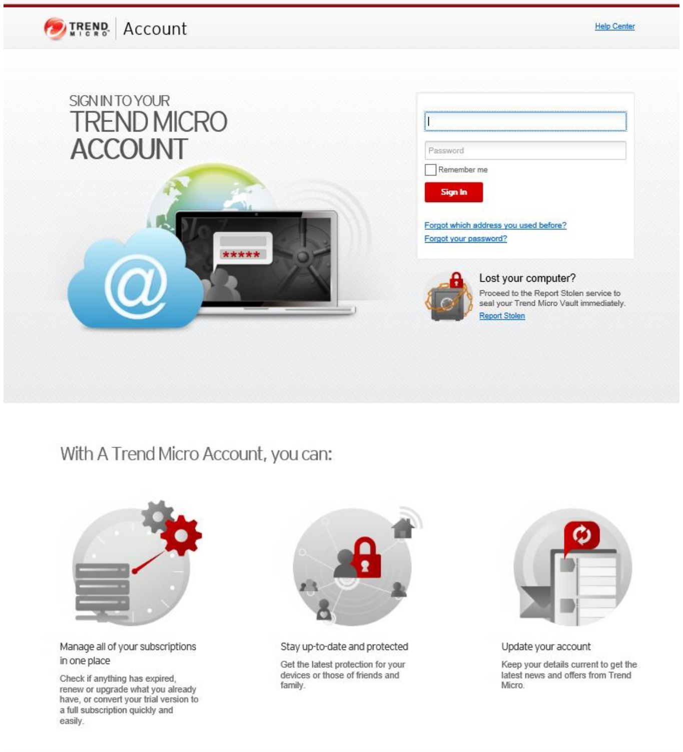
Security Summary: 0 threats stopped

Privacy Scanner: Scan now

Social Networking Protection: On

Subscription:
Expires on 7/18/2014

Figure 211. Titanium Console > Account



SIGN IN TO YOUR TREND MICRO ACCOUNT

Password

□ Remember me

Lost your computer?

Proceed to the Report Stolen service to seal your Trend Micro Vault immediately.

With A Trend Micro Account, you can:

Manage all of your subscriptions in one place

Check if anything has expired, renew or upgrade what you already have, or convert your trial version to a full subscription quickly and easily.

Stay up-to-date and protected

Get the latest protection for your devices or those of friends and family.

Update your account

Keep your details current to get the latest news and offers from Trend Micro.

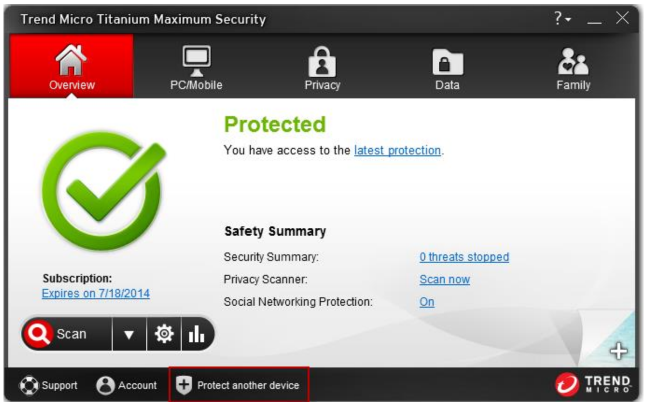
Figure 212. Trend Micro Account Webpage

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: Protect Another Device

Subscriptions to Trend Micro™ Titanium Security™ Internet Security, Maximum Security, and Premium Security variously let you protect other PC, Mac, or mobile devices.

- Titanium Internet Security: 3 PCs
- Titanium Maximum Security: 3 devices, including PC, Mac, and Mobile
- Titanium Premium Security: 5 devices, including PC, Mac, and Mobile


Trend Micro Titanium Maximum Security

Protected

You have access to the latest protection.

Safety Summary

Security Summary: 0 threats stopped

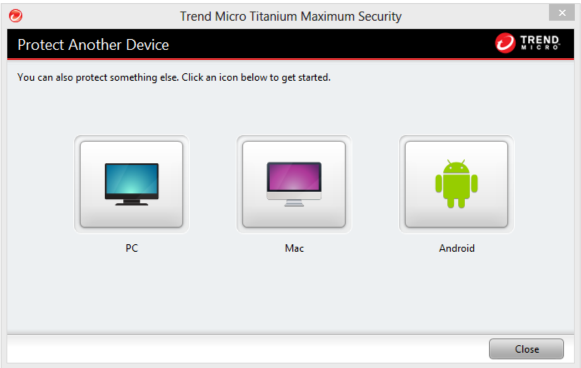
Privacy Scanner: Scan now

Social Networking Protection: On

Subscription: Expires on 7/18/2014

Figure 213. Protect Another Device

1. To get started with your protection for another device, click **Protect Another device.** The **Protect Another Device** screen appears.

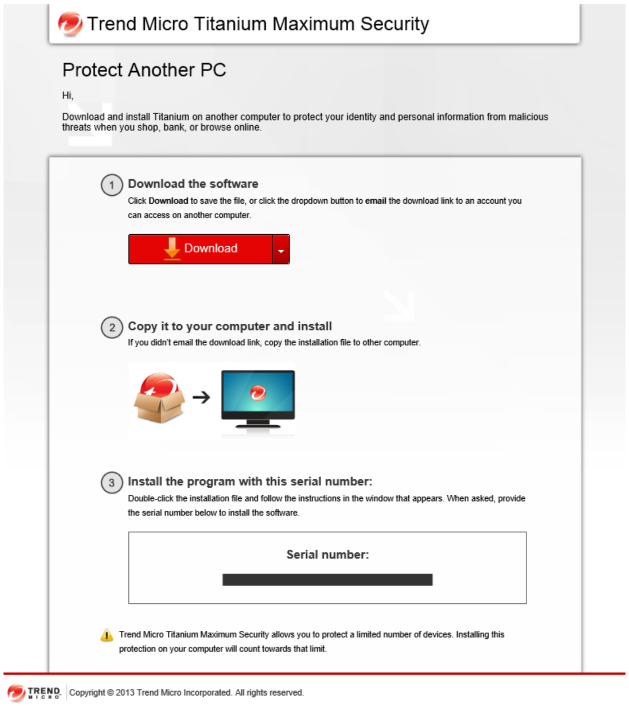

Trend Micro Titanium Maximum Security

Protect Another Device

You can also protect something else. Click an icon below to get started.

Figure 214. Protect Another Device Picklist

2. Click the icon for the type of device you wish to protect. A screen appears for you to download the software.



Trend Micro Titanium Maximum Security

Protect Another PC

Hi,

Download and install Titanium on another computer to protect your identity and personal information from malicious threats when you shop, bank, or browse online.

1 **Download the software**

Click **Download** to save the file, or click the dropdown button to **email** the download link to an account you can access on another computer.

2 **Copy it to your computer and install**

If you didn't email the download link, copy the installation file to other computer.

3 **Install the program with this serial number:**

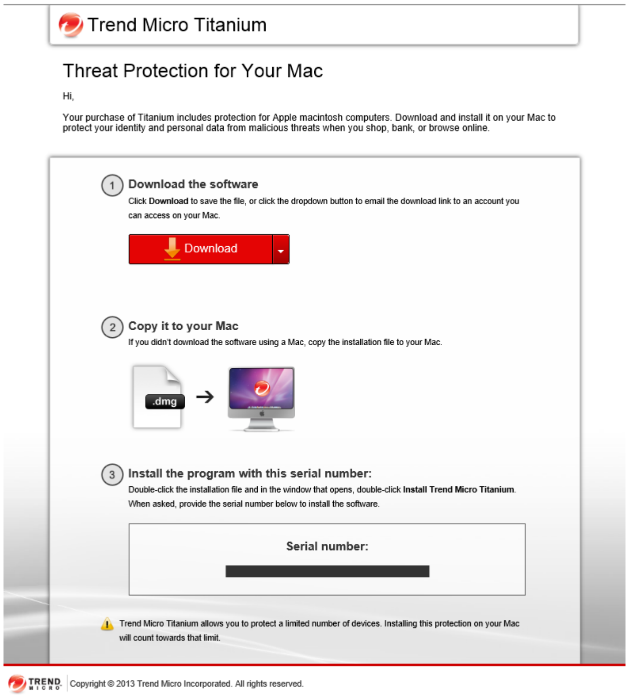
Double-click the installation file and follow the instructions in the window that appears. When asked, provide the serial number below to install the software.

Serial number:

[redacted]

Trend Micro Titanium Maximum Security allows you to protect a limited number of devices. Installing this protection on your computer will count towards that limit.

Figure 215. Protect Another PC



Trend Micro Titanium

Threat Protection for Your Mac

Hi,

Your purchase of Titanium includes protection for Apple macintosh computers. Download and install it on your Mac to protect your identity and personal data from malicious threats when you shop, bank, or browse online.

1 **Download the software**

Click **Download** to save the file, or click the dropdown button to email the download link to an account you can access on your Mac.

2 **Copy it to your Mac**

If you didn't download the software using a Mac, copy the installation file to your Mac.

3 **Install the program with this serial number:**

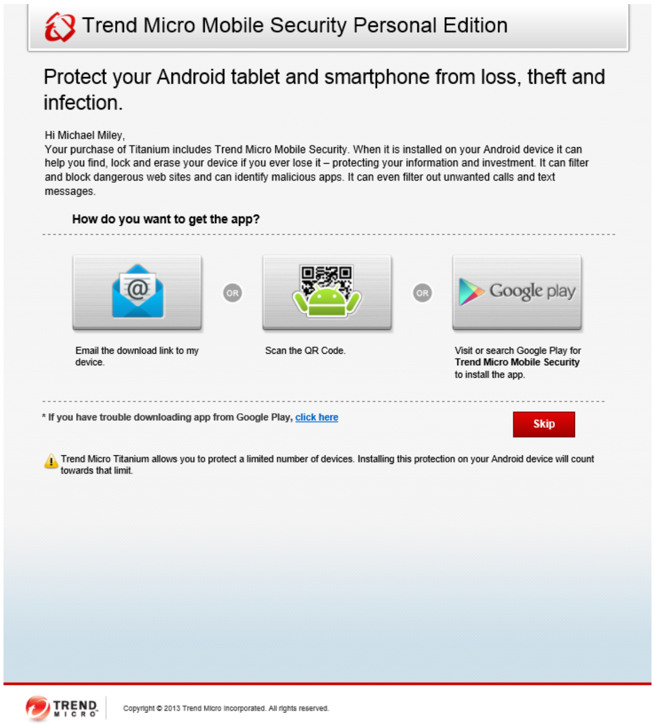
Double-click the installation file and in the window that opens, double-click **Install Trend Micro Titanium**. When asked, provide the serial number below to install the software.

Serial number:

[redacted]

Trend Micro Titanium allows you to protect a limited number of devices. Installing this protection on your Mac will count towards that limit.

Figure 216. Protect Your Mac



Trend Micro Mobile Security Personal Edition

Protect your Android tablet and smartphone from loss, theft and infection.

Hi Michael Miley,
Your purchase of Titanium includes Trend Micro Mobile Security. When it is installed on your Android device it can help you find, lock and erase your device if you ever lose it – protecting your information and investment. It can filter and block dangerous web sites and can identify malicious apps. It can even filter out unwanted calls and text messages.

How do you want to get the app?

Email the download link to my device.

Scan the QR Code.

Visit or search Google Play for **Trend Micro Mobile Security** to install the app.

* If you have trouble downloading app from Google Play, click here

⚠ Trend Micro Titanium allows you to protect a limited number of devices. Installing this protection on your Android device will count towards that limit.

Figure 217. Protect Your Android Tablet or Smartphone

3. Download the software, copy it to the computer you wish to protect, then install it with the serial number displayed on the page.

4. For Android protection, pick how you want to get the app; i.e., Email, QR Code, or Google Play.

5. Note that your subscription to Titanium Internet Security, Maximum Security, and Premium security allows you to protect a limited number of devices. Installing the protection on the additional computer will count towards that limit.

Chapter 9: Applications Bundled with Titanium

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

Table 8. Titanium Bundled Programs

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

*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; the category tabs in the **Titanium Console**, depending on your version of Titanium, as indicated above and in the previous chapters; or right from the **Summary** screen of the **Titanium Console**.

Simply click the **icon** or **hotlink** in the Welcome Page or Titanium Console tab to access the webpage where you can download the applications.

For detailed instructions on how to use these applications, go to www.trendmicro.com to download the relevant Product Guides:

- *Trend Micro™ Mobile Security 3.0 - Product Guide*
- *Trend Micro™ Titanium™ Internet Security for Mac 3.0 - Product Guide*
- *Trend Micro™ DirectPass™ 1.6 - 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*

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.

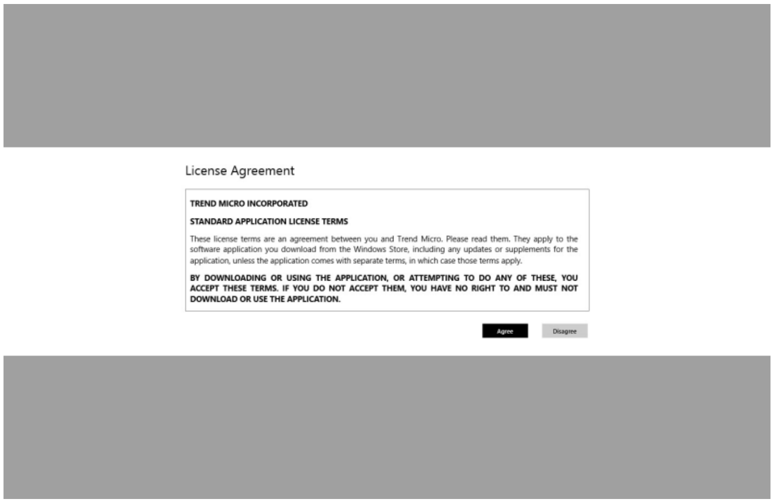
- **Micro™ SafeSurfing** is a secure browser for Windows 8 that has security technology built right in. It provides you with a safer browsing experience by including safe search results ratings, social networking security, and more. Browse the web without worry with Trend Micro SafeSurfing.
- **Trend 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.

SafeSurfing Browser

To use the SafeSurfing browser:

Figure 218. SafeSurfing

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



License Agreement

TREND MICRO INCORPORATED

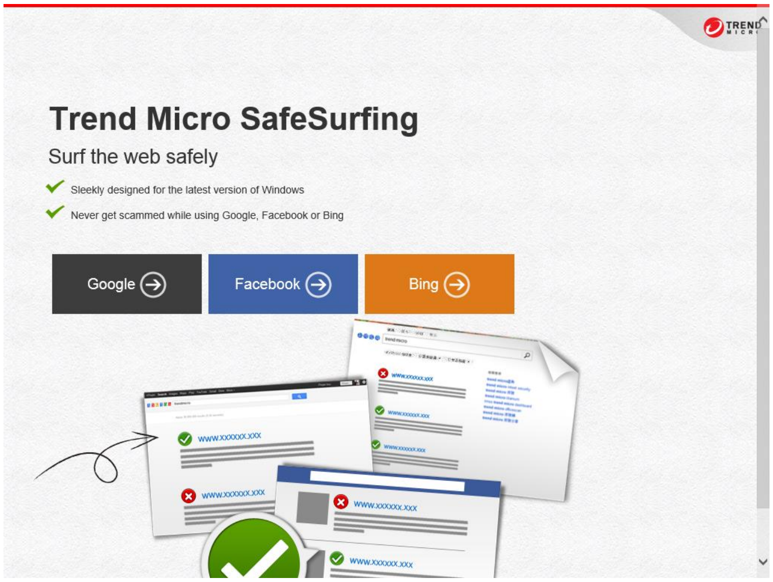
STANDARD APPLICATION LICENSE TERMS

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.

Figure 219. SafeSurfing License Agreement

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



TREND MICRO
Trend Micro SafeSurfing
Surf the web safely
Sleekly designed for the latest version of Windows
Never get scammed while using Google, Facebook or Bing
Google
Facebook
Bing
www.xxxxxx.xxx

Figure 220. SafeSurfing Splash Screen

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

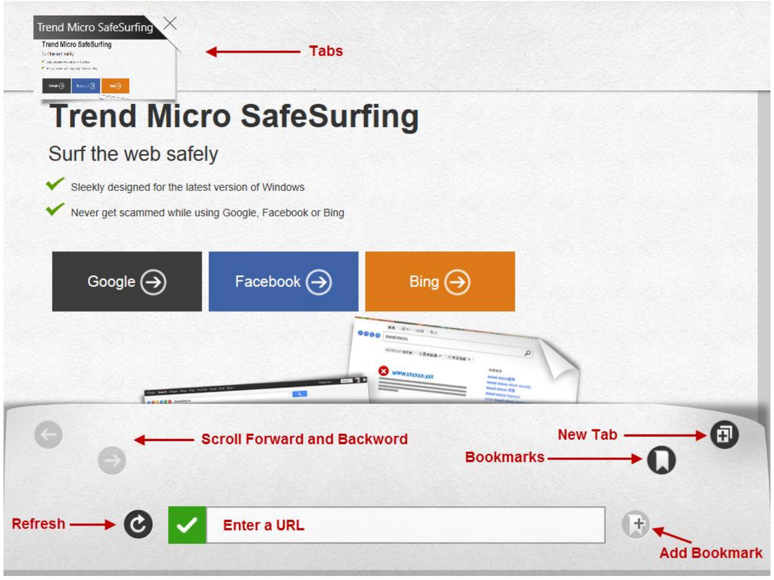
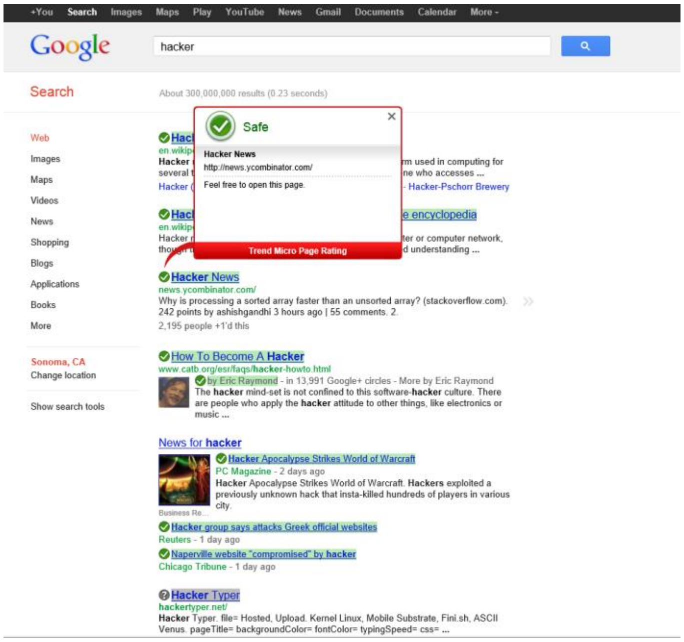


Figure 221. SafeSurfing Menus

4. SafeSurfing'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.



About 300,000,000 results (0.23 seconds)

Hacker News
http://news.ycombinator.com/
Feel free to open this page.

Hacker News
news.ycombinator.com/
Why is processing a sorted array faster than an unsorted array? (stackoverflow.com). 242 points by ashishgandhi 3 hours ago | 55 comments. 2.
2,195 people +1'd this

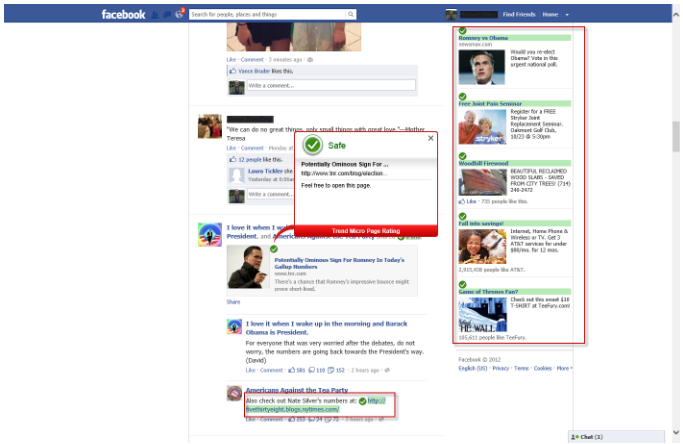
How To Become A Hacker
www.catb.org/esr/faqs/hacker-howto.html
by Eric Raymond - in 13,991 Google+ circles - More by Eric Raymond
The hacker mind-set is not confined to this software-hacker culture. There are people who apply the hacker attitude to other things, like electronics or music ...

News for hacker
Hacker Apocalypse Strikes World of Warcraft
PC Magazine - 2 days ago
Hacker Apocalypse Strikes World of Warcraft. Hackers exploited a previously unknown hack that insta-killed hundreds of players in various city.
Business Re...
Hacker group says attacks Greek official websites
Reuters - 1 day ago
Naperville website "compromised" by hacker
Chicago Tribune - 1 day ago

Hacker Typer
hackertyper.net/
Hacker Typer. file= Hosted, Upload. Kernel Linux, Mobile Substrate, Fini.sh, ASCII Venus. pageTitle= backgroundColor= fontColor= typingSpeed= css= ...

Figure 222. SafeSurfing Safe Search / Link Ratings Results

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


facebook
Search for people, places and things
[redacted]
Find Friends
Home
Like · Comment · 3 minutes ago
Vance Bruder likes this.
Write a comment...
[redacted]
Like · Comment · Monday at
12 people like this.
Laura Tickler
Write a comment...
Safe
Trend Micro Page Rating
Share
Like · Comment · 581 · 110 · 152 · 2 hours ago
Like · Comment · 253 · 24 · 72 · 3 hours ago
Facebook © 2012
English (US) · Privacy · Terms · Cookies · More
Chat (1)

Potentially Ominous Sign For ...
http://www.tnr.com/blog/election...
Feel free to open this page.

"We can do no great things, only small things with great love."—Mother Teresa

I love it when I wake up in the morning and Barack Obama is President. and Americans Against the Tea Party shared

Potentially Ominous Sign For Romney In Today's Gallup Numbers
www.tnr.com
There's a chance that Romney's impressive bounce might prove short-lived.

I love it when I wake up in the morning and Barack Obama is President.
For everyone that was very worried after the debates, do not worry, the numbers are going back towards the President's way. (David)

Americans Against the Tea Party
Also check out Nate Silver's numbers at: http://fivethirtyeight.blogs.nytimes.com/

Romney vs Obama
newsmax.com
Would you re-elect Obama? Vote in this urgent national poll.

Free Joint Pain Seminar
Register for a FREE Stryker Joint Replacement Seminar. Oakmont Golf Club, 10/23 @ 5:30pm

Woodhill Firewood
BEAUTIFUL RECLAIMED WOOD SLABS - SAVED FROM CITY TREES! (714) 240-2472
Like · 735 people like this.

Fall into savings!
Internet, Home Phone & Wireless or TV. Get 3 AT&T services for under $80/mo. for 12 mos.
2,915,438 people like AT&T.

Game of Thrones Fan?
Check out this sweet $10 T-SHIRT at TeeFury.com!
105,611 people like TeeFury.

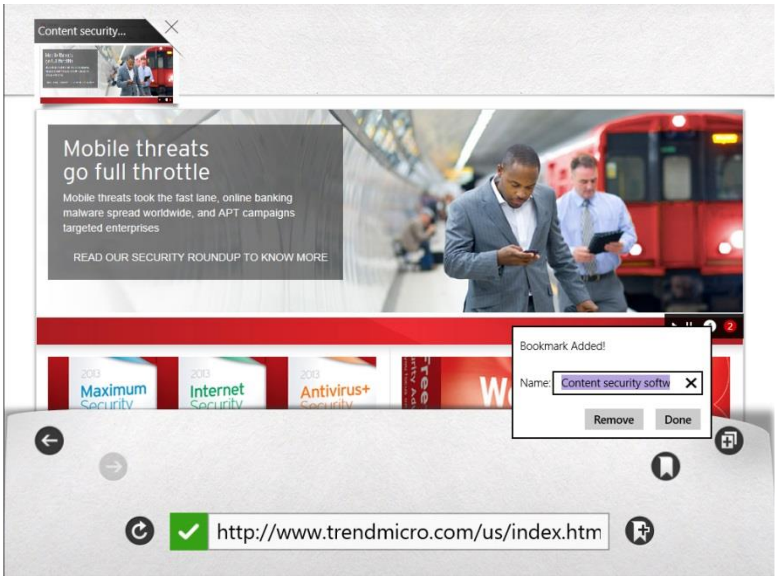
Figure 223. Link Ratings in Facebook

To add / delete a bookmark:

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

3. Open the SafeSurfing menus again by retyping **Windows-Z** on your keyboard.

4. Click the **Add Bookmark** icon. The **Bookmark Added!** popup appears.



Content security...

Mobile threats go full throttle

Mobile threats took the fast lane, online banking malware spread worldwide, and APT campaigns targeted enterprises

READ OUR SECURITY ROUNDUP TO KNOW MORE

Bookmark Added!

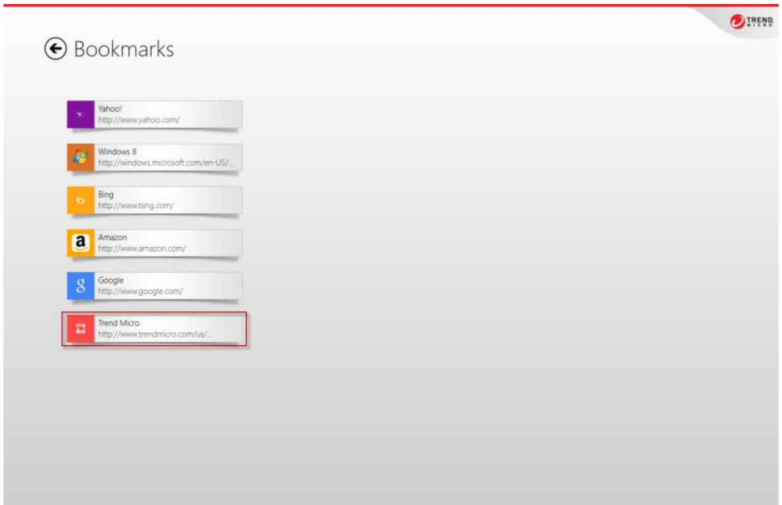
Name: Content security softw

http://www.trendmicro.com/us/index.htm

Figure 224. 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.



Bookmarks

Yahoo!
http://www.yahoo.com/

Windows 8
http://windows.microsoft.com/en-US/...

Bing
http://www.bing.com/

Amazon
http://www.amazon.com/

Google
http://www.google.com/

Trend Micro
http://www.trendmicro.com/us/...

Figure 225. 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.

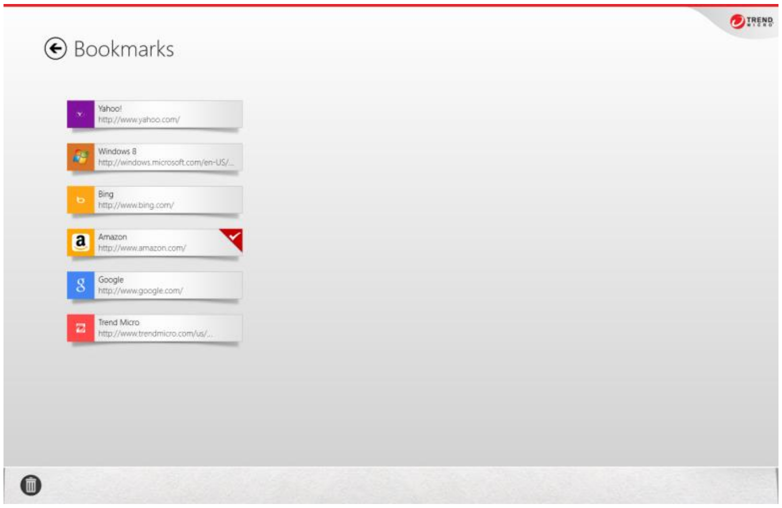


Figure 226. Deleting a Bookmark

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.

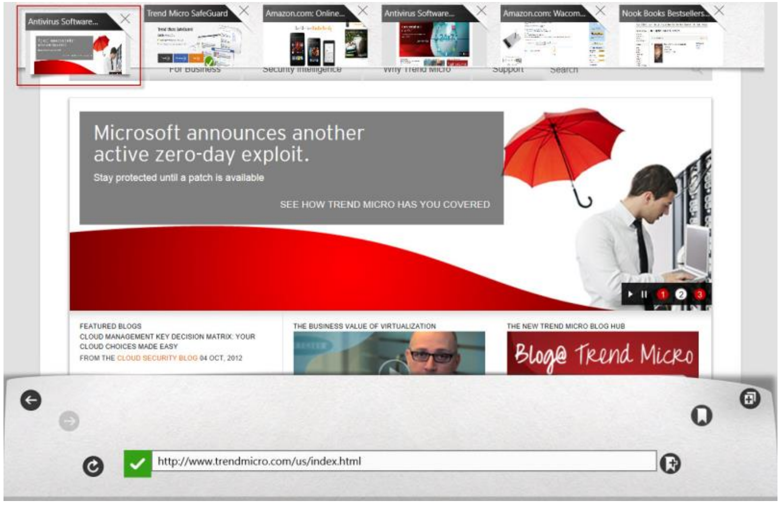

Antivirus Software...
Trend Micro SafeGuard
Amazon.com: Online...
Antivirus Software...
Amazon.com: Wacom...
Nook Books Bestsellers...
Microsoft announces another active zero-day exploit.
Stay protected until a patch is available
SEE HOW TREND MICRO HAS YOU COVERED
FEATURED BLOGS
CLOUD MANAGEMENT KEY DECISION MATRIX: YOUR CLOUD CHOICES MADE EASY
FROM THE CLOUD SECURITY BLOG 04 OCT, 2012
THE BUSINESS VALUE OF VIRTUALIZATION
THE NEW TREND MICRO BLOG HUB
Blog@ Trend Micro
http://www.trendmicro.com/us/index.html

Figure 227. Using Tabs to Browse

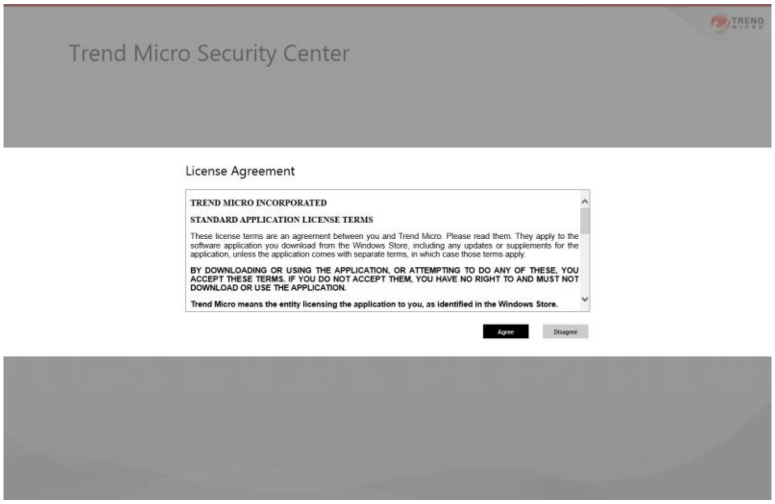
3. Click the **Closebox** (**X**) in a **Tab** to delete it from the **Tabs** menu.

Security Center

To use the Security Center:

Figure 228. Security Center

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



License Agreement

TRENDMICRO INCORPORATED

STANDARD APPLICATION LICENSE TERMS

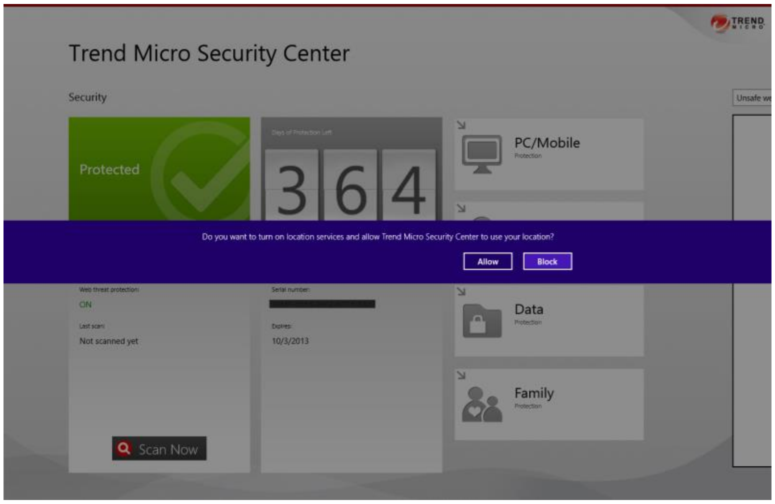
These license terms are an agreement between you and Trend Micro. Please read them. They apply to the software application you download from the Windows Store, including any updates or supplements for the application, unless the application comes with separate terms, in which case those terms apply.

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.

Figure 229. 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?**



Trend Micro Security Center

Do you want to turn on location services and allow Trend Micro Security Center to use your location?

Web threat protection: ON

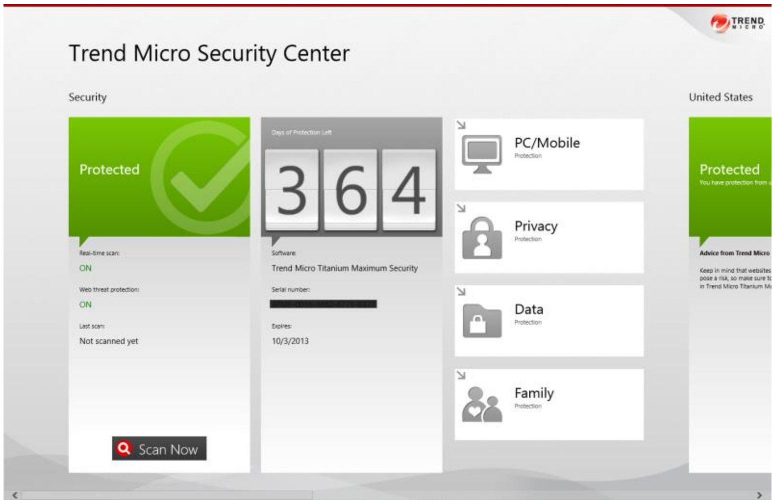
Last scan: Not scanned yet

Serial number: [redacted]

Expires: 10/3/2013

Figure 230. Security Center with Location Popup

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



Trend Micro Security Center

Real-time scan: ON

Web threat protection: ON

Last scan: Not scanned yet

Software: Trend Micro Titanium Maximum Security

Serial number: [redacted]

Expires: 10/3/2013

Figure 231. Protection, License, Titanium Settings

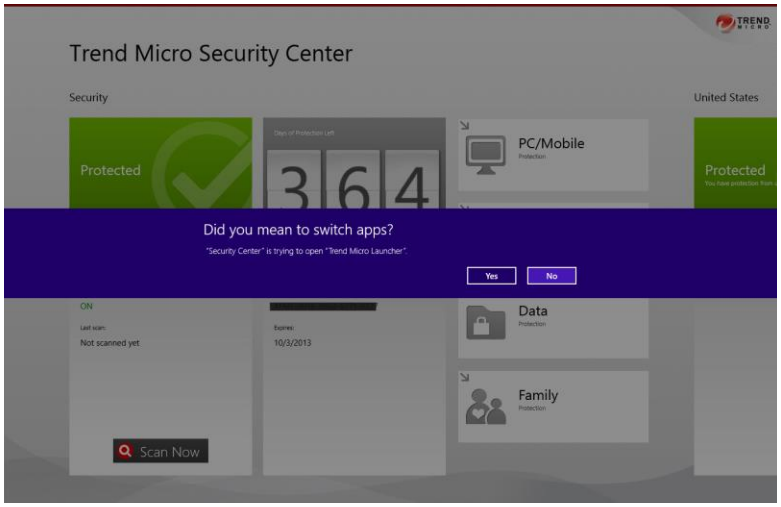
10. The first three panels of the **Security Center** provide essential data and tools:

- **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?**



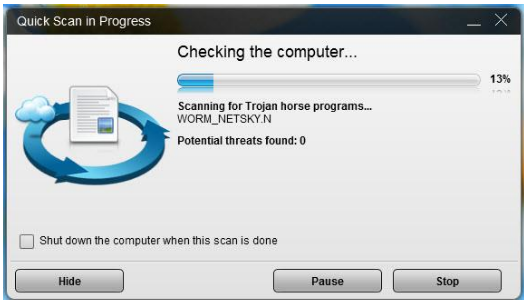
Did you mean to switch apps?

"Security Center" is trying to open "Trend Micro Launcher".

[redacted]

Figure 232. Did You Mean to Switch Apps?

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



Quick Scan in Progress

Checking the computer...

13%

Scanning for Trojan horse programs...
WORM_NETSKY.N

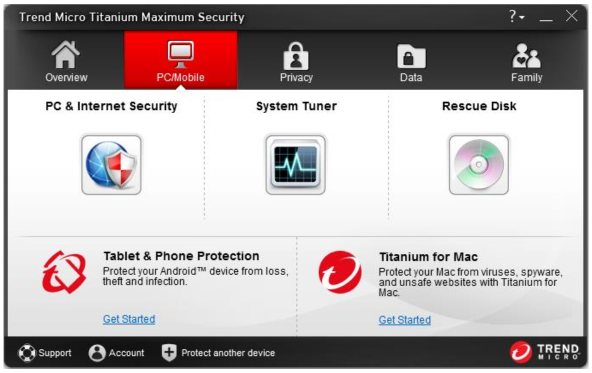
Potential threats found: 0

☐ Shut down the computer when this scan is done

Figure 233. 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.

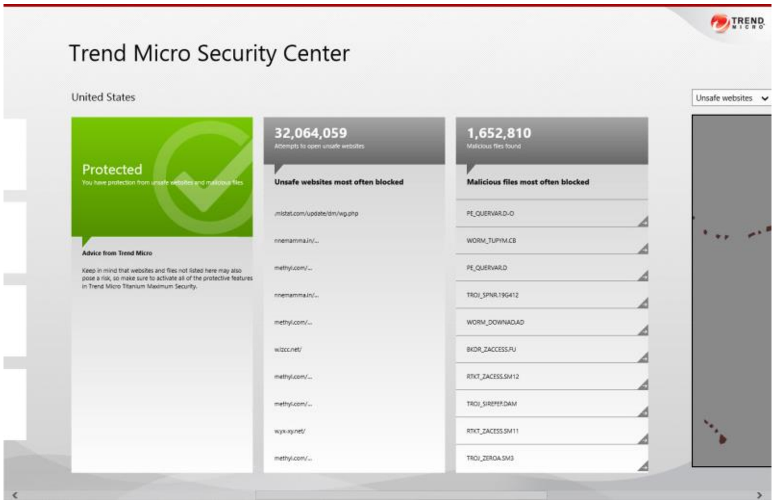


Protect your Android™ device from loss, theft and infection.

Protect your Mac from viruses, spyware, and unsafe websites with Titanium for Mac.

Figure 234. 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.



You have protection from unsafe websites and malicious files

Keep in mind that websites and files not listed here may also pose a risk, so make sure to activate all of the protective features in Trend Micro Titanium Maximum Security.

32,064,059
Attempts to open unsafe websites

Unsafe websites most often blocked

- .mlstat.com/update/dm/wg.php
- nnemamma.in/...
- methyl.com/...
- nnemamma.in/...
- methyl.com/...
- w.izcc.net/
- methyl.com/...
- methyl.com/...
- wyx-xy.net/
- methyl.com/...

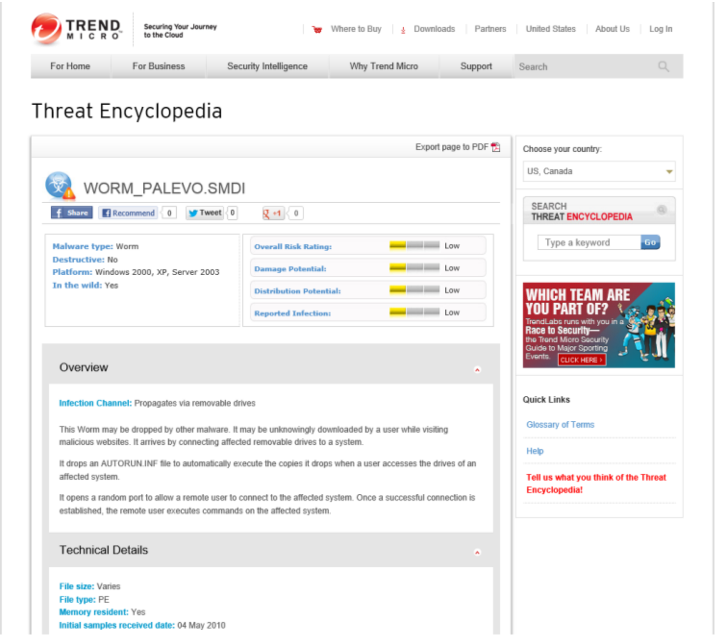
1,652,810
Malicious files found

Malicious files most often blocked

- PE_QUERVAR.D-O
- WORM_TUPYM.CB
- PE_QUERVAR.D
- TROJ_SPNR.19G412
- WORM_DOWNAD.AD
- BKDR_ZACCESS.FU
- RTKT_ZACESS.SM12
- TROJ_SIREFEF.DAM
- RTKT_ZACESS.SM11
- TROJ_ZEROA.SM3

Figure 235. 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**.



Threat Encyclopedia

WORM_PALEVO.SMDI

Malware type: Worm
Destructive: No
Platform: Windows 2000, XP, Server 2003
In the wild: Yes

Overall Risk Rating:	Low
Damage Potential:	Low
Distribution Potential:	Low
Reported Infection:	Low

Overview

Infection Channel: Propagates via removable drives

This Worm may be dropped by other malware. It may be unknowingly downloaded by a user while visiting malicious websites. It arrives by connecting affected removable drives to a system.

It drops an AUTORUN.INF file to automatically execute the copies it drops when a user accesses the drives of an affected system.

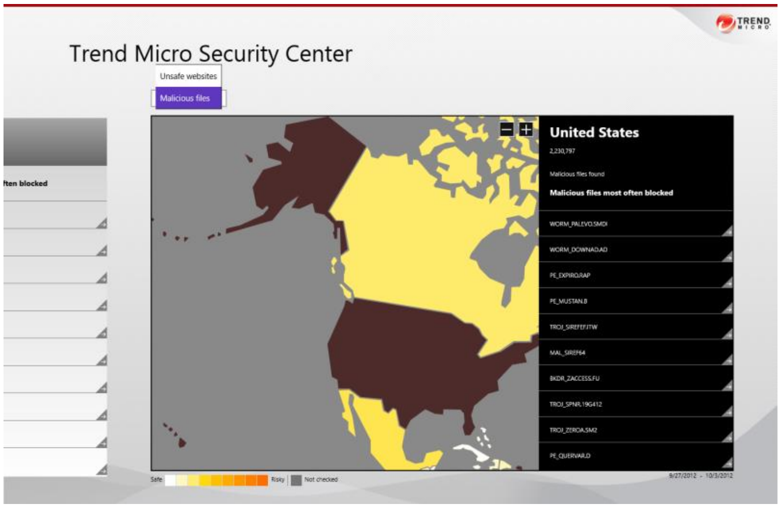
It opens a random port to allow a remote user to connect to the affected system. Once a successful connection is established, the remote user executes commands on the affected system.

Technical Details

File size: Varies
File type: PE
Memory resident: Yes
Initial samples received date: 04 May 2010

Figure 236. 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.



United States
2,230,797
Malicious files found
Malicious files most often blocked

WORM_PALEVO.SMDI
WORM_DOWNAD.AD
PE_EXPIRO.RAP
PE_MUSTAN.B
TROJ_SIREFEF.ITW
MAL_SIREF64
BKDR_ZACCESS.FU
TROJ_SPNR.19G412
TROJ_ZEROA.SM2
PE_QUERVAR.D

9/27/2012 - 10/3/2012

Figure 237. 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.

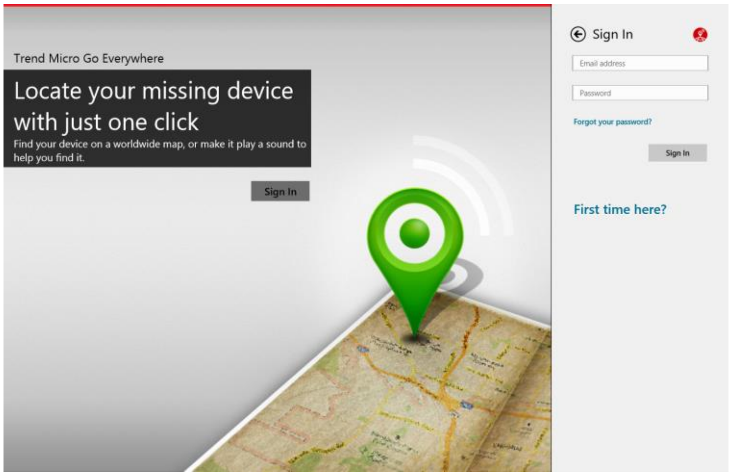
20. Use the popup menu to toggle the Regional Map between **Unsafe Websites** and **Malicious Files** in the **Security Center**.

Go Everywhere

To use Go Everywhere:

Figure 238. Go Everywhere

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



Trend Micro Go Everywhere

Locate your missing device with just one click

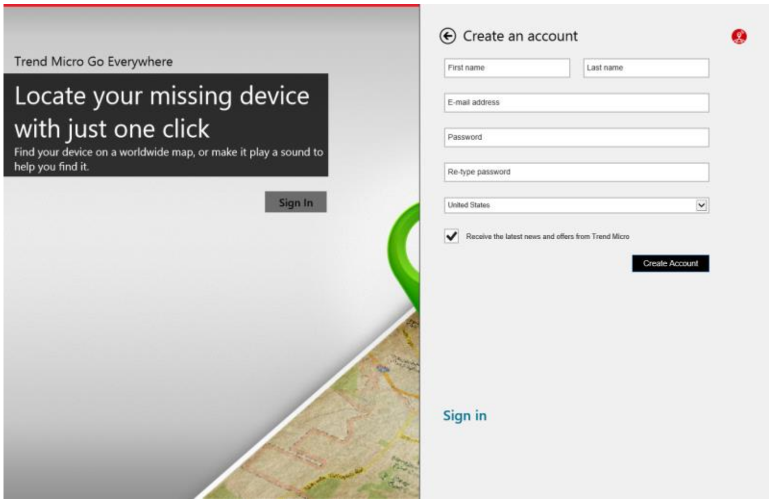
Find your device on a worldwide map, or make it play a sound to help you find it.

Figure 239. 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.



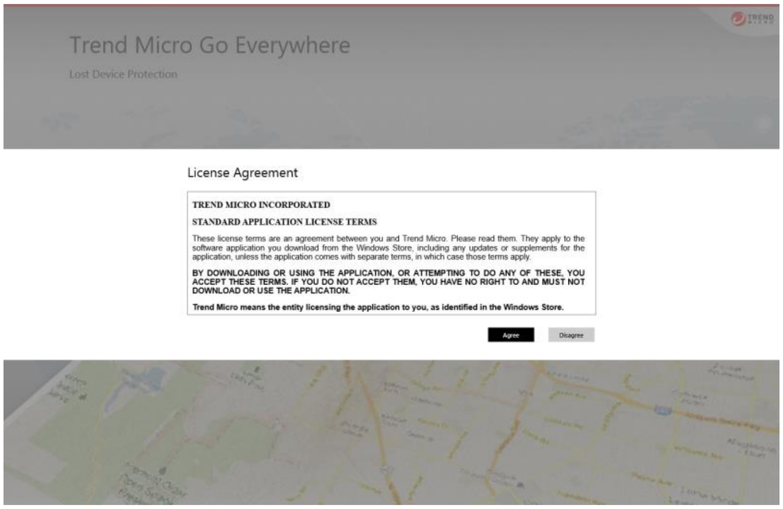
Trend Micro Go Everywhere

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.

Figure 240. Create an Account

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



TRENDMICRO INCORPORATED

STANDARD APPLICATION LICENSE TERMS

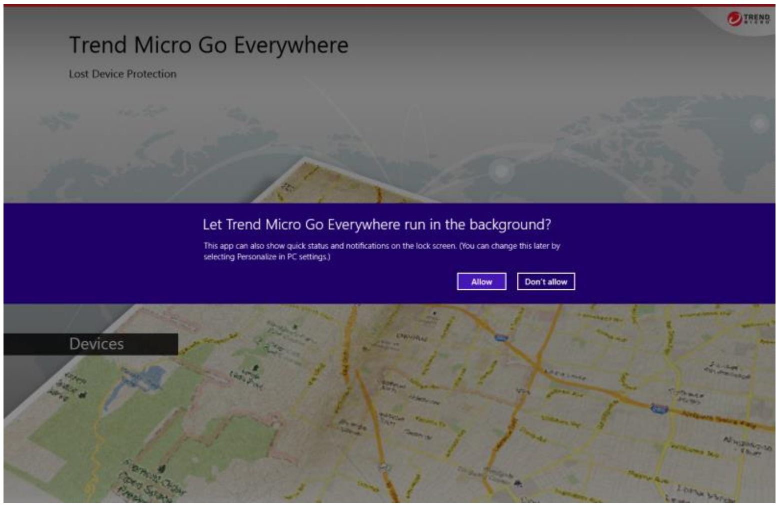
These license terms are an agreement between you and Trend Micro. Please read them. They apply to the software application you download from the Windows Store, including any updates or supplements for the application, unless the application comes with separate terms, in which case those terms apply.

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.

Figure 241. 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?**



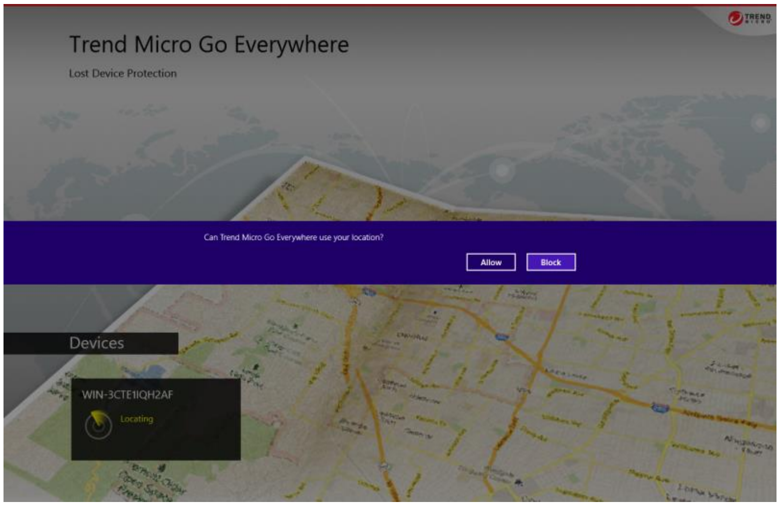
Let Trend Micro Go Everywhere run in the background?

This app can also show quick status and notifications on the lock screen. (You can change this later by selecting Personalize in PC settings.)

Figure 242. Run In The Background?

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

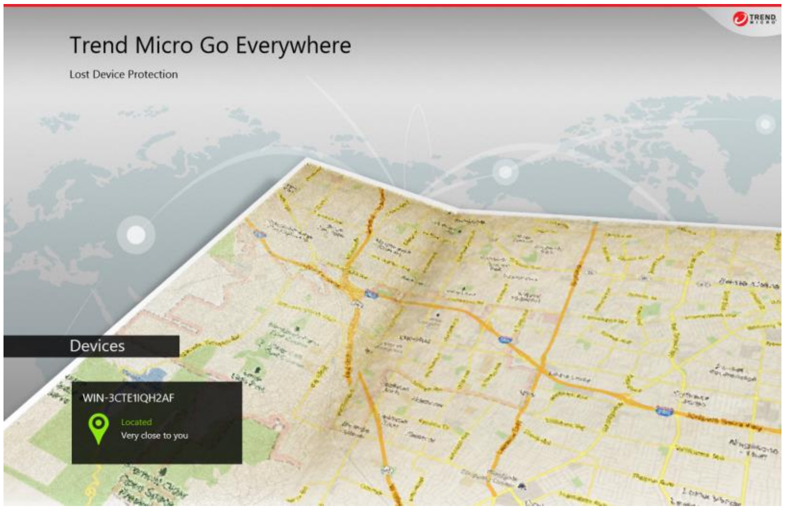
Note: **For tablets and smart phones, Go Everywhere uses GPS. For laptops and desktops, Go Everywhere uses the nearest access point and IP Address, which is less accurate.**



Can Trend Micro Go Everywhere use your location?

Figure 243. Use Your Location?

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



Trend Micro Go Everywhere

Lost Device Protection

Devices

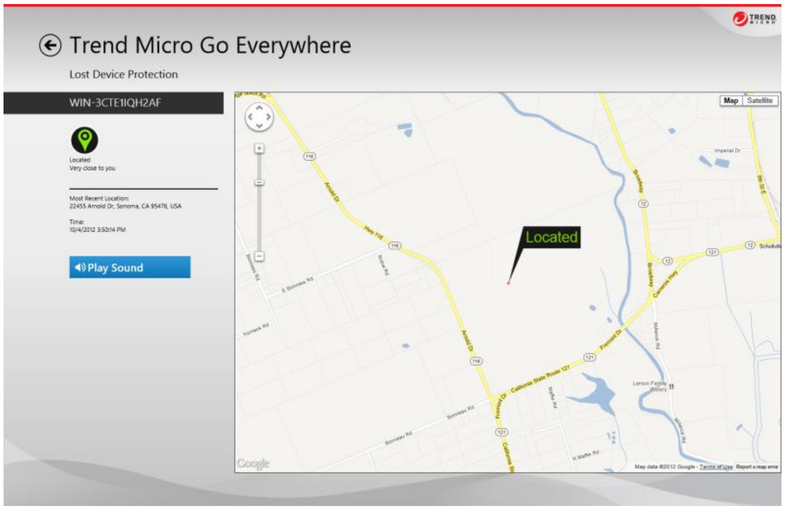
WIN-3CTE1IQH2AF

Located

Very close to you

Figure 244. 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.



Trend Micro Go Everywhere

Lost Device Protection

WIN-3CTE1IQH2AF

Located

Very close to you

Most Recent Location:

22455 Arnold Dr, Sonoma, CA 95476, USA

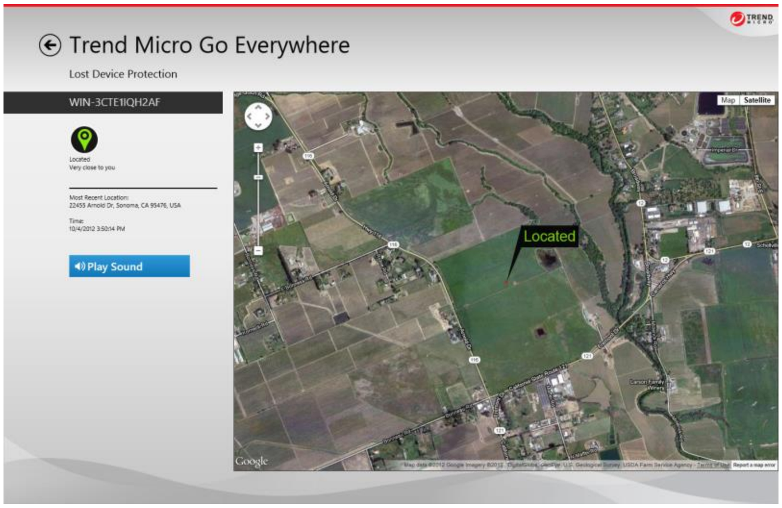
Time:

10/4/2012 3:50:14 PM

Figure 245. 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.



Trend Micro Go Everywhere

Lost Device Protection

WIN-3CTE1IQH2AF

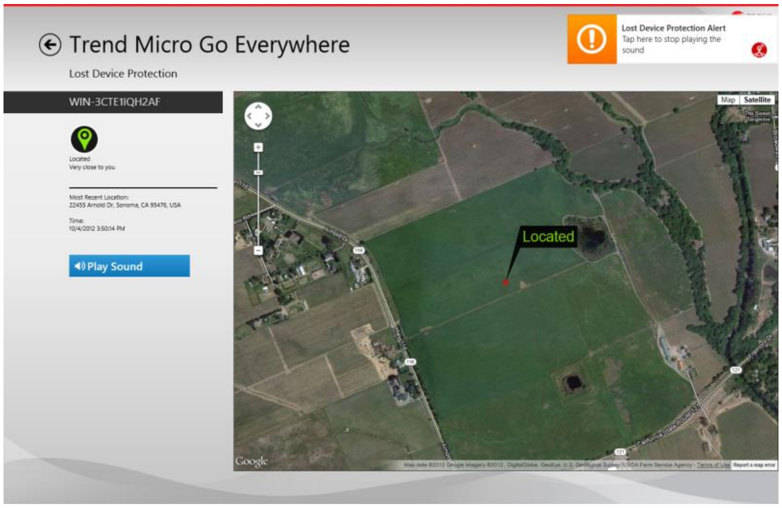
Located:
Very close to you

Most Recent Location:
22455 Arnold Dr, Sonoma, CA 95476, USA

Time:
10/4/2012 3:50:14 PM

Figure 246. 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.



Trend Micro Go Everywhere

Lost Device Protection

Lost Device Protection Alert
Tap here to stop playing the sound

WIN-3CTE1IQH2AF

Located:
Very close to you

Most Recent Location:
22455 Arnold Dr, Sonoma, CA 95476, USA

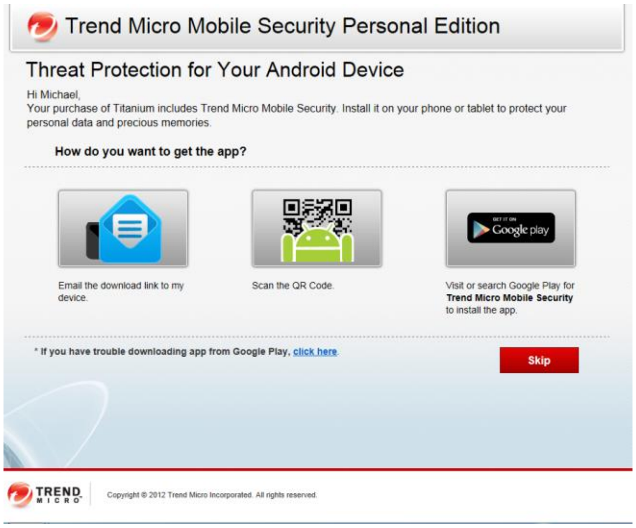
Time:
10/4/2012 3:50:14 PM

Figure 247. Lost Device Protection Alert

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

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.



Trend Micro Mobile Security Personal Edition

Threat Protection for Your Android Device

Hi Michael,
Your purchase of Titanium includes Trend Micro Mobile Security. Install it on your phone or tablet to protect your personal data and precious memories.

How do you want to get the app?

Email the download link to my device.

Scan the QR Code.

Visit or search Google Play for **Trend Micro Mobile Security** to install the app.

* **If you have trouble downloading app from Google Play, click here.**

Copyright © 2012 Trend Micro Incorporated. All rights reserved.

Figure 248. Trend Micro Mobile Security Personal Edition

Mobile Security protections include the following:

Trend Micro Mobile Security for Android

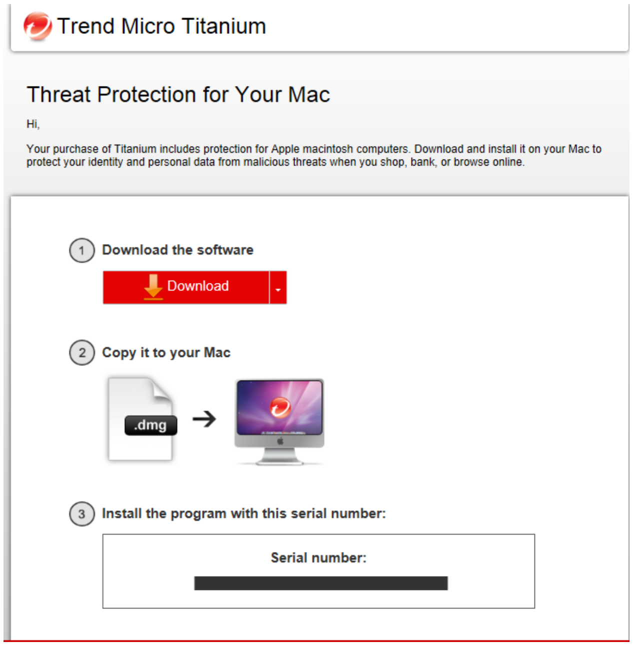
- Locate, lock and remotely erase data if your device is lost or stolen
- Block unwanted calls and texts
- Scan apps for viruses and other threats
- Enable parental controls to keep kids safe

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

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



Trend Micro Titanium

Threat Protection for Your Mac

Hi,

Your purchase of Titanium includes protection for Apple macintosh computers. Download and install it on your Mac to protect your identity and personal data from malicious threats when you shop, bank, or browse online.

1 Download the software

2 Copy it to your Mac

3 Install the program with this serial number:

Serial number: [redacted]

Figure 249. 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

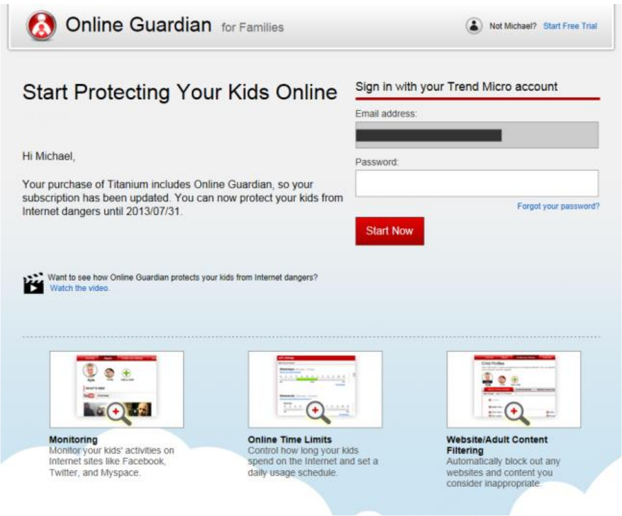
- Restricts Internet access by content categories
- Controls access to chat and IM sites
- Allows you to block specific websites

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 SafeSurfing 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.



Start Protecting Your Kids Online

Hi Michael,

Your purchase of Titanium includes Online Guardian, so your subscription has been updated. You can now protect your kids from Internet dangers until 2013/07/31.

Sign in with your Trend Micro account

Email address: [redacted]

Password:

Want to see how Online Guardian protects your kids from Internet dangers? Watch the video.

Monitoring
Monitor your kids' activities on Internet sites like Facebook, Twitter, and Myspace.

Online Time Limits
Control how long your kids spend on the Internet and set a daily usage schedule.

Website/Adult Content Filtering
Automatically block out any websites and content you consider inappropriate.

Figure 250. Trend Micro Online Guardian for Families

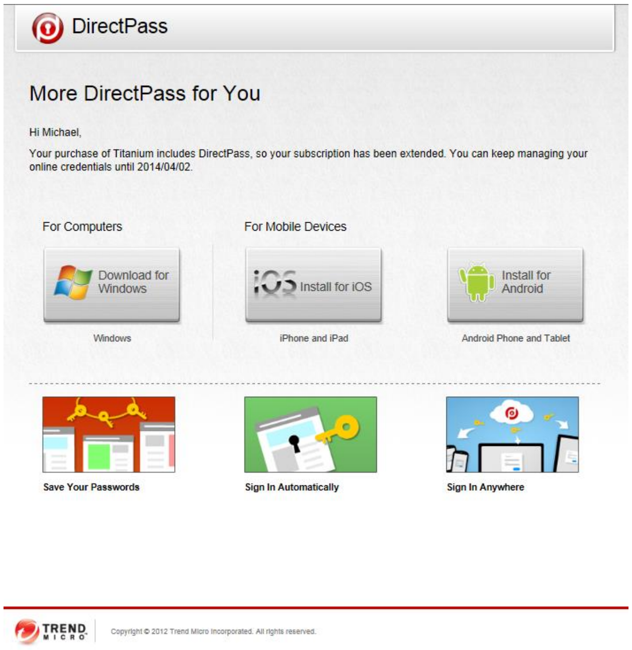
Key features include:

- 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.



More DirectPass for You

Hi Michael,

Your purchase of Titanium includes DirectPass, so your subscription has been extended. You can keep managing your online credentials until 2014/04/02.

Copyright © 2012 Trend Micro Incorporated. All rights reserved.

Figure 251. Trend Micro DirectPass

DirectPass features include:

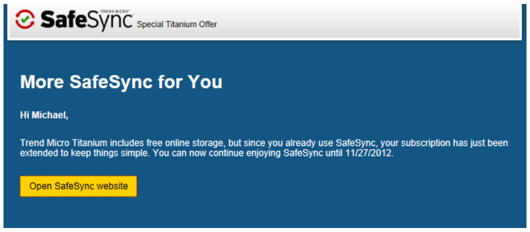
- **URL and Password Management -** Automatically capture your websites and password login credentials in a complete secure environment
- **Cloud Storage and Synchronization -** Credentials are available across all devices where DirectPass is installed
- **Password Generator -** Automatically generate 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.

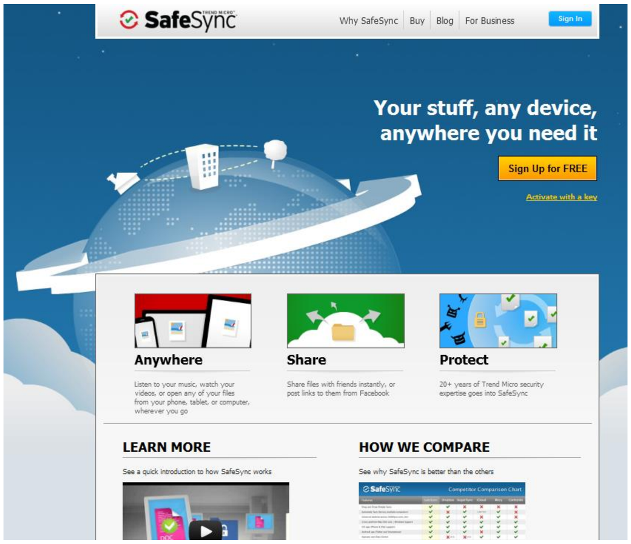


More SafeSync for You

Hi Michael,

Trend Micro Titanium includes free online storage, but since you already use SafeSync, your subscription has just been extended to keep things simple. You can now continue enjoying SafeSync until 11/27/2012.

Figure 252. More SafeSync for You



Your stuff, any device, anywhere you need it

Anywhere

Listen to your music, watch your videos, or open any of your files from your phone, tablet, or computer, wherever you go

Share

Share files with friends instantly, or post links to them from Facebook

Protect

20+ years of Trend Micro security expertise goes into SafeSync

LEARN MORE

See a quick introduction to how SafeSync works

HOW WE COMPARE

See why SafeSync is better than the others

Figure 253. 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 SafeSurfing 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

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.

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.