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**

<table>
<thead>
<tr>
<th>Notices</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copyright License</td>
<td>iii</td>
</tr>
<tr>
<td>Trademarks</td>
<td>iii</td>
</tr>
<tr>
<td>Privacy Policy Considerations</td>
<td>iv</td>
</tr>
</tbody>
</table>

**1. Front Matter**

<table>
<thead>
<tr>
<th>Front Matter</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About this Guide</td>
<td>1</td>
</tr>
<tr>
<td>Need More Information about Rapport?</td>
<td>1</td>
</tr>
<tr>
<td>Sending us Feedback</td>
<td>1</td>
</tr>
<tr>
<td>Support Information</td>
<td>2</td>
</tr>
<tr>
<td>Accessibility</td>
<td>2</td>
</tr>
<tr>
<td>Statement of Good Security Practices</td>
<td>3</td>
</tr>
</tbody>
</table>

**2. What is Rapport?**

<table>
<thead>
<tr>
<th>What is Rapport?</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antivirus: A False Sense of Security</td>
<td>5</td>
</tr>
<tr>
<td>Signature Detection Doesn’t Work</td>
<td>5</td>
</tr>
<tr>
<td>The Rapport Approach</td>
<td>6</td>
</tr>
<tr>
<td>Extra Layer of Protection</td>
<td>6</td>
</tr>
<tr>
<td>How Rapport Protects You</td>
<td>6</td>
</tr>
<tr>
<td>Proven Technology from IBM</td>
<td>7</td>
</tr>
<tr>
<td>The User Experience</td>
<td>7</td>
</tr>
<tr>
<td>Getting More Out of Rapport</td>
<td>8</td>
</tr>
</tbody>
</table>

**3. Installing Rapport**

<table>
<thead>
<tr>
<th>Installing Rapport</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>9</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Stopping Rapport</td>
<td>45</td>
</tr>
<tr>
<td>Starting Rapport</td>
<td>47</td>
</tr>
<tr>
<td>Getting Support</td>
<td>47</td>
</tr>
<tr>
<td>Unblocking Legitimate Browser Add-ons</td>
<td>48</td>
</tr>
<tr>
<td>Disabling Keylogger Blocking</td>
<td>50</td>
</tr>
<tr>
<td>Undoing Accidental Authorizations</td>
<td>53</td>
</tr>
<tr>
<td>Clearing Authorized Invalid SSL certificates</td>
<td>53</td>
</tr>
<tr>
<td>Clearing Trusted Sites for Payment Card Submission</td>
<td>56</td>
</tr>
<tr>
<td>Clearing Trusted Sites for Non-Secure Submissions</td>
<td>58</td>
</tr>
<tr>
<td>Clearing Websites to Which You Allowed Sending Login Information</td>
<td>60</td>
</tr>
<tr>
<td>Handling Errors</td>
<td>63</td>
</tr>
<tr>
<td>Handling a Post Install Webpage Error</td>
<td>63</td>
</tr>
<tr>
<td>Handling an Update Error</td>
<td>64</td>
</tr>
<tr>
<td>Handling Rapport Installer Errors</td>
<td>65</td>
</tr>
<tr>
<td>Handling Uninstall Errors</td>
<td>66</td>
</tr>
<tr>
<td>Configuring a Proxy Server for Automatic Updates</td>
<td>66</td>
</tr>
<tr>
<td>Sending a User Problem Report</td>
<td>69</td>
</tr>
<tr>
<td>Copying the Trusteer Endpoint Protection ID</td>
<td>71</td>
</tr>
<tr>
<td>Sending Rapport Log Files to IBM</td>
<td>72</td>
</tr>
<tr>
<td>Keeping Rapport Updated</td>
<td>73</td>
</tr>
<tr>
<td>Checking the Status of Rapport Updates</td>
<td>73</td>
</tr>
<tr>
<td>Manually Updating Rapport</td>
<td>75</td>
</tr>
<tr>
<td>Disabling Automatic Updates</td>
<td>77</td>
</tr>
</tbody>
</table>
10. Uninstalling Rapport

   Uninstalling Rapport (Windows 8 and Windows 7)

   Uninstalling Rapport (Windows XP)

11. Upgrading Rapport
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](http://www.trusteer.com/support/faq).

On the FAQ web page, type your question into the Instant Answers tool to get answers to additional questions you may have:

Get Instant Answers:

*Type your question here and navigate below to access the answer*

Sending us Feedback

IBM values your feedback.

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

To send feedback about Rapport, please visit:

Suggest new topics or improvements and express your opinion about this User Guide.

To send feedback about the User Guide:

Click the Submit Feedback button at the top of the Rapport User Guide page. This button opens the Product Feedback page on which you can send us your feedback.

Support Information

For support information, refer to our Support website:

http://www.trusteecom/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 online banking communication from being stolen by criminals. Rapport is highly recommended and offered by your bank as an additional layer of security to any antivirus or security software you already use. By protecting your Internet connection and creating a tunnel for safe communication with your bank’s website, Rapport blocks malicious attempts to steal money from your account.

For a short introductory video about Rapport visit:
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 and is capable of detecting, alerting and preventing even the most sophisticated financial attacks.

Rapport is provided free of charge to you to protect your online banking sessions and additional non-enterprise related websites (e.g., 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 actually the computer used to bank with. Criminals use two sophisticated attacks to access online accounts via the computer:

- **Malicious software (or malware)** - automatically and silently downloaded onto the computer when browsing the Internet, malware silently captures
login information and transfers it to criminals as login is performed and can also silently change transactions executed.

- **Phishing** - criminals build fake websites that look very similar to your bank’s website to lure you into visiting 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 may 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 your device and mitigates financial malware infections. IBM also communicates with your bank, allowing the bank 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 your bank has chosen to partner with IBM to offer you 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.

How Rapport Protects You

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

**Proven Technology from IBM**

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

**The User Experience**

Rapport is extremely easy to use. You do not need any technical knowledge to use Rapport. Rapport does not require configuration, does not change the way 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 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 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](#).

Rapport can also generate reports on attempts made to break into your online bank account.
3. Installing Rapport

Installing Rapport is quick and easy. You just 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 using other web browsers, see the following webpage: [http://www.trusteer.com/support/win-install-instructions](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 overinstall 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, and because drivers cannot be installed when installing 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 may:

- 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 on-line 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](http://www.trusteer.com/supported-platforms).
Why am I being told that Rapport already exists on my computer?

If a version of Rapport already 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, this means that there is already an installation of Rapport on your computer. Reinstalling Rapport is perfectly safe (as long as 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. This is done to prevent malware from disabling Rapport.

3. Enter the characters 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. This screen may appear after the installation:

![Restart to Complete Upgrade](image)

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)](http://www.trusteer.com/support/win-install-instructions).

**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:

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 displaying a Download Now button. For example:

![Download screen](image)

2. Click Download Now. The information bar appears at the bottom of the browser window asking if you want to run or save the RapportSetup.exe file.

![Information bar](image)
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?"

![User Account Control dialog box](image)

4. Click **Yes**. The following dialog box may appear.

![IBM Security Trusteer Endpoint Protection Setup dialog box](image)

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

Click **Install**. The following 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.

5. Enter the password and click **Yes** to continue. The following dialog box appears.
6. Click **OK**. Rapport downloads.

The Trusteer Endpoint Protection Installation Wizard appears.

7. 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 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 check **I have a visual impairment, color blindness and/or regularly use assistive screen reading technologies** unless you are installing Rapport on a computer that is needed for use with screen reading software. This setting disables some security features.

8. Click **I accept the terms in the license agreement**.
9. Click **Install**. The installation proceeds. When the installation is finished, the Finish button appears in the wizard.

10. 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, in order to avoid a situation in which one user restarts the system for all users running on the system. For information about disabling restart requests, see IBM Security Trusteer Rapport Virtual Environment Best Practices.

To install Rapport on Windows Server 2003 or 2008:


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, we recommend that you 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. When you have read the document, check the I have read the document 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)

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 you want to switch to.

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

If you are not sure if 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 the **Start** button.
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 the **Start** button.
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 the **Start** button.
2. Click the arrow next to the **Shut Down** button.
3. Click **Switch User**.
4. Press **Ctrl+Alt+Delete**, and then click the user you want to switch to.

---

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

If you are not sure if 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 the **Start** button.
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 the **Start** button.
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 button 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 if 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 the Start button.
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 the Start button.
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.
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 may see a password protection dialog box.

When you browse to a website that is not protected by Rapport, the Rapport icon is gray and when you click the gray Rapport icon, a dropdown dialog box (the Rapport status indicator) tells you that the site is not protected:

You might like to:

- **Protect additional websites** where you login or where you can read or send sensitive information.
- **Open the Rapport Console**. A lot of 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. This includes malware prevention, scanning, and removal. If the icon does not appear and has not been hidden through the Rapport Console, Rapport is not running. Rapport may have been stopped or uninstalled. To start Rapport if it was stopped, select Programs > Trusteer Endpoint Protection > Start Trusteer Endpoint Protection.
5. 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 showing in your browser is protected by Rapport and gray when the website showing in your browser is not protected by Rapport.

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

Rapport enables you to 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.

3. Click OK. The Address bar icon status changes to hidden and a show button 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 ( всегда появляется в вашем системном трее при запуске Rapport.

Figure 1: System Tray Icon
The icon indicates that Rapport's browser-independent protections are working. This includes malware prevention, scanning, and removal. If you want to open the Rapport Console, click the Rapport icon.

Rapport enables you to 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 button 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** dropdown list, select a language, the following message appears.

![Language dropdown message]

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

![Rapport Console in the selected language]
6. 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 caused by malware. Other events may be initiated by malware residing 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 may lead to a data breach. The Activity Report is displayed automatically 12 hours after installing Rapport.

The fact that the Activity Report includes events does not mean that you have malware on your desktop or that you visited fraudulent websites. It does mean that some software or websites which you visited violated the security policy set by your protected website owners or by IBM. For example, you may have software which tried to take a screenshot of your bank statement or software which 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.


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 presented in this report, as it is slightly technical. This information, as mentioned above, does not require any action on your part. You can safely dismiss 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 have an activity report displayed 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.


![Weekly Activity Report](image)
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**.
7. Managing Protected Sites and Passwords

Rapport provides information about which websites and passwords are protected in the Rapport Console and enables you to remove websites and passwords.

There are two categories of protected websites:

- **Trusted Partner Websites.** These are websites 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.

- **Websites you manually added.** These are websites that you added yourself 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 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 Trusteed 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.

   ![Gray Rapport icon](image)

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

   ![YourBankHere](image)
3. In the drop down dialog box, click **Protect this Website**. The Rapport icon on the address bar turns green, indicating that this website is now protected by Rapport.

![Green Rapport icon](https://www.yourbankhere.com/bank/index.php)

**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/faq/supported-platforms](http://www.trusteer.com/support/faq/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 may have for that site. Rapport remembers your choice to protect or not to protect your password on each website and does not offer you again to protect your password when you browse 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 and 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 as well as 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. This is done to prevent malware from accessing the console and effectively disabling Rapport.

4. Enter the characters you see in the image.
5. Click **OK**. The Security Policy screen appears, displaying all the security controls.

6. Scroll down the list of security controls until you find **Warn When Login Information is Used in Unknown Websites**.

7. Click **Warn When Login Information is Used in Unknown Websites**. The protection policy for usernames and passwords on each website is displayed.

8. Uncheck the **Warn if password is used elsewhere** checkbox 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 visit each website.

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


To find out how you can get support, see Getting Support. Find out in the sections below 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. This enables you 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 only stop Rapport if you are logged into 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 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 has stopped running. 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 only start Rapport if you are logged into 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 available 24/7. 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](http://www.trusteer.com/support/submit-ticket) to send us a support request. Please include as much information as you can regarding both the problem and your computer (such as the operating system you use, the browser you use, the behavior you encountered, etc.).

- If you have performance, connectivity, stability, or browser functionality issues, click the "Live Support" link at [http://www.trusteer.com/support](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, please search this guide or use our Instant Answers service on this web page: [http://www.trusteer.com/support/faq](http://www.trusteer.com/support/faq).
Unblocking Legitimate Browser Add-ons

If you have a problem displaying certain web pages correctly in your browser and you think that a legitimate add-on might be blocked, you can check to see if 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. This is done to prevent malware from accessing the console and effectively disabling Rapport.

4. Enter the characters you see in the image.
5. Click **OK**. The Security Policy screen appears, displaying all the security controls.
6. Click **Block Unknown Browser Add-ons**. A list of any blocked add-ons appears. There is an **Always Allow this add-on** checkbox next to the name of each blocked add-on.

7. Check the **Always allow this add-on** checkbox for the blocked add-on that you want to allow.

8. 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 may 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. This is done to prevent malware from accessing the console and effectively disabling Rapport.

4. Enter the characters you see in the image.
5. Click OK. The Security Policy screen appears, displaying all the security controls.

6. From the drop-down list next to **Activate Character Replacement**, select **Never**. This message appears:

   IBM Security Trusteer Endpoint Protection

   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.

   OK

7. Click **OK**.

8. From the drop-down list next to **Activate Kernel Character Replacement**, select **Never**.

9. Click **Save**. A message appears, telling you that your changes will take effect after you restart your computer.
10. Click **OK**.

11. Restart your computer. Rapport's keylogger blocking is disabled.

**Undoing Accidental Authorizations**

Some of Rapport's warnings enable you to authorize websites or certificates that Rapport does not recognize as legitimate. Once 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 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.

---

1 An SSL certificate is a cryptographic digital certificate that validates the identity of a web site 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 it means that a secure connection between your browser and the website has been established using the SSL protocol. However, this does not tell you that the certificate is valid.
To clear authorized invalid SSL certificates:

1. **Open the Rapport Console.**

2. In the dashboard, click 🏛️. The second dashboard screen appears.

   ![Dashboard Screen](image.png)

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. This is done to prevent malware from accessing the console and effectively disabling Rapport.

4. Enter the characters you see in the image.
5. Click **OK**. The Security Policy screen appears, displaying all the security controls.

![Security Policy Screen](image)

6. Click **Validate Website SSL Certificates**. Information about this control appears below it as well as a **clear cache** button.

7. Click **Clear Cache** in the expanded information block. A confirmation box appears.

8. Click **OK**. The cache is cleared.
Clearing Trusted Sites for Payment Card Submission

When Rapport detects that you have entered a protected payment card number into a web page residing 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 enable you to avoid submitting your payment card number 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 ![icon](image). 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. This is done to prevent malware from accessing the console and effectively disabling Rapport.

4. Enter the characters you see in the image.

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

![IBM Security Trusteer Rapport Security Policy](image)

6. Click on the control called **Protect Payment Card Numbers from Theft**. Any sites that you chose to trust are listed in an expanded area. These are sites that you chose to trust by clicking **Ignore, I trust this website** in the payment card submission detection warning dialog box.

7. Either click the **Clear this site** button for each site you want to remove from the list, or click the **Clear all sites** button to remove all trusted sites. A confirmation box appears.

8. Click **OK**.
Clearing Trusted Sites for Non-Secure Submissions

When Rapport detects that you have 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 could 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. This is done to prevent malware from accessing the console and effectively disabling Rapport.

4. Enter the characters you see in the image.

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

6. Click on the control called **Warn when I submit security data to insecure sites**. Any sites that you chose to trust are listed in an expanded area. These are 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.

7. Either click the **Clear this site** button for each site you want to remove from the list, or click the **Clear all sites** button to remove all trusted sites. A confirmation box appears.

8. 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 you have 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. This does not undo any password submissions that have already occurred but it does reset the unknown status of websites that you may have 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. This is done to prevent malware from accessing the console and effectively disabling Rapport.

4. Enter the characters you see in the image.
5. Click **OK**. The Security Policy screen appears, displaying all the security controls.

6. Scroll down to **Warn When Login Information is Used in Unknown Websites** and click on this control name. Information about this control appears below it as well as a **clear cache** button.

7. Click **Clear Cache** in the expanded information block. A confirmation box appears.

8. 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 a Post Install Webpage Error

This is an example of a post install webpage error:

IBM Security Trusteer Endpoint Protection -- Your Attention is Needed

Trusteer Endpoint Protection was unable to open a post install webpage. To check if this indicates an issue with the installation, please open a new browser window and ensure that you can access the internet (for example a website such as google.com) from it.

If you can access the internet, please ignore this message and click here to close this window.

If you cannot access the internet, please click here to stop Trusteer Endpoint Protection and contact IBM Security Trusteer Support at http://www.trusteecom/support for help on resolving this issue.

If you still cannot access the internet after stopping Trusteer Endpoint Protection, please restart your computer and try again. Please contact Trusteer Support for help on restoring Trusteer Endpoint Protection's protection for your computer.

Close

This error appears after an installation of Rapport if Rapport cannot launch your default browser to run a short compatibility test.

If you see this alert, restart your computer and then check that you are able to go online using your web browser. If you are unable to go online using your web browser, stop Rapport, and then contact IBM at:

http://www.trusteecom/support.
Handling an Update Error

This is an example of a Rapport update error:

This error occurs if Rapport was unable to connect to the Internet to check for updates. This is because you connect to the internet via a proxy and Rapport was unable to detect that the proxy details automatically. The dialog box enables you to configure your proxy server so that Rapport can connect to the Internet and obtain updates.

**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 used to connect to your proxy server.

4. If your proxy server requires authentication, enter the username in the **Proxy username** field and the password in the **Proxy password** field.

5. Click **Apply Settings**.

6. Click **Check Connection** to check that Rapport can connect to the Internet, now that you have configured 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 is usually due to firewalls blocking 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](http://www.trusteer.com/support/install-troubleshooting).

Another example of a Rapport installer error is shown below:

![IBM Security Trusteer Endpoint Protection Installer](image)

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:


**Note:** If you do not find the instructions on the website helpful, please contact IBM Trusteer Support at [http://www.trusteer.com/support/submit-ticket](http://www.trusteer.com/support/submit-ticket).

### Handling Uninstall Errors

This is an example of an error that can occur during the uninstall process:

This dialog box 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 our Safe Uninstall utility which enables you to uninstall Rapport from the following website: [http://www.trusteer.com/support/uninstall-troubleshooting](http://www.trusteer.com/support/uninstall-troubleshooting).

**Note:** If you do not find the instructions on the website helpful, please submit a request for support at: [http://www.trusteer.com/support/submit-ticket](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 used to connect to your proxy server.

6. If your proxy server requires authentication, enter the username in the Proxy username field and the password in the Proxy password field.

7. Click Apply Settings.

8. Click Check Connection to check that Rapport can connect to the internet, now that you have configured 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 may 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.

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 bottom right of your screen while Rapport sends your problem report.
When the report is sent, a message appears to confirm that the report was sent.

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

**Copying the Trusteer Endpoint Protection ID**

When you contact IBM Trusteer Support, you may 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.

![Rapport Console Dashboard](image-url)
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](http://www.trusteer.com/support/gathering-rapport-logs).
9. 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 if you so wish.

Checking the Status of Rapport Updates

Information 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 top left of the Dashboard.
The **Pending updates** display field tells 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 system reboot before it will be applied.

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

![IBM Security Trusteer Rapport](image)

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. IBM recommends to 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 top left of the Dashboard.
2. Click **More Settings**. The Product Settings tab appears.

![IBM Security Trusteer Rapport](image)

3. Click **check for updates now**. Rapport checks for updates. While checking for updates, the progress is indicated by text that appears beneath the display fields. One of the following happens:

- Rapport does not detect any pending updates. The following message appears: "You are already running the latest Rapport configuration."

- Rapport detects and downloads 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. IBM does not recommend disabling automatic updates.

To disable automatic updates:

1. Open the Rapport Console. The Product Settings area is displayed at the top left of the Dashboard.
2. Click **More Settings**. The Product Settings tab appears.
3. Uncheck **Automatic software updates**. 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 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**.
10. Uninstalling Rapport

We strongly recommend that you do not uninstall Rapport. If you are experiencing difficulties with Rapport, we recommend you 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. This is 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 into an administrator account.

**Uninstalling Rapport (Windows 8 and Windows 7)**

**Uninstalling Rapport (Windows XP)**

**Note:** In case of difficulty uninstalling 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 checkbox on the uninstall screen?

The **Delete all user settings** checkbox that appears in the screen below deletes all of the changes you've made to Rapport, including the sites you added and the passwords you chose to protect. If you check this 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 may have had with Rapport. Before continuing with the uninstall, close any files and applications you may have open.

6. Click **No Thanks, Uninstall Now**. Rapport completes the uninstall as requested. Once 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 may have had with Rapport. Before continuing with the uninstall, close any files and applications you may have open.

6. Click **No Thanks, Uninstall Now**. Rapport completes the uninstall as requested. Once the uninstall is complete, a new browser window opens, asking for your feedback about Rapport and a few basic questions.
11. 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**. Then click **Next** and continue with the installation as usual.

**Note:** If Rapport was installed from a Windows administrator account, you can only install Rapport over an existing version if you are logged into an administrator account.
The following screen also appears during the installation process:

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

This screen may appear after the installation:

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