

TrustDefender Policy Generator

Introduction

The TrustDefender Policy Generator enables you to define the Information for the GAP Program and also the Secure Policies for the Secure Lockdown. The Output of the Policy Generator is an XML File which contains all the information. You also have the ability to export the Policies to the TrustDefender running on your local computer in order to "test-drive" the Policies.

Note: You need at least TrustDefender v1.2 to use this feature.

How does it work? (Central GAP Database)

The Output of the Policy Generator will be an XML File. Additionally a Hash Value will be generated. This Hash Value is important to make sure that the Information that gets into the TrustDefender GAP Database matches exactly your ones.

The workflow is as follows

- Define the Policies and Save the XML File (e.g. customer.xml)
- Note the Hash Value
- Upload the XML File using the Upload Script in the Protected Area of the TrustDefender Website
- You'll receive an email with the Hash value and a unique ID generated on our Server. If that Hash Value is correct, you can approve the Policies by replying to the email
- After we received your Approval, the Policies will be stored in the GAP Database and will be pushed to all existing TrustDefender Users.

How does it work? (Evaluation)

With the File -> Export to TrustDefender Option, you can test drive the GAP Policies and the Secure Lockdown on your local machine. Just copy the evalgap.db3 File to the conf/ Subdirectory of TrustDefender (typically C:\Program Files\TrustDefender\TrustDefender\conf). TrustDefender will automatically detect this and use it without restarting.

To remove, just delete the evalgap.db3 File from the conf\ Subdirectory

Using the Policy Generator

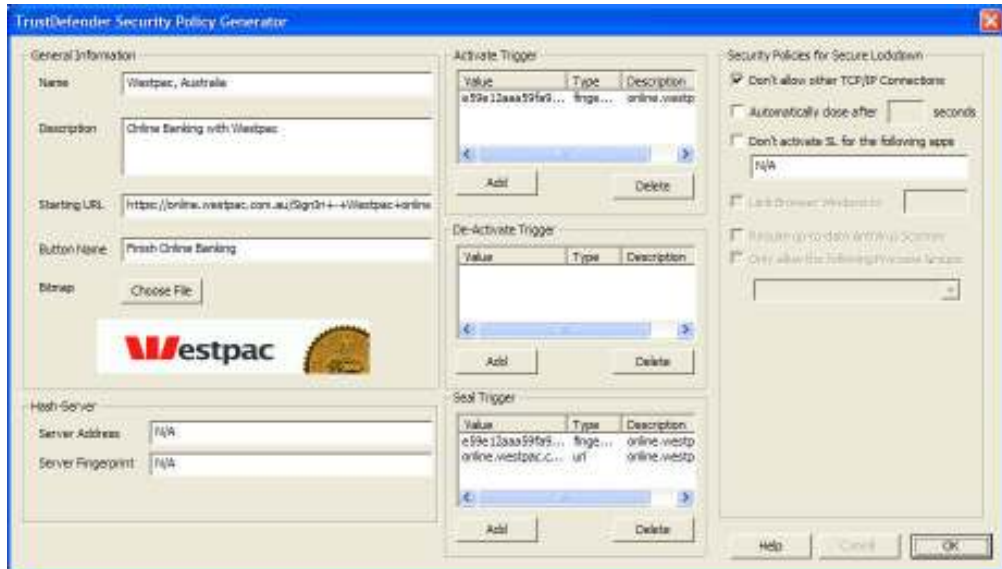
With the Policy Generator you can Load/Save/Export the GAP XML Files and most importantly you can generate them.

File Menu

The File Menu should be straightforward and you can Load and Save GAP XML Files. A history of the recent Files is also available. The Export to TrustDefender will generate a evalgap.db3 File which has to be copied to your TrustDefender conf/ Subdirectory (typically C:\Program Files\TrustDefender\TrustDefender\conf). TrustDefender will automatically recognize it and you can just delete it if you don't need it any more

Policy Menu

The Policy Menu will give you the ability to define the GAP Policies as well as to verify the Integrity of the XML File and the Verification of the Hash Value.



General Information

- Name
This is a short descriptive Name of the GAP Participant including the Country (e.g. Esendex, UK). This Name will be displayed in the GAP Window below the Logo.
- Description
This is a Description and please feel free to describe your Product/Services in detail.
- Starting URL
This is the URL for the Secure Favourites and this URL will be invoked by TrustDefender if a User clicks on the Entry in the Secure Favourites.
- Bitmap
This is the logo/bitmap that will be displayed in the GAP Window.
IMPORTANT: The bitmap will be resized to 250x50! Supported File Formats are BMP, GIF, JPG

Hash Server

- Hash-Server Address
This is the Hostname or IP Address of an independent Hash Server (that you have to provide!). If a Hash Server is configured, TrustDefender will check the local GAP Database and verify the Hash of the GAP Participant with this independent Hash Server to make sure that the GAP Information is accurate.
- Hash Server Fingerprint
If the Hash Server is SSL enabled, you HAVE to specify the SSL SHA-1 Fingerprint of the Certificate.

GAP Trigger

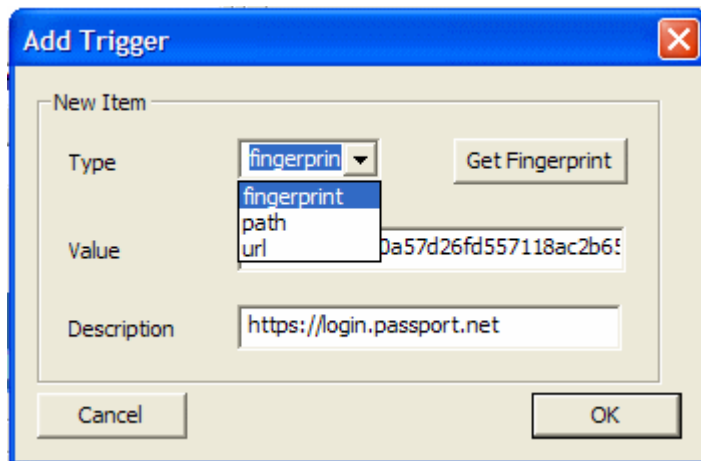
- Activate Trigger
This is a list of URL's and SSL Fingerprints that will trigger the GAP Window. If you specify multiple Entries, please keep in mind that they ALL will be evaluated (AND)
- De-Activate Trigger
The same as Activate Trigger, except that these URL's or SSL Fingerprints will trigger the GAP Window to disappear. This is typically called during Logout

- Seal Trigger
All URL's and SSL Fingerprints that are allowed during a Transaction **HAVE TO** be listed here. This means automatically that all URL's and SSL Fingerprints from Activate Trigger will have to be configured here also.

All of these three Sections have an Add and Delete Button to modify the Entries.

Add

You'll see the following Dialog coming up. You can specify either a Hostname (url), an SSL Fingerprint (fingerprint) or a Path from a HTTP Request (path). The "Get Fingerprint" Button will help you to retrieve the SSL SHA1 Fingerprint of a Webserver.



Delete

Just select the Entry you want to delete and press Delete.

Secure Policies for Secure Lockdown

- Don't allow other TCP/IP Connections
If checked, TrustDefender will lock down the User's Computer to allow only the URL's and SSL Fingerprints specified in Seal Trigger
- Automatically close after x seconds
You can specify that the GAP Window will only be displayed for the specified seconds and automatically disappears after that.
- Don't activate Secure Lockdown for the following apps
You can specify a list of Applications (e.g. myownapp.exe). These applications will never trigger the GAP Window even if they make requests that typically would.