



IBM Security Trusteer Rapport

Reference Guide

Version 3.5.1403

December 2014

Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "**AS IS**" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.



Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

Copyright License

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. 2004, 2014. All rights reserved.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.



Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.



Privacy Policy Considerations

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings.

For more information about the use of various technologies, including cookies, for these purposes, see the "IBM Software Products and Software-as-a-Service Privacy Statement" at <http://www.ibm.com/software/info/product-privacy>.

Contents

Notices	ii
Copyright License	iii
Trademarks	iii
Privacy Policy Considerations	iv
1. Front Matter	1
About this Guide	1
<i>Need More Information about Rapport?</i>	1
<i>Sending us Feedback</i>	1
Support Information	1
Accessibility	2
Statement of Good Security Practices	2
2. What is Rapport?	3
Antivirus: A False Sense of Security	4
Signature Detection Doesn't Work	4
The Rapport Approach	5
Extra Layer of Protection	5
Which Attacks Does Rapport Protect Against?	6
<i>Phishing</i>	6
<i>Pharming or DNS Spoofing</i>	7
<i>Keylogging</i>	7
<i>Man-in-the-Middle</i>	7

<i>Man-in-the-Browser</i>	8
<i>Screen Capturing</i>	8
<i>Session Hijacking</i>	9
<i>Drive-by Download</i>	9
How Does Rapport Protect Your Customers?	9
<i>Safe Communication with Protected Sites</i>	10
<i>Login Protection</i>	10
<i>Browsing Session Protection</i>	11
<i>Keystroke Protection</i>	11
<i>Payment Card Protection</i>	11
<i>Screen Capture Blocking</i>	12
<i>Website Validation</i>	12
<i>Browser Add-on Blocking</i>	12
<i>Process Alteration Blocking</i>	12
<i>Malicious Website Warnings</i>	13
<i>Unauthorized Access Reporting</i>	13
<i>Overlay Attack Prevention</i>	13
The User Experience	13
Getting More Out of Rapport	14
Information for Advanced Users	15
<i>Rapport's PC Footprint</i>	15
<i>Rapport and Your Privacy</i>	16
<i>Rapport Central Service: Powerful Fraud Blockage</i>	16

3. Installing Rapport	18
Installing Rapport on Windows 8 Using Internet Explorer	20
Installing Rapport on Windows Server (2003 or 2008)	23
How do I switch to an Administrator Account?	24
4. Getting Started	25
Open the Rapport Console	26
5. Protecting Your Online Banking	27
6. Using Payment Cards Safely Online	28
7. Responding to Alerts and Warnings	29
Responding to a Password Protection Offer	29
Responding to a Protected Information Warning	33
Responding to a Non-Secure Submission Warning	35
Responding to a Phishing Site Warning	36
Responding to a Payment Card Submission Detection Warning	38
Responding to a Payment Card Protection Message	39
Responding to a Print Screen Attempt Detected Alert	39
Responding to a Browser Protection Alert	40
Responding to an Activate Malware Removal Alert	42
Responding to a Malware Removal Initiated Alert	43
Responding to an Invalid Certificate Warning	43
Responding to a Standard User Account Warning	46
Responding to an Activity Report Notification	46

Responding to a Code Update Confirmation Message	47
Responding to a Screen Reader Compatibility Mode Warning	47
Responding to a Reinstall from Admin Mode Alert	48
<i>Switching to an Administrator Account (Windows 8)</i>	50
<i>Switching to an Administrator Account (Windows 7)</i>	51
<i>Switching to an Administrator Account (XP)</i>	53
8. Customizing Rapport	55
Hiding and Restoring the Rapport Address Bar Icon	55
Hiding and Restoring the System Tray Icon	56
Changing Interface Language	57
9. Viewing Rapport Activity	58
Viewing the Activity Report	58
Configuring the Activity report	59
<i>Clearing the Activity Report</i>	60
<i>Disabling the Activity Report</i>	60
10. Scanning your Computer for Security Improvements	61
Running a Manual Scan	61
Viewing the Security Best Practices Report	62
11. Managing Protected Sites and Passwords	65
Protecting Additional Websites	67
Removing Protected Websites	68
Managing Protected Usernames and Passwords	69

12. Modifying Rapport Security Policy	71
Viewing Security Policy Summary	71
Changing Security Controls	72
Understanding Security Policy Controls	74
<i>Block Screen Capturing</i>	74
<i>Validate Website SSL Certificates</i>	75
<i>Block Unknown Browser Add-ons</i>	76
<i>Block Access to Information inside the Browser</i>	77
<i>Block Access to Sensitive Website Cookies</i>	78
<i>Validate Website IP Addresses</i>	78
<i>Activate Character Replacement</i>	79
<i>Activate Kernel Character Replacement</i>	80
<i>Block unauthorized modules in the browser</i>	80
<i>Warn when browsing to malicious sites</i>	81
<i>Warn When Login Information is Used in Unknown Websites</i>	81
<i>Block Browser Process Alteration</i>	83
<i>Protect Trusteer Endpoint Protection from Unauthorized Removal</i>	83
<i>Early Browser Protection</i>	84
<i>Send Security Events and Errors for Analysis</i>	84
<i>Remove Malware</i>	85
<i>Protect Payment Card Numbers from Theft</i>	86
<i>Warn when I submit security data to insecure sites</i>	87
13. Troubleshooting	88

Stopping Rapport	88
Starting Rapport	89
Getting Support	90
Unblocking Legitimate Browser Add-ons	90
Disabling Keylogger Blocking	91
Undoing Accidental Authorizations	92
<i>Clearing Authorized Invalid SSL certificates</i>	93
<i>Clearing Trusted Sites for Payment Card Submission</i>	94
<i>Clearing Trusted Sites for Non-Secure Submissions</i>	95
<i>Clearing Websites to Which You Allowed Sending Login Information</i>	96
Handling Errors	97
<i>Handling an Update Error</i>	97
<i>Handling Rapport Installer Errors</i>	98
<i>Handling Uninstall Errors</i>	98
Configuring a Proxy Server for Automatic Updates	99
Sending a User Problem Report	100
Copying the Trusteer Endpoint Protection ID	101
Sending Rapport Log Files to IBM	101
Installation Issues	101
<i>Uninstall not Completed</i>	102
<i>Installation Stuck in 'Select Destination' (Mac only)</i>	102
<i>Windows Installation Error 1638</i>	102
<i>Windows Installation Error 16xx</i>	103

<i>Windows does not Support Digital Signatures</i>	104
<i>Installation Ended Prematurely</i>	104
Rapport Icon	106
Splash Screen Issues	108
<i>Splash Screen Appears when Rapport is Not Installed</i>	108
<i>Splash Screen Appears but Rapport is Already Installed</i>	109
Performance Issues	111
<i>Slow Computer or Web Browser</i>	111
<i>High CPU or Memory Usage</i>	112
Interoperability Issues	112
<i>Password Managers</i>	113
<i>Screen Capturing Software</i>	113
<i>Visually Impaired Mode (Screen Readers or Magnifiers)</i>	114
Other Issues	114
14. Keeping Rapport Updated	116
Checking the Status of Rapport Updates	116
Manually Updating Rapport	118
Disabling Automatic Updates	119
15. Uninstalling Rapport	121
Uninstalling Rapport (Windows 8 and Windows 7)	121
Uninstalling Rapport (Windows XP)	122
16. Upgrading Rapport	123

1. Front Matter

About this Guide

This guide explains how to use IBM Security Trusteer Rapport ("**Rapport**") and get the maximum benefit from the product. This guide is for:

- Customers of banks or other financial institutions that offer Rapport for free download as a security tool to protect the online use of financial accounts.
- Customers of Rapport-protected payment cards who use Rapport to secure online payment card transactions.

Need More Information about Rapport?

To complement this guide, IBM provides a complete FAQ (frequently asked questions) here: <http://www.trusteer.com/support/faq>.

On the FAQ web page, type your question into the Instant Answers tool to get answers to extra questions you might have.

Sending us Feedback

IBM values your feedback.

- Suggest new features and improvements and express your opinion about Rapport.

To send feedback about Rapport, go to:

<http://www.trusteer.com/support/product-feedback>.

Support Information

For support information, refer to the Support website:

<http://www.trusteer.com/support>

Accessibility

Accessibility features help users with a disability, such as restricted mobility or limited vision, to use software products successfully. With this product, you can use assistive technologies to hear and navigate the interface.

Statement of Good Security Practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your organization. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM® systems, products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ORGANIZATION IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

2. What is Rapport?

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

For a short introductory video about Rapport, go to:

<http://www.trusteer.com/introduction-to-rapport>

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, Rapport adds an important layer of security on top of desktop and network security products. Rapport can detect, alert, and prevent even the most sophisticated financial attacks.

In partnership with your organization, Rapport is provided free of charge to your customers and enables them to protect their online banking sessions and other non-enterprise related websites (for example, e-commerce, webmail).

Just how prevalent is financial cybercrime?

In 2011, the FBI identified twenty incidents of attempted fraud totaling \$20 million where online banking credentials of small to medium sized US business were compromised and used to initiate wire transfers to Chinese economic and trade companies. According to estimates, cybercrooks are stealing as much as \$1 billion a year from SMBs in the US and Europe. Corporate bank accounts are sensitive targets and are increasingly being attacked by fraudsters. One of the biggest risks is the computer that is used to bank with. Criminals use two sophisticated attacks to access online accounts through the computer:

- **Malicious software (or malware)** - automatically and silently downloaded onto the computer when users browse the Internet, malware silently captures login information and transfers it to criminals as login is performed and can also silently change transactions that are executed.
- **Phishing** - criminals build fake websites that look very similar to your bank's website to lure you into going to them and submitting your online banking login information, which is later used to access your account.

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 might already be too late to prevent fraud from occurring.

The Rapport Approach

IBM's innovative technology picks up where conventional security software fails. From the moment it is installed, Rapport protects the customer's device and mitigates financial malware infections. IBM also communicates with the bank, allowing your team to take immediate action against changes in the threat landscape.

Rapport doesn't look for file signatures. It doesn't bother to examine what the file is, but rather what the file does. Rapport detects the malware installation process and breaks it – keeping the computer clean. Even if malware managed to install on the device, 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, Rapport is able to provide protection above and beyond what is possible with an antivirus solution. This is why the bank works closely with IBM to offer you and your customers the best protection against financial fraud.

Extra Layer of Protection

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.

Which Attacks Does Rapport Protect Against?

Rapport's proprietary browser lockdown technology prevents unauthorized access to information that flows between customers and websites regardless of which specific malware issues the threat.

Rapport is effective in blocking all of these techniques:

- [Phishing](#)
- [Pharming or DNS Spoofing](#)
- [Keylogging](#)
- [Man-in-the-Middle](#)
- [Man-in-the-Browser](#)
- [Screen Capturing](#)
- [Session Hijacking](#)
- [Drive-by Download](#)

Phishing

A *phishing* attack is when the criminal builds a website that looks exactly like a website you know and trust (for example, your bank's website). The criminal then convinces you to go to this website (for example, by sending you a fraudulent email with a link to the website). When you arrive at the fraudulent website, you mistakenly believe that it is the real website. As soon as you try to sign in to this fraudulent website, the criminal grabs your sign-in credentials and can now use them to sign in to the genuine website on your behalf.

To protect you against phishing attacks, Rapport:

- Warns you if you try to access a website that is known to be a malicious website.
- Warns you when you enter a password into a website that does not submit data securely. Sites that do not submit data securely are high risk sites and include legitimate sites that might easily be intercepted by criminals.
- Can automatically redirect you to the genuine banking site that the phishing website pretended to be, or to a phishing FAQ or education campaign site.

Pharming or DNS Spoofing

A *pharming* or *DNS spoofing* attack is when the criminal causes your computer to go to a fraudulent website each time you type a real website's address in your browser's address bar. The attack achieves this using various techniques such as infecting your desktop with malware or by compromising servers in your ISP's network. When you arrive at the fraudulent website and try to sign in, the criminal grabs your login credentials and can now use them to log in to the genuine website, impersonate you and initiate fraudulent transactions. To protect you against pharming attacks, Rapport verifies the IP address and the SSL certificate of the website each time you connect to a protected website. If the verification fails, Rapport terminates the connection and establishes a new connection to the real website.

Keylogging

A *keylogger* is a malicious program that resides unnoticed inside your computer. The keylogger records your keystrokes when you type with the keyboard and then sends this information to the criminal. In this way, keyloggers can grab sign-in credentials as you type, payment card numbers, and other sensitive information and send them to the criminal who can use your credentials to log in to your accounts, impersonate you and initiate fraudulent transactions. Rapport blocks keyloggers by encrypting your keystrokes so that keyloggers cannot read sensitive information.

Man-in-the-Middle

Man-in-the-Middle is an advanced variation of phishing and pharming attacks. In this particular attack, you sign in to the website and start to work, all the while entirely unaware that all the information exchanged between you and the website is passing to the criminal through an intermediate website that can see any private information and can alter your transactions. For example, if you request to transfer a certain amount of money to a specific payee, the criminal can change the payee's identity and transfer the money to a different account.

Rapport prevents malicious redirection of the browser to fraudulent sites by using multiple layers of verification, such as verifying that the website IP address and website certificate are legitimate.

Man-in-the-Browser

Man-in-the-Browser is malware that infiltrates your browser, sometimes in the form of a legitimate add-on, such as a toolbar, BHO, or browser plug-in. This malware controls everything that happens inside your browser. It gathers sensitive information such as your sign-in credentials and passes them to the criminal. It can also generate transactions on your behalf, such as transferring money from your account to the criminal's account.

Rapport prevents malware from touching data within the browser through multiple mechanisms:

- Blocks malware from accessing sensitive information even before the malware is recognized.
- Identifies and removes malware as early as possible. Removing malware stops it from morphing into a variant that is either harder to block or attacks the security solution that is trying to block it. Moreover, Rapport can detect and remove multiple variants of the same malware regardless of the binary file that is used by the variant.
- Prevents you from unknowingly downloading identified malware even from legitimate websites.

Screen Capturing

Malware can include screen capture mechanisms that capture your screen and send them to the criminal. Screen captures might show your account details, balance, and even credentials, if the website uses keypads in the login page. Rapport disables screen capture mechanisms while you are connected to protected websites.

Session Hijacking

Session hijacking malware steals the parameters of your session with a specific website and sends this information to the criminal. The criminal then uses these session parameters to take over your session with the website and bypass the authentication process that is required to log in to the website. Rapport prevents access to session parameters while you are connected to protected websites.

Drive-by Download

In a drive-by download, you unknowingly download malicious malware simply by going to a website. The website might be a legitimate website that has been infected so that it will invisibly download malware to your computer.

How Does Rapport Protect Your Customers?

When installed on your computer, Rapport automatically protects websites that belong to business partners that work with IBM to provide the highest level of security for their enterprise and customers. Rapport's protection can also be manually applied to all the other websites that you use in which you sign in and exchange sensitive information, such as personal financial information or sensitive data.

When you connect to a protected website, Rapport does three main things in the background to make it extremely difficult for criminals to target you:

- Rapport verifies that you are connected to the genuine website as opposed to a fake website created by criminals.
- After verification is complete, Rapport locks down communication between your computer and the protected website. This prevents criminals from hijacking your online connection with the bank.
- Rapport protects your computer and Internet connection by creating a tunnel for safe communication with your bank or enterprise, preventing criminals from using malware to steal your log-in data and tamper with financial transactions or information exchanges.

Rapport adds an important and unique security layer that allows business partners to better protect your sensitive information and promptly react to threats aimed directly at you.

These are some of the specific ways in which Rapport protects your communication, data, and finances:

- [Safe Communication with Protected Sites](#)
- [Login Protection](#)
- [Browsing Session Protection](#)
- [Keystroke Protection](#)
- [Payment Card Protection](#)
- [Screen Capture Blocking](#)
- [Website Validation](#)
- [Browser Add-on Blocking](#)
- [Process Alteration Blocking](#)
- [Malicious Website Warnings](#)
- [Unauthorized Access Reporting](#)
- [Overlay Attack Prevention](#)

Safe Communication with Protected Sites

When you connect to a protected website, Rapport blocks any processes on your computer from accessing the website. You communicate safely with the website, shielded from any hostile access attempts by malware. Even if you have unrecognized hidden malware that is lurking on your computer, it cannot read sensitive information from the website or tamper with your transactions.

Login Protection

When you sign in to a protected website, the website authenticates you with secure login credentials, such as a user name and password. The problem is that criminals have several methods of grabbing your login credentials, such as phishing, and by using them to sign in to your online account.

Browsing Session Protection

When you sign in to a website, the website stores a text file that is called a session cookie in temporary memory for the duration of the session. The session cookie identifies your authenticated session and enables you to repeatedly exchange sensitive information with the website's server without logging in again.

Malware can grab session cookies and use them to bypass authentication and take over your session with the website. To protect you from this type of attack, Rapport blocks applications from accessing session cookies on partner websites.

Note: This feature is supported only for partners that work with IBM to protect their customers' online communication.

Keystroke Protection

Rapport encrypts your keystrokes as they travel to the browser and hides them from malicious programs that are known as keyloggers and from malicious software components inside the operating system. This prevents malware from reading your keystrokes and grabbing sensitive information such as your password or payment card number.

Payment Card Protection

Rapport warns you when you submit payment card information to local and non-secure websites. The warning appears in a dialog box from which you can stop the submission. Rapport also activates anti-keylogging when you enter a payment card number into either a Rapport protected site or any secure (https) site that contains a payment card-related keyword such as Visa, Mastercard, or Amex. The anti-keylogging protection prevents key logging malware from capturing your payment card details.

Note: This feature is supported only for payment cards that are issued by [participating payment card brands](#).

Screen Capture Blocking

Rapport disables any attempts to capture the screen while a protected website is displayed in your browser. This prevents malware from grabbing sensitive information by capturing the screen.

Website Validation

Even when you type in the correct address for your bank or enterprise's website, malicious software can use several methods, called pharming attacks, to redirect your browser to a fraudulent website.

To protect you against pharming attacks, Rapport verifies the IP address and the SSL certificate of the website each time you connect to a protected website. If the SSL certificate is outdated, incorrect, or signed by unknown issuer, Rapport warns you and helps you to avoid connecting to the site. If the IP address is not found in tables of trusted IP addresses for this website, Rapport replaces it with a known good IP address for the website.

Browser Add-on Blocking

When you connect to a protected website, Rapport blocks any browser add-ons that it does not recognize as being legitimate, safe software. Browser add-ons are small, usually third-party, pieces of software that sit inside your browser and can control your browser communication. This protects you from malicious browser add-ons that can steal your login information or tamper with your communication.

Process Alteration Blocking

Rapport analyzes attempts to alter the browser's process and blocks attempts that look suspicious. Altering the browser's process (also known as function patching) is a technique that enables taking over the browser and getting access to your sensitive information.

Malicious Website Warnings

Rapport warns you if you try to access a website that is known to be a malicious website.

Unauthorized Access Reporting

Rapport communicates with IBM's partner websites, providing feedback on security level and reporting any unauthorized attempts to access your online account. This enables your bank or enterprise to take immediate action against threats.

Note: This feature is supported only for partners that work with IBM to protect their customers' online communication.

Overlay Attack Prevention

Overlay attacks attempt to harvest end-user credentials by monitoring end-user access to FI sites and then starting an application window on top of the user's browser. This application window asks for sensitive information and blocks end-user access to the legitimate site until the credentials are submitted. Such attacks can appear as a legitimate step in the FI login process and convince the end user to divulge sensitive information.

Rapport identifies this type of attack and can respond to it in various ways, thus preventing the malware operation and credential theft.


The User Experience

Rapport is easy to use. You do not need any technical knowledge to use Rapport. Rapport does not require configuration, does not change the way that you work, does not alter browser behavior, and does not ask you technical questions when it encounters a security threat.

Most of Rapport's protective activities are silent and do not disturb you or require your participation. Rapport records all the actions that it takes to protect you in an [activity report](#) that you can view whenever you choose. Details about risk levels can be found in the activity report. When Rapport encounters high threat levels, it notifies you. Some protective actions in these cases require simple responses to [Rapport Warnings](#), which are easy to understand.

It's easy to see which websites are protected by Rapport. An icon is displayed on or near the right side of your browser's address bar indicates by its color if the current site is protected.



The Rapport icon () appears in the Windows system tray whenever Rapport is running. Clicking the tray icon opens the Rapport Console, through which you can access various Rapport features and information.

Whenever you use new login information on a protected site, a Rapport dialog box offers to [protect those credentials](#). This dialog box appears only the first time you use the login information.

Getting More Out of Rapport

In addition to the protection you receive automatically when you connect to IBM partner websites, you can manually add Rapport's protection to all other sensitive websites that you use. See [Protecting Additional Websites](#).

Beyond website protection, Rapport offers you other security features, all included free of charge:

- [Scanning your Computer for Security Improvements](#) how to further improve the security on your computer.
- Generate [reports](#) on attempts that are made to break into your online bank account.

Information for Advanced Users

Rapport is a lightweight software application. For specific details about Rapport's footprint, see [Rapport's PC Footprint](#).

Rapport does not compromise your privacy in any way. See [Rapport and Your Privacy](#).

Rapport includes a self-protection mechanism to prevent malware from stopping or removing the software. As a result, you cannot use the task manager to stop its processes. For information about stopping Rapport, see [Stopping Rapport](#).

Rapport's PC Footprint

Rapport's footprint includes the following:

- Executables:
 - Program Files\Trusteer\Rapport\bin\RapportService.exe
 - Program Files\Trusteer\Rapport\bin\RapportMgmtService.exe
- Processes:
 - RapportService.exe
 - RapportMgmtService.exe
- Services:
 - Rapport Management Service (for non-administrative accounts on 64-bit Operating Systems: RapportInjService_x64.exe)
- Drivers:
 - 'RapportPG.sys' (On 64-bit operating systems: 'RapportPG64.sys')
 - 'RapportKELL.sys' (On 64-bit operating systems: 'RapportKE64.sys')
 - 'RapportEI.sys' (RapportEI64.sys for 64-bit operating systems)
- Expect on average 15 MB of user profile space for logs and settings (depending on the number of different browsers that are used on the computer, this might reach higher numbers).
- The program size is 15 MB in addition to the user profile space.

Rapport and Your Privacy

Rapport creates an encrypted signature of your credentials on your computer. This information cannot be used to retrieve your credentials and is used by Rapport to identify any unauthorized leakage of your credentials. Rapport sends anonymous reports about security events and internal errors to a [central server](#). This information is used to improve the product and the policy.

Rapport Central Service: Powerful Fraud Blockage

The Rapport central service is a service that IBM offers partners to enable them to take immediate actions to prevent fraudulent activity in your account.

Whenever Rapport detects suspicious software or website activity, it generates a security event and sends it to the Rapport central service for analysis. The central service runs extensive tests to determine whether the activity is fraudulent. If the activity is fraudulent, the central service instructs Rapport to more aggressively block the threat.

Note: Rapport central service is available to your bank only if you do not disable the sending of security events for analysis. This setting is in the Rapport Setup wizard and is enabled by default. You are assured complete [anonymity](#)¹ when this setting is enabled.

Rapport protects you even if you choose not to send security events for analysis. However, by sending events for analysis, Rapport can detect more sophisticated and even unknown threats.

Some examples of security events that Rapport sends for analysis are:

- A suspicious website
- Attempts to capture your credentials
- Attempts to interfere with sensitive communication

¹ All information sent from your computer to the Rapport central service is anonymous and includes technical details, not private information. When Rapport suspects that your personal information has been compromised it sends your bank or enterprise a warning which includes an identifier that allows your bank or enterprise to associate the incident with your account. IBM is not exposed to this identifier or any other private information.

- Suspicious software

One of the great advantages of the Rapport central service is an early warning system that warns your bank when your user name and password are compromised. The central service can detect threats that were not detected by antivirus and other security software.

In addition to security events Rapport sends from time to time information about internal software errors. This information can help IBM identify and fix software issues.

Can I disable the Sending of Security Events and Error Logs to IBM?

You can reduce the bandwidth that is used by this feature if you want to by sending only critical events to IBM, although it is not recommended. IBM uses this information to provide the highest level of defense against financial malware to you and to other users of Rapport. You are assured complete [anonymity](#)² when the sending of security events and error logs to IBM is enabled. It is not possible to disable the sending of security events and error logs to IBM.

To send only critical security events and error logs to IBM, change the **Send Security Events and Errors for Analysis** setting from **Always** to **Only Critical Events**.

² All information sent from your computer to the Rapport central service is anonymous and includes technical details, not private information. When Rapport suspects that your personal information has been compromised it sends your bank or enterprise a warning which includes an identifier that allows your bank or enterprise to associate the incident with your account. IBM is not exposed to this identifier or any other private information.

3. Installing Rapport

Installing Rapport is quick and easy. You download the installation file from your bank's website, run the file, and follow a standard installation wizard.

For further instructions, see [Installing Rapport on Windows 8 Using Internet Explorer](#). For instructions to install Rapport on other web browsers, see the following webpage: <http://www.trusteer.com/support/win-install-instructions>.

If you install Rapport from a Windows administrator account, standard users can run Rapport from their accounts and cannot stop, start, uninstall, or reinstall Rapport, or change certain policy settings. This restriction is a feature that enables administrators to install Rapport across an enterprise and prevent employees from disabling its security features or from modifying the security policy for all users.

It is highly recommended to install Rapport from an administrator account, since it automatically extends Rapport protection to all users. In addition, drivers cannot be installed when you install Rapport from a standard user account, and Rapport's most important protection mechanisms (malware prevention and removal) are installed through drivers.

If you install Rapport from a standard user account, Rapport will not run on any other user account and cannot be installed on any other account unless it is first uninstalled.

Where can I download Rapport?

If you are a customer of a bank or other organization that offers Rapport, you can download it from your bank's website. Your bank might:

- Display a security section on the bank's website (usually at the bottom of the page) with a link to Rapport or a link to "protect yourself".
- Offer you to download Rapport as part of your online account login process or right after successfully logging in.

Does Rapport work with my Operating System and browser?

Rapport works with these operating systems and browsers: <http://www.trusteer.com/supported-platforms>.

Why am I being told that Rapport already exists on my computer?

If a version of Rapport exists on your computer when you install it, the following dialog box appears during the installation process:



If you see this screen during your installation, there is already an installation of Rapport on your computer. Reinstalling Rapport is perfectly safe (make sure that you don't install an older version over a new version).

➔ To install Rapport over a pre-existing version:

1. Select the option that best describes the reason why you came to install Rapport again.
2. Click **Next**. The installation process begins and interrupts itself to shut down Rapport. Before Rapport shuts down, a security confirmation message appears. The message presents an image of a word for you to type to prevent malware from disabling Rapport.
3. Enter the characters that you see in the image. (It is not case sensitive.)

4. Click **Shutdown**. The following message appears while Rapport shuts down: "Please wait while Trusteer Endpoint Protection shuts down." When the message disappears, Rapport has stopped running. The installation process then continues as usual. A screen might appear after the installation with the following text:

Trusteer Endpoint Protection was upgraded to a new version. Some new features of Trusteer Endpoint Protection will only be available after a restart.

Your computer is safe, even after this message appears. Nevertheless, it is recommended that you restart your computer as soon as possible.

How do I install Rapport in a shared virtual desktop environment?

If you install Rapport on Windows Server (2003 or 2008), the installation wizard detects the OS and installs the server version of Rapport. This version supports multiple sessions. For more information, see [Installing Rapport on Windows Server \(2003 or 2008\)](#).

Note: The following procedure describes the installation when Rapport is deployed to enforce Admin installations. For information about other Rapport deployment options, see the guide *Installing IBM Security Trusteer Rapport from a Standard User Account Best Practices*.

Installing Rapport on Windows 8 Using Internet Explorer

This procedure explains how to download and install Rapport if you are running Windows 8 and using Microsoft Internet Explorer as your browser. For other browsers, see the following webpage:

<http://www.trusteer.com/support/win-install-instructions>.

➔ **To install Rapport:**

1. Browse to the login page of your organization. If your organization offers you Rapport for download, you will see a splash screen that displays a **Download Now** button.
2. Click **Download Now**. The information bar appears at the bottom of the browser window and asks if you want to run or save the RapportSetup.exe file.
3. Click **Run**. Another dialog box appears a few seconds later, asking "Do you want to allow the following program to make changes to this computer?"
4. Click **Yes**. A dialog box with the following text might appear.

You are attempting to install Trusteer Endpoint Protection using a Windows standard user account. Installation using this type of account does not allow Trusteer Endpoint Protection to provide advanced malware removal and may leave your computer at risk, therefore, you must install it using administrator permissions.

To provide Windows administrator permissions and continue with the installation click Install.

If this computer belongs to an organization, you may need to contact your IT department.

This message indicates that you are currently logged in using a standard user Windows account. IBM recommends installing Rapport from an administrator account.

5. Click **Install**. A prompt appears requiring you to enter the administrator password.

Note: If you are unable to install Rapport with administrator permissions, you can close the dialog box. You will not be prompted for the administrator password and the installer will close.

6. Enter the password and click **Yes** to continue. A dialog box with the following text appears.

Firewall or antivirus software may show alert dialogs related to this installation.

Please allow any RapportSetup or RapportService programs to proceed if you see one of these alerts by selecting an option such as:

- Unblock*
- Yes*
- Allow*
- Permit*

If the installation fails you may want to temporarily disable your antivirus or security software and try again as antivirus or personal firewall that is set to a very high level of protection could cause installation to fail.

7. Click **OK**. Rapport downloads.

The Trusteer Endpoint Protection Installation wizard appears.

8. If you need Rapport to be compatible with screen readers, click **Advanced**. The Advanced Options screen opens. Check **I have a visual impairment, color blindness and/or regularly use assistive screen reading technologies** and then click **Continue**. This mode enables compatible screen readers to narrate Rapport menus and dialogs and ensures that Rapport does not prevent screen readers from narrating browser contents. It also disables visual code challenge security dialogs that appear when you stop or uninstall Rapport required for several actions such as stopping and uninstalling it.

Note: Do not select the **I have a visual impairment, color blindness and/or regularly use assistive screen reading technologies** check box unless you are installing Rapport on a computer that is needed for use with screen reading software. This setting disables some security features.

9. Click **I accept the terms in the license agreement**.

10. Click **Install**. The installation proceeds. When the installation is finished, the Finish button appears in the wizard.
11. Click **Finish**. After a few seconds, Rapport opens a new browser window to perform a short compatibility test. When the test is complete, Rapport opens a page in your browser.

The installation is complete.

Installing Rapport on Windows Server (2003 or 2008)

Rapport supports Windows Server (2003 and 2008). Rapport also supports multiple user sessions, enabling a single installation to handle multiple profiles, as required for a shared virtual desktop infrastructure. 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. Disabling the sending of restart requests to users helps to avoid a situation in which one user restarts the system for all users on the computer. For information about disabling restart requests, see *IBM Security Trusteer Rapport Virtual Environment Best Practices*.

➔ To install Rapport on Windows Server 2003 or 2008:

1. Run the file RapportSetup.exe. You can obtain this file from: <http://www.trusteer.com/support/rapport-installation-links>.
2. Proceed through the installation process, which downloads the complete installation package and initiates the installation wizard. The installation wizard detects the server OS and displays the **Windows Server host Detected** screen.
3. When you see this screen, click **View Document**. Your web browser opens a [Rapport business support page](#), which explains how Rapport helps to protect enterprises. From the business support page, click the link to view the *IBM Security Trusteer Rapport Virtual Implementation Scenarios* document, which provides important information about implementing Rapport in a virtual desktop environment.

4. After you read the document, select the **I have read the document** check box and continue with the installation.

Other than the **Windows Server host Detected** screen, the installation is identical to installations on other operating systems.

How do I switch to an Administrator Account?

- [Switching to an Administrator Account \(Windows 8\)](#)
- [Switching to an Administrator Account \(Windows 7\)](#)
- [Switching to an Administrator Account \(XP\)](#)

4. Getting Started

Immediately after installation, Rapport starts running and protecting your communication with partner websites. The Rapport icon appears on or near the right side of the address bar in your browser. If you browse to your bank or enterprise's website, the Rapport icon is green, indicating that the site is already protected.



The first time you log in to your online account, you might see a [password protection](#) dialog box.

When you browse to a website that is not protected by Rapport, the Rapport icon is gray. When you click the gray Rapport icon, a dialog box (the Rapport status indicator) indicates that the site is not protected.




You might like to:

- [Protect additional websites](#) where you log in or where you can read or send sensitive information.
- [Open the Rapport Console](#). Many procedures in this guide start with opening the console.
- Skim the topic headings for information that interests you.
- Start feeling more secure when you do your work, banking, and shopping over the Internet.

Open the Rapport Console


The Rapport Console is a portal to various Rapport features and information.

➔ To open the Rapport Console:

- Click the Rapport icon () in the system tray. The Rapport Console appears.



I don't see the Rapport icon in the system tray

The Rapport system tray icon () appears by default when Rapport is running. It is possible to hide the icon (see [Hiding and Restoring the System Tray Icon.](#)) The icon indicates that Rapport's browser-independent protections are working. The browser protection includes malware prevention, scanning, and removal. If the icon does not appear and is not hidden because of the setting in the Rapport Console, Rapport is not running. Rapport might be stopped or uninstalled. To start Rapport if it was stopped, select **Programs > Trusteer Endpoint Protection > Start Trusteer Endpoint Protection.**

5. Protecting Your Online Banking

If your bank is an IBM partner, you can download Rapport from your bank's website and enjoy fully protected online banking as soon as you install Rapport.

Rapport identifies security hazards and neutralizes threats without having to inform you. In a few cases where Rapport detects some level of risk, Rapport might prompt you for confirmation before it neutralizes the threat. For information about responding to Rapport alerts and warnings, see [Responding to Alerts and Warnings](#).

6. Using Payment Cards Safely Online

Rapport protects you from payment card theft when you use your payment cards online.

Rapport provides the following protection features for cards that are issued by participating card brands:

- Detects when you enter the BIN of a participating card brand into a web page.
- Activates keylogger blocking immediately after you type the BIN to prevent key-logging malware from capturing your payment card number.
- Notifies you when keylogger blocking is activated.
- Alerts you when you might be entering your payment card number into a suspicious or non-secure site, and enables you to choose to trust the site or stop the submission of your card number.

Note: Rapport does not know or learn your personal payment card numbers. Rapport recognizes the sequence of digits at the beginning of your card number that identifies the issuing brand. This is known as the bank identification number (BIN).

When you enter payment card numbers, you might see a warning with the following text:

It seems like you are entering payment card information into an unsecured or high-risk website. We recommend not entering card information into unsecured sites.

For information about this warning, see [Responding to a Payment Card Submission Detection Warning](#).

It seems you are entering payment card data. Trusteer automatically protects your payment card information from online theft.

For information about this message, see [Responding to a Payment Card Protection Message](#).

7. Responding to Alerts and Warnings

The product displays security alerts and warnings that require your response. When you see a dialog box, read it carefully and select the appropriate response. Taking the required action might be crucial to your security. To find an alert or warning, search this guide for the text that appears on your screen.

Responding to a Password Protection Offer

The following text is an example password protection offer:

*Trusteer Endpoint Protection has identified password submission.
Do you want Trusteer Endpoint Protection to start protecting this password?
If you click 'Protect this password' Trusteer Endpoint Protection will warn you when you enter this password into a new website where it was not previously entered. This would help you identify fraudulent websites that ask for your login information.*

A password protection offer appears one time for each protected website. This offer appears the first time Rapport detects that you are entering a password on a protected website. For example, if you recently downloaded Rapport from your bank's website, and after, you logged in to that website, you will see this message. Another example would be if you recently manually protected a website and then logged in to that website.

If you enter a protected password into a website that Rapport does not recognize, Rapport [warns you](#) that you are using the password in a different website. The warning helps you to prevent your password from being submitted to a fraudulent website, which helps to protect you from [phishing attacks](#)³.

³ A phishing attack is an attempt to lure you into visiting a forgery of a website you trust, such as your bank's website, and submitting your online login information so that it can be used by the criminals to access your online bank account and commit fraud, for example by transferring money out of your bank account.

When you see this offer, choose one of these options:

- **Protect:** After you click **Protect**, Rapport protects your password for this website. When your password changes, Rapport automatically protects the new password without asking you.
- **Don't protect:** If you choose this option, Rapport does not protect any passwords on this site and does not offer to protect passwords again when you go to this site.
- **Never protect passwords:** Disables Rapport's anti-phishing protection on all websites. After you click **Never protect passwords**, Rapport will no longer present any warnings about password submission and it will not offer you to protect any passwords on any website.

I protected the wrong password! What do I do now?

Type in the correct password. Rapport will protect it.


I typed my password incorrectly and chose to protect it. What now?

Retype the password correctly. Rapport will protect the correct password.

I chose never to protect passwords and now I want to protect passwords. What do I do now?

When you chose never to protect passwords, a policy definition was set in the Rapport security policy. You can change this policy.

➔ To change the password protection policy:

1. [Open the Rapport Console](#).
2. In the dashboard, click . The second dashboard screen appears.
3. In the Security Policy area, click **Edit Policy**. A User Approval screen appears. The screen shows you an image of a word for you to type to prevent malware from accessing the console and effectively disabling Rapport.
4. Enter the characters that you see in the image.


Click **OK**. The Security Policy screen appears, displaying all the security controls.

5. Locate the control **Warn When Login Information is Used in Unknown Websites**. From the list at the right side of this control, select **On partner & my sensitive websites** to reset the policy to its default setting. Select **On partner websites** if you want to be offered to protect passwords only on partner websites.
6. Click **Save**. Your policy change is saved.

I chose "Don't protect" and now I want to protect my password. How do I protect it?

You can change your password protection decision for this specific website.

➔ To enable password protection when disabled for a specific website:


1. [Open the Rapport Console](#).
2. In the dashboard, click . The second dashboard screen appears.
3. In the Security Policy area, click **Edit Policy**. A User Approval screen appears. The screen shows you an image of a word for you to type to prevent malware from accessing the console and effectively disabling Rapport.
4. Enter the characters that you see in the image.

Click **OK**. The Security Policy screen appears, displaying all the security controls.
5. Click **Warn When Login Information is Used in Unknown Websites**. The protection policy for user names and passwords on each website is displayed.
6. Select the **Warn if password is used elsewhere** check box for the website for which you want to enable password protection. Rapport will now protect your password for this website.
7. Click **Save**. Your policy change is saved.

I got an alert for a password that is no longer in use. How can I stop that?

Depending on our arrangement with partner websites, passwords are often protected even after you replace them. Continuing to protect passwords is rarely a problem since secure passwords are not used for other purposes. If you do need to stop Rapport protecting an old password, you can clear the Personally Identifiable Information (PII) cache to reset the password protection mechanism. Clearing the cache stops Rapport from protecting the old password but it also generates a new password protection offer the next time you go to each protected website.

➔ **To clear the PII cache:**

1. [Open the Rapport Console](#).
2. In the dashboard, click . The second dashboard screen appears.
3. In the Security Policy area, click **Edit Policy**. A User Approval screen appears. The screen shows you an image of a word for you to type to prevent malware from accessing the console and effectively disabling Rapport.
4. Enter the characters that you see in the image.

Click **OK**. The Security Policy screen appears, displaying all the security controls.
5. Click **Warn When Login Information is Used in Unknown Websites**. The protection policy for user names and passwords on each website is displayed.
6. Click **Clear Cache**. All password protection is cleared and all password protection policies are reset, causing Rapport to display a password protection offer again the next time you go to each website.

I typed a protected password on a site different than the one where I protected the password, but I didn't get a warning. Why?

Some legitimate sites are already identified by Rapport as legitimate. Since typing your password on those sites will not lead to fraud, Rapport does not generate a warning on those sites.

Responding to a Protected Information Warning

The following text is an example protected information warning:

*You have just entered text similar to your login on:
yourbankhere.com*

*You are receiving this warning because you are about to send your
information to a different website: sourbankhere.com*

*Please ensure that you recognize the site to which you are about to
submit your login information. Your security information could be
stolen if submitted to an unknown website.*

A protected information warning appears whenever you enter text that matches a protected user name or password into a website that Rapport does not recognize. The purpose of this message box is to verify that the website into which you are currently submitting information is not a fraudulent website that is trying to steal your sensitive credentials. This is known as a *Phishing* attack.

In the preceding example, Rapport wants to ascertain that the website sourbankhere.com (not a real site) is not pretending to be yourbankhere.com and that it is not trying to tempt you to enter your yourbankhere.com credentials into it.

When you see this warning, choose one of the following options:

- **Trust this site:** If you are happy to send your login information to this website and you know that the website is not asking for another website's credentials. After you click this **Trust this site**, you will not be warned again if you enter this protected user name or password into this website. If the text that you typed was not login information or was login information that you use on several websites and you want to be able to type it without being alerted each time that you type it, you can also check **Do not protect this login information on any website**.

Note: The security best practice is to choose passwords that contain unique, difficult to predict phrases *and* not to use the same password for more than one website. If you follow this practice, you are unlikely to need to check **Do not protect this login information on any website.**

- **Get me out of here!** If you do not want to send your login information to this website. A dialog box prompts you to choose which site you want to be redirected to.

Why do I get so many protected information warnings?

If you use text that you regularly type on numerous different sites as a password, you will receive a protected information warning every time that you enter that word into any website other than the site for which the password is protected. To avoid any irritation, do not protect passwords that you regularly use. If you are using this type of password for a website with which you exchange sensitive information, change your password to a more secure password. A secure password is unique for the website on which you use it and consists of a sequence of characters that is difficult to predict. It usually consists of a combination of letters, digits, and symbols.

I typed a protected password into a website that is not protected by Rapport, but it didn't alert me. Why?

Rapport uses several methods to recognize some websites as legitimate. If you believe that Rapport did not correctly alert you about a particular site, contact [Getting Support](#).

I received a protected information warning but I didn't type a protected password. Why?

For some protected websites, Rapport protects all passwords that you ever enter on that website after you install Rapport. This protection includes old passwords and even words you've accidentally typed there. This may explain why you received this warning.

Responding to a Non-Secure Submission Warning

The following text is an example non-secure submission warning:

Any information you enter into this page, including usernames and passwords, is to be sent over an unencrypted connection and could easily be read by a third party.

This warning appears when you enter a password into a website that does not submit data securely. The purpose of this warning is to protect you from submitting sensitive data to high risk sites, including legitimate sites that might easily be intercepted by criminals.


When you see this message, choose one of the following options:

- **Do not submit:** Stop the submission and automatically redirect your browser to an IBM webpage that explains the risk of submitting to non-secure sites.
- **Submit anyway:** Continue with the submission despite the warning.
- **I trust this site, do not alert me again:** Continue with the submission despite the warning and to tell Rapport to trust this site in the future. If you click this button, the site is added to a list of sites that you trust and that you don't want Rapport to warn you about in the future. If you decide you want to remove the site from the list, see [Clearing Trusted Sites for Non-Secure Submissions](#).
- **Change settings:** Open the Rapport security policy screen and change the **Warn when I submit security data to insecure sites** policy, which controls whether you receive warnings like this.

I clicked "I trust this site, don't alert me again." Can I remove the site from the list of trusted sites?

Yes, you can.

➔ To remove a site from the list of sites you chose to trust:

1. [Open the Rapport Console](#).
2. In the dashboard, click . The second dashboard screen appears.

3. In the Security Policy area, click **Edit Policy**. A User Approval screen appears. The screen shows you an image of a word for you to type to prevent malware from accessing the console and effectively disabling Rapport.
4. Enter the characters that you see in the image.
Click **OK**. The Security Policy screen appears, displaying all the security controls.
5. Click the policy control **Warn when I submit security data to insecure sites**. The words "You chose to trust the following sites:" appear, followed by a list of the sites you chose to trust.
6. Find the site that you whitelisted and click **Clear this site** that appears next to the site.
7. Click **Save**. Your policy change is saved.

Responding to a Phishing Site Warning

The following text is an example phishing site warning:

You are trying to access a web page at www.sourbankhere.com. This website is a known phishing site and was blocked by Trusteer to protect your security.

Phishing sites are designed to trick you into revealing sensitive information by imitating legitimate sites.

Entering information on this page may result in identity theft and financial losses.

This warning appears when Rapport blocks a website you intended to go to because Rapport verified that the website is a forgery, often known as a phishing website. Rapport has comprehensive capabilities to accurately detect phishing websites. This warning that appears when you go to any suspicious website is provided to stop you from falling victim to phishing related fraud. If this warning appeared after you clicked a link to a website, the link is most likely fraudulent and the risk is greater.

If you see this warning, choose one of the following options:


- **Get me out of here:** Redirects your browser to the previous site that you went to.
- **Why was this page blocked?** Opens a webpage that explains why this warning appears.
- **Ignore this warning:** Loads the website despite the reported risks. You will go to a website that is verified as a site that is created by criminals for the fraudulent purpose of stealing confidential account log-in credentials. In some phishing websites, even entering data without pressing submit is enough for criminals to receive and then use it to commit identity theft and fraud. We strongly recommend that you **do not choose this option**.

What should I do if I believe a legitimate website has been flagged as a phishing site?

If you believe that a legitimate website was flagged as a phishing site, take a screen capture of the site, make a note of the warning that you received, and open a support ticket at <http://www.trusteer.com/support/submit-ticket>.

How do I disable fraud prevention warnings?

➔ To disable fraud prevention warnings:

1. [Open the Rapport Console](#).
2. In the dashboard, click . The second dashboard screen appears.
3. In the Security Policy area, click **Edit Policy**. A User Approval screen appears. The screen shows you an image of a word for you to type to prevent malware from accessing the console and effectively disabling Rapport.
4. Enter the characters that you see in the image.

Click **OK**. The Security Policy screen appears, displaying all the security controls.
5. Set the control **Warn when browsing to malicious sites** to **Never**.
6. Click **Save**. Your policy change is saved.

Responding to a Payment Card Submission Detection Warning

The following text is an example payment card submission detection warning:

It seems like you are entering payment card information into an unsecured or high-risk website. We recommend not entering card information into unsecured sites.

This warning appears whenever you enter a protected payment card number into a webpage that is on a local drive or any non-secure website. The purpose of this message box is to help you to avoid submitting your payment card number to a phishing website or to a legitimate website that is not secure.

When you see this warning, choose one of the following options:

- **Get me out of this site:** Choose this option if you do not want to send your card information to this website. Your browser loads your home page instead.
- **Ignore, I trust this website:** Choose this option if you are happy to send your card information to this website. The dialog box closes but Rapport continues to block key loggers from capturing your payment card information. The issuer of your payment card receives notification of this submission. If you decide you want to remove a site that you chose to trust, see [Clearing Trusted Sites for Payment Card Submission](#).

Note: If you ignore this warning, you are either sending your payment card information to a known malicious website or you are sending your payment card information to a site that does not encrypt it and allows it to be viewed by a third party.

- **Always trust this site:** Rapport now trusts this site and does not present this warning again when you enter any payment card number on this site. Rapport continues to block key loggers from capturing your payment card information.
- **Stop protecting cards:** Disables the payment card protection feature. If you want to re-enable this feature, change the **Protect Payment Card Numbers from Theft** policy from **Never** to **Always**. For instructions for how to modify the security policy, see [Changing Security Controls](#).

Note: Payment card protection is enabled only for participating payment card brands.

Responding to a Payment Card Protection Message

The following text is an example payment card protection message:

It seems you are entering payment card data. Trusteer automatically protects your payment card information from online theft.

This message informs you that Rapport detected that you are submitting a payment card number to a webpage and is encrypting your keystrokes on the page to prevent key-logging malware from capturing your payment card number. This message appears when you enter a protected payment card number into either a Rapport protected site or any secure (https) site that contains a payment card-related keyword such as Visa, Mastercard, or Amex.

When this message appears, you do not have to do anything. You can optionally click **OK** to close the message. If you do nothing, it will disappear by itself after a short time.

If you do not want to receive notifications when Rapport activates anti key-logging, click **Do not show this message again**. If you want to re-enable these notifications, go into the security policy and check **Notify me when Trusteer activates payment card protections** under the **Protect Payment Card Numbers from Theft** policy. For instructions for how to access and modify the security policy, see [Changing Security Controls](#).

Note: Payment card protection is enabled only for [participating payment card brands](#).

Responding to a Print Screen Attempt Detected Alert

The following text is an example print screen attempt detected alert:

*The captured screen may contain sensitive information from:
yourbankhere.com*

This alert appears if the print screen key on your computer is pressed at a time when your browser is displaying a partner website. The alert helps you to choose whether to block or allow the mechanism to capture the screen.

The Print Screen key on your keyboard is used legitimately to capture screens. However, it is possible for malware to activate the same mechanism that this key activates and grab sensitive information for fraudulent purposes.

Note: This alert is part of the screen capture blocking feature, which is enabled by default on partner websites. Learn more about Rapport's screen capture blocking feature in [Understanding Security Policy Controls](#).

When you see this warning, choose one of the following options:

- **Allow:** Allows the Print Screen command to capture your screen. Choose this option if you intentionally pressed Print Screen to capture the screen.
- **Block:** Prevents the Print Screen command from capturing your screen. Choose this option if you did not intentionally press the Print Screen key on your keyboard.

I get the dialog even though I'm not trying to capture a sensitive site.

Minimize or close all browser windows and try again.

Responding to a Browser Protection Alert

The following text is an example browser protection alert:

The following Internet Explorer add-on uses an unfamiliar method to access the browser and as such cannot be monitored by Trusteer Endpoint Protection. You can either permanently allow or block this toolbar.


This alert appears when a browser add-on (toolbar, extension, or the like) is trying to access information that belongs to a protected website using a method that is not currently monitored by Rapport.

When you see this alert, choose one of the following options:

- **Permanently Allow:** This causes Rapport to allow the add-on to work on any website. Choose this option if you are aware of the add-on's functionality in the browser, if you are using it, and if you trust its source.
- **Permanently Block:** This causes Rapport to block the add-on from operating on any website and anonymously sends IBM a security report about the add-on that was blocked so that IBM's security experts can analyze it. This submission enables IBM to globally and permanently block the add-on if it is found to be malicious.

Can I unblock an add-on that I blocked or block an add-on that I allowed?

➔ To change the status of add-ons that you blocked or allowed:

1. [Open the Rapport Console.](#)
2. In the dashboard, click . The second dashboard screen appears.
3. In the Security Policy area, click **Edit Policy**. A User Approval screen appears. The screen shows you an image of a word for you to type to prevent malware from accessing the console and effectively disabling Rapport.
4. Enter the characters that you see in the image.

Click **OK**. The Security Policy screen appears, displaying all the security controls.
5. Click the **Block Unknown Browser Add-ons** policy name. A list of any add-ons that are allowed or blocked appears beneath the policy name.
6. Toggle the blocked or allowed status of each add-on as necessary.
7. Click **Save**. Your changes are saved.

Responding to an Activate Malware Removal Alert

The following text is an example activate malware removal alert:

```
Trusteer Endpoint Protection detected and blocked <malware_name>  
malware. Malware removal was aborted as your Malware Removal  
policy is set to 'Never'.  
ACTIVATE THE MALWARE REMOVAL POLICY NOW TO MAXIMIZE  
SECURITY.
```

This alert appears when the malware removal policy is disabled and Rapport detects and blocks malware. The purpose of the alert is to prompt you to activate the malware removal policy so that Rapport can remove the malware. Malware removal is enabled by default but might be disabled in the Rapport security policy (see [Modifying Rapport Security Policy](#)).

When you see this alert, choose one of the following options:

- **Activate Removal Policy Now:** The malware removal policy is activated and Rapport initiates the removal of the blocked malware. Another dialog box might appear that asks you to restart. You will be able to save and close open files and applications before you click **Restart Computer Now**. The restart completes the malware removal.
- **Ignore:** The alert appears again the next time Rapport detects the malware again. The malware remains on the computer but is blocked. Blocked malware that is on your computer is risky since it can become active at some time in the future if Rapport is ever stopped or removed or if you use a browser that Rapport does not support.

Responding to a Malware Removal Initiated Alert

The following text is an example malware removal initiated alert:

*Trusteer Endpoint Protection detected and blocked <malware_name>
malware, malware removal initiated.
RESTART YOUR COMPUTER NOW TO COMPLETE REMOVAL*

An alert like this one appears after Rapport detects, blocks, and begins to remove malware from your computer. To complete the malware removal, Rapport requires you to restart your computer.

When you see this alert, choose one of the following options:

- **Restart Computer Now:** Restarts the computer immediately, which completes the malware removal. After the computer restarts, make sure Rapport's icon is green when you log in to your account on a Rapport protected website. The Malware Removal Initiated alert should not appear again after you restart your computer. If it does appear again after you restart your computer, send a user problem report from the Rapport console.
- **Ignore:** The malware removal will be completed the next time you restart. Until you restart your computer, avoid any sensitive online activities. Rapport will not alert you again about this malware removal.
- **Do not alert me about this for a week:** You will receive this alert again in a week if the malware is still present. If you restart in the meantime, the malware removal will be completed and the alert will not appear again.

Responding to an Invalid Certificate Warning

The following text is an example invalid certificate warning:

*This website is using an invalid certificate.
Unless it is an internal website used by your organization it is
recommended to block access to this website.*

This warning appears when you go to a protected website and Rapport detects that the website's [certificate](#)⁴ is invalid. An invalid certificate might be outdated, incorrect, or signed by an unknown issuer. The purpose of this warning is to protect you from submitting information to a fraudulent website.

Note: This warning can often appear on websites with valid certificates if the date or time on the computer is set incorrectly. If this warning appears frequently, check the date and time on your computer.

The invalid certificate warning displays the following information:

Display Field	Description
Reason for error	<p>The reason why Rapport triggered this warning.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • Addresses do not match: The address that you tried to access and the address on the certificate do not match. The addresses must match for the certificate to be valid. Review the two addresses. If the address on the certificate seems suspicious or unrelated to the website you are trying to access, choose to block access. • Unknown certificate signer: The authority that signed the certificate is unknown to IBM. Do not trust unknown authorities to produce valid certificates. Banks and financial institutions always use certificates from known signers. • Certificate out of date: The certificate has expired and is no longer valid. A website that uses an outdated certificate has low security standards. Banks and financial institutions never use expired certificates. Check your computer clock to make sure that the date on your computer is correct. If the date on your computer is ahead of time, this message might appear erroneously. • Bad certificate: The certificate's format is incorrect.
Address on the certificate	The address that is on the certificate that is presented by this website. Each certificate is issued for a specific web address. A website should present a certificate that lists its own address.
Address in the request	The web address to which your browser is directed. This is the address that you tried to access.

⁴ An SSL certificate is a cryptographic digital certificate that validates the identity of a website and creates an encrypted connection for sending sensitive private data to the website. When you see the SSL padlock in the browser's address bar or at the bottom of the browser, a secure connection between your browser and the website exists using the SSL protocol. However, the presence of the padlock does not provide an indication that the certificate is valid.

Display Field	Description
Certificate expiration date	Each certificate is limited in time. A website that uses outdated certificates has low security standards
Signer	The authority that issued this certificate. Do not trust certificates from unknown authorities.


If you see this warning, choose one of the following options:

- **Block Access.** Blocks access to the site. Choose this option if the website is a financial or shopping website in which users submit sensitive information.
- **Allow Access.** Allows access to the site. You can choose this option if the website is on your local network (intranet) or if the website does not deal with sensitive information. If you do allow access, proceed with caution and do not submit sensitive information to the site. Check **Do not warn me about this website again** only if you want to prevent Rapport from alerting you about this website in the future.

How can I disable this feature?

You can use the Rapport Console to disable SSL certificate validation, which stops Rapport checking the validity of websites' certificates and therefore prevents these warnings from appearing.

➔ To disable SSL certificate validation:

1. [Open the Rapport Console.](#)
2. In the dashboard, click . The second dashboard screen appears.
3. In the Security Policy area, click **Edit Policy**. A User Approval screen appears. The screen shows you an image of a word for you to type to prevent malware from accessing the console and effectively disabling Rapport.
4. Enter the characters that you see in the image.

Click **OK**. The Security Policy screen appears, displaying all the security controls.
5. Locate the control **Validate Website SSL Certificates**.
6. From the list to the right side of this control, select **Never**.

7. Click **Save**. SSL certificate validation is now disabled.

Responding to a Standard User Account Warning

The following text is an example standard user account warning:

Trusteer Endpoint Protection identified high risk financial malware on this computer. It is recommended that you refrain from banking using this particular computer until the issue is resolved or until you re-install Trusteer Endpoint Protection from a Windows user account with Administrator rights.

This warning appears when you install Rapport from a standard user account, also known as a limited user account (LUA). If Rapport is installed using a standard user account, it cannot provide advanced malware removal and might leave your computer at risk. Rapport requires administrator privileges to offer your computer full protection.

Try again to install Rapport with administrator privileges. You might need to contact your IT administrator if you do not have administrator privileges.

For more information, see:

<http://manage.trusteer.com/support/what-admin-mode-windows>

Responding to an Activity Report Notification

The following text is an example weekly activity report notification:

Your periodic activity report is ready.

This notification appears weekly if you select an option in the Rapport Console to [generate a weekly activity report](#).

If you see this notification, choose one of the following options:

- **Open report:** Opens the Rapport Console and displays the weekly activity report.

- **Close:** Closes the alert and does not display the activity report. However, you can [view an activity report](#) any time.

It's been over a week and I haven't received the Weekly Activity Report notification. Why?

The weekly activity report appears only if there was at least one event in the past week. It is possible that no events were logged.

Responding to a Code Update Confirmation Message

If User Account Control (a Windows 8 and Windows 7 protection feature) is enabled on your computer, you might see the following message occasionally when Rapport is automatically updating:

To complete the software update process Trusteer Endpoint Protection needs to replace application files. A confirmation dialog may be presented by the Operating System. Please confirm it to successfully complete the update.

If you see this message, click **OK**. You might then see a User Account Control dialog box, requesting your permission to continue the Rapport update process. If you do see a User Account Control message, click **Continue** and the update will be completed.

Note: If the code update confirmation message appears frequently, submit a request for support at:
<http://www.trusteer.com/support/submit-ticket>.

Responding to a Screen Reader Compatibility Mode Warning

The following text is an example screen reader compatibility mode warning:

Trusteer Endpoint Protection is currently installed in screen-reader compatibility mode which enables screen-readers. Activating this policy may disable some screen readers. Are you sure you want to activate this policy?

This warning appears if Rapport is installed in screen reader compatibility mode and you attempt to enable one of the following security policies. For information about enabling and disabling security policies, see [Changing Security Controls](#):

- **Block Screen Capturing**
- **Block Access to Information inside the Browser**

These policies are disabled by default if Rapport is installed in screen reader compatibility mode. Enabling either of these policies might interfere with your screen reading software, preventing it from narrating web pages and Rapport menus and dialogs.

If you see this warning, choose one of the following options:

- **Activate policy.** Choose this option if you are sure you want to enable the policy, and you don't mind if screen readers on your computer cannot access Rapport.

Note: If you do not need to run screen readers, reinstall Rapport without choosing screen reader compatibility mode. Before reinstalling, you must remove all folders that are associated with Rapport. Directions for removing the folders can be found here:
<http://www.trusteer.com/support/remove-rapport-folders>

- **Cancel.** Choose this option if you want to cancel the policy activation.

Responding to a Reinstall from Admin Mode Alert

The following text is an example reinstall from admin mode alert:

You have previously installed Trusteer Endpoint Protection from an account with Limited User privileges. To maximize your security, it is recommended you re-install Trusteer Endpoint Protection from an account that has Admin User privileges.

This alert indicates that your Rapport provider recently restricted Rapport installation to Windows administrator accounts. You installed Rapport from a standard user account. The provider now recommends that you uninstall Rapport from the standard user account in which you installed Rapport and reinstall Rapport from an administrator account. After Rapport is installed from an administrator account, it will be active on all Windows user accounts on the computer.

A Windows administrator account is a Windows user account in which you can make changes that affect all users of the computer or that affect specific users. These changes include security settings, software installations, and file access. Although every Windows computer has an administrator account, Microsoft recommends that you use a standard user account for most day to day computing usage.

If you see this alert, choose one of the following options:

- **Close.** The alert closes. You can then reinstall Rapport by using the following procedure.
- **Alert me in 7 days.** The alert closes and reappears seven days later to remind you to do the reinstallation.

➔ **To reinstall Rapport:**

1. Uninstall Rapport from the same standard user account that you used to install Rapport:

- [Uninstalling Rapport \(Windows 8 and Windows 7\)](#)
- [Uninstalling Rapport \(Windows XP\)](#)

Note: On the Uninstall IBM Security Trusteer Endpoint Protection dialog box, select the **Delete all user settings** check box. This is necessary to ensure a smooth reinstallation.

2. Switch to an administrator account:

- [Switching to an Administrator Account \(Windows 8\)](#)
- [Switching to an Administrator Account \(Windows 7\)](#)
- [Switching to an Administrator Account \(XP\)](#)

3. Download your provider's latest version of Rapport:
 - a. Go to <http://www.trusteer.com/support/rapport-installation-links>.
 - b. Locate the correct download link for your provider (your bank, enterprise, or whichever organization offered you Rapport).
 - c. Click the provider link to download the installation file.
 - d. When prompted, save the file to your computer.
 - e. Run the file to install it. For full installation instructions, see [Installing Rapport](#).

Switching to an Administrator Account (Windows 8)

To switch to an administrator account, you need to know the user name and password of an administrator user account. If you do not know the user name and password of an administrator user, you need to ask your administrator to change your account type, or to install Rapport.

➔ To switch to an administrator user account:

1. On the **Start** screen, click your account picture.
2. Click the user that you want to switch to.

I don't know if the account I am using is an administrator account

If you are not sure that a user account is an administrator account or a standard user account, you can check the account type by switching to it and then doing the following.

➔ If your computer is in a domain:

1. Click **Start**.
2. Click **Control Panel**.
3. Click **User Accounts**.
4. Click **User Accounts**.

5. Click **Manage User Accounts**.
6. If you're prompted for an administrator password or confirmation, type your password or provide confirmation. (If your password is not accepted, you can assume that the account you are using is a standard user account.) Your user name is highlighted and your account type is shown in the Group column.

➔ **If your computer is in a workgroup:**

1. Click **Start**.
2. Click **Control Panel**.
3. Click **User Accounts and Family Safety**.
4. Click **User Accounts**.
5. Click **Manage another account**. If you're prompted for an administrator password or confirmation, type the password or provide confirmation. (If your password is not accepted, you can assume that the account you are using is a standard user account.) Your account type is displayed below your user name.

Switching to an Administrator Account (Windows 7)

To switch to an administrator account, you need to know the user name and password of an administrator user account. If you do not know the user name and password of an administrator user, you need to ask your administrator to change your account type, or to install Rapport.

➔ **To switch to an administrator user account:**

1. Click **Start**.
2. Click the arrow next to **Shut Down**.
3. Click **Switch User**.
4. Press **Ctrl+Alt+Delete**, and then click the user that you want to switch to.

I don't know if the account I am using is an administrator account

If you are not sure that a user account is an administrator account or a standard user account, you can check the account type by switching to it and then doing the following.

➔ If your computer is in a domain:

1. Click **Start**.
2. Click **Control Panel**.
3. Click **User Accounts**.
4. Click **User Accounts**.
5. Click **Manage User Accounts**.
6. If you're prompted for an administrator password or confirmation, type your password or provide confirmation. (If your password is not accepted, you can assume that the account you are using is a standard user account.) Your user name is highlighted and your account type is shown in the Group column.

➔ If your computer is in a workgroup:

1. Click **Start**.
2. Click **Control Panel**.
3. Click **User Accounts and Family Safety**.
4. Click **User Accounts**.
5. Click **Manage another account**. If you're prompted for an administrator password or confirmation, type the password or provide confirmation. (If your password is not accepted, you can assume that the account you are using is a standard user account.) Your account type is displayed below your user name.

Switching to an Administrator Account (XP)

To switch to an administrator account, you need to know the user name and password of an administrator user account. If you do not know the user name and password of an administrator user, you need to ask your administrator to change your account type, or to install Rapport.

➔ To switch to an administrator user account:

- If Fast Switching is enabled (default for Windows XP Home Edition and Professional on computers with more than 64 MB RAM):
 1. Click **Start**.
 2. Click **Log Off**.
 3. Click **Switch User**. The Windows XP logon screen appears and displays the number of running programs for each user under that user name.
 4. Click the user that you want to switch to.
 5. Type your password, and then click the arrow to log on to the computer.
- If Fast Switching is disabled or not supported (Windows XP Professional-based computers that are part of a domain network):
 1. Restart your computer
 2. Log on with the user name and password of an administrator user.

I don't know if the account I am using is an administrator account

If you are not sure that a user account is an administrator account or a standard user account, you can check the account type by switching to it and then doing the following.

➔ If your computer is in a domain:

1. Click **Start**.
2. Click **Control Panel**.
3. Click **User Accounts**.
4. Click **User Accounts**.

5. Click **Manage User Accounts**.
6. If you're prompted for an administrator password or confirmation, type your password or provide confirmation. (If your password is not accepted, you can assume that the account you are using is a standard user account.) Your user name is highlighted and your account type is shown in the Group column.

➔ **If your computer is in a workgroup:**

1. Click **Start**.
2. Click **Control Panel**.
3. Click **User Accounts and Family Safety**.
4. Click **User Accounts**.
5. Click **Manage another account**. If you're prompted for an administrator password or confirmation, type the password or provide confirmation. (If your password is not accepted, you can assume that the account you are using is a standard user account.) Your account type is displayed below your user name.

8. Customizing Rapport

You can change the language of the Rapport Console and dialog boxes and you can hide the Rapport icon that appears near your browser's address bar and you can hide the Rapport icon that appears in your system tray.

Hiding and Restoring the Rapport Address Bar Icon

By default, the Rapport icon always appears on or near the right side of your browser's address bar. The icon is green when the website in your browser is protected by Rapport and gray when the website in your browser is not protected by Rapport.



In addition to indicating which websites are protected, you can click the Rapport icon and select **Protect this Website** to protect an unprotected website.

You can hide this icon if you prefer it to be hidden. When the Rapport icon is hidden, Rapport continues to provide the same protection to protected websites, but you cannot see which websites are protected and you cannot choose to protect an unprotected website.

The showing or hiding of the icon is controlled in the Rapport Console. When the icon is hidden, you can access the Rapport Console only from the Windows Start menu.

➔ To hide the Rapport icon:

1. [Open the Rapport Console.](#)
2. In the Product Settings area of the Dashboard, next to the **Address bar icon** status, click **hide**. A message box appears with the following text:

You may need to restart your browser for the settings to take effect.


3. Click **OK**. The **Address bar icon** status changes to hidden and a **show** link appears.

The icon is now hidden in the browser or will be after browser restart.

➔ **To restore the icon:**

- Click **show**.

Hiding and Restoring the System Tray Icon

By default, the Rapport icon () always appears in your system tray when Rapport is running.

The icon indicates that Rapport's browser-independent protections are working. This protection includes malware prevention, scanning, and removal. If you want to open the Rapport Console, click the Rapport icon.

You can hide this icon if you prefer it to be hidden. When the Rapport icon is hidden from the system tray, Rapport continues to provide the same protection.

The showing or hiding of the icon is controlled in the Rapport Console. When the icon is hidden, you can access the Rapport Console only from the Windows Start menu.

➔ **To hide the Rapport icon from the system tray:**

1. [Open the Rapport Console](#).
2. In the Product Settings area of the Dashboard, next to the **Tray icon** status, click **hide**. The **Tray icon** status changes to hidden and a **show** link appears.

The icon is now hidden in the system tray.

➔ **To restore the icon:**

- Click **show**.

Changing Interface Language

By default, Rapport displays the Rapport Console and all other dialog boxes with English text. The Rapport Console and dialog boxes can be changed to use one of several other languages.

➔ To change the Rapport Console language:

1. [Open the Rapport Console](#).
2. In the Product Settings area of the Dashboard, click **More Settings**. The Product Settings tab appears.
3. From the **Language** list, select a language. The following message appears.

*The change will take full effect after all browser windows are closed.
Switch language and reload Trusteer Endpoint Protection console?*

4. Click **OK**. The Rapport Console reloads in the selected language.

9. Viewing Rapport Activity

Rapport's protection mechanisms are triggered by several different types of events. Some of those events are legitimate events that resemble events that are caused by malware. Other events might be initiated by malware that is on your computer. Each event is counted and recorded in an activity report that you can view whenever you want. The report shows the activity in the last seven days. You can reset the counting or stop the counting and enable or disable a dialog box that appears on your screen at the beginning of each week and offers to show you the weekly activity report.

Viewing the Activity Report

The weekly Activity Report shows you how many events triggered each of Rapport's protection mechanisms over the last seven days. This report is for your information only. No action is necessary, as Rapport blocks all security events that might lead to a data breach. The Activity Report is displayed automatically 12 hours after Rapport is installed.

The fact that the Activity Report includes events does not mean that you have malware on your desktop or that you went to fraudulent websites. It does mean that some software or websites that you went to violated the security policy set by your protected website owners or by IBM. For example, you might have software that tried to take a screen capture of your bank statement or software that tried to read information that you were typing into your online banking website. This policy violation caused Rapport to block the software from reaching the sensitive information.

➔ To view the Weekly Activity Report at any time:

1. [Open the Rapport Console.](#)
2. In the **Weekly Activity Report** area of the dashboard, click **Full Report**. The Weekly Activity Report appears.

The report displays nine counters for nine categories of events. The categories of the activity report list different event types that Rapport encountered and mitigated while you were browsing the Internet.

3. Click each counter name to see a description of the security event that it counts and a list of the events in this category that were counted.

Note: Do not be concerned if you do not understand some or even all of the information that is presented in this report, as it is slightly technical. This information does not require any action on your part. You can safely close this report and never look at it again. It is there for users who want to review Rapport's activity over time.

Configuring the Activity report

There is an option to show the activity report automatically every seven days. The report first appears automatically 12 hours after you install Rapport. By default, the report does not appear weekly but you can view it in the Rapport Console whenever you want.

Clearing the weekly activity report clears all the event counters. Disabling the weekly activity report stops all event counters.

➔ To configure the activity report:

1. [Open the Rapport Console.](#)
2. In the **Weekly Activity Report** area of the dashboard, click **Full Report**. The Weekly Activity Report appears.

You can now:

- Enable the weekly activity report by checking **Automatically present this report at the beginning of each week**. Every seven days, a dialog box will appear offering to display the report.
- [Clearing the Activity Report](#).
- [Disabling the Activity Report](#).

Clearing the Activity Report

➔ To clear the activity report:

1. Click **Clear Report**. A confirmation box appears.
2. Click **OK**. All counters are reset.

Disabling the Activity Report

➔ To disable the weekly activity report:

1. Click **Disable Report**. A confirmation box appears.
2. Click **OK**. The event counters are cleared and the Weekly Activity Report is disabled. The Weekly Activity Report area of the Rapport Console dashboard now displays the message "Activity report is disabled". You can re-enable the report by clicking **Enable activity report**.

10. Scanning your Computer for Security Improvements

Keeping the software on your computer up to date is important for security. New threats are always emerging and software companies regularly update their programs to include fixes for security vulnerabilities and other bugs. Some software programs are especially vulnerable to abuse if they are not up to date.

Rapport scans your computer every three days to check that your computer has an antivirus program that is installed. It also checks that your computer is running up-to-date versions of the antivirus program and various other software programs, such as Adobe Flash, Adobe Reader, Java, and Skype. The Security Best Practices report lists the programs that Rapport found to be out-of-date and how to update them. You can access the Security Best Practices report from the Rapport Console.

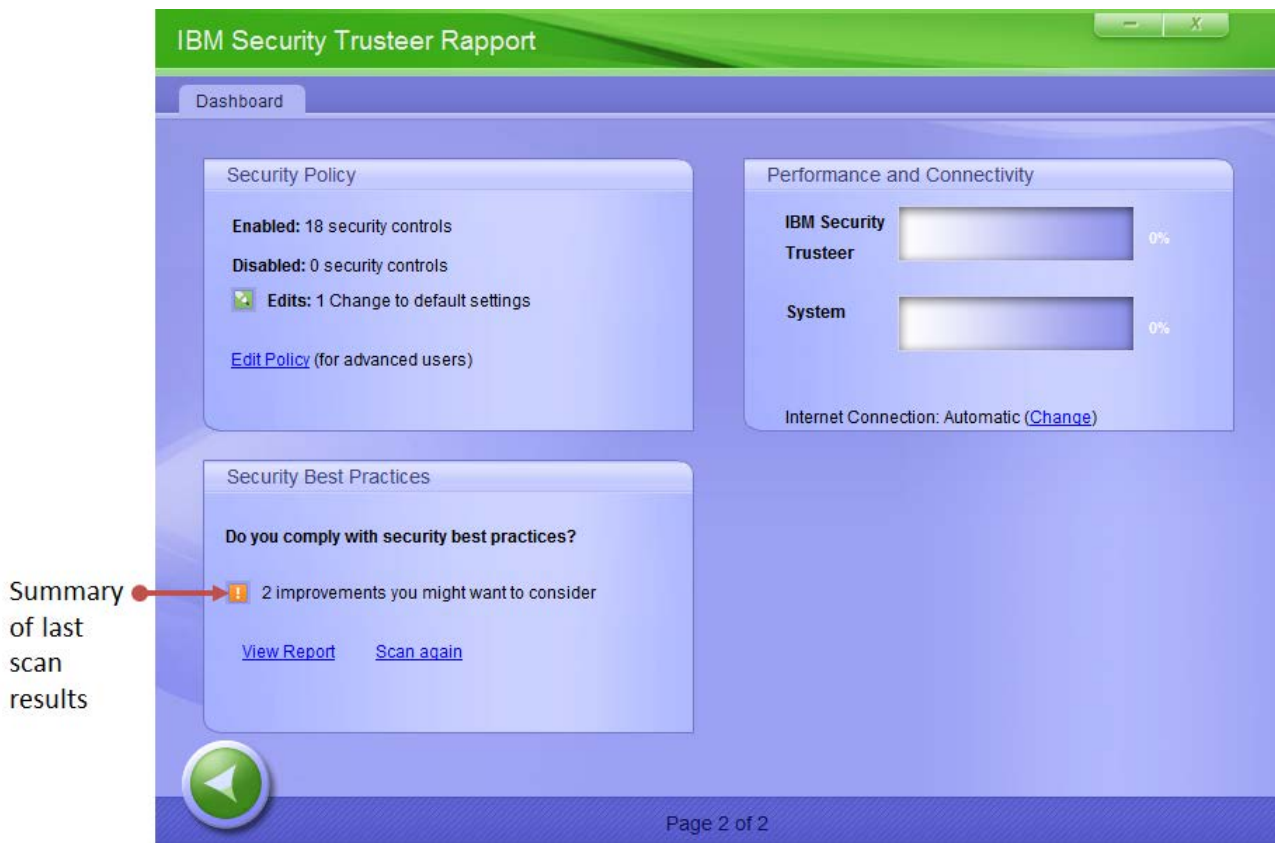
Running a Manual Scan

Although Rapport scans your computer regularly, you can scan again whenever you want.

➔ To scan your computer for security improvements:

1. [Open the Rapport Console.](#)

- In the dashboard, click . The second dashboard screen appears, displaying the Security Best Practices summary at the lower left.




Summary of last scan results

- In the Security Best Practices area of the dashboard, click **Scan again**. While the scan is in process, the **Scan again** link disappears and the words "Scanning..." appear. When the scan is finished, the **Scan again** link reappears and the scan results are updated.

Viewing the Security Best Practices Report

The Security Best Practices report lists the programs that Rapport found to be out-of-date and how to update them.

➔ To view the Security Best Practices report:

1. [Open the Rapport Console](#).
2. In the dashboard, click . The second dashboard screen appears, displaying the Security Best Practices summary at the lower left.

Summary of last scan results

IBM Security Trusteer Rapport

Dashboard

Security Policy

Enabled: 18 security controls
 Disabled: 0 security controls
 Edits: 1 Change to default settings

[Edit Policy](#) (for advanced users)

Performance and Connectivity

IBM Security Trusteer 0%
 System 0%

Internet Connection: Automatic ([Change](#))

Security Best Practices

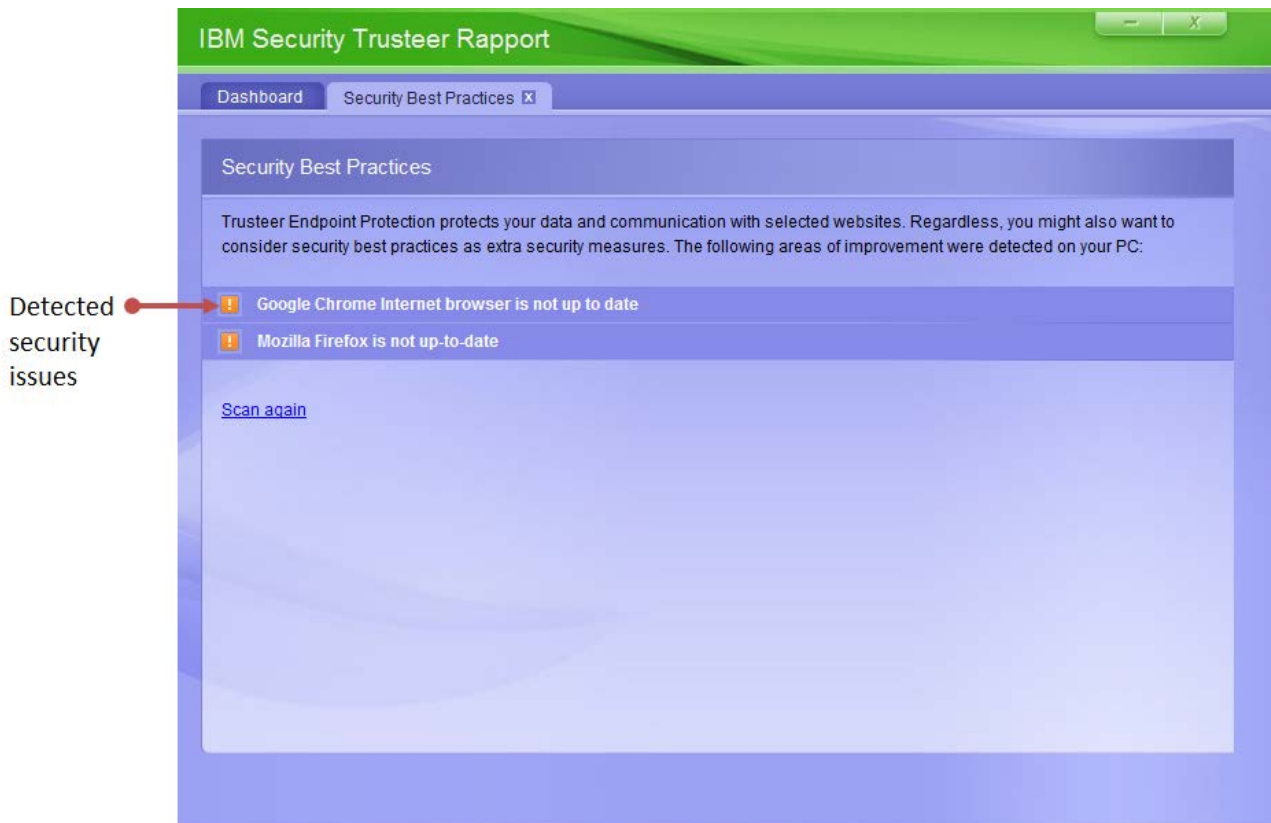
Do you comply with security best practices?

2 improvements you might want to consider

[View Report](#) [Scan again](#)

Page 2 of 2

3. Click **View report**. The Security Best Practices tab appears, displaying a report of the security issues that were detected by the scan.



4. Click each security issue. A full description of the risk that is posed by the issue and a recommendation of what you should do about the issue is displayed.

11. Managing Protected Sites and Passwords

Rapport provides information about which websites and passwords are protected in the Rapport Console. You can use the Rapport Console to remove websites and passwords.

There are two categories of protected websites:

- **Trusted Partner Websites.** These are websites that are owned by IBM's partners. Trusted partners work directly with IBM to provide the best security policy for their applications. When you access a partner website, you are automatically protected. You cannot remove Rapport's protection from these websites. The number of protected partner sites does not place any burden on your system.

Trusted Partner Websites also provide extra support mechanisms:

- IBM Partners can access the Trusteer Management Application, which allows partners to define security policy configuration and get detailed reports about infected devices.
 - IBM Partners receive detailed notification about events that occur on end user devices. Partners can subscribe to these event reports (Feeds) and take actions that are based on these events and contact end users when required.
 - IBM Partners have access to the IBM security analysis team and can work closely with the team to get step-by-step guidance to help end users remove infections.
 - IBM Partners can access IBM Trusteer Support services whenever the need arises for troubleshooting, support queries, software compatibility issues, setting up the Rapport client, and for ongoing customer education.
- **Websites you manually added.** These are websites that you added because you wanted to benefit from Rapport's protection when you connect to these sites. There is no limit to the number of websites you can protect. IBM recommends that you activate Rapport protection on all additional websites

with which you exchange private and personal information or any type of sensitive information. Examples of websites that you might want to protect include:

- Online bank accounts
- Mutual fund accounts
- Online brokerage accounts
- Online merchants
- Web-based email sites (such as Outlook, Yahoo! Mail, and Gmail)
- Social networking sites (such as Facebook, Orkut, and LinkedIn)
- Insurance applications
- Personal medical information sites
- Online merchants (such as eBay, Amazon, Walmart.com, and Target.com)

You can remove Rapport protection from these websites by removing them from the list.

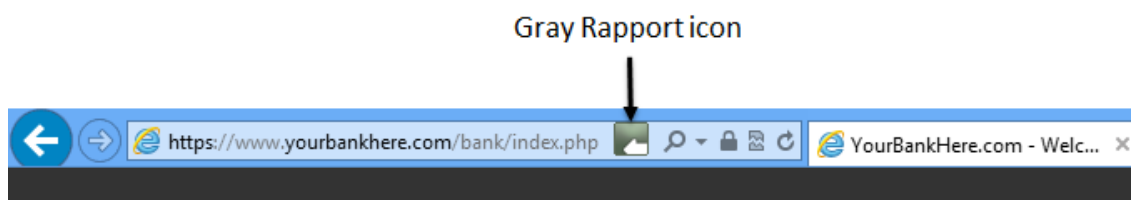
Note: In some installations of Rapport, manually protecting websites is disabled.

The Trusted Websites area of the Rapport Console shows how many websites in each category are currently protected. You can see a list and description of our protected partner websites by clicking **Trusted Partner Websites**. You can see a list of websites you manually added by clicking **Websites you manually added**.

Protecting Additional Websites

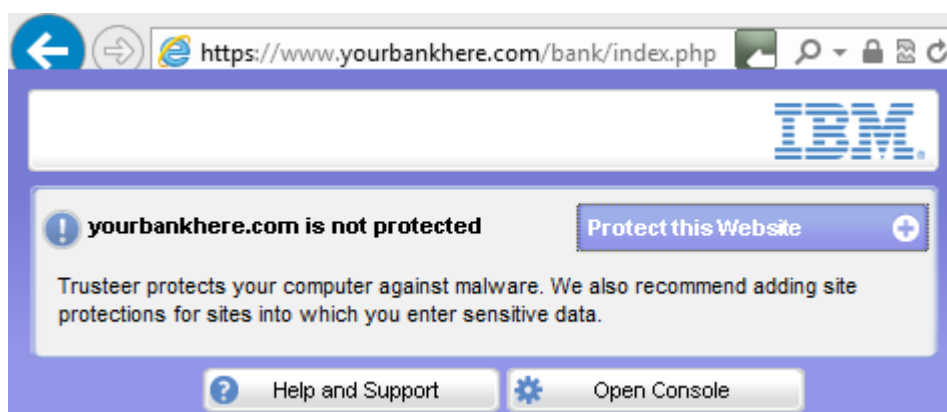
➔ To protect an additional website:

1. Browse to the website you want to protect. If Rapport is not yet enabled to protect this website, the Rapport icon in the address bar is gray.

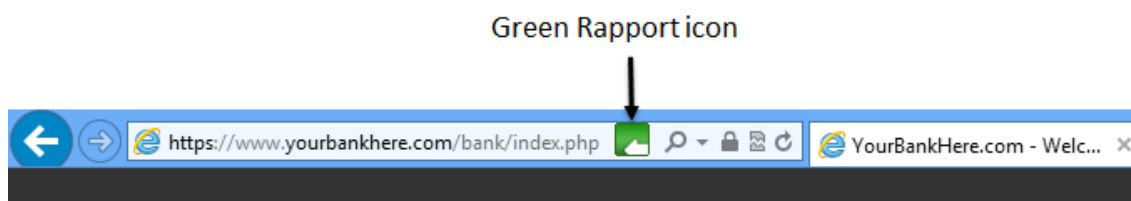


YourBankHere

2. Click the gray Rapport icon in the address bar. A dialog box appears.



3. In the dialog box, click **Protect this Website**. The Rapport icon on the address bar turns green, indicating that this website is now protected by Rapport.



YourBankHere

The icon appears by default. You can choose to [hide the Rapport icon](#).

Why doesn't the Rapport icon appear in my browser?

If the Rapport icon does not appear in your browser, there are three possible reasons:

- You chose to hide the icon from the address bar. Rapport is still protecting you but the icon is hidden. You can restore the icon. For information about hiding and restoring the Rapport icon, see [Hiding and Restoring the Rapport Address Bar Icon](#).
- Rapport does not support your browser. For a list of currently supported browsers, see: <http://www.trusteer.com/support/supported-platforms>.
- Rapport has been stopped and is not running. You can start Rapport again. See [Starting Rapport](#).

Removing Protected Websites

➔ To remove manually added websites:


1. [Open the Rapport Console](#).
2. In the Trusted Websites area, click **Browse Trusted Websites**. A Trusted Websites tab is displayed.
3. Click **Websites you manually added**. A list of all websites that were manually added is displayed.
4. Click the **remove** link next to the website on this list. A confirmation box appears.
5. Click **OK**. The website is removed from the list. The Rapport icon will now be gray when you browse to the website you removed, indicating it is no longer protected.

Managing Protected Usernames and Passwords

After you accept Rapport's offer to protect your password on a protected site, Rapport not only protects that password but also protects any future passwords you might have for that site. Rapport remembers your choice to protect or not to protect your password on each website. It does not offer you again to protect your password when you go to that site unless you clear the password protection cache. The Rapport Console indicates which websites currently have Rapport password protection enabled. You can disable password protection for any protected website if you want to. You can also clear the password protection cache, which clears all password protections and password protection decisions.

Note: For some of IBM's partner websites, Rapport protects user names and passwords. The Rapport Console also indicates user name protection policy per website.

➔ To disable password protection on a protected website:

1. [Open the Rapport Console.](#)
2. In the dashboard, click . The second dashboard screen appears.
3. In the Security Policy area, click **Edit Policy**. A User Approval screen appears. The screen shows you an image of a word for you to type to prevent malware from accessing the console and effectively disabling Rapport.
4. Enter the characters that you see in the image.

Click **OK**. The Security Policy screen appears, displaying all the security controls.
5. Scroll down the list of security controls until you find **Warn When Login Information is Used in Unknown Websites**.
6. Click **Warn When Login Information is Used in Unknown Websites**. The protection policy for user names and passwords on each website is displayed.
7. Clear the **Warn if password is used elsewhere** check box for the website for which you want to disable password protection. Rapport will no longer protect your password for this website.

Note: Clicking **Clear Cache** clears all password protection and resets all password protection policies, causing Rapport to display a password protection offer again the next time you go to each website.

8. Click **Save**. Your changes are saved.

12. Modifying Rapport Security Policy


Note: Modifying the Rapport security policy is for advanced users.

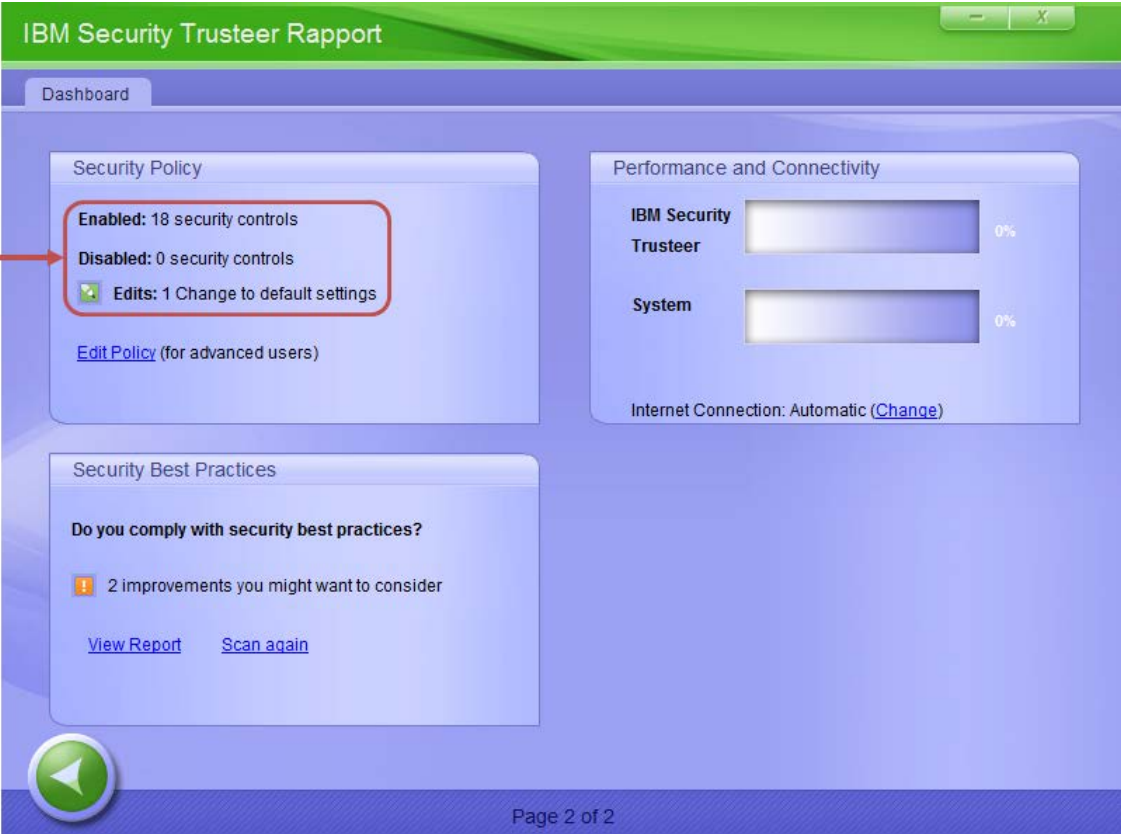
Rapport security features do not require any configuration, but you can make changes to a number of features to suit your needs.

Viewing Security Policy Summary

The Rapport Console displays a summary of your security policy. The summary shows you how many security policy controls are enabled and how many are disabled.

➔ To view the security policy summary:

1. [Open the Rapport Console](#).
2. In the dashboard, click . The second dashboard screen appears, displaying the security policy summary in the Security Policy area.



The screenshot shows the IBM Security Trusteer Rapport dashboard. The 'Security Policy' section is highlighted with a red box and a red arrow pointing to it from the text 'Security policy summary'. The 'Security Policy' section displays the following information:

- Enabled: 18 security controls
- Disabled: 0 security controls
- Edits: 1 Change to default settings
- [Edit Policy](#) (for advanced users)

The 'Performance and Connectivity' section shows progress bars for IBM Security Trusteer (0%) and System (0%). The 'Internet Connection' is set to Automatic with a [Change](#) link.

The 'Security Best Practices' section asks 'Do you comply with security best practices?' and shows '2 improvements you might want to consider'. It includes links for [View Report](#) and [Scan again](#).

At the bottom of the dashboard, there is a green circular button with a white arrow pointing left and the text 'Page 2 of 2'.

The security policy summary includes the following information:

Display Field	Description
Enabled	The number of security controls that are currently enabled.
Disabled	The number of security controls that are currently disabled.
Edits	The number of changes that were made to the default policy.


Changing Security Controls

The Rapport security policy provides the best security while minimizing possible conflicts with legitimate programs. For example, blocking screen captures is set by default to protect only partner websites. This is because many legitimate products capture the screen and IBM prefers only to interfere with screen capturing software when such interference is crucial for your online banking or enterprise security.

You can modify the Rapport security policy by changing each security control. Modifying the security policy can help you to enable a legitimate task that is blocked by the default security policy or resolve a compatibility issue with another security application. Any modifications that you make to the default policy are likely to reduce the level of protection that Rapport provides. Make sure that you understand the risk that is involved before you change security policies.

Note: If Rapport was installed from a Windows administrator account, there are some policy changes you can do only if you are logged in to an administrator account.

➔ To change security controls:

1. [Open the Rapport Console.](#)
2. In the dashboard, click . The second dashboard screen appears.
3. In the Security Policy area, click **Edit Policy**. A User Approval screen appears. The screen shows you an image of a word for you to type to prevent malware from accessing the console and effectively disabling Rapport.

4. Enter the characters that you see in the image.

Click **OK**. The Security Policy screen appears, displaying all the security controls.

5. From the menu at the right side of the control that you need to change, select the setting that you want. Before you change any settings, make sure that you understand the change that you are making to the level of protection that is provided by Rapport. See [Understanding Security Policy Controls](#) for information about the security policy controls, the options available, and any relevant additional information. The settings that you might see are:

- **Always:** the control is always enabled and is not website dependent.
- **Never:** the control is always disabled.
- **On partner websites:** the control is available for partner websites and is based on the policy set by the website owner. Partner websites work directly with IBM to provide the most suitable security policy.
- **On partner & my sensitive websites:** the control is available for partner websites and for websites that you [manually protected](#).

Clicking each control name displays a description of the control and any specific functions for the control.

If you want to return all settings to their default values, click **Restore Defaults**.

Note: If Rapport was installed in Visually Impaired mode, the default values for the **Block Screen Capturing** and **Block Access to Information Inside the Browser** settings are **Never**.

6. Click **Save**. Your policy changes are saved. Some changes require browser or computer restart to take effect.

Note: If Rapport was installed in Screen Reader Compatibility mode and you activate either the **Block Screen Capturing** policy or the **Block Access to Information Inside the Browser** policy, a message with the following text appears:

Trusteer Endpoint Protection is currently installed in screen-reader compatibility mode which enables screen-readers. Activating this policy may disable some screen readers. Are you sure you want to activate this policy?

If you want to activate the policy, click **Activate policy**. If you do not want to activate the policy because doing so might disable screen readers, click **Cancel**.

Understanding Security Policy Controls

Before you modify Rapport security policy, make sure that you understand the change that you are making to the protection Rapport provides.

Block Screen Capturing

Description

Disables any attempts to capture the screen while a protected website is showing. Programs on your computer that try to capture the screen produce a black image.

The purpose is to prevent malware from capturing the screen to grab sensitive information.

Options

- **Never.** Allows screen capturing always. (Certain operations, such as stopping Rapport, result in security confirmation message screens that cannot be captured even if this policy control is set to "Never".)
- **On partner websites** (default). Blocks all screen capturing on the computer only when any partner website is open in the browser
- **On partner & my sensitive websites.** Blocks all screen capturing on the computer only when any protected website (partner or manually added) is open in the browser.

Additional Information

The Print Screen command is handled differently from other screen capture mechanisms. If the Print Screen key is pressed, Rapport displays a [Print Screen Attempt Detected Alert](#) asking the user to choose whether to block or enable the capture.

Even if you need to capture screens on your computer, you might not need to disable this feature. Rapport's screen capture blocking feature does not prevent screen capture mechanisms from capturing any screens at times when protected websites are not displayed. By default, the screen capture blocking feature applies only to partner protected websites. Even at times when screen capturing is blocked, you can take a screen capture by using the Print Screen key on your keyboard. If you use the Print Screen key, a Rapport dialog box appears on which you can block or enable the screen capture. Click **Allow** to capture the screen.

Therefore, disable screen capture blocking only if you need to capture screens that are displayed on partner websites by using a screen capture mechanism other than the Print Screen key on your keyboard. When you finish capturing screens, you can re-enable the screen capture blocking feature to restore the protection that is provided by this feature.

If Rapport blocks you when you try to capture something on your screen that is not a protected website, minimize all open browsers or close all windows and tabs that contain protected webpages. You can then capture your screen without being blocked.

Validate Website SSL Certificates

Description

When you browse to a protected website, Rapport checks the website's SSL certificate. If the certificate is outdated, incorrect, or signed by an unknown issuer, Rapport triggers an [Invalid Certificate Warning](#) that requires your action. Rapport's SSL certificate validation is stronger than a browser's validation mechanism and should be used for Partner websites even if your browser warns about invalid certificates.

The purpose is to prevent you from going to fraudulent websites.

Options

- **Never.** Does not check website SSL certificates.
- **On partner websites** (default). Checks SSL certificates that are used by partner websites when you go to them.
- **On partner & my sensitive websites.** Checks SSL certificates that are used by partner websites and manually added websites when you go to them.

Description

For information about how to respond to an invalid certificate warning, see [Responding to an Invalid Certificate Warning](#).

You can clear Rapport's cache from invalid certificates that you authorized before. After the cache is cleared, the certificates that were removed from the cache generate a warning if you go to a website that uses them.

To clear the invalid certificates cache, click **Clear Cache** below the Validate Website SSL Certificates drop down list.

Block Unknown Browser Add-ons

Description

Blocks unrecognized browser add-ons. Browser add-ons (also known as toolbars or BHOs) are small (usually third-party) pieces of software that sit inside your browser and can control your browser communication. Most browser add-ons (such as the Google toolbar) are legitimate. However, there are also malicious add-ons.

The purpose is to protect you from malicious browser add-ons that can steal your login information or tamper with your communication.

Options

- **Never.** Allows all browser add-ons on all sites.
- **On partner websites.** Blocks unrecognized browser add-ons when you are connected to partner websites.

- **On partner & my sensitive websites** (default). Blocks unrecognized browser add-ons when you are connected to partner websites or manually protected websites.

Additional Information

The console displays a list of unknown add-ons that Rapport detected and blocks when you are connected to a protected website. You can manually unblock specific add-ons that you know to be safe by selecting the **Allow** check box for each add-on.

[Block Access to Information inside the Browser](#)

Description

Blocks processes on your computer that access websites by using a DOM programming interface (API). These processes can read sensitive information or tamper with your transactions. Rapport blocks these processes regardless of whether they are legitimate or malicious.

The purpose is to prevent malicious processes from illegitimately reading sensitive information or tampering with your transactions.

Options

- **Never.** Does not block processes from accessing websites.
- **On partner websites** (default). Blocks processes when you are connected to partner websites.
- **On partner & my sensitive websites.** Blocks processes when you are connected to both partner websites and manually protected websites.

Additional Information

A common example is password managers, which learn your passwords and can enter them automatically on login webpages. Rapport blocks them from accessing this information because the information is sensitive and the software might be abused by malware to retrieve your financial website credentials. Do not use such products for

your online financial websites. Some legitimate programs access this information and are blocked by Rapport on partner websites.

Block Access to Sensitive Website Cookies

Description

Blocks applications from accessing cookies such as session cookies that a partner website's owner set as sensitive cookies.

The purpose is to prevent session cookies from being used to take over your session with the website.

Options

- **Never.** Does not block applications from accessing sensitive cookies.
- **On partner websites** (default). Blocks access to sensitive cookies when you are connected to a partner website.

Additional Information

IBM must be familiar with the website's cookies before Rapport can be configured to protect them. Otherwise, a conflict with the website can occur. For this reason, this type of protection is only available for partner websites.

Validate Website IP Addresses

Description

Validates website IP addresses against trusted IP address translation tables. When you access a protected website, Rapport checks the website's IP address against a list of known good addresses for this website. If the IP address is not found in the list, Rapport replaces it with a known good IP address for the website.

The purpose is to protect you from connecting to a fraudulent website due to a [pharming attack](#)⁵.

⁵ Pharming attacks are attempts to redirect your website traffic to spoofed websites.

Options

- **Never.** Does not check website IP addresses against trusted IP address tables.
- **On partner websites.** Checks website IP addresses against trusted IP address tables when you connect to partner websites.
- **On partner & my sensitive websites** (default). Checks website IP addresses against trusted IP address tables when you connect to both partner websites and manually protected websites.

Additional Information

The clear cache feature for this control is not currently supported.

[Activate Character Replacement](#)

Description

Encrypts all keystrokes as they travel to the browser and hides them from malicious programs that are known as keyloggers.

The purpose is to prevent keyloggers from reading your keystrokes and grabbing sensitive information such as passwords.

Options

- **Never.** Does not encrypt keystrokes.
- **On partner websites.** Encrypts keystrokes when you are connected to partner websites.
- **On partner & my sensitive websites** (default). Encrypts keystrokes when you are connected to both partner websites and manually protected websites.

Additional Information

This feature can conflict with other anti keyloggers and lead to scrambled keystrokes. Therefore, if you have another anti keylogger running (for example, as part of your antivirus software), you might need to disable this feature. Alternatively, you might be able to disable your existing software's keylogging protection.

If you find this policy is disabled even though you did not disable it, it indicates that Rapport detected a conflict between your hardware or software configuration and Rapport. To avoid the conflict, Rapport disabled this mechanism.

Activate Kernel Character Replacement

Description

Encrypts all keystrokes as they travel to the browser and hides them from malicious software components inside the operating system (known as kernel keyloggers).

Kernel character replacement is a stronger version of character replacement. When kernel character replacement is enabled, Rapport encrypts the keystrokes at the system kernel level, not allowing keyloggers to read the keystrokes at any part of the way from the keyboard to the browser. If *Activate Character Replacement* is disabled, *Activate Kernel Character Replacement* is also disabled, even if the policy is set to **always**. *Activate Kernel Character Replacement* complements *Activate Character Replacement* making it stronger, but cannot work alone.

The purpose is to prevent malicious software components from reading your keystrokes and grabbing sensitive information such as payment card numbers.

Options

- **Never**
- **Always** (default)

Additional Information

If Rapport was installed from an administrator-level Windows account, you can change this setting only if you are logged in to an administrator account.

Block unauthorized modules in the browser

Description

Monitors DLL files that are loaded into browsers and prevents malicious files from being loaded into the browser.

Options

- **Never**
- **Always** (default)

Additional Information

Since this protection operates when the browser starts, it protects all websites and does not differentiate between partner sites and sites that were added manually.

Warn when browsing to malicious sites

Description

Warns you if you try to access a website that is known to be a malicious website.

Options

- **Never**
- **Always** (default)

Warn When Login Information is Used in Unknown Websites

Description

Passwords that you enter into your sensitive websites are classified by Rapport as Personally Identifiable Information (PII). For Partner Websites, Rapport might classify additional information, such as your user name, as PII, based on the policy that is chosen by the website's owner. Rapport [offers to protect your password](#) the first time you log in to a protected website. Your choice to protect your password creates a policy of password protection for that site. When you browse the web and enter text that matches your password into other websites, Rapport analyzes these websites. If they are unknown, Rapport triggers a warning that requires your action. See [Responding to a Protected Information Warning](#).

The purpose is to protect you against fraudulent websites that try to steal your PII: an attack that is known as [phishing](#)⁶.

Options

- **Never.** Rapport does not offer to protect your password when you log in to a website for the first time and does not warn you if you enter passwords in unrecognized websites.
- **On partner websites.** Rapport offers to protect your password when you log in to a partner website for the first time and, if you click **clear cache**, the first time after you click **clear cache**. For each website that you choose to protect your password, Rapport warns you if you enter the protected password into unrecognized websites.
- **On partner & my sensitive websites** (default). Rapport offers to protect your password when you log in to any partner or manually protected website for the first time, and, if you click **clear cache**, the first time after you click **clear cache**. For each website that you choose to protect your password, Rapport warns you if you enter the protected password into unrecognized websites.

Additional Information

You can see the password and user name protection policies for the individual websites by clicking **Warn When Login Information is Used in Unknown Websites**.

If you want to disable password or user name protection for a specific website, clear the check box. Rapport will not warn you when you enter this password or user ID into unknown websites.

⁶ A phishing attack is an attempt to lure you into visiting a forgery of a website you trust, such as your bank's website, and submitting your online login information so that it can be used by the criminals to access your online bank account and commit fraud, for example by transferring money out of your bank account.

You can clear the cache of protected PII. After you clear the cache, Rapport no longer protects any passwords. Clearing the cache also resets all of your password protection decisions for all individual protected websites. The first time you log in to each protected website after you clear the cache, Rapport offers to protect your password again. To clear the cache, click **Warn When Login Information is Used in Unknown Websites** and then click **Clear Cache**.

Block Browser Process Alteration

Description

Blocks attempts to alter the browser's process. Altering the browser's process (also known as function patching) is a technique that allows taking over the browser and getting access to your sensitive information. This technique is used by malware but also by some legitimate software. Rapport analyzes each process alteration attempt and blocks attempts that look suspicious.

Options

- **Never**
- **Always** (default)

Additional Information

Since this protection operates when the browser starts, it protects all websites and does not differentiate between partner sites and sites that were added manually.

Protect Trusteer Endpoint Protection from Unauthorized Removal

Description

Protects Rapport itself against unauthorized removal and tampering. Rapport protects its process against termination; its files against deletion and tampering; and its registry keys against deletion and tampering. As a result it is impossible to perform simple operations such as End Process or Delete Files on Rapport. Rapport does this to prevent malware from removing it from the computer.

Options

- **Never**
- **Always** (default)

Additional Information

If Rapport was installed from an administrator-level Windows account, you can change this setting only if you are logged in with an administrator account.

Rapport can and should be removed only through the control panel, as described in [Uninstalling Rapport](#).

Early Browser Protection

Description

Starts protecting the browser at the earliest possible stage when the browser starts.

Options

- **Never**
- **Always** (default)

Additional Information

Since this protection operates when the browser starts, it protects all websites and does not differentiate between partner sites and sites that you manually added.

If Rapport was installed from an administrator-level Windows account, you can change this setting only if you are logged in with an administrator account.

Send Security Events and Errors for Analysis

Description

Whenever Rapport detects suspicious software or website activity it generates a security event and sends it to the Rapport central service for analysis. The central service runs extensive tests to determine whether the activity is fraudulent. In an event of fraudulent activity, the Rapport central service instructs Rapport to more aggressively block the threat. In addition to security events, Rapport sends from time

to time information about internal software errors. This information can help IBM identify and fix software issues. All information that is sent from your computer to the Rapport central service is anonymous and includes technical details, not private information.

Disabling this feature might significantly compromise your security. If there is a real threat to your online security, this feature enables the owner of the attacked website, such as your bank or enterprise, to be alerted and to take pre-emptive measures to secure your sensitive information and funds.

Options

- **Only Critical Events**
- **Always** (default)

Additional Information

If Rapport was installed from an administrator-level Windows account, you can change this setting only if you are logged in with an administrator account.

To learn about IBM's privacy policy and IBM's practices about user information, see <http://www.trusteer.com/support/privacy-policy> and <http://www.trusteer.com/support/end-user-license-agreement>.

Remove Malware

Description

Rapport removes certain types of malware from your computer. This provides an important extra layer of security that complements Rapport's ability to prevent malware from accessing your sensitive information.

Options

- **Never**
- **Always** (default)

Additional Information

If Rapport was installed from an administrator-level Windows account, you can change this setting only if you are logged in from an administrator account.

Note: In some installations of Rapport, this setting cannot be disabled.

Protect Payment Card Numbers from Theft

Description

Warns you when you submit payment card information to local and non-secure websites. The warning appears in a dialog box on which you can stop the submission.

Activates anti keylogging when you enter a payment card number into either a Rapport protected site or any secure (HTTPS) site that contains a payment card related keyword such as Visa, Mastercard, or Amex. This is to prevent key logging malware from capturing your payment card details.

The purpose is to protect you from payment card theft by helping you to avoid submitting your payment card number to a phishing website or to a legitimate website that is not secure and by preventing malware from capturing your payment card details.

This protection is available only for cards that are issued by [participating payment card brands](#).

Options

- **Never**
- **Always** (default)

Additional Information

If Rapport was installed from an administrator-level Windows account, you can change this setting only if you are logged in from an administrator account.

The sites that are listed under "You chose to trust the following sites" are any sites that you chose to trust by clicking **Ignore, I trust this website** in the [payment card submission detection warning](#) dialog box.

To remove a specific site from the list of trusted sites, click **Clear this site** next to the site you want to remove. To remove all sites, click **Clear all sites**.

If you do not want to be notified when Rapport activates anti key-logging, uncheck **Notify me when Trusteer activates payment card protections** (enabled by default).

If you do not want to be warned when you submit payment card information to local and non-secure websites, uncheck **Alert me when Trusteer Endpoint Protection detects high risk payment card submission** (enabled by default).

[Warn when I submit security data to insecure sites](#)

Description

Warns you when you enter a password into a website that does not submit data securely. The purpose is to protect you from submitting sensitive data to high risk sites, including legitimate sites that might easily be intercepted by criminals.

Options

- **Never**
- **Always** (default)

Additional Information

If Rapport was installed from an administrator-level Windows account, you can change this setting only if you are logged in from an administrator account.

The sites that are listed under "You chose to trust the following sites" are any sites that you chose to trust either by clicking **I trust this site, don't alert me again** in the [non-secure submission warning](#) dialog box or by clicking **Trust this site** in the [protected information warning](#) dialog box.

To remove a specific site from the list of trusted sites, click **Clear this site** next to the site you want to remove. To remove all sites, click **Clear all sites**.

13. Troubleshooting

Having a problem with Rapport? A troubleshooting FAQ is available here: <http://www.trusteer.com/support/faq>.

To find out how you can get support, see [Getting Support](#). Find out in the following sections how to do some procedures that can be involved in troubleshooting situations.

Note: You can always [turn off Rapport](#) without removing Rapport from your computer to check whether a specific problem is Rapport related. Try to avoid removing Rapport while troubleshooting. [Stopping Rapport](#) has the same effect and allows IBM to quickly and efficiently resolve the issue when you contact support.

Stopping Rapport

Stopping Rapport shuts down Rapport functionality quickly and easily without uninstalling. You can stop Rapport to find out if Rapport is the cause of a problem you are experiencing. When you want to run Rapport again, [start Rapport](#), with no need to reinstall.

If you have a problem and you suspect that Rapport might be the cause, try stopping Rapport. If the problem remains after Rapport is stopped, Rapport is unlikely to be the cause of the problem. If the problem disappears when you stop Rapport, Rapport is likely to be at least a partial cause of the problem.

IBM recommends not to uninstall Rapport. If you are thinking of uninstalling Rapport, contact IBM Trusteer Support for assistance, see [Getting Support](#).

Note: If Rapport was installed from a Windows administrator account, you can stop Rapport only if you are logged in from an administrator account.

➔ To stop Rapport:

1. Save your work and close all open windows.

Note: Do not stop Rapport when the browser is open. Stopping Rapport when the browser is open can cause a crash.


2. From the Windows Start menu, select **Programs > Trusteer Endpoint Protection > Stop Trusteer Endpoint Protection**. A security confirmation message appears. The message displays an image of some characters for you to type. This is done to prevent malware from disabling Rapport.
3. Enter the characters that you see in the image.
4. Click **Shutdown**. The following message appears while Rapport shuts down: "Please wait while Trusteer Endpoint Protection shuts down." When the message disappears, Rapport is stopped. You can verify that Rapport is no longer running by opening your browser and checking that the Rapport icon no longer appears at the right of the address bar.

Starting Rapport

Starting Rapport resumes Rapport if it was previously stopped.

Note: If Rapport was installed from a Windows administrator account, you can start Rapport only if you are logged in from an administrator account.

➔ To start Rapport:

From the Start menu, select **Programs > Trusteer Endpoint Protection > Start Trusteer Endpoint Protection**. The message "Please wait while Trusteer Endpoint Protection starts" appears. When the message disappears, Rapport has restarted. You can verify that Rapport is running by checking for the Rapport icon in the system tray ()

Getting Support

IBM Trusteer Support is always available. IBM provides several support options:


- If Rapport is installed on your computer and you do not have a connectivity problem, you can start by reporting your problem from the Rapport Console. See [Sending a User Problem Report](#). When you report a problem from the Rapport Console, Rapport sends a support request to IBM with your problem report and important log files that help IBM solve your problem.
- If Rapport is not installed or you are unable to send a support request through it, use the form at <http://www.trusteer.com/support/submit-ticket> to send a support request. Include as much information as you can about both the problem and your computer, including the operating system, the browser, the behavior you encountered, and other relevant details.
- If you have performance, connectivity, stability, or browser issues, click the "Live Support" link at <http://www.trusteer.com/support> to start an online chat with a support representative.

Note: If you have a question about Rapport and you are not experiencing a problem, search this guide or use the Instant Answers service on this web page: <http://www.trusteer.com/support/faq>.

Unblocking Legitimate Browser Add-ons

If certain webpages do not display correctly in your browser and you think that a legitimate add-on might be blocked, you can check to see whether Rapport is blocking the add-on.

➔ To unblock a legitimate browser add-on:


1. [Open the Rapport Console](#).
2. In the dashboard, click . The second dashboard screen appears.

3. In the Security Policy area, click **Edit Policy**. A User Approval screen appears. The screen shows you an image of a word for you to type to prevent malware from accessing the console and effectively disabling Rapport.
4. Enter the characters that you see in the image.
Click **OK**. The Security Policy screen appears, displaying all the security controls.
5. Click **Block Unknown Browser Add-ons**. A list of any blocked add-ons appears. There is an **Always Allow this add-on** check box next to the name of each blocked add-on.
6. Select the **Always allow this add-on** check box for the blocked add-on that you want to allow.
7. Click **Save**. The add-on is now unblocked.

Disabling Keylogger Blocking

Rapport's keylogger blocking feature can conflict with other anti keyloggers, leading to scrambled keystrokes. Therefore, if you have another anti keylogger running (for example, as part of your antivirus software), you might need to disable this feature. Alternatively, you might be able to disable your existing software's keylogging protection.

➔ To disable keylogger blocking:

1. [Open the Rapport Console](#).
2. In the dashboard, click . The second dashboard screen appears.
3. In the Security Policy area, click **Edit Policy**. A User Approval screen appears. The screen shows you an image of a word for you to type to prevent malware from accessing the console and effectively disabling Rapport.
4. Enter the characters that you see in the image.
Click **OK**. The Security Policy screen appears, displaying all the security controls.

- From the list next to **Activate Character Replacement**, select **Never**. The following message appears:

When 'Activate Character Replacement' is set to 'never', Trusteer Endpoint Protection does not protect your payment cards. You can either restore defaults, enable character replacement or disable payment card protection for the settings to be consistent.

- Click **OK**.
- From the list next to **Activate Kernel Character Replacement**, select **Never**.
- Click **Save**. A message appears, informing you that your changes will take effect after you restart your computer.
- Click **OK**.
- Restart your computer. Rapport's keylogger blocking is disabled.


Undoing Accidental Authorizations

With some of Rapport's warnings, you can authorize websites or certificates that Rapport does not recognize as legitimate. After a website or certificate is authorized, you are not warned again about the same website or certificate, since it is stored in a cache. If you accidentally authorized a website or certificate, you can clear the cache so that the same website or certificate would generate a warning if you connect to it again.

Clearing Authorized Invalid SSL certificates

When Rapport detects that a website's [certificate](#)⁷ is invalid, Rapport displays an [Invalid Certificate Warning](#) to protect you from submitting information to a fraudulent website. If you check **Do not warn me about this website again** in an Invalid Certificate Warning dialog box, the certificate of the website to which you are connecting is added to a cache of authorized invalid certificates. Clearing that cache removes your authorization of any certificates in the cache and causes Rapport to warn you again if you browse to the same websites again.

➔ To clear authorized invalid SSL certificates:

1. [Open the Rapport Console](#).
2. In the dashboard, click . The second dashboard screen appears.
3. In the Security Policy area, click **Edit Policy**. A User Approval screen appears. The screen shows you an image of a word for you to type to prevent malware from accessing the console and effectively disabling Rapport.
4. Enter the characters that you see in the image.


Click **OK**. The Security Policy screen appears, displaying all the security controls.
5. Click **Validate Website SSL Certificates**. Information about this control appears below it as well as a **clear cache** link.
6. Click **Clear Cache** in the expanded information block. A confirmation box appears.
7. Click **OK**. The cache is cleared.

⁷ An SSL certificate is a cryptographic digital certificate that validates the identity of a website and creates an encrypted connection for sending sensitive private data to the website. When you see the SSL padlock in the browser's address bar or at the bottom of the browser, a secure connection between your browser and the website exists using the SSL protocol. However, the presence of the padlock does not provide an indication that the certificate is valid.

Clearing Trusted Sites for Payment Card Submission

When Rapport detects that you entered a protected payment card number into a webpage on a local drive or a non-secure website, Rapport displays a [payment card submission detection warning](#). The purpose of this message box is to prevent your payment card number from being submitted to a phishing website or to a legitimate website that is not secure. If you click **Ignore, I trust this website** in a payment card submission detection warning dialog box, the website is added to a list of websites you chose to trust and you are not warned again if you enter your payment card number into that site. You can remove a site from that list.

➔ To clear sites you chose to trust for payment card submission:

1. [Open the Rapport Console](#).
2. In the dashboard, click . The second dashboard screen appears.
3. In the Security Policy area, click **Edit Policy**. A User Approval screen appears. The screen shows you an image of a word for you to type to prevent malware from accessing the console and effectively disabling Rapport.
4. Enter the characters that you see in the image.


Click **OK**. The Security Policy screen appears, displaying all the security controls.
5. Click the control **Protect Payment Card Numbers from Theft**. Any sites that you chose to trust are listed in an expanded area. The expanded area lists the sites that you chose to trust by clicking **Ignore, I trust this website** in the payment card submission detection warning dialog box.
6. Either click **Clear this site** for each site you want to remove from the list, or click **Clear all sites** to remove all trusted sites. A confirmation box appears.
7. Click **OK**.

Clearing Trusted Sites for Non-Secure Submissions

When Rapport detects that you entered a password into a website that does not submit data securely, Rapport displays a [non-secure submission warning](#). The purpose of this warning is to protect you from submitting sensitive data to high risk sites, including legitimate sites that might easily be intercepted by criminals.

If you click **I trust this site, don't alert me again** in this dialog box, the website is added to a list of websites you chose to trust and you are not warned again if you enter your payment card number into that site. You can remove a site from that list.

➔ To clear non-secure websites that you chose to trust:

1. [Open the Rapport Console](#).
2. In the dashboard, click . The second dashboard screen appears.
3. In the Security Policy area, click **Edit Policy**. A User Approval screen appears. The screen shows you an image of a word for you to type to prevent malware from accessing the console and effectively disabling Rapport.
4. Enter the characters that you see in the image.


Click **OK**. The Security Policy screen appears, displaying all the security controls.
5. Click the control **Warn when I submit security data to insecure sites**. Any sites that you chose to trust are listed in an expanded area. The expanded area lists the sites that you chose to trust either by clicking **I trust this site, don't alert me again** in the [non-secure submission warning](#) dialog box or by clicking **Trust this site** in the [protected information warning](#) dialog box.
6. Either click **Clear this site** for each site you want to remove from the list, or click **Clear all sites** to remove all trusted sites. A confirmation box appears.
7. Click **OK**.

Clearing Websites to Which You Allowed Sending Login Information

When you enter text that matches a protected password into an unknown website, Rapport displays a [Protected Information Warning](#). If you choose to ignore the warning, the website becomes an authorized website and Rapport no longer warns you if you enter a protected password into that website. Websites that you authorize in this way are stored in a cache. Clearing that cache removes any such authorizations that you previously made.

If you clicked **Ignore this warning** by accident in a Protected Information Warning dialog box, you might want to clear the cache of authorized websites to which you allowed sending login information. Clearing the cache does not undo any password submissions that already occurred, but it does reset the unknown status of websites that you authorized by accident.

➔ **To clear the cache of authorized websites to which you allowed sending login information:**

1. [Open the Rapport Console](#).
2. In the dashboard, click . The second dashboard screen appears.
3. In the Security Policy area, click **Edit Policy**. A User Approval screen appears. The screen shows you an image of a word for you to type to prevent malware from accessing the console and effectively disabling Rapport.
4. Enter the characters that you see in the image.

Click **OK**. The Security Policy screen appears, displaying all the security controls.
5. Scroll down to **Warn When Login Information is Used in Unknown Websites** and click the control name. Information about this control appears below it as well as a **clear cache** link.
6. Click **Clear Cache** in the expanded information block. A confirmation box appears.
7. Click **OK**. The cache is cleared.

Handling Errors

If you see a Rapport error, and you'd like some information about it, read here.

Handling an Update Error

The following text is an example of a Rapport update error:

*Trusteer Endpoint Protection was unable to receive updates.
Click OK to configure your proxy username and password.*

This error occurs if Rapport was unable to connect to the Internet to check for updates. This error can occur if you connect to the internet through a proxy and Rapport was unable to detect that the proxy details automatically.

➔ If you receive this error:

1. Click **OK**. The Rapport Console opens, displaying the Internet Connection tab.
2. Select **Use proxy server**. Enter the proxy server name or IP address in the field provided.
3. In the **Port** field, enter the TCP port to use to connect to your proxy server.
4. If your proxy server requires authentication, enter the user name in the **Proxy username** field and the password in the **Proxy password** field.
5. Click **Apply Settings**.
6. Click **Check Connection** to check whether Rapport can connect to the Internet after you configure a proxy server.

Handling Rapport Installer Errors

Installing Rapport uses a two stage installation:

1. The user downloads RapportSetup.exe (a bootstrap file).
2. When the user runs this file, the full installation file is downloaded. If this download fails, which sometimes occurs due to a firewall that blocks the download, you might see an error message "Error extracting Rapport setup package".

To resolve this issue, download the full setup package from the following website:

<http://www.trusteer.com/support/install-troubleshooting>.

The following text is an example of a Rapport installer error:

*Sorry, the setup package could not be downloaded.
Click 'OK' to close Setup. You will be automatically taken to a download page, where you can directly download the setup package and install it.
If the problem persists, check your network and firewall settings.*

This error appears during Rapport installation if the Rapport installer cannot download the full setup package.

If you see this error, click **OK**. The IBM website opens. You can download the full setup package from the following website:

<http://www.trusteer.com/support/install-troubleshooting>.

Note: If you do not find the instructions on the website helpful, contact IBM Trusteer Support at <http://www.trusteer.com/support/submit-ticket>.

Handling Uninstall Errors

The following text is an example of an error that can occur during the uninstall process:

Some of Trusteer Endpoint Protection files are locked by another software. If you have an open browser please close it and then try to uninstall Trusteer Endpoint Protection. If the problem persists, please see this site: http://rapport.trusteer.com/installer/troubleshoot_uninstall

This message appears if any of Rapport's files are locked by another program when you try to uninstall Rapport.


If you see this error, follow the instructions in the dialog box. You can download the Safe Uninstall utility, which you can use to uninstall Rapport, from the following website: <http://www.trusteer.com/support/uninstall-troubleshooting>.

Note: If you do not find the instructions on the website helpful, submit a request for support at: <http://www.trusteer.com/support/submit-ticket>.

Configuring a Proxy Server for Automatic Updates

Rapport connects to the Internet automatically to check for updates and download security policies. Most proxy configurations are automatically detected by Rapport without any configuration. However, if for some reason Rapport is unable to automatically detect your proxy, you will need to configure it.

➔ To configure a proxy server:

1. [Open the Rapport Console](#).
2. In the dashboard, click . The second dashboard screen appears.
3. In the Performance and Connectivity area, next to the Internet Connection field, click **Change**. The Internet Connection tab appears.
4. Select **Use proxy server**. Enter the proxy server name or IP address in the field provided.
5. In the **Port** field, enter the TCP port to use to connect to your proxy server.
6. If your proxy server requires authentication, enter the user name in the **Proxy username** field and the password in the **Proxy password** field.
7. Click **Apply Settings**.
8. Click **Check Connection** to check whether Rapport can connect to the Internet after you configure a proxy server.

Sending a User Problem Report

When you use the Rapport problem reporting feature, Rapport sends a technical report with important internal Rapport log files along with your problem description. This technical report can help IBM identify and resolve the issue. This is the best way to report a problem, since it gives IBM the most comprehensive information about your problem, which helps IBM to provide the best support.

Note: The information inside the log files is technical and does not include sensitive or private information about you.

➔ To report a problem:

1. [Open the Rapport Console](#). The Dashboard appears.
2. In the Help and Support area, click **Report a problem**. The Report a Problem tab appears.
3. In the **Name** field, optionally enter your name.
4. In the **Email** field, enter your email address. IBM will use this address to send you a solution to your problem.
5. In the **Problem description** field, enter a full description of the problem. Include as many details as you can.
6. Click **Submit**. The following message appears at the lower right of your screen while Rapport sends your problem report.

Trusteer Endpoint Protection is sending your problem report...

When the report is sent, a message appears to confirm that the report was sent.

Your last support request was successfully sent to Trusteer.

An IBM representative will contact you over email to help you with the issue.

Copying the Trusteer Endpoint Protection ID

When you contact IBM Trusteer Support, you might be asked for your Trusteer Endpoint Protection ID number. You can copy your Trusteer Endpoint Protection ID number from the Product Settings in the Console.

➔ To copy your Trusteer Endpoint Protection ID:

1. [Open the Rapport Console](#). The Dashboard appears.
2. In the Product Settings area, click **More Settings**. The Product Settings tab appears.
3. Click **Copy Trusteer Endpoint Protection ID**. Your Trusteer Endpoint Protection ID is saved to your computer's clipboard.
4. In your email window, press Ctrl+V to paste your Trusteer Endpoint Protection ID into your email message.

Sending Rapport Log Files to IBM

If IBM Trusteer Support asks you to locate Rapport log files on your computer and send them to IBM to help them solve your problem, follow the procedure on the following webpage: <http://www.trusteer.com/support/gathering-rapport-logs>.

Installation Issues

IBM provides a short and simple installation process that does not require any technical knowledge from the end user. However, in certain cases users might encounter problems when they try to install Rapport.

Uninstall not Completed

If you uninstalled Rapport and want to reinstall, you must first restart your computer. If you try to reinstall without restarting the computer after uninstalling, the following message appears:

Cannot install Trusteer Endpoint Protection at this time. Please try again, after rebooting your computer. If the problem persists contact <http://www.trusteer.com/support> with the following reference code: PREVUNIS.

To resolve this issue, restart the computer and try again.

Installation Stuck in 'Select Destination' (Mac only)

The Mac installation wizard allows the user to select the destination in which to install Rapport. In some cases, users are unable to proceed past this stage and **Continue** is unavailable.

This indicates that users are using an old and unsupported version of the Mac OS X operating system. Rapport can be installed only on Mac OS X 10.6 Snow Leopard or newer. For a list of supported platforms, see the following website:

<http://www.trusteer.com/support/supported-platforms>.

Windows Installation Error 1638

If a user attempts to install a new version of Rapport on top of a very old version, the user might see an error message "An error occurred installing the package. Windows Installer returned '1638'."

➔ To resolve this issue:

1. Remove all Rapport folders as described here:

<http://www.trusteer.com/support/remove-rapport-folders>.

2. Run the Windows cleanup utility:

http://support.microsoft.com/mats/Program_Install_and_Uninstall.

3. Restart the computer and try again.

Windows Installation Error 16xx

If users receive an error message similar to the message described in [Windows Installation Error 1638](#), it usually indicates a problem with the Windows installer.

➔ To resolve this issue for Windows XP, Windows Vista, or Windows Server:

1. Update the Windows installer:
<http://www.microsoft.com/download/details.aspx?id=8483>.
2. Restart the computer and try to install Rapport again.

➔ To resolve this issue for Windows 7 or Windows 8:

1. Verify that the installer's service is enabled:
 - a. Open the list of services by opening the "Run" command (Windows key + 'R') and run the following command:

```
services.msc
```

- b. Locate the Windows Installer Service in the list, right-click it and click **Properties**. Make sure that the **Startup Type** is set to **Manual**.
 - c. Restart the computer and check if the problem persists.
2. If the problem persists, try to register the Windows Installer:

- a. Open the "Run" command (Windows key + 'R'), and run the following command:

```
msiexec /unreg
```

- b. On the confirmation message, click **OK**.
 - c. Open the "Run" command (Windows key + 'R'), and run the following command:

```
msiexec /regserver
```

- d. On the confirmation message, click **OK**.

- e. Restart the computer and try again.
3. If the problem persists, open a command line with administrator privileges, and run the following command:

```
sfc.exe /scannow
```

4. After the process finishes, try to install Rapport again.

Windows does not Support Digital Signatures

The user might see the following error message if the crypt32.dll file is missing or corrupted: "This version of Windows does not support digital signatures.". The crypt32.dll is an important Windows system file. If it is missing or corrupted, the user might also be experiencing difficulties when they install other programs.

The user should contact Microsoft to retrieve the missing file.

Installation Ended Prematurely

In some cases, users might describe having a problem when they install Rapport. The installation process begins normally, but at some point the progress bar rolls back to the beginning, and the setup wizard shows the following message:

Trusteer Endpoint Protection Setup Wizard ended prematurely because of an error. Your system has not been modified. To install this program at a later time, run Setup Wizard again. Click the Finish button to exit the Setup Wizard.

There are several possible causes for this error. Step through the following procedure until you resolve the issue.

➔ To resolve this issue:

1. Remove all Rapport folders as described here:
<http://www.trusteer.com/support/remove-rapport-folders>.
2. Restart the computer and try again.

3. If the problem persists, make sure that the following system files exist on the computer:

- a. c:\windows\system32\srclient.dll
- b. c:\windows\system32\winpool.drv
- c. For Windows XP: c:\windows\system32\wbem\framedyn.dll
- d. For Windows Vista/7/8: c:\windows\system32\framedyn.dll

If any of these files are missing, the user should contact Microsoft to retrieve the missing system files.

4. Try to create an Internet shortcut on the computer:

- a. Right-click the desktop, and then click **New > Shortcut**.
- b. Type <http://www.trusteer.com>.
- c. Click **Next > Finish**.

If this does not work, the operating system might be blocking many installation types. If so, the user should contact Microsoft support to resolve the problem.

5. Right-click My Computer, and then click **Properties > Advanced tab > Environment variables**. Locate the PATH variable and make sure that the **Variable Value** field begins with the string:

```
%SystemRoot%\system32;%SystemRoot%;%SystemRoot%\System32\Wbem;
```

If the PATH variable does not begin with that string, add it to the beginning of the field.

If the PATH variable does not exist, create it by going to **System Variables > New**. Name the variable **PATH** and copy the preceding string to the **Variable Value** field.

Click **OK** on all open menus and try installing Rapport.

6. If the problem persists, escalate the issue to the IBM Trusteer Support team:

<http://www.trusteer.com/support>.

Rapport Icon

By default, the Rapport icon always appears on or near the right side of your browser's address bar. The icon is green when the website in your browser is protected by Rapport and gray when the website in your browser is not protected by Rapport.



A common issue that users experience is that the Rapport icon is missing.

➔ To resolve this issue for PC users:

1. Restart the computer. After Rapport is installed, the icon does not appear until the computer is restarted.
2. Make sure that the user is using a supported browser.
See <http://www.trusteer.com/support/supported-platforms>.
3. Make sure that the user is using the latest version of Rapport. See [Checking the Status of Rapport Updates](#).
4. Check whether there are any conflicts with other programs on the computer.
For a list of compatible security software, see:
<http://www.trusteer.com/support/compatibility-other-security-software>.

Note: Not every conflict is related to the Rapport icon. Clicking the name of a program in the list of software shows the type of conflict it might cause, and how to solve it.

5. Make sure that the user has not hidden the Rapport icon, see [Hiding and Restoring the Rapport Address Bar Icon](#).
6. If the problem persists, the user should submit a problem report. See [Sending a User Problem Report](#).

➔ **To resolve this issue for Mac users:**

1. Restart the computer. After Rapport is installed, the icon does not appear until the computer is restarted.
2. Make sure that the user is using a supported browser.
See <http://www.trusteer.com/support/supported-platforms>.
3. Make sure that the user is using the latest version of Rapport. The Rapport version is shown in the Rapport console on the **Product Settings** page.
4. Check whether there are any conflicts with other programs on the computer.
For a list of compatible security software, see:
<http://www.trusteer.com/support/compatibility-other-security-software>.

Note: Not every conflict is related to the Rapport icon. Clicking the name of a program in the list of software shows the type of conflict it might cause, and how to solve it.

5. Try to Force Quit the browser (CMD+Q) and then reopen the browser and check if the icon appears. If the icon appears, configure the browser so that it doesn't start automatically when the computer starts:
 - a. For Snow-Leopard OS (10.6): Go to **System Preferences > Accounts > Login Items**. If the web browser appears in the list, remove it.
 - b. For Lion and Mountain Lion OS (10.7 and 10.8): Go to **System Preferences > Users & Groups > Login Items**. If the browser appears in the list, remove it.
 - c. Do not select the **Reopen windows when logging in** check box when shutting down or rebooting the computer.
 - d. Restart the computer and check if the icon is still missing.
6. If the problem persists, the user should submit a problem report. See [Sending a User Problem Report](#).

Splash Screen Issues

Users might complain that the splash screen that promotes Rapport appears when they try to log in to their online banking account. Several issues can cause the splash screen to appear; therefore, it is important to understand when this message appears and whether Rapport is installed.

Splash Screen Appears when Rapport is Not Installed

On most splash screens, users can click **No, thanks** or **Remind me later**. If the user clicks **Remind me later**, the splash screen reappears at an interval that was configured by the bank when the splash screen was implemented on the website. It is considered normal if the splash screen appears up to once a week; however, if it reappears every day or on every login, it might indicate a problem.

➔ To resolve this issue:

1. Make sure that the browser is set to save or allow cookies.
<http://www.trusteer.com/support/i-keep-getting-offered-download-rapport>.
2. Make sure that the browser is not set to delete cookies when closed:
 - a. Internet Explorer: Go to **Internet Options > General**. Make sure that the **Delete browsing history on exit** check box is not selected.
 - b. Google Chrome: Go to **Settings > Privacy > Content Settings**. Make sure that **Keep local data only until I quit my browser** is not selected.
 - c. Mozilla Firefox: Go to **Tools > Options > Privacy**. Make sure that the **Clear history when Firefox closes** check box is not selected.
3. Try to clear cookies and login again. The user will see the splash screen on the first attempt, but after they click **No, thanks**, the splash screen will not reappear.
4. If the problem persists, escalate the issue to the IBM Trusteer Support team:
<http://www.trusteer.com/support>.

Splash Screen Appears but Rapport is Already Installed

The splash screen normally recognizes if Rapport is already installed and appears only when it is not installed. When you troubleshoot a splash screen issue, always first verify whether Rapport is installed and working properly.

➔ Troubleshooting for PC users:

1. Restart the computer and try again.
2. Make sure that the user is using the latest version of Rapport. See [Checking the Status of Rapport Updates](#).
3. Make sure that the Rapport icon appears in the browser address bar. See <http://www.trusteer.com/support/how-can-i-tell-rapport-working>.
 - a. If the icon doesn't appear, see [Rapport Icon](#).
 - b. If the icon appears, but is gray on a protected site, escalate the issue to the IBM Trusteer Support team: <http://www.trusteer.com/support>.
 - c. If the icon appears and is green and the splash screen appears, continue with this procedure.
4. Restart the browser and try again.
5. If the problem persists, try to clear browser cookies and check if the splash screen still appears.

<http://www.trusteer.com/support/i-keep-getting-offered-download-rapport>.
6. If the problem persists, it might be a networking problem:
 - a. Add the address of the splash screen to the Internet Explorer's trusted sites: Go to **Tools > Internet Options > Security > Trusted Sites**, click **Sites**, and then add the site.
 - b. Ask the user to go to the address of the splash screen. If the browser shows a 403-forbidden error message, it indicates that the user has a firewall, web filter, or proxy server that is blocking the splash screen. They need to add the address of the splash screen to the service that is blocking it.

7. If the problem persists, the user should submit a problem report. See [Sending a User Problem Report](#).

➔ **Troubleshooting for Mac users:**

1. Restart the computer and try again.
2. Make sure that the user is using the latest version of Rapport. The Rapport version is shown in the Rapport console on the **Product Settings** page.
3. Make sure that the Rapport icon appears in the browser address bar. See <http://www.trusteer.com/support/how-can-i-tell-rapport-working>.
 - a. If the icon doesn't appear, see [Rapport Icon](#).
 - b. If the icon appears, but is gray on a protected site, escalate the issue to the IBM Trusteer Support team: <http://www.trusteer.com/support>.
 - c. If the icon appears and is green and the splash screen appears, continue with this procedure.
4. Try to Force Quit the browser (CMD+Q) and then reopen the browser and check if the splash screen appears. If the splash screen appears, configure the browser so that it doesn't start automatically when the computer starts:
 - a. For Snow-Leopard OS (10.6): Go to **System Preferences > Accounts > Login Items**. If the web browser appears in the list, remove it.
 - b. For Lion and Mountain Lion OS (10.7 and 10.8): Go to **System Preferences > Users & Groups > Login Items**. If the browser appears in the list, remove it.
 - c. Do not select the **Reopen windows when logging in** check box when shutting down or rebooting the computer.
 - d. Restart the computer and check if the splash screen still appears.
5. If the problem persists, the user should submit a problem report. See [Sending a User Problem Report](#).

Performance Issues

If a computer complies with Rapport's [System Requirements](#), installing Rapport does not normally affect system performance.

Slow Computer or Web Browser

In rare scenarios, Rapport might cause the computer to respond slowly. This slowness is experienced when the user opens the browser or goes to different websites. IBM takes these issues seriously; however, slight slowness is expected after any new security program is installed. Since slowness is a problem that might sometimes be hard to detect or analyze, always first verify that the slowness is indeed related to Rapport.

1. Try to stop Rapport and use the computer normally for a few minutes to see whether the slowness occurs only when Rapport is running. You can also try to start Rapport and see whether the computer starts to respond slowly.

To start or stop Rapport, see [Starting Rapport](#) and [Stopping Rapport](#).

Note: When Rapport is stopped, it has no effect on the browser. If the slowness persists, it indicates that the problem is unrelated to Rapport.

2. Make sure that the computer has sufficient RAM:
 - a. Press Windows+R to open the Run dialog box, and then type:

`msinfo32`
 - b. Click **OK**.
 - c. In the **System Information** window, in the navigation pane, click **System Summary**, and in the details pane locate the entries for **Total Physical Memory** and **Available Physical Memory**.

If the computer has less than 1 GB of total physical memory, or less than 100 MB of available physical memory, it cannot run Rapport.

3. If the computer has sufficient RAM and the slowness is associated with Rapport, escalate the issue to the IBM Trusteer Support team:

<http://www.trusteer.com/support>.

High CPU or Memory Usage

Rapport normally uses two services that always appear in the task manager: RapportService.exe and RapportMgmtService.exe.

The following table shows normal memory and CPU consumption for these services:

	Memory Usage (MB)	CPU Usage (%)
RapportService.exe	Up to 40	0-1
RapportMgmtService.exe	Up to 30	0-1

Short CPU spikes are normal during Rapport operations such as opening the browser, logging in to an account, or opening the Rapport console. However, end users might sometimes complain that Rapport is using excessive resources.

If a customer complains about high CPU or memory consumption, verify the following information:

- Is the problem with RapportService.exe or RapportMgmtService.exe?
- Is it using too much of the CPU, or too much memory?
- How much CPU or Memory is this process using?

If consumption is excessive, escalate the issue to the IBM Trusteer Support team:

<http://www.trusteer.com/support>.

Interoperability Issues

Rapport uses a multi-layered security system that blocks malware and malicious activity from your online browsing in many different ways. Unfortunately, these security mechanisms can sometimes conflict with legitimate programs. If a conflict occurs, you can choose to edit or disable the relevant security policies. See [Changing Security Controls](#).

Note: You are not protected by Rapport's mechanisms that are disabled. Although you are protected by all other Rapport protection layers, leaving the policies in their default state provides the most protection. If you are not sure which changes you made, you can restore the default settings by clicking **Restore Defaults**.

Password Managers

Processes on your computer can access the browser and read sensitive information or tamper with your transactions. When you are connected to a protected website, Rapport blocks processes from accessing the browser regardless of whether the process is malicious or not. Unfortunately, blocking processes from accessing the browser might cause Rapport to block legitimate programs from trying to access the browser, such as password managers and fingerprint verifiers.

If the password manager stopped working after Rapport was installed, disable the policy **Block access to information inside the browser**.

Screen Capturing Software

Rapport blocks screen capture attempts when users go to protected websites. Programs on your computer that try to capture the screen get a black image. Malware might try to capture the screen when sensitive information (such as personal information) is presented. If you try to manually take a screen capture while on a protected site, Rapport presents a message on which you can approve this screen capture. Unfortunately, blocking screen capture attempts might block legitimate snipping tools and screen capturing utilities. Additionally, some screen sharing and remote access tools that use screen capturing technologies might be blocked.

If your snipping tool or remote access tool is blocked or displays blank or black screens, disable the policy **Block screen capturing**.

Visually Impaired Mode (Screen Readers or Magnifiers)

Some of Rapport's security mechanisms might conflict with assistive technologies for the visually impaired, such as screen readers or screen magnifiers. Additionally, any change in the Rapport settings requires the user to submit a CAPTCHA, which is a security code that cannot be read by automatic programs.

To allow these customers to enjoy the added security that Rapport offers, an installation of Rapport is included that is designed for the visually impaired. Installing Rapport in this mode automatically disables policies that might conflict with these assistive technologies.

To install Rapport in Visually Impaired mode, download and run the Rapport installation file normally. In the installation wizard, click **Advanced** and select the **I have a visual impairment, color blindness and/or regularly use assistive screen reading technologies** check box. Click **Continue** and proceed with the installation.

Other Issues

If you encounter a problem with Rapport that is not covered in this troubleshooting section, try the following general troubleshooting steps:

1. Restart the computer and check if the problem persists.
2. Make sure that the computer is running an updated version of Rapport.
 - a. For PC users, see [Checking the Status of Rapport Updates](#).
 - b. For Mac users, the Rapport version is shown in the Rapport console on the **Product Settings** page.
 - c. If a Rapport update is available, download the latest version, restart the computer and check if the problem is resolved. See <http://www.trusteer.com/support/rapport-installation-links>.
3. Check whether other programs are installed on the computer, and if they might be conflicting with Rapport.
See <http://www.trusteer.com/support/compatibility-other-security-software>.

4. If the problem occurs when using a certain web browser, make sure that this browser is supported and that you have the latest version.
See <http://www.trusteer.com/support/supported-platforms>.
5. If the problem might be unrelated to Rapport, try [stopping Rapport](#) and checking whether the problem persists. You can also try [starting Rapport](#) to check whether the problem resumes.
6. If the problem persists, escalate the issue to the IBM Trusteer Support team:
<http://www.trusteer.com/support>.

14. Keeping Rapport Updated

Regular updates are essential to the effectiveness of Rapport. For that reason, Rapport updates itself automatically. The updates occur independently and silently. However, you can update Rapport manually whenever you want to and you can also disable automatic updates.

Checking the Status of Rapport Updates

Information that is related to the status of Rapport updates is displayed in the Product Settings area of the Rapport Console.

➔ To check the status of Rapport updates:

1. [Open the Rapport Console](#). The Product Settings area is displayed at the upper left of the Dashboard.

The screenshot shows the IBM Security Trusteer Rapport Dashboard. The 'Product Settings' section is highlighted, showing the following information:

- Report is running ([stop](#))
- Address bar icon: visible ([hide](#))
- Tray icon: visible ([hide](#))
- Version: Emerald Build 1403.21**
- Pending updates: no (up to date)**
- [More Settings](#)

Other sections visible on the dashboard include:

- Weekly Activity Report:** Blocked Screen Capture: 0, Certificate Mismatch: 0, Blocked IP Addresses: 0. Includes a [Full Report](#) link.
- Trusted Websites:** Trusted Partner Websites: 383, My Sensitive Websites: 3. Includes a [Browse Trusted Websites](#) link and a lock icon.
- Help and Support:** [Report a problem](#), [Frequently Asked Questions](#), [User Guide](#), [Send us feedback](#). Includes a question mark icon.

A red arrow points from the text 'Version and update information' to the version and update status in the Product Settings section.

The **Pending updates** field informs you if there are any pending updates, and, therefore, if Rapport is up to date. This field displays *yes* if the last update that was downloaded requires a system restart before it will be applied.

2. Optionally, click **More Settings**. The Product Settings tab appears, displaying more information.

The following display fields are relevant to updates:

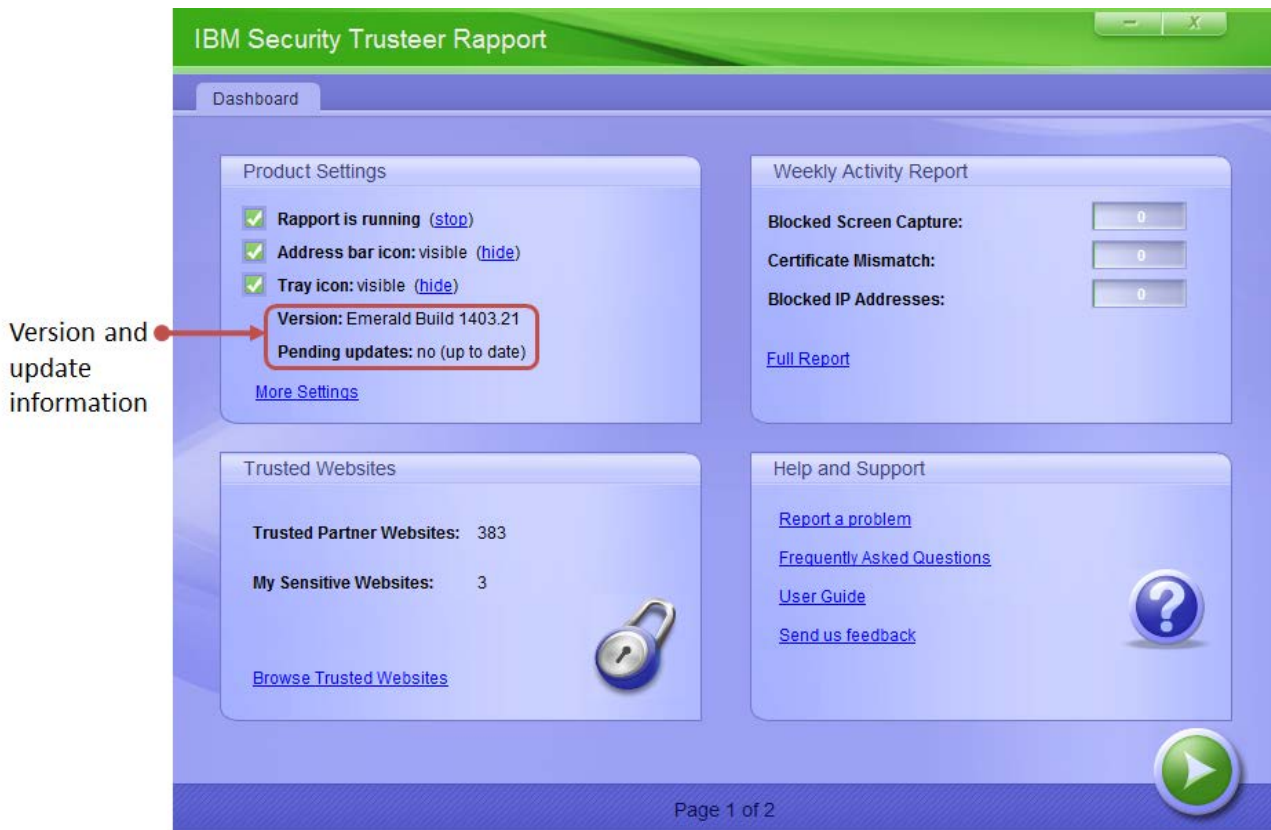
- **Last query for updates.** The date and time of the last time Rapport submitted a query to discover any new updates.
- **Automatic software updates.** Whether automatic updates are enabled or disabled. The default is enabled. Leave the default setting enabled to be sure to receive all updates.

Manually Updating Rapport

Rapport is updated automatically, by default. You can also update Rapport manually.

➔ To update Rapport manually:

1. [Open the Rapport Console](#). The Product Settings area is displayed at the upper left of the Dashboard.



2. Click **More Settings**. The Product Settings tab appears.
3. Click **check for updates now**. Rapport checks for updates. When Rapport checks for updates, the progress is indicated by text that appears beneath the display fields. The following list describes the possible results of the check for updates:
 - Rapport does not detect any pending updates. The following message appears: "You are already running the latest Rapport configuration."
 - Rapport detects and downloads and applies an update. The following message appears: "Configuration updated. You are now running with the

latest Rapport configuration." The number in the **Configuration file** display field is incremented.

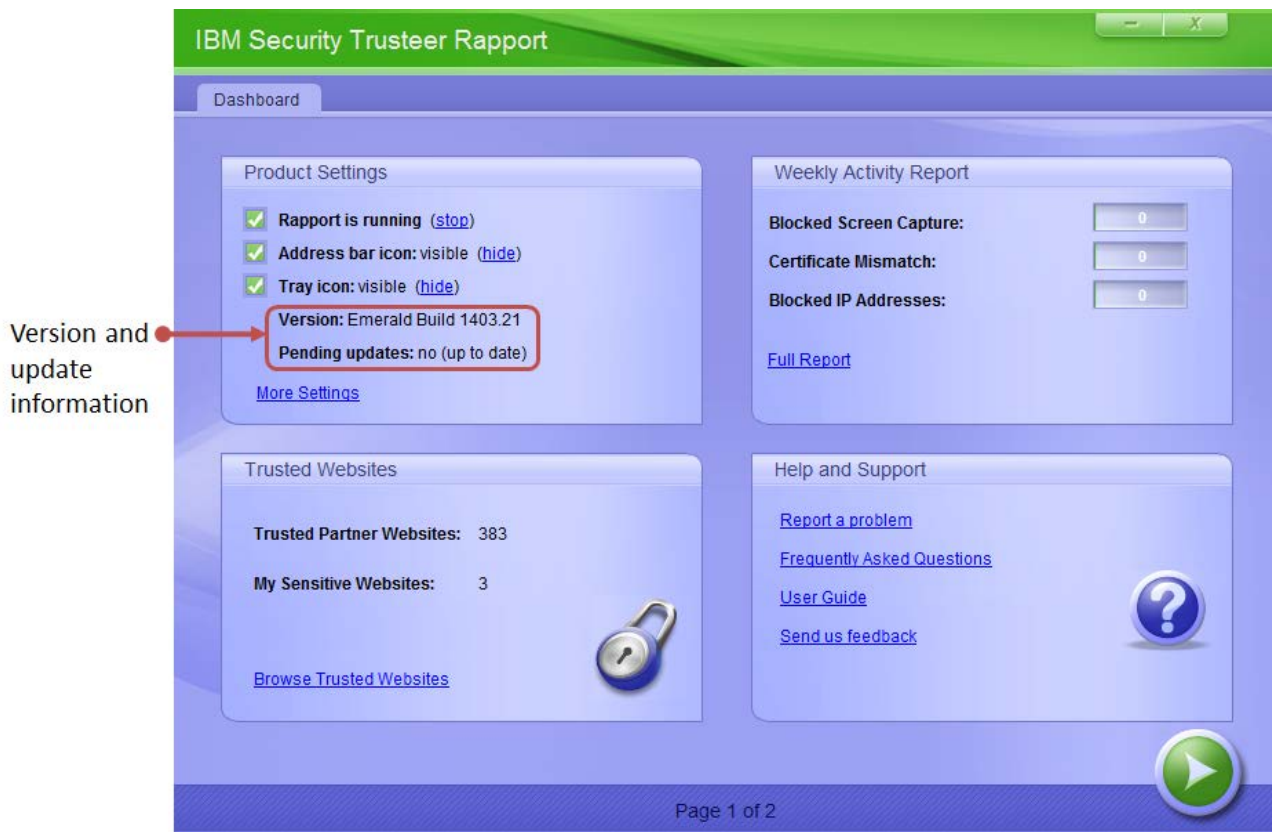
- Rapport detects and downloads an update to be applied on computer restart. The following message appears: "A software update is ready. The configuration is up to date." The **Pending updates** display field changes to "yes (restart PC to apply)".
- Rapport detects and downloads more than one update. Some updates are applied immediately and others will be applied on computer restart. The following message appears: "A software update is ready. The configuration was updated." The number in the **Configuration file** display field is incremented. The **Pending updates** display field changes to "yes (restart PC to apply)".

Disabling Automatic Updates

By default, Rapport updates itself automatically. The updates occur independently and silently. Regular updates are essential to the effectiveness of Rapport. You can disable automatic updates, but you will not receive any updates to Rapport if updates are disabled.

➔ To disable automatic updates:

1. [Open the Rapport Console](#). The Product Settings area is displayed at the upper left of the Dashboard.



2. Click **More Settings**. The Product Settings tab appears.
3. Clear the **Automatic software updates** check box. The User Approval tab appears. The screen shows you an image of some characters for you to type. This is done to prevent malware from accessing the console and effectively disabling Rapport.
4. Enter the characters that you see in the image.
5. Click **OK**. Automatic updates are now disabled. While automatic updates are disabled, Rapport is not updated unless you manually update it. See [Manually Updating Rapport](#).

15. Uninstalling Rapport

We strongly recommend that you do not uninstall Rapport. If you are experiencing difficulties with Rapport, submit a support request at <http://www.trusteer.com/support/submit-ticket>. While a problem is being resolved, you can [stop Rapport](#) without uninstalling.

Rapport supports only one uninstall method to protect Rapport from unauthorized uninstallation.

Note: If Rapport was installed from a Windows administrator account, you can uninstall Rapport only if you are logged in from an administrator account.

[Uninstalling Rapport \(Windows 8 and Windows 7\)](#)

[Uninstalling Rapport \(Windows XP\)](#)

Note: If you encounter difficulty when you uninstall Rapport, and for information about uninstalling Rapport using the safe uninstall utility, see: <http://www.trusteer.com/support/uninstalling-rapport-using-safeuninstall-utility>.

What's this Delete all user settings check box on the uninstall screen?

The **Delete all user settings** check box that appears on the Uninstall IBM Security Trusteer Endpoint Protection dialog box deletes all of the changes you've made to Rapport, including the sites you added and the passwords you chose to protect. If you select this check box and then install Rapport again in the future, Rapport will not remember any of your changes.

Uninstalling Rapport (Windows 8 and Windows 7)

➔ To uninstall Rapport:

1. Open the Control Panel.
2. Under **Programs**, click **Uninstall a program**.
3. In the list of programs, double-click Trusteer Endpoint Protection. A confirmation message appears.

4. Click **Yes**. A Rapport dialog box appears, showing you recent events Rapport successfully prevented.
5. Click **Continue**. Another Rapport dialog box appears, offering you assistance with technical problems you might have had with Rapport. Before you continue with the uninstall, close any files and applications you have open.
6. Click **No Thanks, Uninstall Now**. Rapport completes the uninstall as requested. When the uninstall is complete, a new browser window opens, asking for your feedback about Rapport and a few basic questions.

Uninstalling Rapport (Windows XP)

➔ To uninstall Rapport:

1. Open the Control Panel.
2. Click **Add/Remove Programs**.
3. Find Trusteer Endpoint Protection in the list of programs, and click the **Change/Remove** button for Trusteer Endpoint Protection. A confirmation message appears.
4. Click **Yes**. A Rapport dialog box appears, showing you recent events Rapport successfully prevented.
5. Click **Continue**. Another Rapport dialog box appears, offering you assistance with technical problems you might have had with Rapport. Before you continue with the uninstall, close any files and applications you have open.
6. Click **No Thanks, Uninstall Now**. Rapport completes the uninstall as requested. When the uninstall is complete, a new browser window opens, asking for your feedback about Rapport and a few basic questions.

16. Upgrading Rapport

To upgrade to a new version of Rapport, install the new version without removing the old version first. The installation process is the same as the regular installation process with some additional steps.

For installation instructions, see [Installing Rapport](#). During the installation process, the following screen appears:



This screen appears because you are installing a new version over an existing version. When you see this screen, select **It works - I just want to update it**. Click **Next** and continue with the installation as usual.

Note: If Rapport was installed from a Windows administrator account, you can install Rapport over an existing version only if you are logged in from an administrator account.

A security confirmation screen appears during the installation process:

This screen appears because the setup wizard needs to shut down the existing version of Rapport to install the new version. The shutdown requires user confirmation so that malware cannot disable Rapport. When you see this screen, enter the characters that you see in the image and click **Shutdown**. The installation continues as usual.

The following text might appear in a message box after the installation:

Trusteer Endpoint Protection was upgraded to a new version. Some new features of Trusteer Endpoint Protection will only be available after a restart.

Your computer is safe, even after this message appears. Nevertheless, it is recommended to restart your computer as soon as possible.