



## Quickstart Guide

- 1. TRUSTDEFENDER SOFTWARE .....1**
- INTRODUCTION ..... 1
- INSTALLATION .....2
- LIVE-DEMONSTRATION / WALKTHROUGH .....2
- FEATURES .....3
- GAP Protection / Secure Lockdown* .....3
- Safe & Secure Mode* .....4
- Website GAP Policies* .....5
- GapXchange*.....5
- TrustedSurfing Internet Database* .....6
- Control Center*.....8
- Secure Favorites* .....9
- Preferences*.....9
- History* .....9
- LIMITATIONS OF THE BETA RELEASE OF THE GOLD EDITION.....9
- 2. TRUSTDEFENDER WEBSITE GAP POLICY GENERATOR....10**

### 1. TrustDefender Software

#### Introduction

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<sup>1</sup>. 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 Webserver) into a security chain to protect the enduser at home as well as the online business.

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.

---

<sup>1</sup> For participants Third Parties only

## Installation

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

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

When using your Webbrowser, you should see that the orange logo is "pumping". In this case the Installation was successful and TrustDefender will now analyze all your outgoing internet transmissions.

If the orange logo is not "pumping" and TrustDefender seems to do nothing, please report this situation to the TrustDefender team by clicking on File/Help → Report Problem. Most probably the reason is that by default TrustDefender will use the Configuration-Free Mode to analyze the Internet Traffic. However as this feature is still in a beta stage, it can be deactivated in the Preferences → General. The other Possibility is to use the Proxy Feature. If selected in the Preferences → General Tab, TrustDefender will automatically update your Browser to use TrustDefender as outgoing Proxy for Mozilla FireFox and Microsoft Internet Explorer (including the System's Default Proxy). For all other Browsers, please manually update the browsers proxy settings and choose the proxy as follows:

- The Proxy location is 127.0.0.1 with port 2309 for HTTP AND HTTPS (Encrypted HTTP)

## Live-Demonstration / Walkthrough

To see the various Features of TrustDefender in Action, please go through this Live-Demonstration

1. go to <http://www.westpac.com.au>
2. click on Internet Banking in the left hand side menu

- 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

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.

4. You can not safely log in (we skip this part in the demonstration)
5. To see that TrustDefender will only allow Webrequests belonging to Westpac, please open another browser window, and
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 Webrequests that belong to the Application of the GAP Participant (Westpac Bank in this case)

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**)

## Features

### GAP Protection / Secure Lockdown

The Guaranteed Authentication Protection (GAP Protection) provides a non-forgable, 99.9% secure system to tell end-users whether they really are on the right server. A non-forgable picture (e.g. logo of the bank) will be displayed. The system utilizes approved algorithms to generate Webfingerprints (including SSL Certificate Fingerprints) to uniquely identify the remote website and issue a seal for those sites that participates in the GAP-Program. For the first time ever, you can be sure that you are really talking to your online bank.

For Websites that are part of the Guaranteed Authentication Protection (GAP Protection), the user's computer will be locked down to secure the actual transmission. No other internet connections except the actual site will be allowed (based on

the Fingerprint of the SSL Certificate and depending on the used Security Policy), providing a general solution to all attacks like the popular XSS Attack or key loggers and/or other greyware.

To demonstrate the technology, the following online banking applications have been integrated into the GAP Database (marked with "demonstration only - demonstration only").

- Australia – Onlinebanking
  - Westpac Banking (<http://www.westpac.com.au>)
  - Macquarie Bank (<http://www.macquarie.com.au>)
  - Commonwealth Bank (<http://www.cba.com.au>)
  - Bank of Queensland (<http://www.boq.com.au>)
- Germany – Onlinebanking
  - Deutsche Bank (<http://www.deutschebank.de>)
  - Citibank (<http://www.citibank.de>)
  - Postbank (<http://www.postbank.de>)

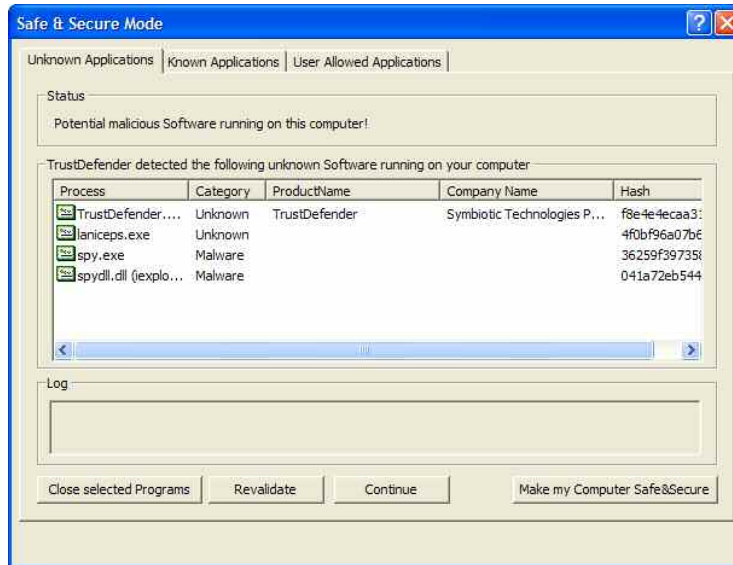
Protection for many other Financial Institutions and other Online Businesses is available from the GapXchange (see below or <http://www.trustdefender.com/content/view/150/114/>)



### Safe & Secure Mode

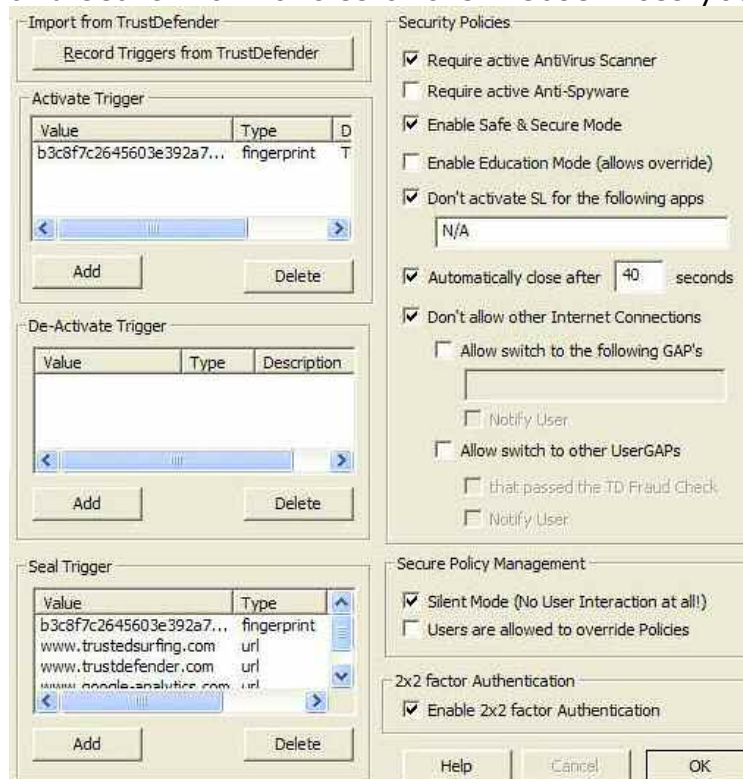
The Safe & Secure Mode is the answer to the growing Problem of Trojans/Worms and Viruses that circumvent the existing signature based Antivirus Scanners. It is based on a "white list" approach that will only allow known and allowed applications to run during an Online Transaction. It can be either activated manually from the TrustDefender

Tray Menu, or automatically as part of a GAP Policy.



## Website GAP Policies

In Addition to the „official“ GAP Participants, TrustDefender Gold gives you the ability to define your very own Security Policies for the Online Services you use. Use the Website GAP Policy Editor to define the Policies or browse the GapXchange and search for Policies of the Webservices you use.



## GapXchange

The GapXchange is a public repository of Website GAP Policies for all TrustDefender Users. You can benefit from the Knowledge and the Work of others to secure the Online

Services you use.

The GapXchange is available at <http://www.trustdefender.com/content/view/150/114/>

GapXchange

This is the GapXchange - a Repository of Website GAP Policy Items for TrustDefender. A Website GAP Policy Item is a complete Security Definition of the Home User's Computer as well as the Website Backend. It will protect your personal and confidential information like no other product on the market.

TRUSTDEFENDER GAPXCHANGE

- ▶ [\(Top\)](#)
- ▶ [Financial Institution](#) (0)
  - ▶ [Internet Banking](#) (0)
    - ▶ [Australia](#) (14) | [USA](#) (1) | [Germany](#) (1) | [UK](#) (1)
  - ▶ [Internet Broking](#) (0)
    - ▶ [Australia](#) (1)
  - ▶ [Stock Exchange](#) (1)

[Add new Category](#)  
[Submit new GapXchange](#)

## TrustedSurfing Internet Database

Whenever TrustDefender will see an outgoing internet transmission or an SSL Connection for a Webfingerprint that is not yet known to the user, it will automatically connect to the TrustedSurfing Internet Database and display its contents. (e.g. like the following Dialog for [online.westpac.com.au](http://online.westpac.com.au))

Note:

1. Although we do not recommend this, but this feature can be disabled in the Preferences.
2. By default, TrustDefender will automatically allow Community Approved Webfingerprints

TrustDefender Warning

**TrustedSurfing Internet Database** ✓

for URL

Known since	7 Weeks, 4 Days
Verified by	TrustedSurfing
Average Rating	●●○○○ (2 Ratings)
How did other users decide?	100% Users allowed it 0% Users blocked it (5 unique Users)

TrustedSurfing Recommendation:  
**You can trust it!**

[Show IP-Block Information](#)

[Show User Ratings](#)

report phishing  
write review

OK No Ask me later show certificate

The following Information is available in the TrustedSurfing Database:

- **Known since**  
This tells you how long the Webfingerprint is known to the community. Latest figures from the Antiphishing Workgroup showed that Phishing Websites are typically brought down in about 5 days. So if the Webfingerprint is known longer, this attribute alone is a pretty good countermeasure against phishing
- **Verified by**  
This tells you whether this Webfingerprint was cross-checked against a different Database. This could be a blacklist from other sources.
- **Average Rating**  
This tells you whether there are already user ratings for this Webfingerprint together with the average rating.
- **How did other users decide?**  
This is one of the powerful features of the TrustDefender Internet Database, because you can "learn" from the other TrustDefender users.
- **Show IP-Block information**  
You'll find the Name and the Country of the Owner of the IP-Address that corresponds to the Webfingerprint. This is really the Name and the Country of the computer your request is going to and NOT just the Name and Country of the person who owns the Domain.
- **Show User Ratings**  
You can see all the current user ratings to make up your mind whether the site is trustworthy or not.

The most important functions are:

- **Report phishing**  
If you are registered to the TrustedSurfing Internet Community, you can report a phishing website straight out of this dialog, making the window-of-vulnerability as small as possible.
- **Write Review**  
Here you can write a user review of the website that will help others to evaluate whether the site is trustworthy or not.
- **Show certificate**  
The advanced users can verify the SSL Certificate BEFORE any data is transmitted to the server. This is not possible with any browsers resulting in explicitly acknowledging the Terms and conditions without any choice!
- **Ask me later**  
This will allow the current Webfingerprint, but will not globally accept it. It will be allowed for the next 5 minutes and you will be asked again after that period
- **Allow**  
This will tell TrustDefender to establish Trust with the

current Webfingerprint

## **Control Center**

You'll enter the TrustDefender Control Center either by double-clicking on the tray icon or by selecting "Control Center" from the TrustDefender Tray Menu (by right-clicking on the TrustDefender Tray Icon)

The Control Center has three pages.

### ***Statistics***

This shows you details on the number of internet requests and the number of internet requests that are checked

### ***Webfingerprints***

You can see a list of all Webfingerprints that are either allowed or blocked. By selecting a Webfingerprint and opening the context-menu (by right-clicking), you can

- Change the action (block or allow),
- Delete the Webfingerprint, or
- View Details, like the SSL-Certificate or the Contents of the TrustedSurfing Internet Database.

### ***Guaranteed Authentication***

Here you see a list of all GAP Protection Participants. You can see the details and the associated Picture. Additionally, you can customize your very own "Secure Favorites". This way, you can just "import" the needed ones. Just select in the Favorite Tree where you want to import the new Favorite and click on "Add to Favorites". These "Secure Favorites" will then automatically be available in the Tray-Menu.

Note: The URL that will be opened by the Favorite cannot be changed or altered. Only the GAP-Participant can change this.

### ***Website GAP***

You'll see a list of all the Website GAP Policies that you have either defined using the Policy Editor or that you have imported e.g. using the GapXchange.

Website GAP Policies are your own Policies for a specific Webservice. Say e.g. you are using the Webmail Service of your ISP, you can use the Policy Editor to define all Hostnames/SSL Fingerprints/... that belong to it.

### ***UserLockdown***

The UserLockdown enables you to define your own Policies in regards to the Secure Lockdown for the Website GAP Policies. Because the Website GAP Policies can come from various sources, you have the ability to define one global Lockdown Policies that apply to all Website GAP Policies.

## **Secure Favorites**

The "Secure Favorites" you have defined in the previous section will be available in the TrustDefender Tray-Menu. Your default browser will automatically be opened to load the respective page.

## **Preferences**

You can define the behaviour of TrustDefender here...

### ***Firewall***

TrustDefender has a personal Firewall built in to prevent any attacks during the "Secure Lockdown". The Firewall is activated during startup and will block any internet requests to port 80 (HTTP) and port 443 (HTTPS) except for TrustDefender. During the "Secure Lockdown" the Security is even tighter as it is guaranteed that all communication is analyzed by TrustDefender.

Note: During the "Secure Lockdown" no other programs can connect to the internet, meaning that e.g. Instant-Messengers, or any other software running in background will stop working during this time. However they should recover nicely after the "Secure Lockdown" is finished.

### ***Community***

It is not mandatory, but you are highly encouraged to login to the TrustedSurfing Community when using TrustDefender. This will enable the "write review" and the "report phishing" options in the TrustedSurfing Dialog. Just register as a new user and enter your credentials here.

## **History**

There is a history of Webfingerprints that have been checked by TrustDefender. This option is available from the TrustDefender Tray Menu ("History"). You can easily change the action for a Webfingerprint (e.g. from allow to block or vice versa).

## **Limitations of the Beta Release of the Gold Edition**

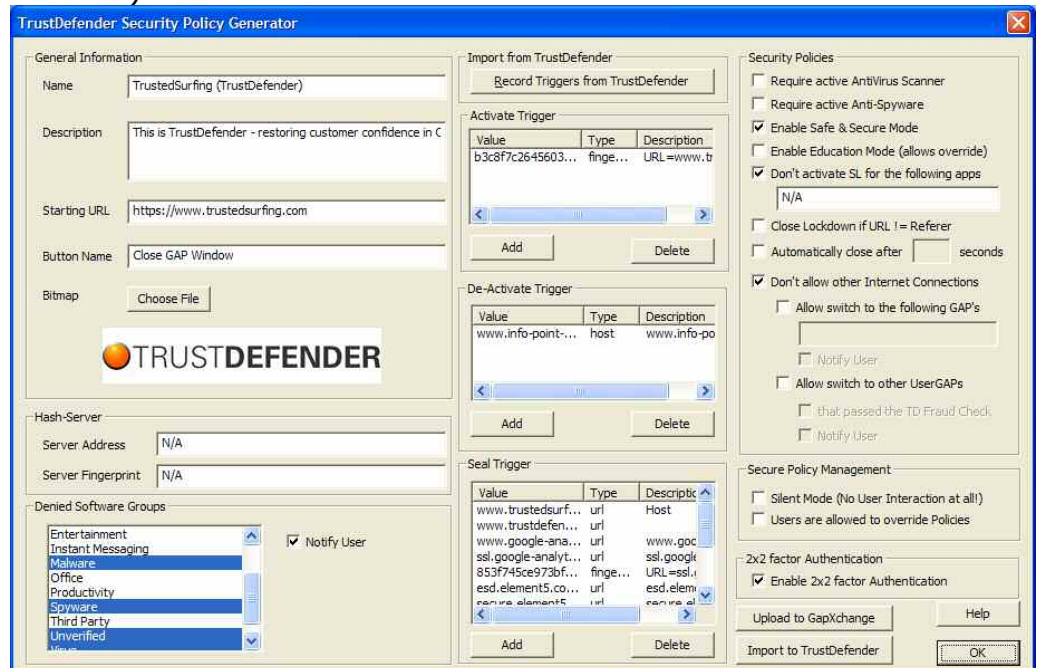
There are a few limitations of the Release Candidate software of TrustDefender.



- The Beta Release will expire at the End of September

## 2. TrustDefender Website GAP Policy Generator

The Policy Generator can be used to define the Website GAP Policies. The Policies will be stored as an XML File (Extension .gap). From the Startup Window, you have basically the following Options

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



- 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.