Commercial Banking Customers

Trusteer
an IBM Company

Securing Your Business's Bank Account

Trusteer Rapport Resource Guide For Business Banking

January 2014

new threats, ***new thinking***

Table of Contents

1. Introduction

Welcome to Trusteer Rapport! We're proud to provide you with multi-layer security, protecting your banking customers' assets and your bank's reputation while meeting federal guidance for online security.

This **Resource Guide to Trusteer Rapport for Business Banking** has been specifically designed to educate business banking customers and IT and Security professionals about Trusteer Rapport. The document explains how to deploy Trusteer in an enterprise network and how Trusteer protects online business banking.

Who is Trusteer?

Trusteer, an IBM company, is the leading provider of endpoint cybercrime prevention solutions that protect organizations against financial fraud and data breaches. Hundreds of organizations and millions of end users rely on Trusteer to protect their web applications, computers and mobile devices from online threats that are invisible to legacy security solutions. Trusteer's Cybercrime Prevention Architecture combines multi-layer security software with real-time threat intelligence to achieve sustainable protection against malware and phishing attacks and meet regulatory compliance requirements. Leading organizations such as HSBC, Santander, SunTrust and Fifth Third are among Trusteer's clients.

For more information visit: www.trusteer.com.

2. What is Trusteer Rapport?

Trusteer Rapport is advanced security software that protects your online banking communication from being stolen by criminals. Trusteer Rapport is highly recommended and offered by your bank as an additional layer of security to any antivirus or security software your organization already uses. By protecting your internet connection and creating a tunnel for safe communication with your bank's website, Trusteer Rapport blocks malicious attempts to steal money from your business account.

Video: **Introduction to Trusteer Rapport**
Or visit: http://www.trusteer.com/introduction-to-rapport

Trusteer Rapport should be used even if the computer and network are protected with other desktop and network security solutions. Recent studies show that security solutions such as antivirus and firewalls are only partially effective against financial malware attacks, including Zeus, SpyEye, Gozi and Torpig, to name a few. Integrated with the bank's fraud prevention processes, Trusteer Rapport adds an important layer of security on top of desktop and network security products and is capable of detecting, alerting and preventing even the most sophisticated financial attacks.

The service is free as long as it is used by online banking customers to protect online banking sessions and additional non-enterprise related web sites (e.g. ecommerce, web mail). If you intend to use Trusteer Rapport to protect access to enterprise applications of employees and other corporate users, or to prevent critical data exfiltration from your organization, please contact Trusteer for additional information on Trusteer Apex.

Antivirus: A False Sense of Security

There's something that the antivirus industry doesn't want you to know: their products aren't very effective at stopping sophisticated viruses. According to Krebs On Security, statistics indicate that **antivirus software detects only about 25% of the most popular malware** currently being emailed to people. That's because the virus creators move too quickly. By the time antivirus products are able to block new viruses, it is often too late. The bad guys have already managed to tap into a customer's bank account.

Signature Detection Doesn't Work

To identify new viruses (also known as 'malware'), antivirus solutions calculate a special signature for each incoming file, and compare it to a dictionary of known virus signatures. Antivirus solutions cannot defend against malware unless a file sample has already been obtained and a signature created. The problem is that malware authors are also very, very clever. They are able to create millions of files, each with a unique signature every month. The same malware can be masked in many different files, each with its own signature that is unknown to the antivirus. Antivirus solutions take days, sometimes even weeks, to detect new financial malware signatures and remove them. However, fraud can occur hours after a new malware file with an unknown signature is released. So, by the time the antivirus provider eventually cleans the computer of the malware, it may already be too late to prevent fraud from occurring.

The Trusteer Rapport Approach

Trusteer's innovative technology picks up where conventional security software fails. From the moment it is installed, Trusteer Rapport protects the customer's device and mitigates financial malware infections. Trusteer also communicates with the bank, allowing your team to take immediate action against changes in the threat landscape. Trusteer Rapport doesn't look for file signatures. It doesn't bother to examine what the file is, but rather what the file does. Trusteer Rapport detects the malware installation process and breaks it – keeping the computer clean. Even if malware managed to install on the device, Trusteer Rapport detects and blocks any attempt by the malware to compromise the browser and your online banking session. By stopping the malware's malicious behavior, Trusteer Rapport is able to provide protection above and beyond what is possible with an antivirus solution. This is why the bank has chosen to partner with Trusteer to offer you and your customers the best protection against financial fraud.

Extra Layer of Protection

Trusteer Rapport is optimized to stop financial malware and prevent financial fraud. But that doesn't mean you should discard your antivirus solutions entirely. Many other viruses exist. They will slow down your computer or interfere with your work, but they will not attempt to steal money from you. Your antivirus solutions should be used to protect you from these types of viruses.

How Trusteer Rapport Protects

- Removes existing financial malware from your computer immediately
- Prevents financial malware infections when accessing malicious websites or downloading malicious applications
- Stops phishing attacks from stealing your credentials and data
- Automatic updates are done in the background keeping up with the latest threats
- Compact software that won't slow down your computer or interfere with your applications
- Protection starts with a quick installation (to ensure full protection please restart your computer)

Proven Technology from Trusteer

Trusteer Rapport was developed by the online security experts at Trusteer and currently protects tens of millions of users worldwide. In an independent study, Trusteer Rapport stopped 100% of all financial malware used by testers to try and infect a protected machine.

3. Installing and Using Trusteer Rapport

Trusteer Rapport should be installed on every computer used for online banking.

Desktop Installations

Trusteer Rapport can either be installed manually on each computer or remotely using a software distribution solution such as System Center Configuration Manager (SCCM).

When installing manually, Trusteer Rapport software should be downloaded from the link provided by the end user's bank. The download is as simple as running the installer and following instructions.

It is highly recommended to install the software as an administrator. The end-user will then be able to use Trusteer Rapport from any limited account; that is, the end-user will not need administrative rights to use Trusteer Rapport.

It is also possible to install Trusteer Rapport as a limited user without administrative rights. However, the level of security provided is reduced when installing in such a scenario.

Some banks require users to install Trusteer Rapport using an administrator account and do not allow end users to connect to the online banking service otherwise. In this type of deployment, if more than one end-user uses the computer, Trusteer Rapport must be installed with administrator rights to enable all end users to benefit from it. However, if the bank does not require installation using an administrator account, all users on a single computer with a limited user account can install their own instance of Trusteer Rapport.

Server Installations

Trusteer Rapport supports Windows Server (2003 and 2008). Trusteer Rapport also supports multiple user sessions, enabling a single installation to handle multiple profiles, as required for a shared virtual desktop infrastructure. Trusteer Rapport detects when you run the installation process on Windows Server (2003 or 2008) and installs a server version that includes the ability to disable the sending of restart requests to users, in order to avoid a situation in which one user restarts the system for all users running on the system. For information about disabling restart requests, see Trusteer Rapport Virtual Environment Best Practices.

To install Trusteer Rapport on Windows Server 2003 or 2008:

Run the file RapportSetup.exe. You can obtain the standard version of this file from http://www.trusteer.com/support/rapport-installation-links. If you are a business customer, you can obtain your customized version of this setup file from your Trusteer project manager.

For further details on Trusteer Rapport installation options please contact Trusteer support using this form: http://www.trusteer.com/support/submit-ticket-step-2.

Virtual and Remote Implementations

Trusteer Rapport can be installed on a few virtual environments. If Trusteer Rapport is installed remotely, we recommend using some of the installer command parameters. Trusteer Rapport setup is based on Microsoft Installer (MSI) technology and, like every MSI based installation, the Trusteer Rapport installer also gets command line parameters through the MSI properties mechanism.

The following properties are supported:

- **NOBROWSER**: When set to true, Trusteer Rapport does not open a post-install page.
- **NOICONS:** Do not create Trusteer Rapport shortcuts in the start menu.

Both the bootstrap file (RapportSetup.exe) and the full installation file (RapportSetup-Full.exe) support passing parameters to the MSI they control.

The following command line flags are supported:

- **/s**: Silent installation. This must be the first parameter.
- **/p** <*list of properties*>: These are properties to pass on to the MSI.

For example, to start a silent installation without installing shortcuts, use the following command:

```
RapportSetup-Full.exe /s /p NOICONS=true
```

The installer also provides the ability for the administrator to set a password for uninstalling Trusteer Rapport and shutting down the Trusteer Rapport process. In order to set the administrator password, the following arguments should be passed during the installation process:

- SHUTDOWNPASSWORD with the desired password. When you set this password, every time users attempt to stop Trusteer Rapport, they will be prompted to enter this password.
- UNINSTALLPASSWORD with the desired password. When you set this password, if users attempt to uninstall Trusteer Rapport, they will be prompted to enter this password.

Note: SHUTDOWNPASSWORD and UNINSTALLPASSWORD are independent of each other.

Examples:

To install Trusteer Rapport and configure the shutdown and uninstall passwords:

```
msiexec /I RapportSetup-Full.msi SHUTDOWNPASSWORD=123456 UNINSTALLPASSWORD=123456
```

To uninstall Trusteer Rapport using the password configured during installation:

```
msiexec /x{1DD81E7D-0D28-4ceb-87B2-C041A4FCB215} /quiet PASSWORD=123456 SKIPOPTIONS=true
```

To stop Trusteer Rapport using the password configured during installation:

```
RapportService.exe -shutdown -password=123456
```

For further information about virtual implementations, see *Trusteer Rapport Virtual Implementation* Scenarios. You can obtain this document from your Trusteer representative.

User Experience

Once installed, Trusteer Rapport's software-based service is virtually transparent and non-invasive. It aims to avoid interfering with the end user's computer and is simple, requiring no prior knowledge or training. End users can continue banking and using the Internet in exactly the same way as before. The end user log-in process remains unchanged and no configuration changes are required. Trusteer Rapport's service works in the background and unlike typical desktop security solutions, does not interrupt end users with security issues. The green favicon appearing on the right side of the browser address bar indicates that Trusteer Rapport is helping to protect that website against malware attacks.

Supported Platforms and Configuration

Trusteer Rapport works with all major browsers and operating systems. For more information, see http://www.trusteer.com/support/supported-platforms.

Machine Footprint

Processes	• RapportService.exe • RapportLaunService64.exe (64-bit machines)
Services	• RapportMgmtService.exe
Drivers	• RapportPG.sys (RapportPG64.sys on 64-bit machines) • RapportKELL.sys (RapportKE64.sys on 64-bit machines) • RapportCerberus • RapportEI • RapportIaso
Program size (including end user profile space for logs and settings)	Approximately 250 MB, depending on the number of different browsers used on the machine.
Icons	• Start Menu icons (appear as Trusteer Endpoint Protection) • Browser icon • Task bar con
Virtual memory usage	35 MB This is combined between the services and the backend process, depending on other software installed on the machine. The value may be slightly higher on 64 bit machines.

Troubleshooting & Support

A complete troubleshooting FAQ is available at the following link:
http://www.trusteer.com/support/faq.

Questions from end users about the issues mentioned below are most likely a result of activity blocked by Trusteer.

- Unable to take screen captures of Trusteer-protected web pages using automated tools
- Browser add-ons that stop working while on the bank's website
- Keyboard issues on Trusteer Rapport protected websites
- Trusteer warning dialogs

The solution to these issues is documented in the FAQ link above and requires a small change to the Trusteer Rapport policy. Note that the end user can always turn off Trusteer Rapport by opening the console and clicking "Stop". This allows you to check whether a specific problem is Trusteer Rapport related. We recommend avoiding the removal of Trusteer Rapport while troubleshooting. Stopping Trusteer Rapport has the same effect and allows Trusteer to quickly and efficiently resolve any issues when end users contact the Trusteer support team.

4. Trusteer Rapport Updates

Fighting fraudsters is a constant battle. Trusteer's security and intelligence teams consistently adapt and monitor the effectiveness of Trusteer Rapport protections by issuing new protections and software updates or upgrades which include security and product enhancements.

Product updates are not expected to cause any additional load on your network. These are normally a few megabytes in size and are similar to a user surfing online to a few webpages. You can expect these updates to occur quite frequently.

Product upgrades are less frequent and occur once every a few months. During the upgrade a certain increase in network resources could be seen if Trusteer Rapport is installed on a large number of machines.

Product upgrades can also be controlled using the Trusteer Rapport Console, by defining a proxy to manage the connection with the Trusteer Cloud. This ensures all communication of Trusteer Rapport agents will be done via your organization's proxy. For further instructions please visit this page.

5. Trusteer Rapport Self Protection

Trusteer Rapport includes a self-protection mechanism to help prevent malware from terminating or removing the software. As a result, the task manager cannot be used to kill its processes.

➡ **To stop Trusteer Rapport:**

- From the Windows Start menu, select **Programs** > **Trusteer Endpoint Protection** > **Stop Trusteer Endpoint Protection**. A CAPTCHA appears which you must enter.

6. Uninstall Instructions

Instructions on how to remove Trusteer can be found at the following link:
http://www.trusteer.com/book/uninstalling-rapport.

For instructions on the removal of Trusteer Rapport by force in case of errors during the normal procedure, please go to the following link:
http://www.trusteer.com/book/uninstalling-rapport-using-safeuninstall-utility.