

**Volume**

**6**

TRUSTDEFENDER CLIENT

---

Symbiotic Technologies Pty Ltd

# TrustDefender User Guide

SYMBIOTIC TECHNOLOGIES PTY LTD

# TrustDefender User Guide

---

© Symbiotic Technologies Pty Ltd  
5 Gladstone St,  
Lilyfield, NSW, 2040, Australia  
<http://www.trustdefender.com>

---

# Table of Contents

1	Introduction .....	1
1.1	Overview .....	1
1.2	Supported Platforms.....	1
1.2.1	Platform Roadmap.....	1
1.2.2	Hardware .....	2
2	Installation.....	3
2.1	Software Installation .....	3
2.2	First Time Startup of TrustDefender .....	3
2.2.1	License Choose Wizard.....	4
2.2.2	Tutorial.....	4
2.2.3	TrustDefender Login.....	5
2.2.4	TrustDefender Evaluation Message .....	6
2.3	Quick start / Walkthrough .....	6
2.3.1	Scenario 2: Client only protection.....	6
2.3.2	Scenario 1: Website is secured with the TrustDefender Enterprise Server (Client / Server Protection).....	8
3	Introduction / How TrustDefender works .....	10
4	Features.....	11
4.1	Free Edition vs. Gold Edition.....	11
4.2	GAP Protection.....	12
4.3	Secure Lockdown.....	14
4.4	TrustedSurfing Database .....	14
4.5	Menu .....	17
4.6	Control Center .....	18
4.6.1	Control Panel / Security Status.....	18
4.6.2	Webfingerprints.....	20
4.6.3	GAP Protection .....	22
4.6.4	Add Secure Favorite .....	24
4.6.5	Show GAP Participant Info / GAP Participant .....	24
4.6.6	Show GAP Participant Info / Secure Policies .....	25
4.6.7	Auto Safe&Secure .....	25

---

	4.6.8	Web Protection .....	27
	4.6.9	User Lockdown Policies.....	27
4.7		Preferences .....	28
	4.7.1	General .....	28
	4.7.2	Trust & Scan Settings .....	31
	4.7.3	My Account / Privacy .....	33
	4.7.4	.....	33
4.8		Safe&Secure Mode .....	34
	4.8.1	Unknown Applications .....	35
	4.8.2	Security Status.....	36
	4.8.3	Known Applications .....	37
	4.8.4	User Allowed Applications .....	38
4.9		Web Browser Extension .....	38
4.10		Secure Favorites .....	39
	4.10.1	Add Secure Favorites to the Quick-Launch Menu.....	39
	4.10.2	Use Secure Favorites in the Quick-Launch Menu .....	40
4.11		TrustDefender in Corporate Environments .....	41
	4.11.1	Administrator vs. Non-Administrator Rights.....	41
	4.11.2	Internet Access / Upstream Proxy Servers.....	41
5		Web Protection Policy Editor .....	43
6		Appendix.....	45
	6.1	Figures .....	45
	6.2	Index .....	45

---

# 1 Introduction

## 1.1 Overview

TrustDefender is a security software that will analyze all outgoing internet transmissions on your computer. With its GAP Protection (Guaranteed Authentication Program) TrustDefender is able to guarantee the Authenticity of Web-Servers . Once the GAP Protection Mode can be established, TrustDefender will automatically activate the "Secure Lockdown" – a framework of checks to evaluate whether your computer complies with the Security Policies defined by the Online Business. Together with the Safe&Secure Mode, the Website GAP Policies and the Two Factor Authentication, TrustDefender is the only complete On Demand Endpoint Security Solution available on the market today – one that truly integrates both ends of the connection (User's PC and Web server) into a security chain to protect the end user at home as well as the online business.

### General Solution

TrustDefender has been proven to be a general solution against threats like Phishing, Pharming, Trojan/Virus/Malware and Keylogger Attacks and also for online injection attacks like XSS.

## 1.2 Supported Platforms

The TrustDefender Client runs on all major Microsoft Operating Systems:

- Windows™ NT
- Microsoft Windows™ 98/98 Second edition
- Windows™ ME
- Windows™ XP Home Edition/Professional SP1 and SP2
- Windows™ 2000
- Windows™ Vista

### 1.2.1 Platform Roadmap

- MacOS

- Linux
- Symbian

**1.2.2 Hardware**

- Intel Pentium 3 or above
- All platforms running Windows

**Browser Note:** TrustDefender software operates independently of the Browsers giving greater flexibility, application to meet varying customer requirements and security

Therefore operating with but not limited to:

- Microsoft™ IE
- Netscape
- AOL
- Firefox
- Opera

## 2 Installation

### 2.1 Software Installation

The Installation of the TrustDefender Client Software should be straightforward. The Software itself is just a 1.3 MByte Download.

Please follow the installation instructions and TrustDefender will automatically be installed on your machine.



**Note:** The TrustDefender Installation will need Administrator Privileges to run. However only restricted user privileges are needed to run the software.

There is no need to restart Windows after Installation; however you should close all open Web browser Windows.

### 2.2 First Time Startup of TrustDefender

After the Installation, you should see the orange TrustDefender Logo in the System Tray on the lower right corner of your screen.



TrustDefender will need to configure itself during the first startup of the software.

In the first dialog, you can choose the TrustDefender License. For a complete comparison of the different Editions, please refer to Chapter “Free Edition vs. Gold Edition”.

2.2.1 License Choose Wizard

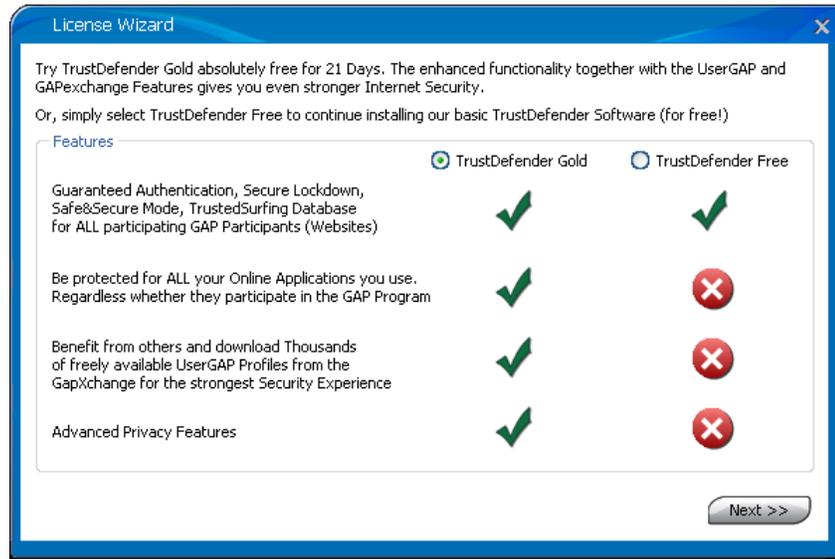


Figure 1 - License Choose Wizard

After choosing the TrustDefender Gold-Edition, you'll have to enter your License details. Please enter the Name and License Key that you have obtained either on your CD or via email from the Online Shop.

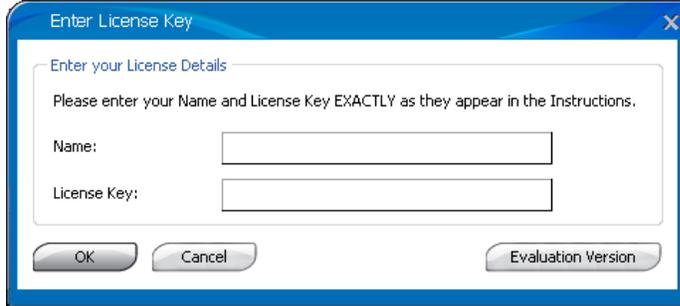


Figure 2 - License Key Dialog

In case you want to try TrustDefender for 21 days, just click on the “Evaluation Version” Button.

2.2.2 Tutorial

TrustDefender will show a short tutorial during startup. Please take a minute and read through the different pages. Use the buttons “Back” and “Next” for navigation. If you do not wish to see the tutorial again, please check the box “Don't show this page again”.



Note: You can always reactivate the tutorial from the Preferences Menu at a later stage.

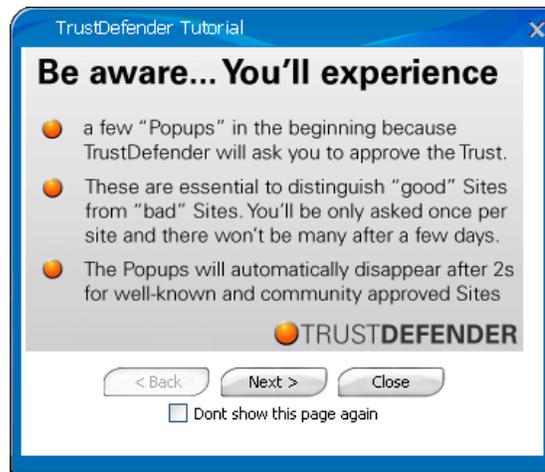


Figure 3 - Tutorial

### 2.2.3 TrustDefender Login

If you haven't done so, it is highly recommended to register as a TrustDefender User on our website at <http://www.trustdefender.com>. You can use the same Username and Password for the TrustDefender Software.



Figure 4 - TrustDefender Login

If you do not wish to use this feature, just click on "Disable this Feature" and click on "Sign In". This will disable this feature and you won't be asked again.

### 2.2.4 TrustDefender Evaluation Message

If you have an evaluation license of TrustDefender, you will be notified of the period during the startup of the software.

- **Leave Feedback** – Allows the user to leave feedback in respect to their user experience and make suggestions.
- **Upgrade to Gold Edition** – Allows the user to upgrade their evaluation edition to the Gold Edition.
- **Continue** – Allows the user to continue to use the evaluation edition of TrustDefender.

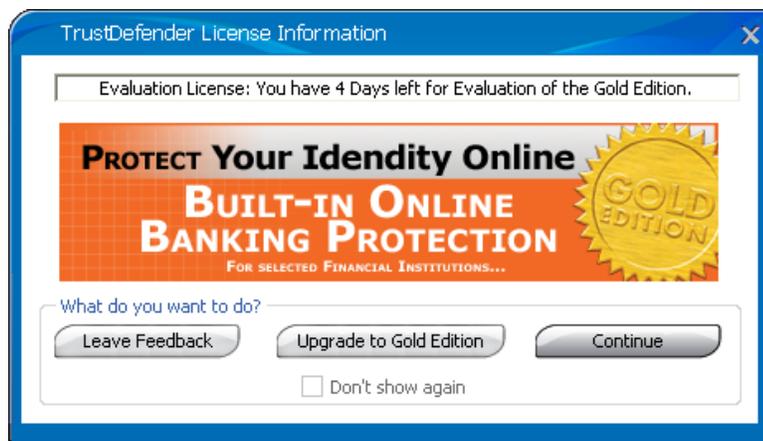


Figure 5 - TrustDefender License Information Dialog

## 2.3 Quick start / Walkthrough

For the impatient reader, the Quick Start will walk you through the main features of the software.

### 2.3.1 Scenario 2: Client only protection

To see the various features of TrustDefender in action, please go through this live-demonstration.

- Step 1. Open a new Web browser and go to <http://www.macquarie.com.au>
- Step 2. Click on Login → Personal on the right hand side of the screen.

- You'll see the GAP Window appear in the lower right corner of your Screen.
- At the same time, TrustDefender will activate the Safe&Secure Mode to check the Authenticity of all running applications and programs.
- Once the GAP Window is activated, the Secure Lockdown will also be activated.

Step 3. The Login Screen for the Internet Banking Application appears. Before you actually submit any info, click on the “Show GAP Info” Button of the GAP window

- The "Show GAP Info" provides further evidence and business information to assure that you are connected to the correct site.
- The "Security Policies" Tab further educates about the Internet Security Policy.

Step 4. You can now safely log in (we skip this part in the demonstration).

Step 5. To see that TrustDefender will only allow Web requests belonging to Macquarie Bank, please open another browser window, and

Step 6. Go to e.g. <http://www.google.com> and you should see a window of TrustDefender telling you that he has blocked the Request

- During the Secure Lockdown Situation, TrustDefender will only allow Web requests that belong to the Application of the GAP Participant (Westpac Bank in this case)

Step 7. Click on “Finish Secure Lockdown” to end the Secure Lockdown Situation and refresh the Request to Google and you should see the Google homepage.

- Whenever the Secure Lockdown Situation is terminated, all Internet Requests are allowed again.

We have seen in this little demonstration how TrustDefender

- Shows you that you are really where you want to be (→ Authentication)
- Prevents any online Attack (like XSS) or keyloggers trying to interfere with the Webrequests of the Online Application. (→ Secure Lockdown)
- Educates about the Security Policies of the Online Business (→ GAP Window, Security Policies)
- Shows all unknown and potential malicious Software/Applications that run on your computer. (→ Safe&Secure Mode)

**2.3.2 Scenario 1: Website is secured with the TrustDefender Enterprise Server (Client / Server Protection)**

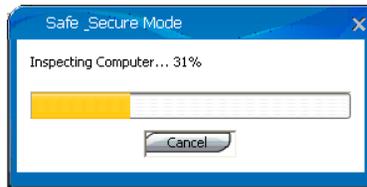
Step 1. Open a new Web browser and go to <http://www.trustdefender.com>.

**Note:** You should see that the orange icon in the Tray Bar is “pumping”.

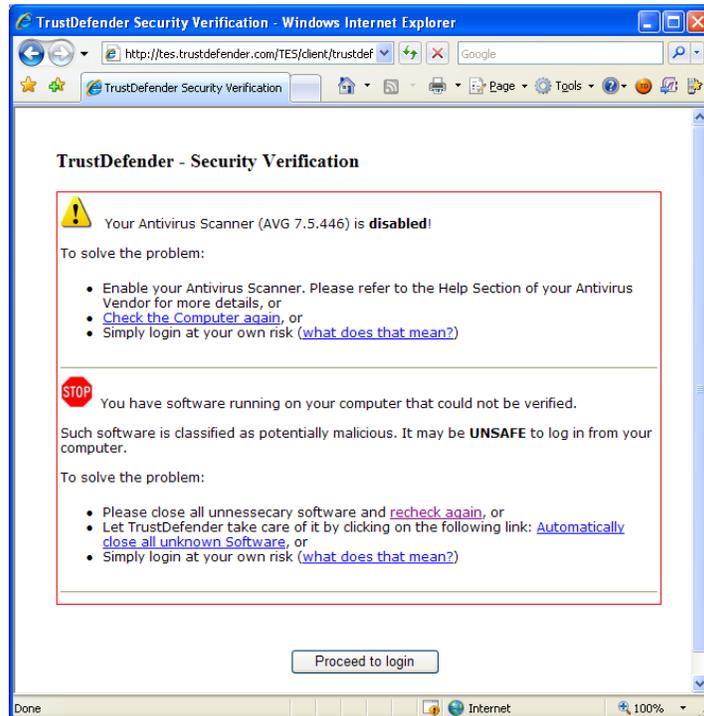
Step 2. Click on the “Live Demonstration” Button on the left hand side of the Menu.



a. You should not automatically see the Safe&Secure scan window coming up, scanning your computer.

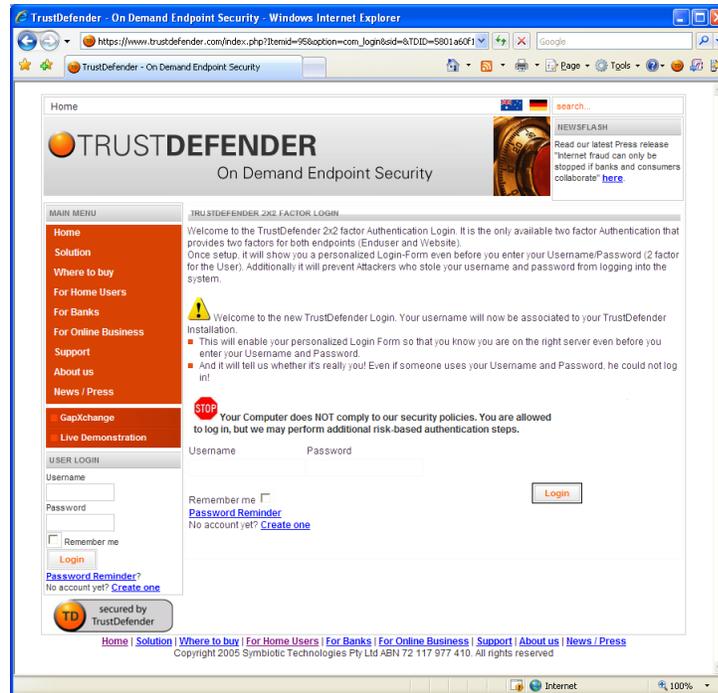


Step 3. TrustDefender will now automatically check the security policies on your computer and will automatically forward you to the login form if everything is fine. If your computer does not comply to all security policies, you'll get an information message from the TrustDefender Enterprise Server which may look similar to this:

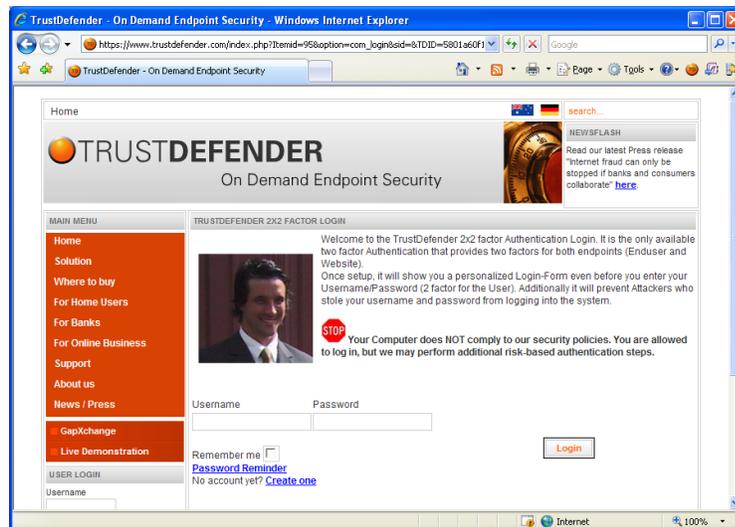


## TRUSTDEFENDER USER GUIDE

Step 4. If you click on “Proceed to login”, you’ll be forwarded to the login form with a notice that you knowingly accepted the verification



Step 5. Once logged in, you can choose a picture that relates to you personally and select it. This picture will from now on be displayed on the page \_before\_ you put in your credentials. See the following screenshots:



## **3 Introduction / How TrustDefender works**

## 4 Features

TrustDefender is a true online security solution and offers many features missing from traditional Antivirus products. It allows a strong security chain including the online service (e.g. bank) and your computer. Furthermore the Safe&Secure Mode with its white listing approach fills the Gap that is left open by existing security solutions in the market today.

### 4.1 Free Edition vs. Gold Edition

The following matrix compares the features of the Free and the Gold Edition of TrustDefender.

	Free Edition	Gold Edition
<b>GAP Protection</b> <ul style="list-style-type: none"> <li>- GAP Window</li> <li>- Secure Lockdown</li> <li>- Safe &amp; Secure Mode</li> </ul>		
<b>Website Protection</b> <ul style="list-style-type: none"> <li>- GAP Window</li> <li>- Secure Lockdown</li> <li>- Safe &amp; Secure Mode</li> </ul>		
<b>Secure Favorites</b>		
<b>Built-in Banking Protection</b>		
<b>Advanced Privacy Features</b>		
<b>Auto Safe&amp;Secure Mode</b>		

TrustedSurfing Database		
Auto Community Approval		

## 4.2 GAP Protection

GAP is an acronym for “Guaranteed Authentication Profile” and stands for a complete security protection for one particular website. The “Guaranteed Authentication Program” (GAP) Mode is part of the TrustDefender software and provides a means to unambiguously identify the web service provider (e.g. online bank) and enables the “Secure Lockdown” of a user’s computer described later.

We have two different types of Web Protections:

- The “official” GAP Protection – comprised by Online Services which have submitted their Web Protection Profile and maintain it.
- The Website Protection – this is a list of online services that are maintained either from the Community itself or from TrustDefender.

Depending on the policies used, TrustDefender will activate the Safe&Secure Mode (see chapter “Safe&Secure Mode”). Once the GAP Protection has been activated, you’ll see the following dialog in the lower right corner of your screen.



Figure 6 - GAP Window



Please note that this dialog box is partly transparent to prevent spoofing.

As long as this window is open, you can be assured that TrustDefender is protecting the current online transaction as follow:

## TRUSTDEFENDER USER GUIDE

- The Safe&Secure Mode will check your computer for unknown software (depending on the Security Policies)
- The Secure Lockdown will be activated and TrustDefender will only allow Internet Requests to the chosen Online Service (depending on the Security Policies)
- **Show Gap Info** button provides the user with verification information regarding the secured website being visited by the user. See figure.....
- **Close Protection** button allows the user to shut down the security provided by TrustDefender during the online session.

### 4.3 Secure Lockdown

Once the GAP Protection described in the previous section can be enabled, TrustDefender will “lock down” the user’s computer as defined in the Security Policies by the GAP Participant. For the first time ever, the Online Business’ can not only give security advices to their customers, but they can pro-actively make sure that only “safe” computers that comply with the Security Policies are granted access to their systems (or at least notify the user that his computer doesn’t comply).

This Lockdown is doe using a built-in low-level TCP/IP Firewall that works on a Host, IP or SSL Certificate level. During the Secure Lockdown only Requests that are approved in the GAP Policies will be allowed.

The GAP Program and the Secure Lockdown are best described by the illustration on the following page.

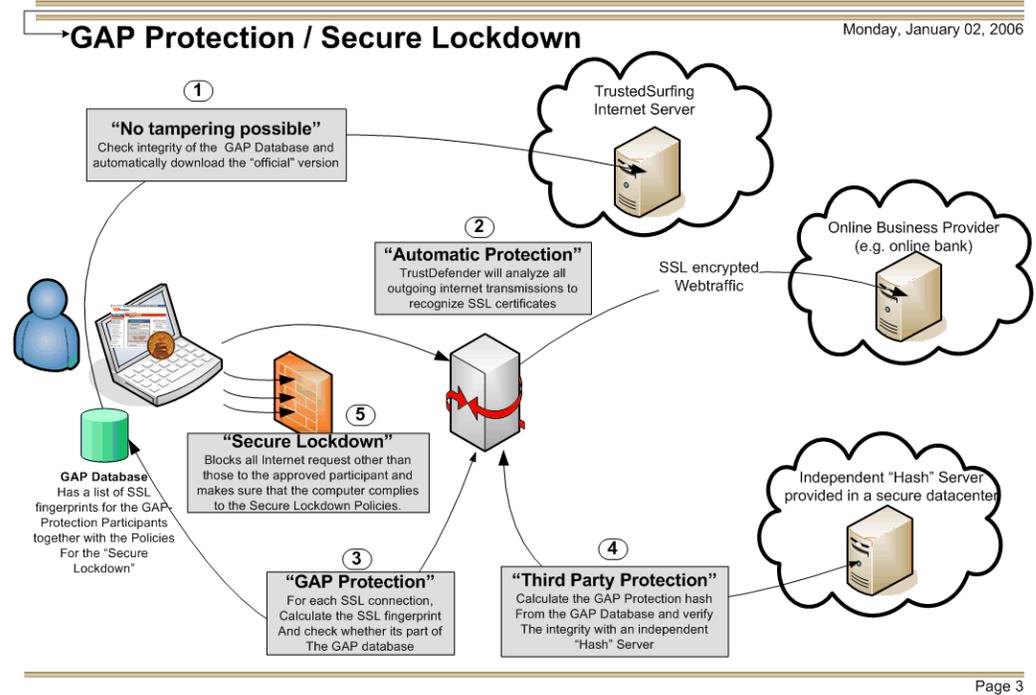


Figure 7 - GAP Illustration

### 4.4 TrustedSurfing Database

The biggest challenge is to decide whether a site is trustworthy or not for websites that are not part of the GAP Program.

This is where the biggest advantage of the TrustDefender solution comes into play. It enables you to be part of the TrustedSurfing community where experienced users can “help” others. It provides a platform that connects the Internet security savvy

professionals and the end-users at home. Tightly integrated into the TrustDefender Solution, Users can get all the information they need to evaluate whether they should trust a certificate or not. It works pretty much like in the real world - if you are unsure, you ask someone who knows.

The following information is available in the TrustedSurfing Community:

- **Known since**  
This will tell the user whether this Web-Fingerprint has a longstanding history or not.
- **Verified by a Trust Provider**  
This is an additional check whether the URL is part of a black list from a third-party vendor (like Netcraft or Microsoft)
- **Pharming Check**  
This check will verify whether the IP-Address you are connecting to really does belong to the Organization that has registered the domain.
- **Average User Rating**  
A Score from 1 to 5 stars with a "subjective" classification from an author
  - o **User Reviews**  
User-Reviews of the Web-Fingerprint. Anybody can write a review, BUT a valid email address is required and reviews are moderated (plus other anti-fraud techniques are deployed).
- **How did other TrustDefender users decide**  
This shows what other TrustDefender users decided. One user may make a wrong decision, but the collective will not!

This community based rating approach has proven to be very effective and extremely fault-resistant, as shown by high profile examples such as eBay, Amazon, Tripadvisor and others.

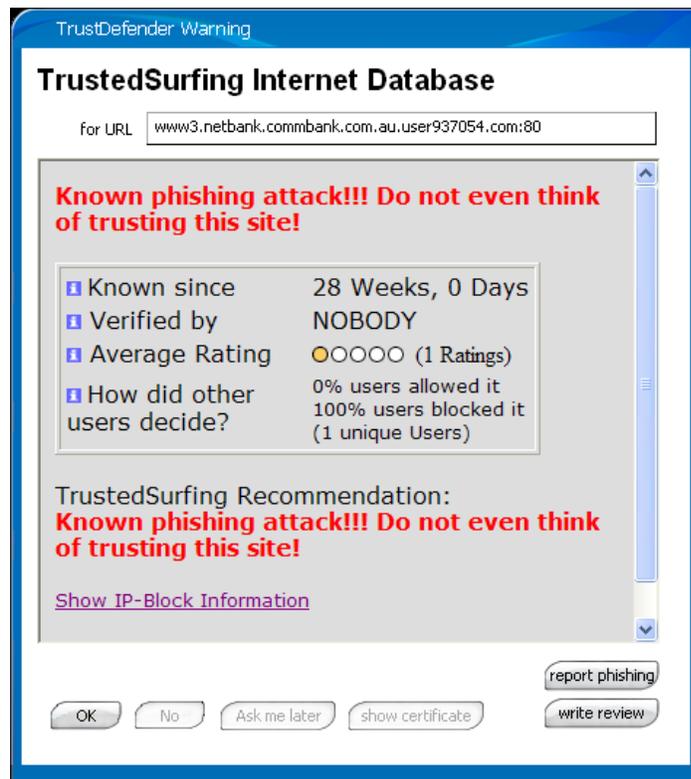


Figure 8 - TrustedSurfing Information Dialog

The TrustedSurfing Database is enabled by default and all TrustDefender Users can benefit from the TrustedSurfing Database, however it can be disabled in the Preferences Dialog (see chapter “Trust Settings”)

## 4.5 Menu

The following screenshot shows the Tray-Menu of TrustDefender. The menu is mainly used for configuration purposes and to access additional features.

You can access the menu with a left-click or a right-click with your mouse on the orange Tray Icon.

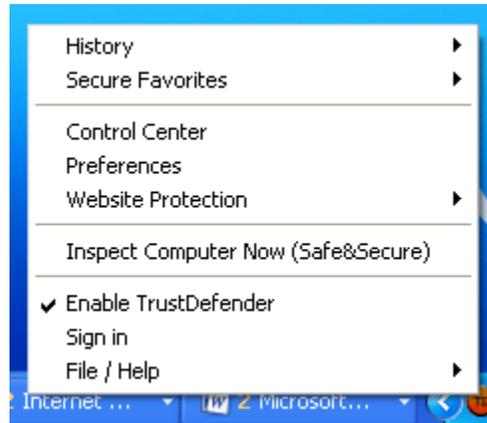


Figure 9 - TrustDefender Tray Menu

### 4.5.1.1.1



Note: You can use a shortcut to the Control Center, if you double-click on the Tray-Icon.

## 4.6 Control Center

The Control Center gives you all information in regards to all GAP Participants, to all Security Policies, special Web Protection, the Safe&Secure Mode and much more. Lets start with the Control Panel itself.

### 4.6.1 Control Panel / Security Status

The Control Panel shows the Security Status of your computer on one screen. It features the following four sections:



Figure 10 - Control Panel / Overview

1. Windows Update: TrustDefender will display the current Windows Update Status. This can be one of the following:
  - a. **“Not Configured”**, means that Windows Update is not configured at all;
  - b. **“Disabled”** means that Windows Update is configured, but disabled;
  - c. **“Notify Before Download”** means that Windows will automatically check whether a new Windows Update is available, but will ask the user before downloading the update.

- d. **“Notify Before Installation”** means that Windows will automatically check for new Windows Updates and download them immediately, but will ask the User before it installs the Updates.
- e. **“Automatic”** means that Windows automatically downloads new Updates and install them whenever they are available. This is the recommended setting.



**Note:** If you want to change any of these settings, please refer to the Microsoft Windows User Manual, or select ‘Security Center’ in the Windows Control Panel. You can then change the security settings for Windows Update.

- 2. **Antivirus Engine:** This shows your Antivirus Engine, in case one is installed. It shows furthermore the Status of the Antivirus Engine, i.e. whether it is up-to-date and whether it is enabled.
- 3. **Firewall:** This shows your current Personal Firewall. If you use Microsoft Windows XP with Service Pack 2, you have a built-in firewall.
- 4. **Safe&Secure Mode:** This shows the status of TrustDefender’s Safe&Secure Mode. The Safe&Secure Mode fills the Gap that your Antivirus Scanners leave open by assuring you that all applications on your system are verified to be good. Please click on ‘Inspect Computer Now’ to check the status.

4.6.2 Webfingerprints

As discussed earlier in Chapter “Introduction / How TrustDefender works”, TrustDefender will check the trust-relationship for every single website that you use.

The Web fingerprints dialog shows all (dis-) allowed websites and lets you perform additional operations.

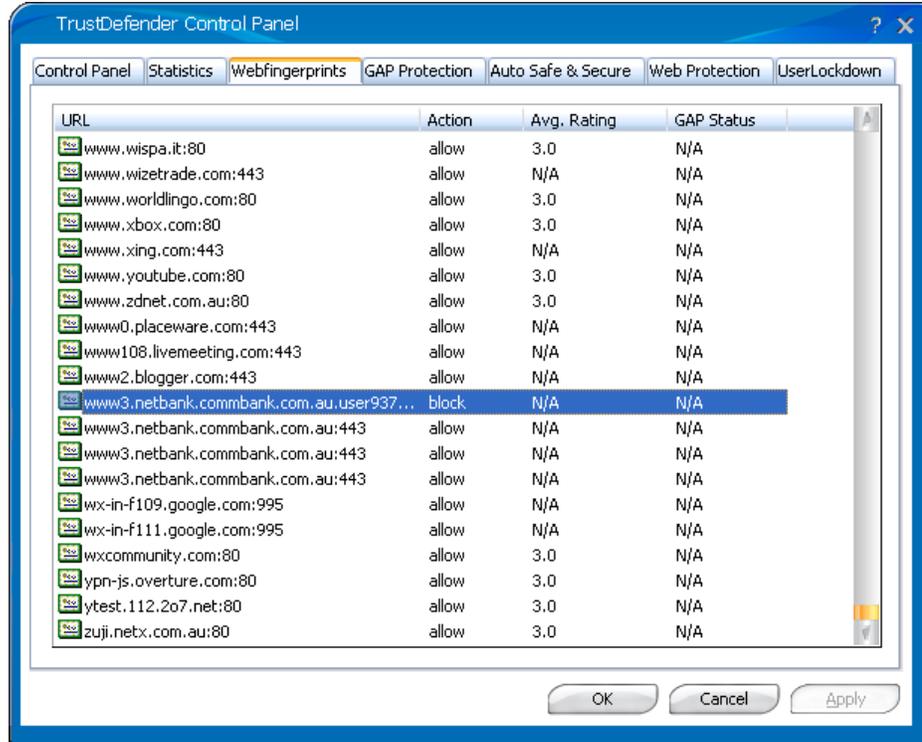


Figure 11 - Control Panel / Webfingerprints

This list shows the URL in the first column and the chosen action in the next column. The action can be either ‘allow’ or ‘block’ depending on your earlier choice. The average rating will display the average user rating of the whole TrustedSurfing Community.



Note: You can get a context menu with more options if you right-click on a menu item.

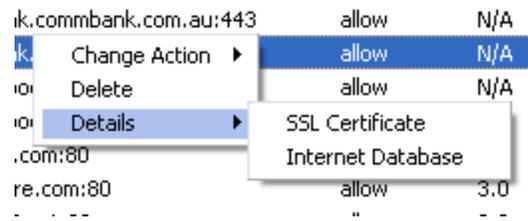


Figure 12 - Webfingerprints Context Menu

You can either

- Change the action (from allow to block or vice versa), or
- Delete the Webfingerprint completely, or
- Get more information.

If you choose 'Internet Database', TrustDefender will automatically connect to the TrustedSurfing Database and display the information on hand. See the following screenshot for a legitimate Website.

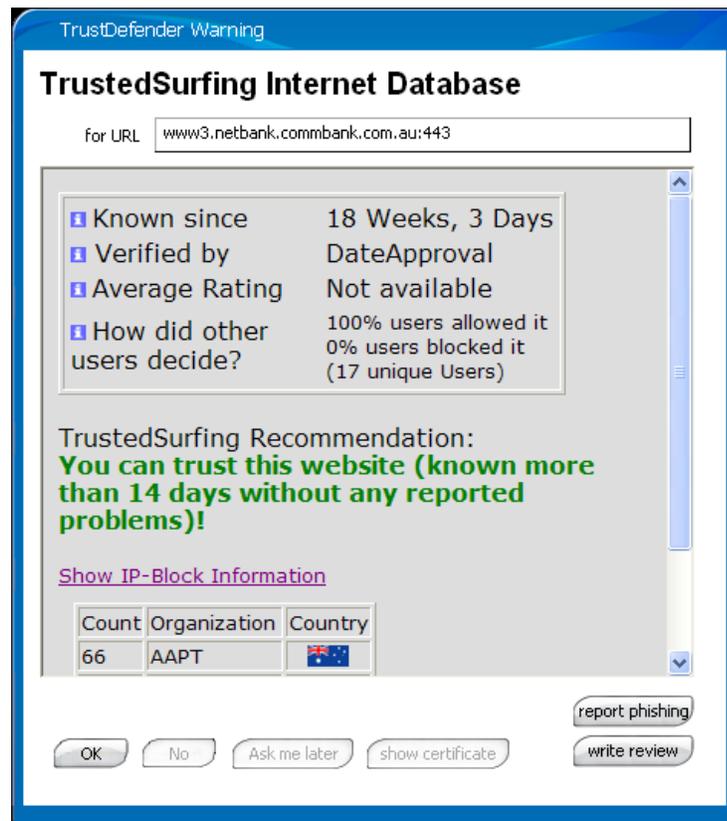


Figure 13 - TrustedSurfing Information (good site)

The next example is the result for a known phishing site.

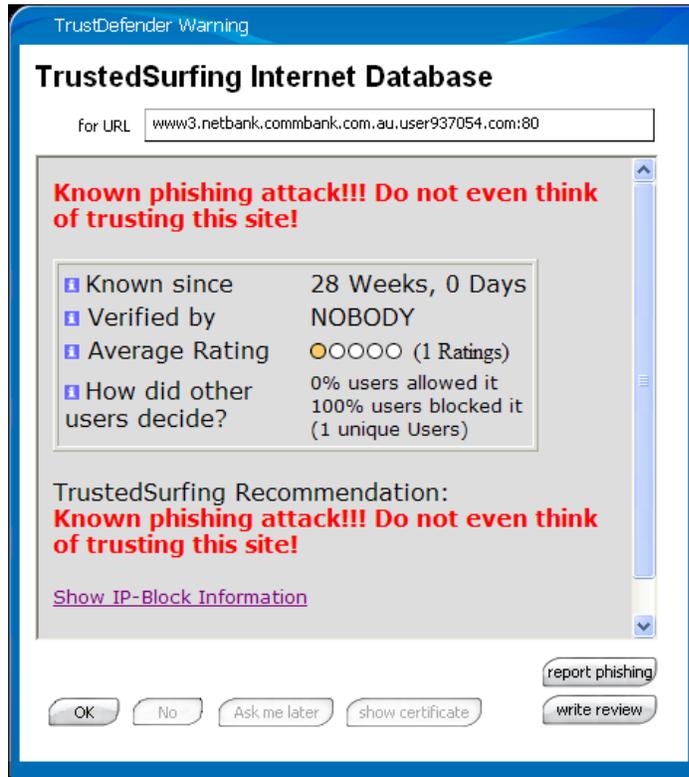


Figure 14 - TrustedSurfing Information (phishing site)

#### 4.6.3 GAP Protection

The GAP Protection Dialog shows information about all GAP Participants. GAP Participants are Online Businesses that have submitted their Security Policies to TrustDefender to provide a superior protection for all TrustDefender users.

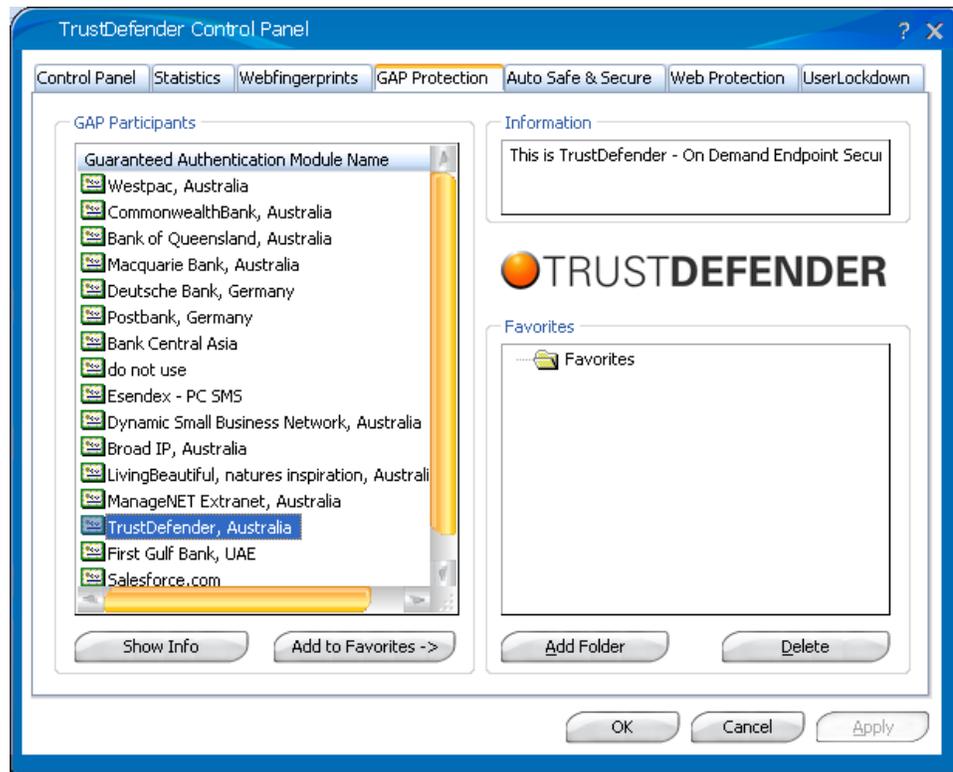


Figure 15 - Control Panel / GAP Protection

This dialog is for information purposes only. You cannot do any changes to the official submitted information, but you can add the Websites to the Secure Favourites.



Note: In addition to the buttons at the bottom of the page, you can also activate a context menu by right-clicking a participant.

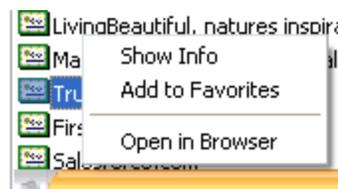


Figure 16 - Control Panel / GAP Protection context menu

**4.6.4 Add Secure Favorite**

To add a particular web service to the Secure Favorites Section, just click on “Add to Favorites” and you’ll see the following dialog box which lets you choose the Folder to store the Favorite to.



Note: If you want to create a new Favorites folder, just click on “Add Folder” in the GAP Participants Dialog box.

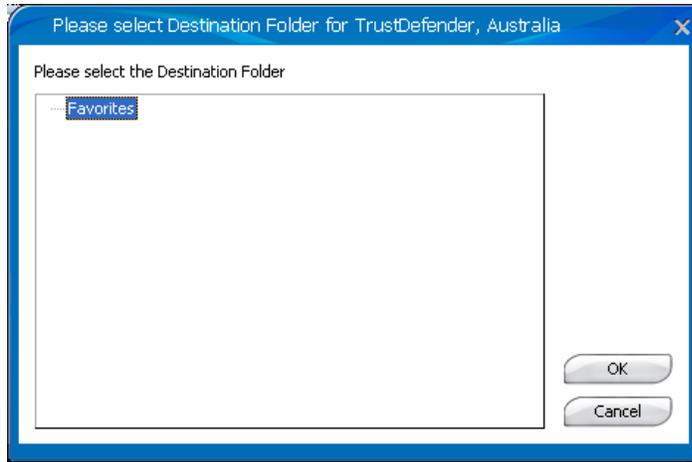


Figure 17 - GAP Protection / Add Favorite

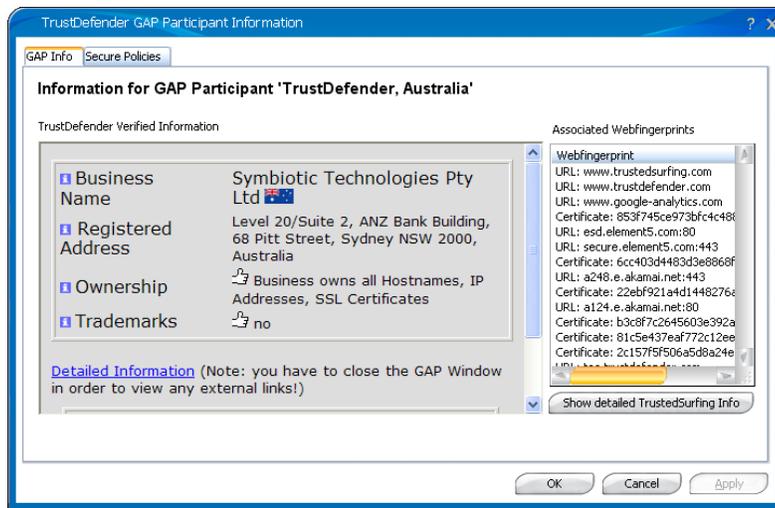
By pressing the “OK” Button, TrustDefender will store the selected GAP Participant in the Secure Favorites Folder. The GAP Participant will then be visible in the Tray Menu.

**4.6.5 Show GAP Participant Info / GAP Participant**

If you click on the “Show Info” Button, TrustDefender displays additional Information about the GAP Participant.

Figure 18 - GAP Protection / Show Info

This



additional

Information includes:

- Registered Business Name
- Registered Business Address
- Information about Ownership and Trademarks
- Information about all related Webfingerprints.

#### 4.6.6 Show GAP Participant Info / Secure Policies

The second Tab shows information about the selected Security Policies by the online business. Again, this is an official policy of the selected web service and cannot be changed by the user. This is for information only.

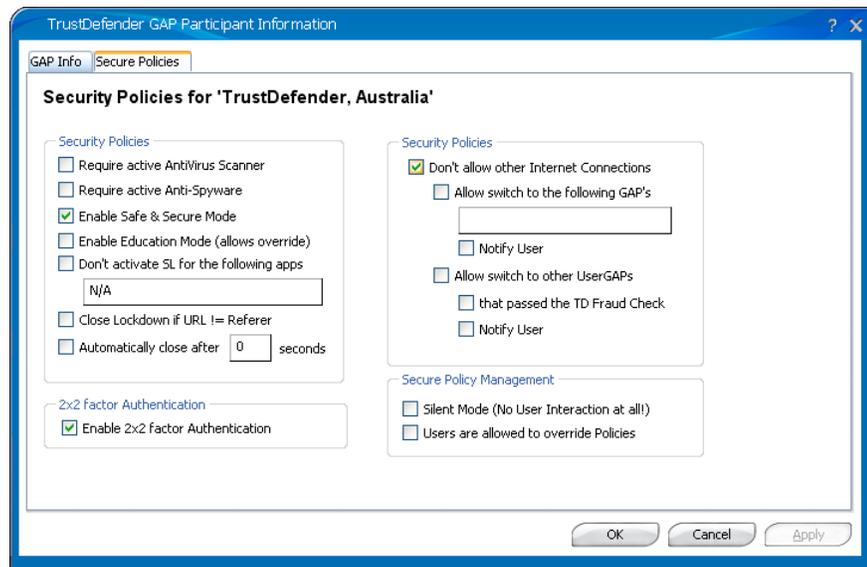


Figure 19 - GAP Protection / Secure Policies

#### 4.6.7 Auto Safe&Secure

The "Auto Safe&Secure" Dialog lets you configure websites where TrustDefender will automatically start the Safe&Secure Mode whenever you go to one of these websites. This is an easy and convenient way to make sure that your computer is safe & secure without a complex configuration.

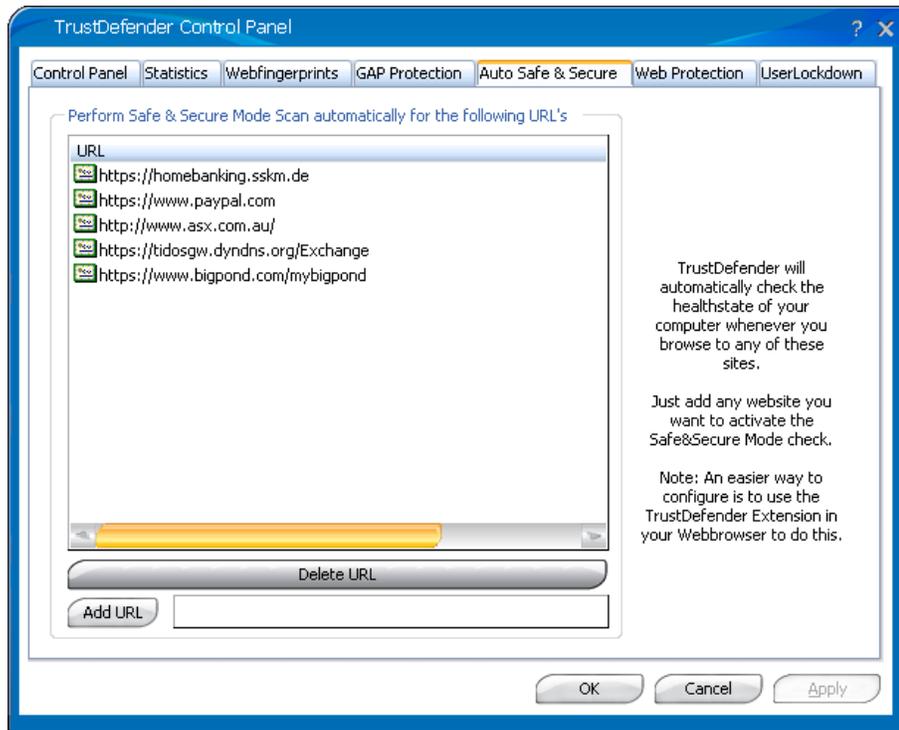


Figure 20 - Control Panel / Auto Safe&Secure

You can easily add and delete URL's from this list by using the respective buttons at the bottom of the page.

A much easier way to configure this is by using the TrustDefender button from your web browser. Just select "Always scan my computer for this website" and TrustDefender will automatically scan your computer from now on whenever you go to the website you are looking at.

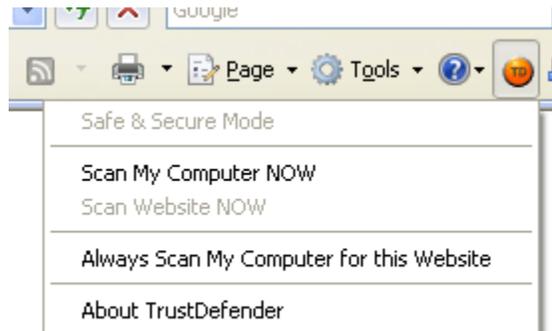


Figure 21 - Web Browser Extension (IE)

**4.6.8 Web Protection**

TrustDefender does not only feature the “official” GAP Participants where the Online Business can define Security Policies for their own Web Services.

TrustDefender allows you to create customized Web Protections for all kinds of online services. As a customer of the TrustDefender Gold Edition, you can even define your very own Web Protections.

TrustDefender has a built-in protection for a large number of Online Services (mostly banks) which will be visible in the “Web Protection” Tab.

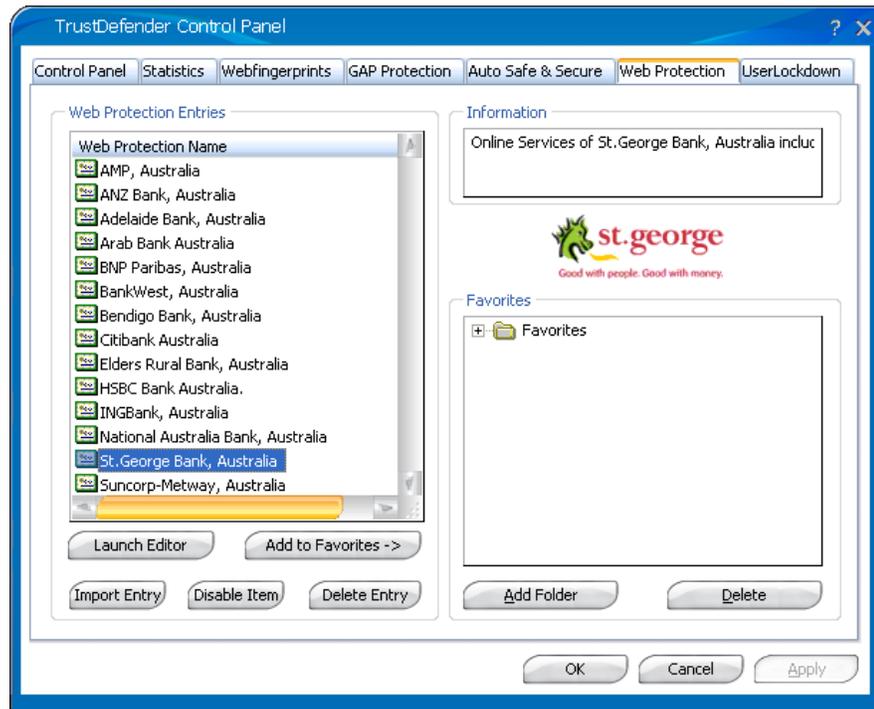


Figure 22 - Control Panel / Web Protection



Note: You can also add the Web Protection Profiles to the Secure Favourites.

**4.6.9 User Lockdown Policies**

For all the “non-official” Web Protection websites discussed in the previous chapter, TrustDefender lets you define your own Security Policies.

This is an advanced setting and it is highly recommended not to change any settings – unless you are an experienced TrustDefender user.

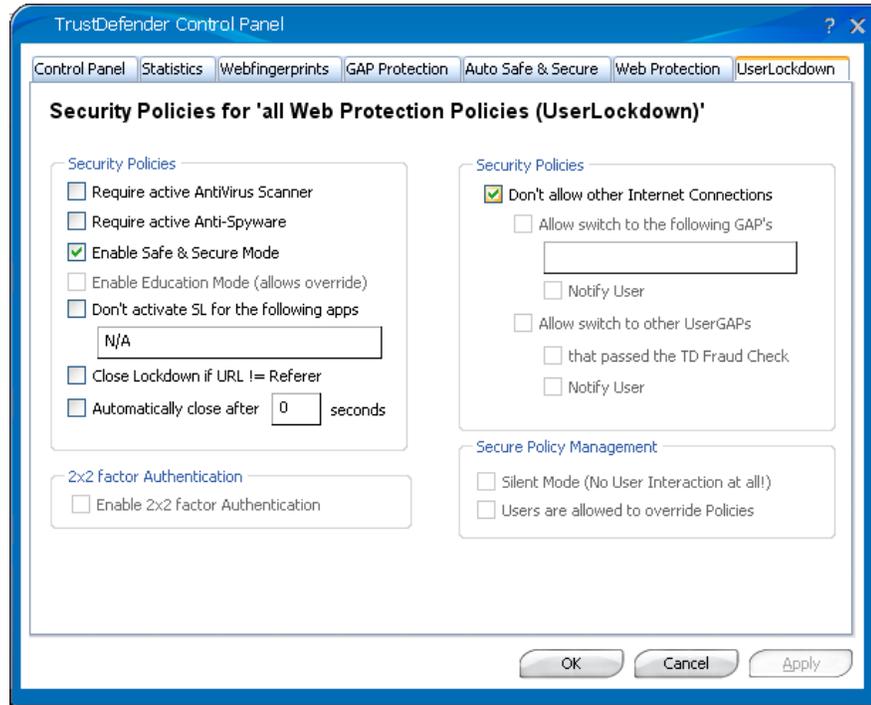


Figure 23 - Control Panel / UserLockdown Preferences

## 4.7 Preferences

The Preferences dialog box lets you configure core features of TrustDefender. Typically it is not recommended to change any settings unless you experience any problems.

### 4.7.1 General

The General Tab lets you configure general TrustDefender settings.

TrustDefender can be operated in two ways. The Browser Configuration Free Mode is the default and this mode will automatically check the internet traffic without any changes to the system at all.

If this mode is turned off, the Proxy Mode automatically activates. TrustDefender listens on IP 127.0.0.1, port 2309 for Proxy Requests and if the checkbox is turned off, you have to configure the Web Proxy to the above address.

If you have connectivity problems with TrustDefender's Browser Configuration Free Mode, please click the 'Advanced' Button as this will show additional configuration parameters.

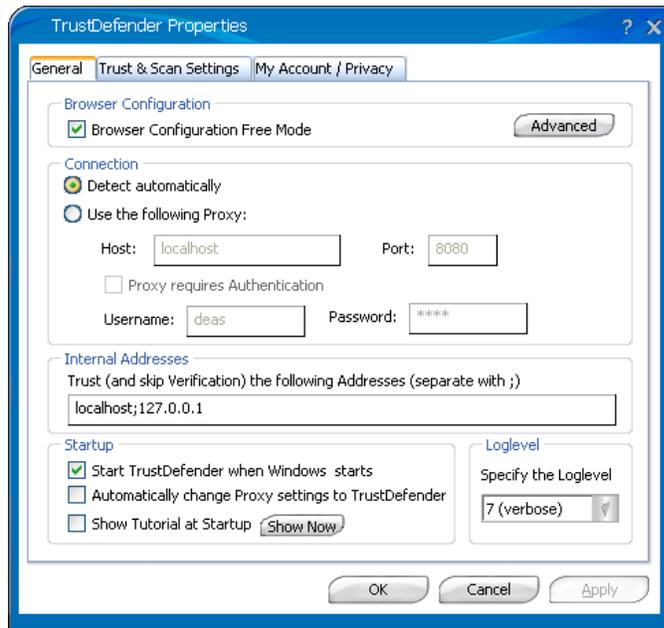


Figure 24 - Properties / General Browser Configuration

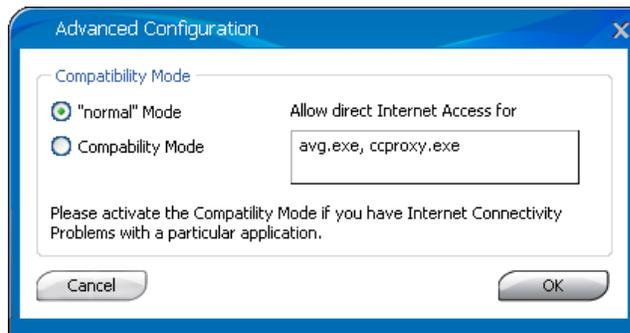


Figure 25 - Preferences / Advanced Browser Configuration

The Advanced Configuration comprises two modes:

- **“Normal” Mode** – which is the default mode. This mode will analyze all internet Traffic from all applications except the ones showed in the edit box on the right hand side
- **Compatibility Mode.** This mode should be used in case you experience any internet connectivity problems with a particular software (e.g. VPN Client). This mode will only analyze the internet traffic of well-known Web browsers.

4.7.1.1.1.1.1 Connection

TrustDefender will automatically detect how it should connect to the Internet. Especially in corporate environment, TrustDefender will choose the correct Proxy and the correct authentication method (Basic Authentication or NTLM Authentication) to connect to the Internet.

## TRUSTDEFENDER USER GUIDE

However you have the possibility to provide an upstream Proxy Server where TrustDefender sends all the outgoing internet requests to.

### *Internal Addresses*

You can specify a list of internal addresses (separated by semicolon) where TrustDefender established trust automatically without asking the user and without sending any details to the global TrustedSurfing Database.

### *Startup*

This section lets you define TrustDefenders' behavior when starting up.

- Start TrustDefender when Windows starts – TrustDefender will automatically be started. (This option should not be changed)
- Automatically change Proxy settings to TrustDefender – This setting should only be used if (!) the Browser Configuration Free Mode is not activated
- Show Tutorial at Startup – this allows you to see the tutorial at startup.

### *Loglevel*

You can specify different log levels (error, normal, debug). This only applies to the TrustDefender Log Window and should only be changed if asked by the TrustDefender Support Personnel.

#### 4.7.2 Trust & Scan Settings

The Trust & Scan Settings lets you configure the behavior of TrustDefender when it comes to what checks TrustDefender will perform.

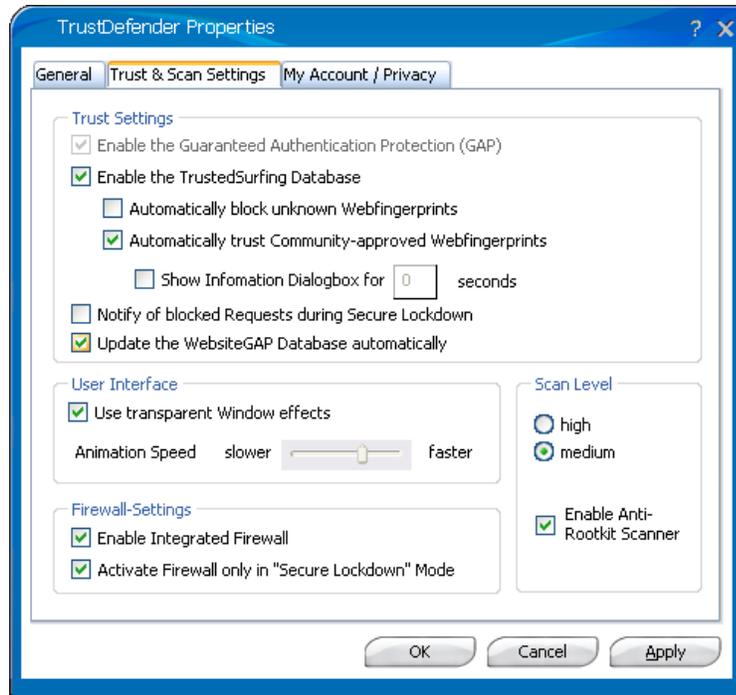


Figure 26 - Configuration / Trust & Scan Settings

##### *Trust Settings*

This section lets you configure the Trust Settings of TrustDefender.

- “Enable the Guaranteed Authentication Protection” – this is a core feature of TrustDefender and cannot be changed
- “Enable the TrustedSurfing Database” – the TrustedSurfing Database is the community based Anti-Phishing and Trust Database. It will automatically leverage the knowledge of all TrustDefender users worldwide and can therefore provide much more information. You should only deactivate this checkbox
  - “Automatically block unknown Web fingerprints” – this option will automatically block Requests to sites you have never ever been before.
  - “Automatically trust Community-approved Webfingerprints” – this option will instruct TrustDefender to automatically allow Webfingerprints that are trusted by the community. For this to happen, a Webfingerprint must be known in the community for more than 14 days without any problems. This option should be checked as it will eliminate most of the “popups”.

- “Show Information Dialogbox for \_\_\_ seconds” – in case you want to see the Information Dialogbox even for the Community-approved Webfingerprints, you can check this option. After the specified number of seconds, the Dialogbox will automatically close.
- “Notify of blocked Requests during Secure Lockdown” – Once TrustDefender activates a GAP Policy, it may limit the Internet Requests to the chosen Online Business. Other unrelated Internet Requests may be blocked. You can specify whether you want to be notified of every Request that gets blocked.
- “Update the Website Protection Database automatically” – this option will instruct TrustDefender to automatically update the Website Protection Database in case it gets updated. This option is highly recommended as it will make sure your database is up-to-date whenever our team releases a new version.

#### *User Interface*

In this section, you can specify whether you want to have transparent Window effects and the animation speed of the Fingerprint Animation.

#### *Firewall Settings*

The integrated firewall of TrustDefender will automatically be activated once a GAP Participant Profile or a Web Protection Profile is detected. It will restrict the outgoing Internet Requests to the chosen Online Service and deny all unrelated Internet Requests. You can configure whether you want to have this protection at all and also whether this protection is enabled all the times or only during the time of the GAP Profile (Activate Firewall only in “Secure Lockdown” Mode)

#### *Scan Level*

In this section, you can specify the Scan Level of TrustDefender. TrustDefender will automatically analyze all outgoing internet requests that contain data attached to it. The problem is that a large number of websites request data from the user seamlessly. This includes e.g. Screen Resolution, Operating System, ... The two Scan Levels helps TrustDefender as a “tradeoff” between Security and Usability.

- Scan Level = high. This means that every single request that contains data will be checked. Warning: This may result in a large number of Information dialogue boxes
- Scan Level = medium. This means that only websites where the data is submitted as a POST Request will be scanned. This is the recommended setting.

Additionally the Anti-Rootkit Scanner can be en- or disabled in this section. It is highly recommended to enable the Anti-Rootkit Scanner as this will allow TrustDefender to detect hidden applications on your system.

**4.7.3 My Account / Privacy**

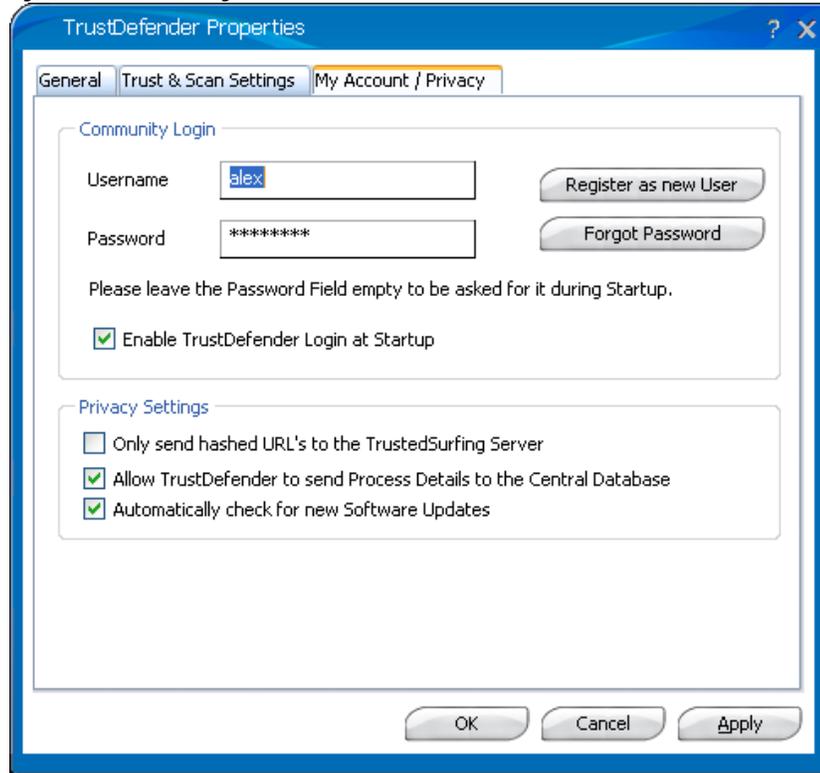


Figure 27 - Configuration / My Account/Privacy

*Community Login*

In this section, you can change the Username and Password used for the TrustDefender Login. This will enable a number of additional features in TrustDefender. Please click on “Register as new User” in case you haven’t done so.



Note: The Username and Password can also be used on the website at <http://www.trustdefender.com>.

*Privacy Settings*

- “Only send hashed URL’s to the TrustedSurfing Server” – To check the trust status of a particular web service, TrustDefender will automatically leverage the TrustedSurfing Database to retrieve additional information. The real URL will be used for this request. If you activate this checkbox, TrustDefender will only submit a hashed version and the URL cannot be reengineered from the hash.

- “Allow TrustDefender to send Process Details to the Central Database” – this option allows TrustDefender to send details of the running applications to the global Safe&Secure Mode database. This option is highly recommended.

**Note:** No personal related information is submitted.

- “Automatically check for new Software Updates” – this will allow TrustDefender to automatically check and download new TrustDefender versions once they become available.

## 4.8 Safe&Secure Mode

The Safe&Secure Mode of TrustDefender can be activated in various ways:

- Automatically activated based on a GAP Policy of a website
- Manually activated either through the Tray-Menu, the Web Browser Extension or through the Control Panel

The Safe and Secure Mode is TrustDefender's answer to all Adware, Spyware, Trojans, Virus and other malicious code attacks. The Safe&Secure Mode follows a white listing approach rather than heuristics and/or blacklisting approaches. TrustDefender has a huge Database with known and approved software and any TrustDefender User will be warned if there is an unknown process running on his computer to make sure that only known and "good" software is running. All unknown progresses are marked as potentially malicious and the user has then the choice to close the corresponding programs, to let TrustDefender try and close them or to proceed without closing the Programs. However the result of this decision will be submitted to the Online Business during the TrustDefender handshake.

The Safe & Secure Mode will also inspect the Computer for Rootkits (i.e. a Process that hides itself from the System). Hidden Processes will be automatically marked as malicious.

During the Safe&Secure Mode scan, you'll notice the following dialog box which shouldn't take longer than 30 seconds to complete.

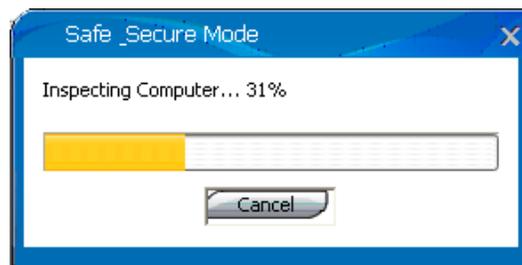


Figure 28 - Safe&Secure Mode Scan Dialog

Once the Scan is complete, you'll see the following dialogue.

#### 4.8.1 Unknown Applications

The first tab shows the unknown or potential malicious software on running on the computer.

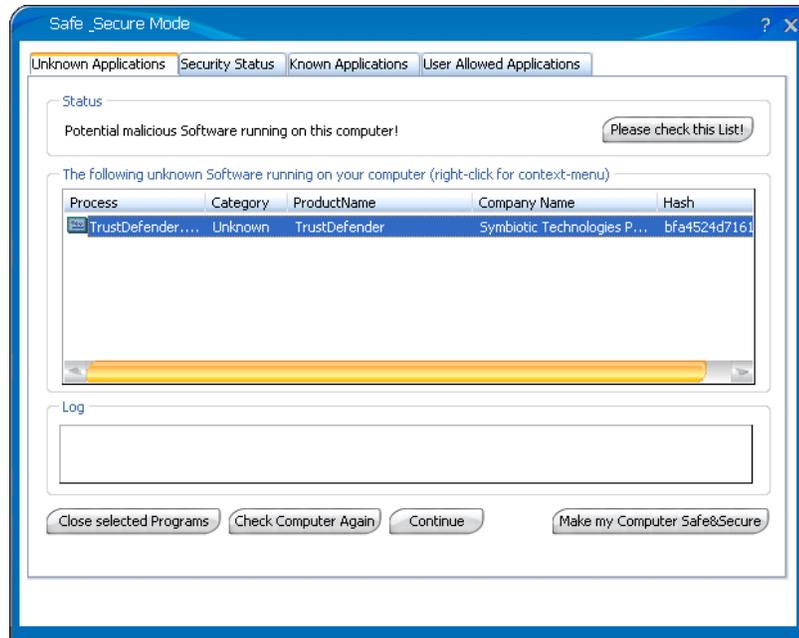


Figure 29 - Safe&Secure Mode / Unknown Applications

You have the following options:

- **“Close selected Programs”** – this will close all programs that you have selected in the list box. TrustDefender will rescan the Computer.
- **“Check Computer Again”** – this will simply rescan the computer. Use this option if you manually closed unknown applications.
- **“Make my Computer Safe&Secure”** – this will automatically close all unknown software and rescan the Computer.

You can activate a context-menu by right-clicking on an unknown software. You’ll see the following context menu.

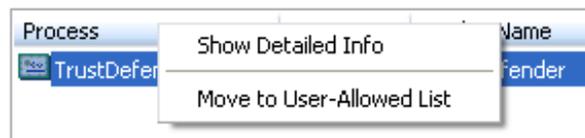


Figure 30 - Safe&Secure Mode Dialog / context menu

The “Show detailed Info” will bring up a Website with more information about the selected Application.

The “Move to User-Allowed List” Option allows you to allow the list manually on your system. No information will be sent to a TrustDefender Server and only your system will recognize the application. You will be asked to enter a Category and an optional description.

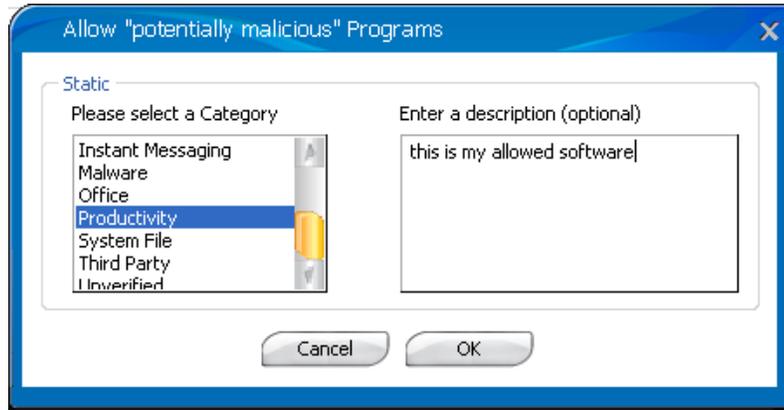


Figure 31 - Safe&Secure Mode / manual application allow

**4.8.2 Security Status**

This will display the security status of your computer. Please refer to chapter “Control Panel / Security Status” for a complete description.



Figure 32 - Safe&Secure Mode / Security Status

**4.8.3 Known Applications**

This tab will display all known and approved applications. You cannot do any changes and this dialog is for your information only.

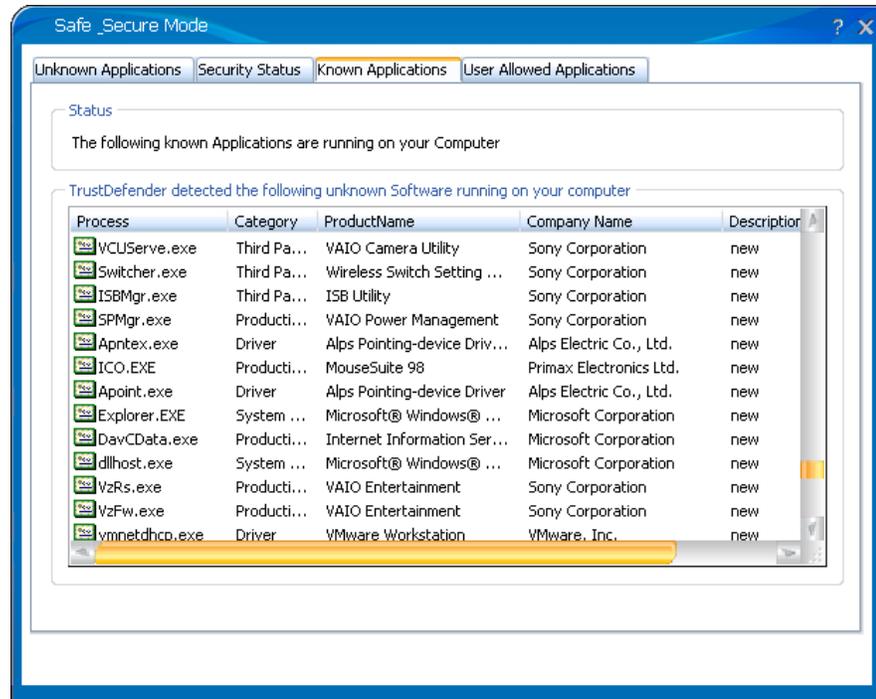


Figure 33 - Safe&Secure Mode / Known Applications

#### 4.8.4 User Allowed Applications

This tab will show all Applications that have been allowed manually in the above chapter. This is empty by default.

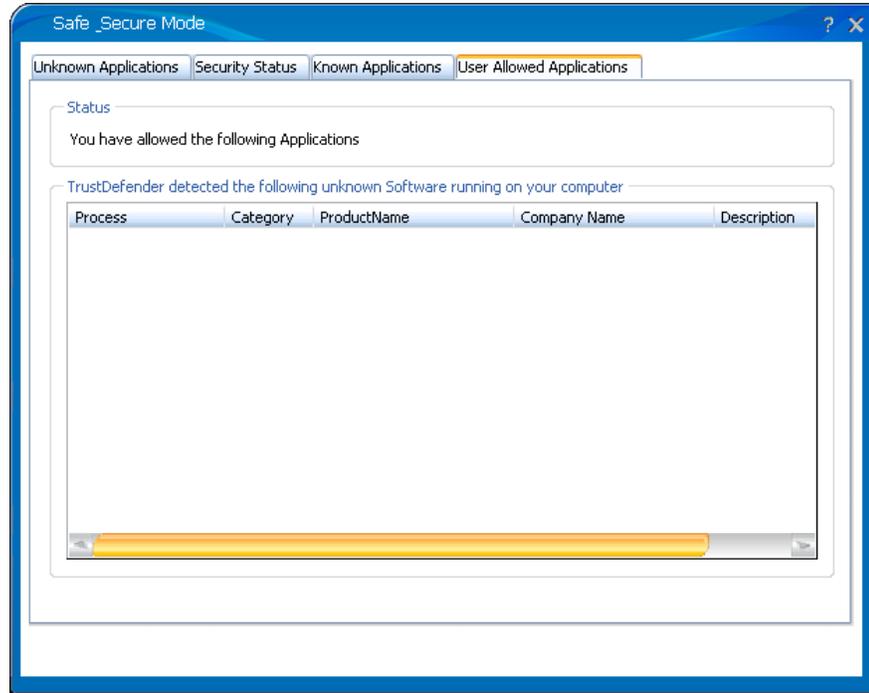


Figure 34 - Safe&Secure Mode / User allowed Applications

## 4.9 Web Browser Extension

TrustDefender will install a Browser Component to enable a convenient and fast way to interact with TrustDefender. This Browser Component is available for Microsoft Internet Explorer and Mozilla Firefox.



Figure 35 – Web browser Extension (IE)

You have the possibility to “Scan My Computer NOW” which will immediately scan the computer. Please use this option before sending any confidential information to a website.

The Option “Always Scan My Computer for this Website” will automatically scan your Computer whenever you visit the actual website in the future.

## **4.10 Secure Favorites**

The Secure Favorites are a special, highly secure System to start your online business session. It can be used for all official GAP Participants and also for all Participants of the Web Protection.

The Secure Favorites will do much more than just store and open a URL – which is basically what the “normal” Favorites of your Web browser does. The Secure Favorites will do the following:

1. Load the Web Protection Profile
2. Start the Safe&Secure Mode to scan your computer and to make sure that no unknown application (Trojan/virus) is running on your computer.
3. Activate the Web Protection Policies – including the Secure Lockdown, which will only allow Internet Requests to the chosen Online Service
4. Open the URL of the Online Service in your default web browser.

This way, the Secure Favorites will also protect you against Pharming as the Secure Lockdown would block all Internet Requests to sites that are not related to the “official” Web Service.

### **4.10.1 Add Secure Favorites to the Quick-Launch Menu**

To add a particular web service to the Secure Favorites Section, just click on “Add to Favorites” in the TrustDefender Control Panel either in the “GAP Protection” or in the “Web Protection” Section and you’ll see the following dialog box which lets you choose the Folder to store the favourite to.

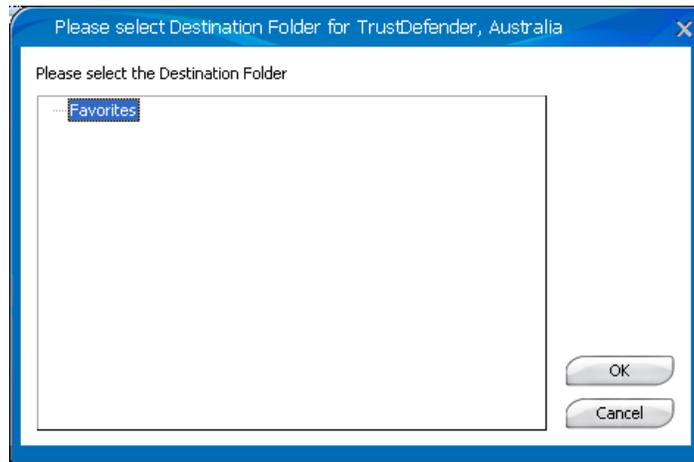


Figure 36 - Add Favorites Dialog



Note: If you want to create a new Favourites Folder, just click on “Add Folder” in the GAP Participants Dialog box.

#### 4.10.2 Use Secure Favorites in the Quick-Launch Menu

Once the Secure Favorites are configured, they will automatically appear in the Quick-Launch Menu of the TrustDefender Tray Menu as shown in the screenshot below. Simply choose the web service you want to use and TrustDefender will activate it.



Figure 37 - Secure Favorites Quick Launch Menu

## 4.11 TrustDefender in Corporate Environments

TrustDefender has been designed for home use as well as corporate use. TrustDefender has a number of features to comply with corporate Security Policies and Corporate Lockdown Restrictions.

### 4.11.1 Administrator vs. Non-Administrator Rights

TrustDefender only needs Administrator Rights during the Installation.



Figure 38 - Installation Error Message

After initial installation, a restricted user account is sufficient to use TrustDefender.



**Note:** TrustDefender can even be installed on a Non-Administrator Account using the Proxy Engine; however this would involve configuring a proxy server. (TrustDefender will also do this automatically, but in many locked down situations this option is not suitable)

### 4.11.2 Internet Access / Upstream Proxy Servers

TrustDefender will automatically detect which upstream proxy server needs to be used and also which type of authentication is needed. Basically TrustDefender does everything in the background and it should work straight out of the box.

TrustDefender needs Internet Access for the access to the global TrustDefender Databases (TrustedSurfing + Safe&Secure Mode Database) and for all Internet requests you are submitting.

TrustDefender will analyze the current system-wide proxy settings and use the correct proxy server. It supports the following Proxy Schemes:

- automatic configuration script
- Manual proxy configuration

TrustDefender supports the following Authentication Schemes:

- Basic Authentication
- NTLM

In case of NTLM Authentication, TrustDefender can automatically complete the NTLM Handshake without any user information, however in case Basic Authentication is used, TrustDefender typically needs a username and password to access the internet. You'll encounter the following dialog box which asks for these credentials.

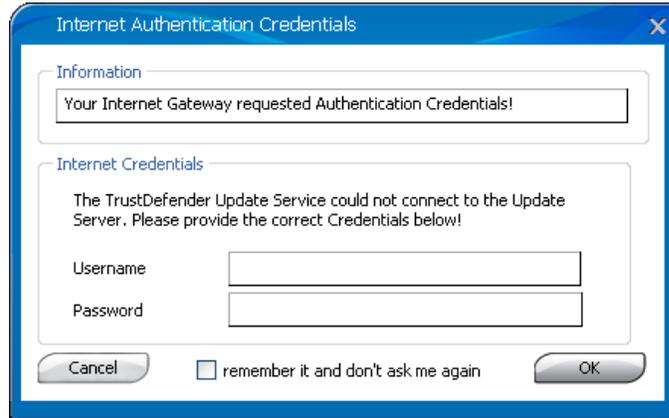


Figure 39 - Internet Authentication Credentials Dialog

## 5 Web Protection Policy Editor

TrustDefender has a special web protection for many online services already built in; however you can add your own online services at any time. The Web Protection Policy Editor lets you define all Security Policies for a particular Web Service.

You can invoke the Web Protection Policy Editor from the TrustDefender Tray Menu.

From there you have basically the following Options:

- File → Load/Save/...
- Policies → Edit Policies (or click on the Pencil in the Toolbar)

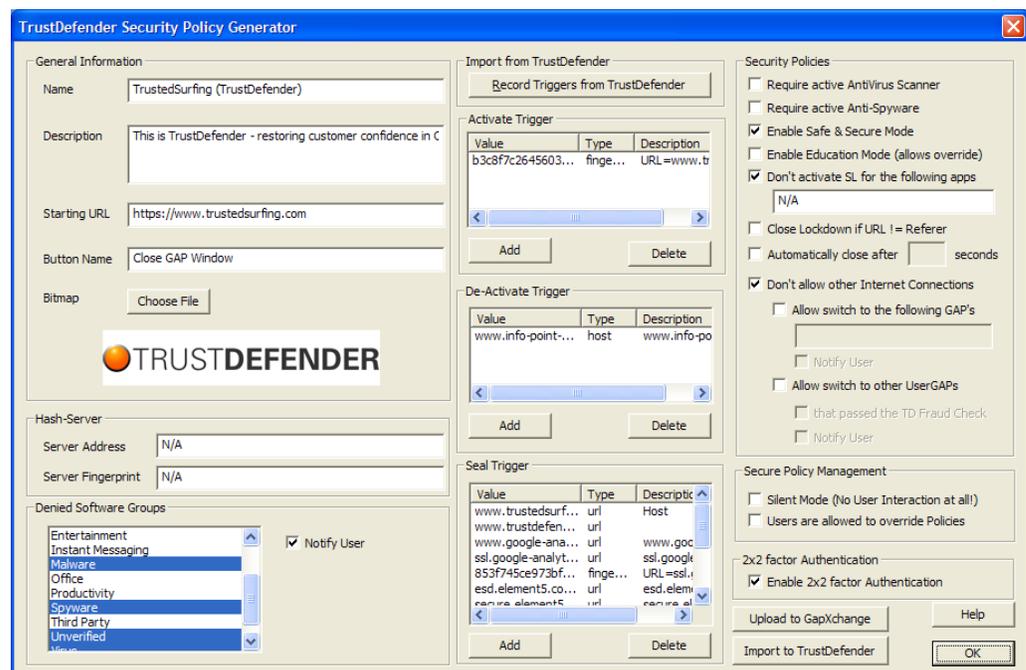


Figure 40 - TrustDefender Web Protection Policy Editor

- You can define the Description, the Triggers (when to activate the Website GAP Policy, when to deactivate and which Hostnames/SSL-Fingerprints/... belong to the Web Service

- **Note:** The “Record Triggers from TrustDefender” provides an easy method of getting the needed information.
- For detailed information, please refer to the Policy Editor Manual located at <http://www.trustdefender.com/content/view/53>
- File → Upload to GapXchange (or clicking on )
  - Store the Website GAP Policy in the global TrustDefender Repository GapXchange for other Users to download;
- File → Save as Website GAP Policy in TrustDefender (or clicking on )
  - Exports the Policy directly into your running TrustDefender Instance for immediate use.

## 6 Appendix

### 6.1 Figures

Figure 1 - License Choose Wizard	4
Figure 2 - License Key Dialog	4
Figure 3 - Tutorial	5
Figure 4 - TrustDefender Login	5
Figure 5 - TrustDefender License Information Dialog	6
Figure 6 - GAP Window	12
Figure 7 - GAP Illustration	14
Figure 8 - TrustedSurfing Information Dialog	16
Figure 9 - TrustDefender Tray Menu	17
Figure 10 - Control Panel / Overview	18
Figure 11 - Control Panel / Webfingerprints	20
Figure 12 - Webfingerprints Context Menu	21
Figure 13 - TrustedSurfing Information (good site)	21
Figure 14 - TrustedSurfing Information (phishing site)	22
Figure 15 - Control Panel / GAP Protection	23
Figure 16 - Control Panel / GAP Protection context menu	23
Figure 17 - GAP Protection / Add Favorite	24
Figure 18 - GAP Protection / Show Info	24
Figure 19 - GAP Protection / Secure Policies	25
Figure 20 - Control Panel / Auto Safe&Secure	26
Figure 21 - Web Browser Extension (IE)	26
Figure 22 - Control Panel / Web Protection	27
Figure 23 - Control Panel / UserLockdown Preferences	28
Figure 24 - Properties / General	29
Figure 25 - Preferences / Advanced Browser Configuration	29
Figure 26 - Configuration / Trust & Scan Settings	31
Figure 27 - Configuration / My Account/Privacy	33
Figure 28 - Safe&Secure Mode Scan Dialog	34
Figure 29 - Safe&Secure Mode / Unknown Applications	35
Figure 30 - Safe&Secure Mode Dialog / context menu	35
Figure 31 - Safe&Secure Mode / manual application allow	36
Figure 32 - Safe&Secure Mode / Security Status	36
Figure 33 - Safe&Secure Mode / Known Applications	37
Figure 34 - Safe&Secure Mode / User allowed Applications	38
Figure 35 - Webbrowser Extension (IE)	38
Figure 36 - Add Favorites Dialog	40
Figure 37 - Secure Favorites Quick Launch Menu	40
Figure 38 - Installation Error Message	41
Figure 39 - Internet Authentication Credentials Dialog	42
Figure 40 - TrustDefender Web Protection Policy Editor	43

### 6.2 Index

GAP Protection, 10

**TRUSTDEFENDER USER GUIDE**