MULTILINE

Installation of MultiLine with IBM Security Trusteer and the IBM Security Trusteer User Guide

March 2017

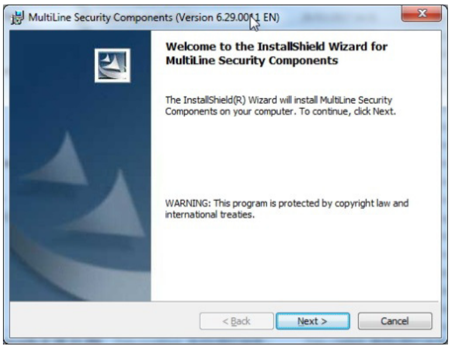
Table of contents

1. MultiLine MSI: installation process

To enable the connection and security of exchanges with MultiLine, it’s mandatory to install an applicative layer in charge of security and access to LuxTrust functionalities, such as Smartcard or USB token authentication, and electronic signature of the transactions.

This implies installing the MultiLine MSI by double-clicking on the uploaded file located on the MultiLine internet site at URL: https://www.multiline.lu,“Uploads” frame on the right side of the screen, link “Software and documentation”

After starting the program, a welcome screen will appear



MultiLine Security Components (Version 6.29.0011 EN)

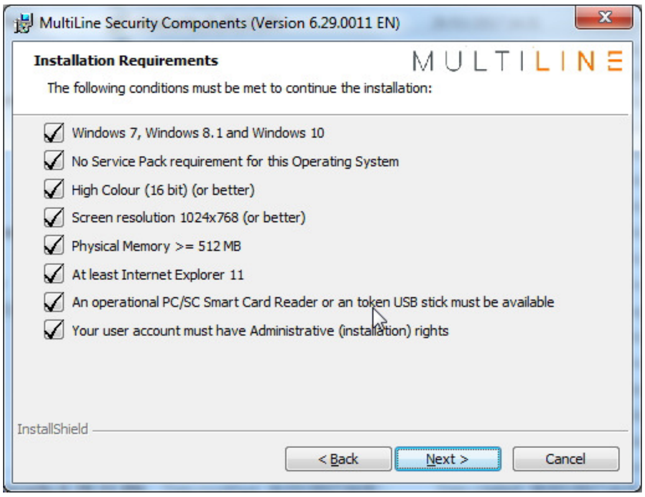
Welcome to the InstallShield Wizard for MultiLine Security Components

The InstallShield(R) Wizard will install MultiLine Security Components on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

After some automatic verification, you will have to click on the “next” button to continue the **installation.**

A screen containing the status of all requirements will appear.



MultiLine Security Components (Version 6.29.0011 EN)

Installation Requirements

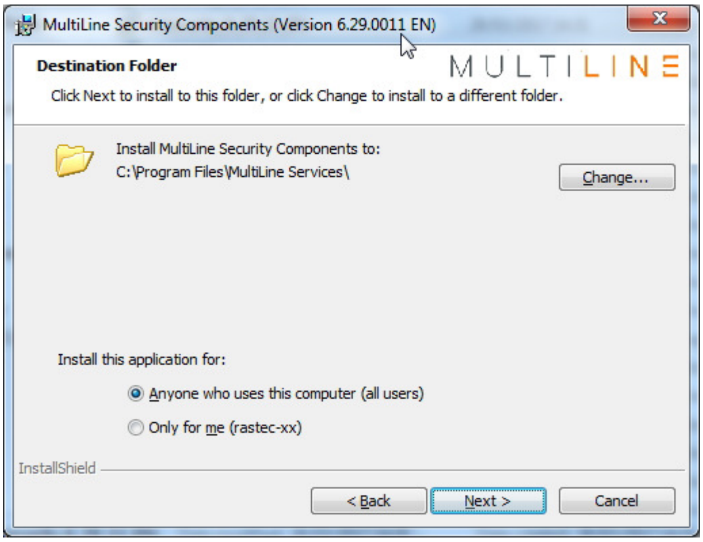
The following conditions must be met to continue the installation:

☑ Windows 7, Windows 8.1 and Windows 10
☑ No Service Pack requirement for this Operating System
☑ High Colour (16 bit) (or better)
☑ Screen resolution 1024x768 (or better)
☑ Physical Memory >= 512 MB
☑ At least Internet Explorer 11
☑ An operational PC/SC Smart Card Reader or an token USB stick must be available
☑ Your user account must have Administrative (installation) rights

In case of a failed requirement, a red cross will appear in the corresponding checkbox. You have to correct all the reported errors and restart the setup application (.msi) to allow continuation of the installation process.

When all the requirements are met, you'll have the possibility to click on the "next" button to continue the installation.

The next screen shown below will allow you to change the destination folder of the installed application files (this option is not recommended). You can also choose to make the installed application available to you only or to all of the PC's users. The default is to install the application for all users and is the recommended option.



MultiLine Security Components (Version 6.29.0011 EN)

Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

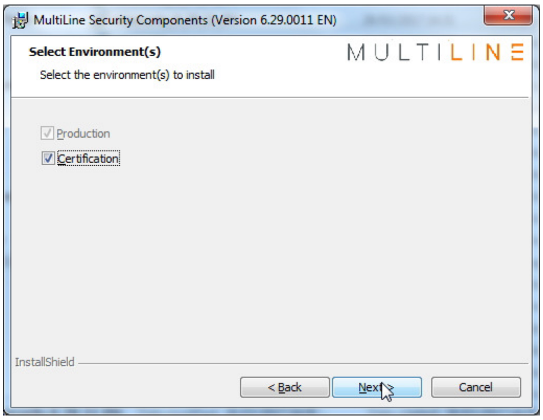
Install MultiLine Security Components to:
C:\Program Files\MultiLine Services\

Install this application for:

● Anyone who uses this computer (all users)

○ Only for me (rastec-xx)

On the next screen, you can, if the option is available, choose the installed environments to access MultiLine. The default, and only required option, is to install the Production environment. Click on the “next” button to continue.



MultiLine Security Components (Version 6.29.0011 EN)

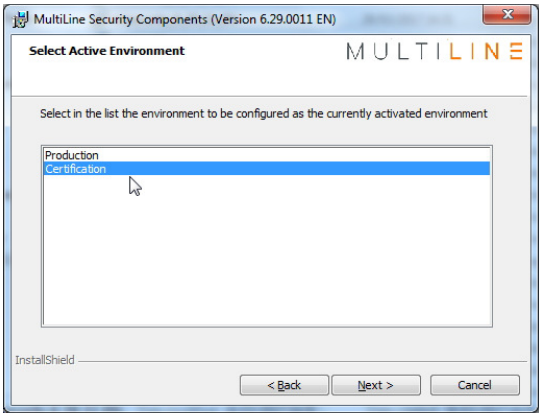
Select Environment(s)

Select the environment(s) to install

☑ Production

☑ Certification

In case a certification environment is proposed and has been selected on the previous screen, you will have to choose which one is active by default. A normal operation will not go to this screen as Production is normally the only choice.



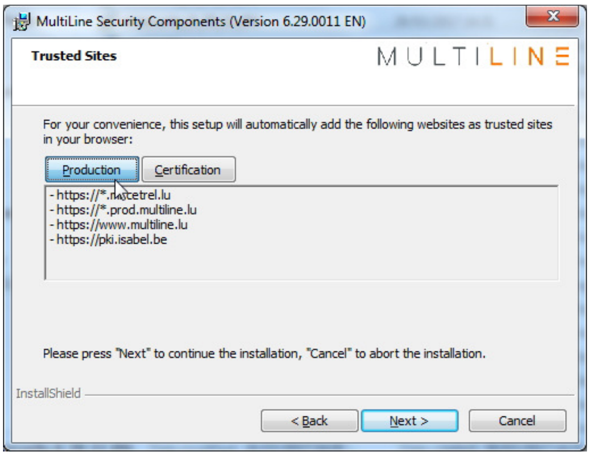
MultiLine Security Components (Version 6.29.0011 EN)

Select Active Environment

Select in the list the environment to be configured as the currently activated environment

Production
Certification

The screen will then show you the trusted sites that will be automatically added to your browser configuration (Internet Explorer). As for the environment, only Production values are shown in normal operation.



MultiLine Security Components (Version 6.29.0011 EN)

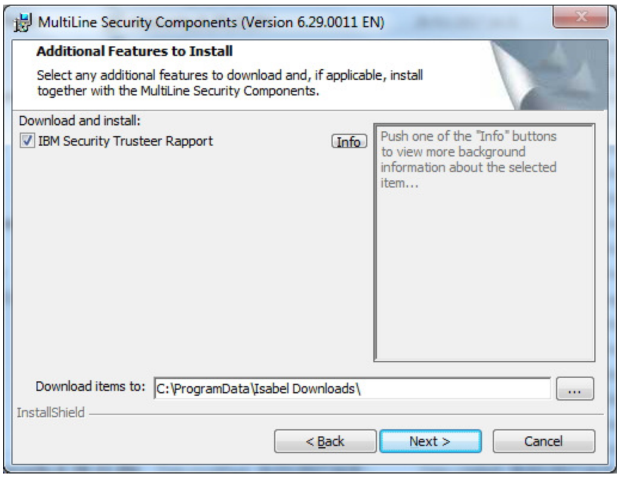
Trusted Sites

For your convenience, this setup will automatically add the following websites as trusted sites in your browser:

- https://*.n[illegible]cetrel.lu
- https://*.prod.multiline.lu
- https://www.multiline.lu
- https://pki.isabel.be

Please press "Next" to continue the installation, "Cancel" to abort the installation.

On the next screen, you will have to choose to install additional services if any exist. This will be the case for IBM Security Trusteer which adds more security when you access MultiLine.



MultiLine Security Components (Version 6.29.0011 EN)

Additional Features to Install

Select any additional features to download and, if applicable, install together with the MultiLine Security Components.

Download and install:

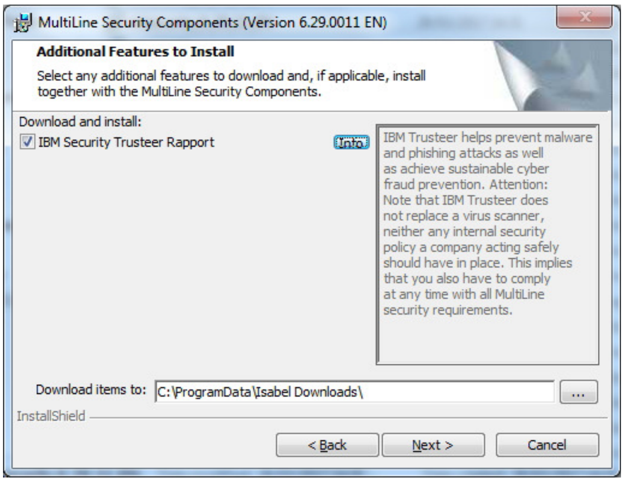
☑ IBM Security Trusteer Rapport

Push one of the "Info" buttons to view more background information about the selected item...

Download items to: C:\ProgramData\Isabel Downloads\

The optional services will be installed later if the checkbox beside of the service name is selected. By default, IBM Security Trusteer is selected and will be installed.

Clicking on the “Info” button will give you information about the selected product’s functions:



MultiLine Security Components (Version 6.29.0011 EN)

Additional Features to Install

Select any additional features to download and, if applicable, install together with the MultiLine Security Components.

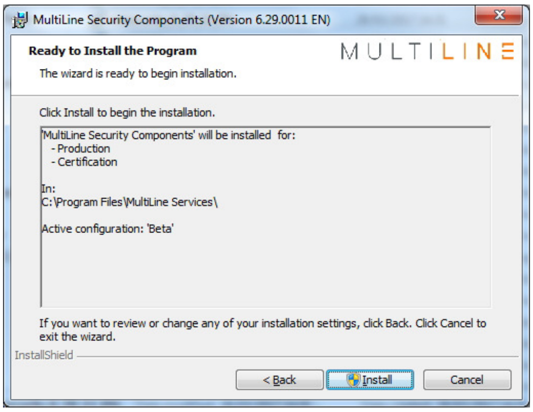
Download and install:

☑ IBM Security Trusteer Rapport

IBM Trusteer helps prevent malware and phishing attacks as well as achieve sustainable cyber fraud prevention. Attention: Note that IBM Trusteer does not replace a virus scanner, neither any internal security policy a company acting safely should have in place. This implies that you also have to comply at any time with all MultiLine security requirements.

Download items to: C:\ProgramData\Isabel Downloads\

The next screen gives a summary of the installation setting you have previously chosen.



MultiLine Security Components (Version 6.29.0011 EN)

Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

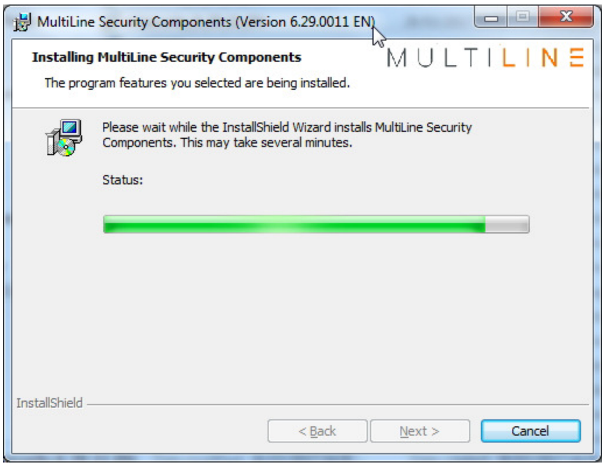
'MultiLine Security Components' will be installed for:
- Production
- Certification

In:
C:\Program Files\MultiLine Services\

Active configuration: 'Beta'

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

/!\ After clicking on the "Install" button, you will obtain a screen requesting the authorization to modify the system and the access to the Administrator rights. In this case, you have to accept the authorization request to continue the installation which will then give you the progress status.



MultiLine Security Components (Version 6.29.0011 EN)

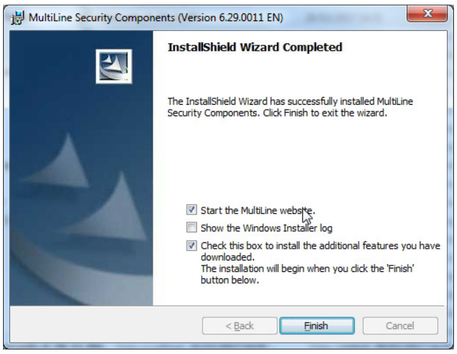
Installing MultiLine Security Components

The program features you selected are being installed.

Please wait while the InstallShield Wizard installs MultiLine Security Components. This may take several minutes.

Status:

At the end of the MultiLine MSI installation, you will be able to confirm the upload and installation of the optional components (i.e. Trusteer) you previously selected.



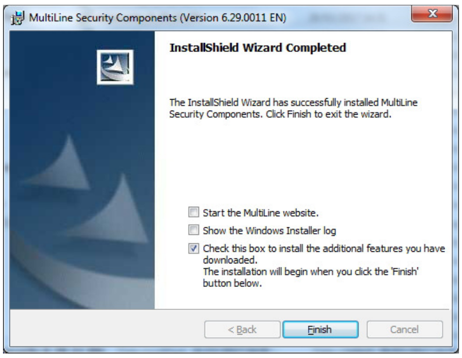
MultiLine Security Components (Version 6.29.0011 EN)

InstallShield Wizard Completed

The InstallShield Wizard has successfully installed MultiLine Security Components. Click Finish to exit the wizard.

☑ Start the MultiLine website.
☐ Show the Windows Installer log
☑ Check this box to install the additional features you have downloaded.
The installation will begin when you click the 'Finish' button below.

For Trusteer, and as the installation process needs to update Internet Explorer functionalities, you need to uncheck the "Start the MultiLine website" checkbox and keep the third one checked. It's also recommended that any Internet Explorer Browser functions running be interrupted before clicking on the "Finish" button.



MultiLine Security Components (Version 6.29.0011 EN)

InstallShield Wizard Completed

The InstallShield Wizard has successfully installed MultiLine Security Components. Click Finish to exit the wizard.

☐ Start the MultiLine website.
☐ Show the Windows Installer log
☑ Check this box to install the additional features you have downloaded.
The installation will begin when you click the 'Finish' button below.

Clicking on the "Finish" button when the third checkbox is checked will start the download of the IBM Security Trusteer installation files or of any other optional service you requested. Once the software is downloaded, its installation will be automatically launched.

You'll find hereunder the detail of the Trusteer installation process.

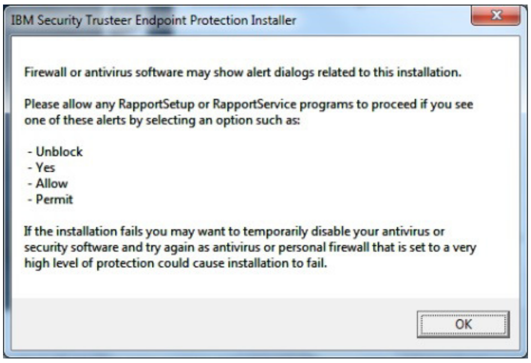
2. IBM Security Trusteer: installation process

/!\ You need to be connected to the Internet for the IBM Security Trusteer installation process. To allow the download and installation of the software, you need to have access to the following URLs:

- *https://www.multiline.lu/fileadmin/media/downloads/FR/info2.txt*
- *https://www.multiline.lu/fileadmin/media/downloads/RapportSetup.exe*

In case these accesses are not possible, you'll be invited to download IBM Security Trusteer directly from the IBM website during the setup process.

After the launch of the setup, a message will inform you about possible configuration changes to make to your Firewall and/or anti-virus software. In case of a problem, you can temporarily deactivate your anti-virus software.



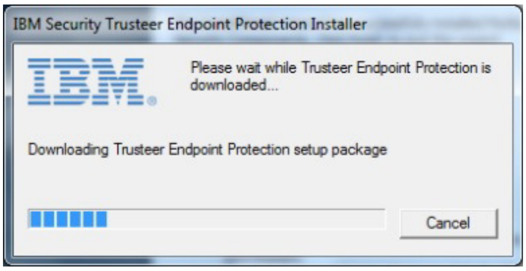
Firewall or antivirus software may show alert dialogs related to this installation.

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.

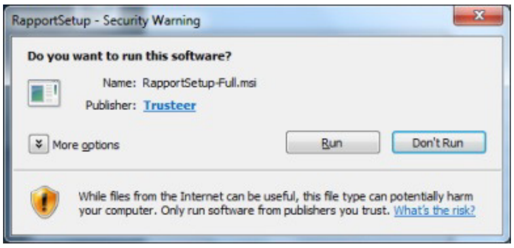
After validation of the message, the IBM Security Trusteer download will start.



Please wait while Trusteer Endpoint Protection is downloaded...

Downloading Trusteer Endpoint Protection setup package

After the download, you'll have to confirm that you want to run the application (RapportSetup-Full.msi).

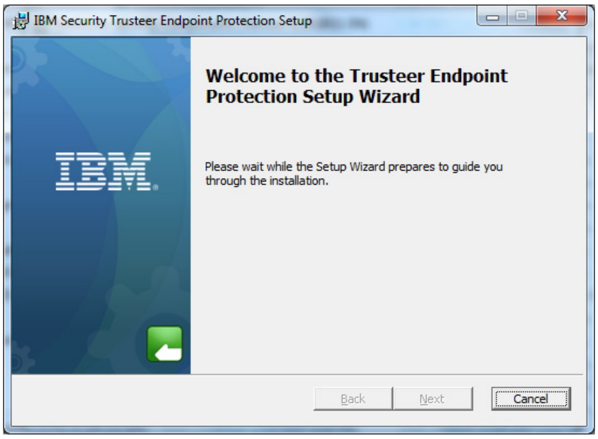


Do you want to run this software?

Name: RapportSetup-Full.msi
Publisher: Trusteer

While files from the Internet can be useful, this file type can potentially harm your computer. Only run software from publishers you trust. What's the risk?

You‘ll see the IBM Security Trusteer Welcome screen

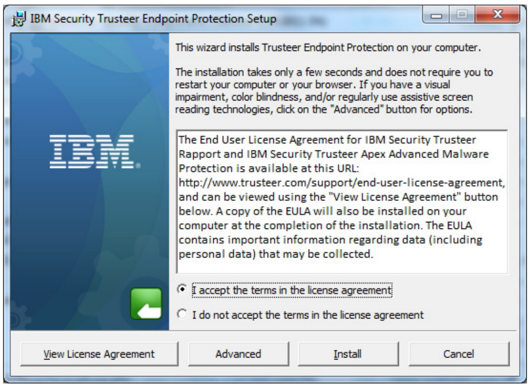


Welcome to the Trusteer Endpoint Protection Setup Wizard

Please wait while the Setup Wizard prepares to guide you through the installation.

The setup process will take a little time to do some system checking before allowing you to click on the “Next” button to continue the setup process. When available, click on the “Next” button to continue.

You then have to accept the End User License Agreement to continue the setup.



This wizard installs Trusteer Endpoint Protection on your computer.

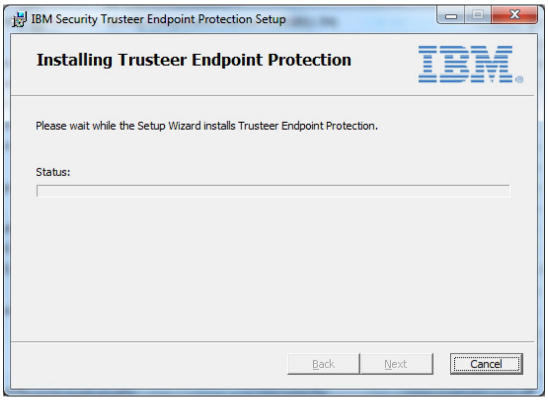
The installation takes only a few seconds and does not require you to restart your computer or your browser. If you have a visual impairment, color blindness, and/or regularly use assistive screen reading technologies, click on the "Advanced" button for options.

The End User License Agreement for IBM Security Trusteer Rapport and IBM Security Trusteer Apex Advanced Malware Protection is available at this URL: http://www.trusteer.com/support/end-user-license-agreement, and can be viewed using the "View License Agreement" button below. A copy of the EULA will also be installed on your computer at the completion of the installation. The EULA contains important information regarding data (including personal data) that may be collected.

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

Click on the “Install” button to start the setup process. If needed, you will be asked to allow modification to the system and will switch to Administrator mode during the installation.

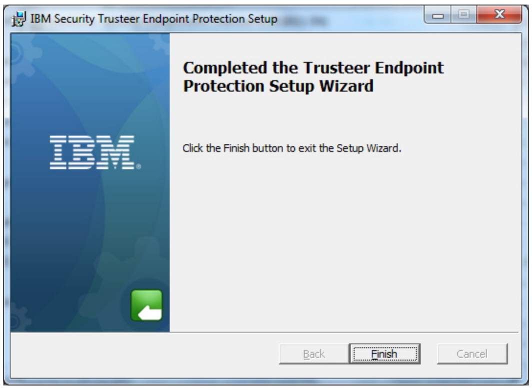


Installing Trusteer Endpoint Protection

Please wait while the Setup Wizard installs Trusteer Endpoint Protection.

Status:

At the end of the installation, you will have to click on the "Finish" button. At this point, IBM Security Trusteer is installed on your system.



Completed the Trusteer Endpoint Protection Setup Wizard

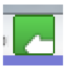
Click the Finish button to exit the Setup Wizard.

/!\ You need to restart your system to fully take into account all of the modifications done by the installation process.

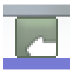
3. IBM Security Trusteer: usage

3.1. Validation of the protected site

After the installation of IBM Security Trusteer and the reboot of the system, the Trusteer icon will be visible in your browser. A green one indicates a site under Trusteer protection and a grey one a site not under Trusteer protection.

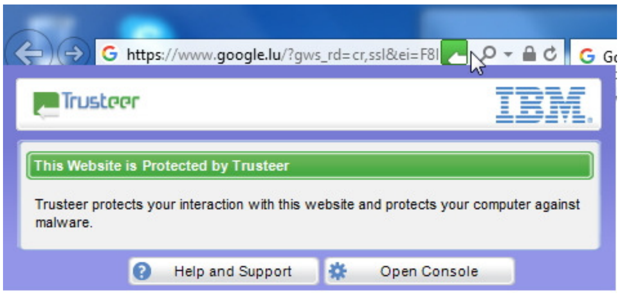


Protected site



Unprotected site

A left click on the icon will pop up a window containing more details and enable access to the Trusteer menu ("Open Console" button).

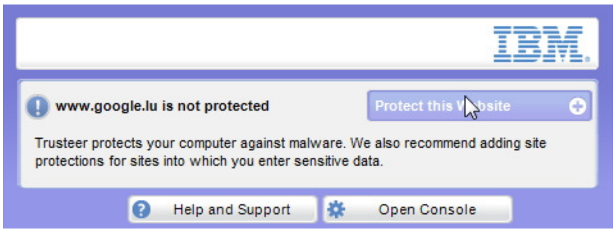


This Website is Protected by Trusteer

Trusteer protects your interaction with this website and protects your computer against malware.

3.2. Add a site to the protected site list

Trusteer uses a predefined list of sites to protect (unmanageable by the user) and a user list of sites to protect (user manageable). When a site is unprotected (Grey Trusteer icon), you have the possibility to add it to Trusteer protection by adding the site to the user protected site list. For this, you have to click on the Trusteer grey icon, then click on the "Protect this site" button. When done, the Trusteer icon will switch to green, informing you that the site is under its protection.



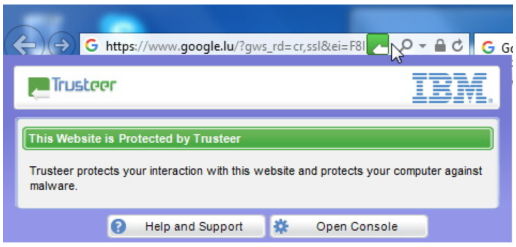
www.google.lu is not protected

Trusteer protects your computer against malware. We also recommend adding site protections for sites into which you enter sensitive data.

3.3. Open the Trusteer console

The Trusteer console can be accessed in multiple ways:

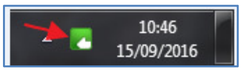
- In the browser:



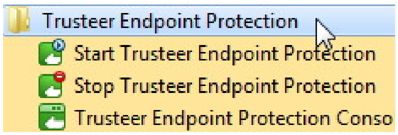
This Website is Protected by Trusteer

Trusteer protects your interaction with this website and protects your computer against malware.

- In the taskbar:

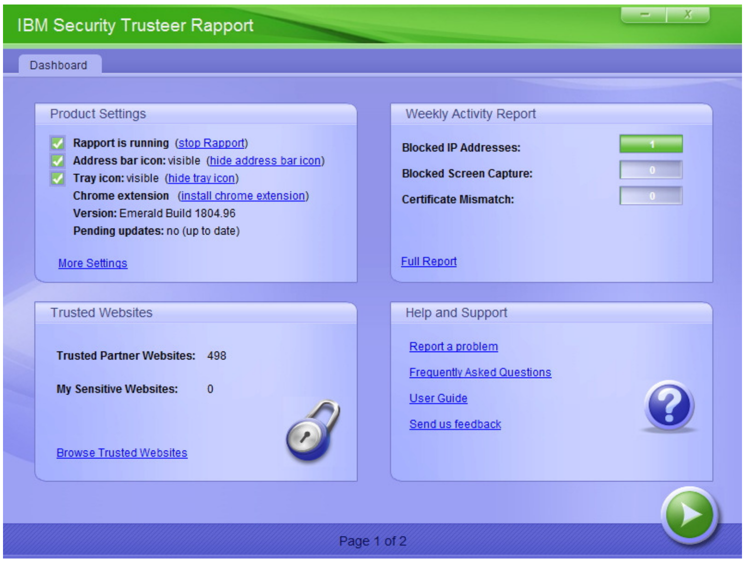


- In the Windows start menu:



Trusteer Endpoint Protection
Start Trusteer Endpoint Protection
Stop Trusteer Endpoint Protection
Trusteer Endpoint Protection Conso

The Trusteer console allows configuration and checking of the activity:



Product Settings

☑ Rapport is running (stop Rapport)
☑ Address bar icon: visible (hide address bar icon)
☑ Tray icon: visible (hide tray icon)
Chrome extension (install chrome extension)
Version: Emerald Build 1804.96
Pending updates: no (up to date)

More Settings

Weekly Activity Report

Blocked IP Addresses: 1
Blocked Screen Capture: 0
Certificate Mismatch: 0

Full Report

Trusted Websites

Trusted Partner Websites: 498
My Sensitive Websites: 0

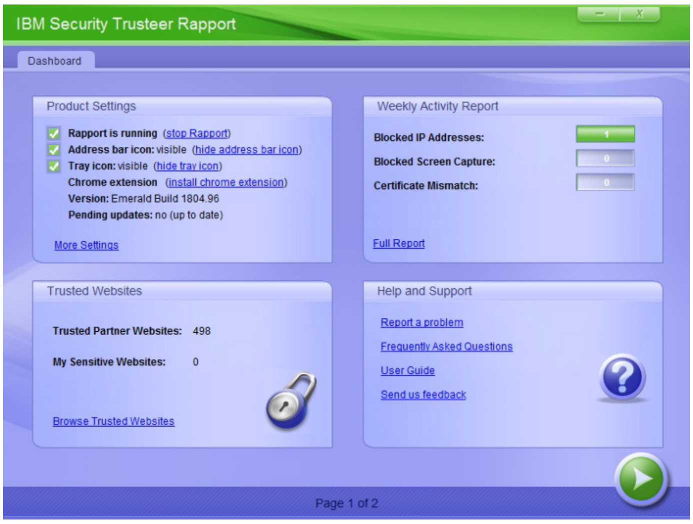
Browse Trusted Websites

Help and Support

Report a problem
Frequently Asked Questions
User Guide
Send us feedback

3.3.1. Trusteer console: configuration options

General Trusteer information and configurations are located on the main console page. More configuration options can be accessed by clicking on the “More Settings” link in the lower part of the upper left frame in the console:



Product Settings

☑ Rapport is running (stop Rapport)
☑ Address bar icon: visible (hide address bar icon)
☑ Tray icon: visible (hide tray icon)
Chrome extension (install chrome extension)
Version: Emerald Build 1804.96
Pending updates: no (up to date)

More Settings

Weekly Activity Report

Blocked IP Addresses: 1
Blocked Screen Capture: 0
Certificate Mismatch: 0

Full Report

Trusted Websites

Trusted Partner Websites: 498
My Sensitive Websites: 0

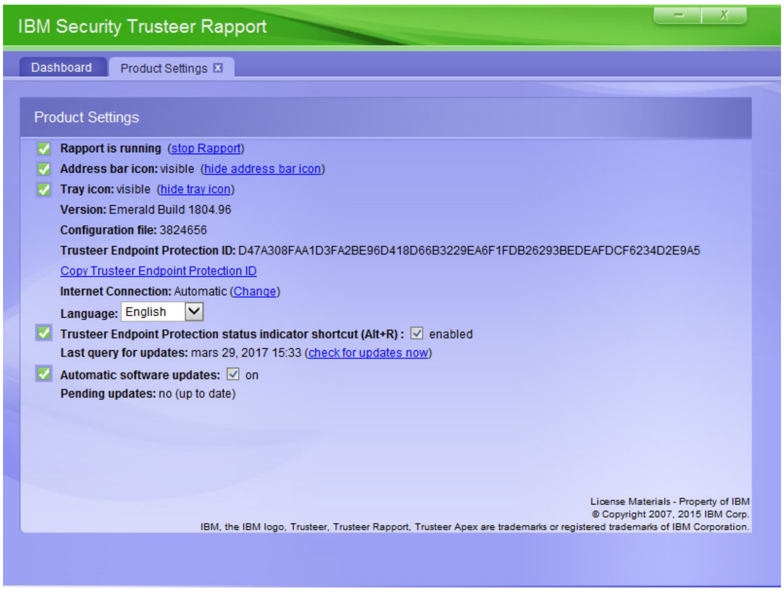
Browse Trusted Websites

Help and Support

Report a problem
Frequently Asked Questions
User Guide
Send us feedback

Page 1 of 2

For example, it’s possible to hide the Trusteer icon in the taskbar, choose the interface language, or the update method.



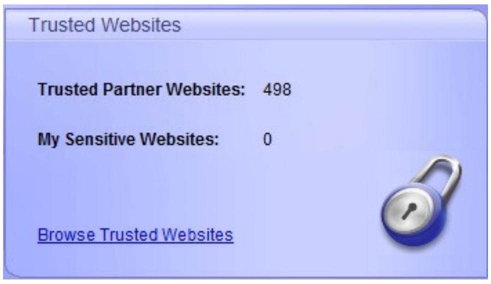
Product Settings

☑ Rapport is running (stop Rapport)
☑ Address bar icon: visible (hide address bar icon)
☑ Tray icon: visible (hide tray icon)
Version: Emerald Build 1804.96
Configuration file: 3824656
Trusteer Endpoint Protection ID: D47A308FAA1D3FA2BE96D418D66B3229EA6F1FDB26293BEDEAFDCF6234D2E9A5
Copy Trusteer Endpoint Protection ID
Internet Connection: Automatic (Change)
Language: English
☑ Trusteer Endpoint Protection status indicator shortcut (Alt+R) : ☑ enabled
Last query for updates: mars 29, 2017 15:33 (check for updates now)
☑ Automatic software updates: ☑ on
Pending updates: no (up to date)

License Materials - Property of IBM
© Copyright 2007, 2015 IBM Corp.
IBM, the IBM logo, Trusteer, Trusteer Rapport, Trusteer Apex are trademarks or registered trademarks of IBM Corporation.

3.3.2. Trusteer console: trusted site list

In the “Trusted site” part, on the lower left frame of the console, you can check the predefined and user list of trusted sites.



Trusted Websites

Trusted Partner Websites: 498

My Sensitive Websites: 0

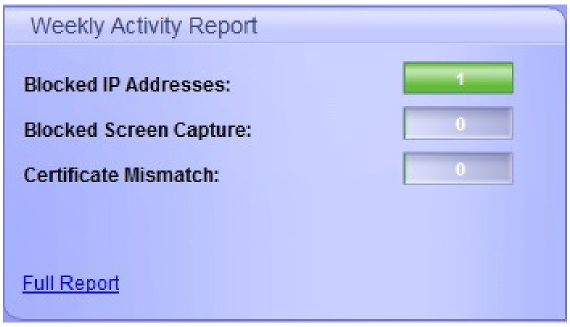
Browse Trusted Websites

You will have the ability to check the predefined sites list (unmanageable by the user) and check or manage the user list (i.e. remove previously manually added sites).

3.3.3. Trusteer console: weekly reporting

The upper right part of the console is dedicated to the weekly reporting of Trusteer activity. The frame contains the three main counters of the application:

- Blocked screenshots.
- Certificate problems encountered.
- Blocked IP addresses.



Weekly Activity Report

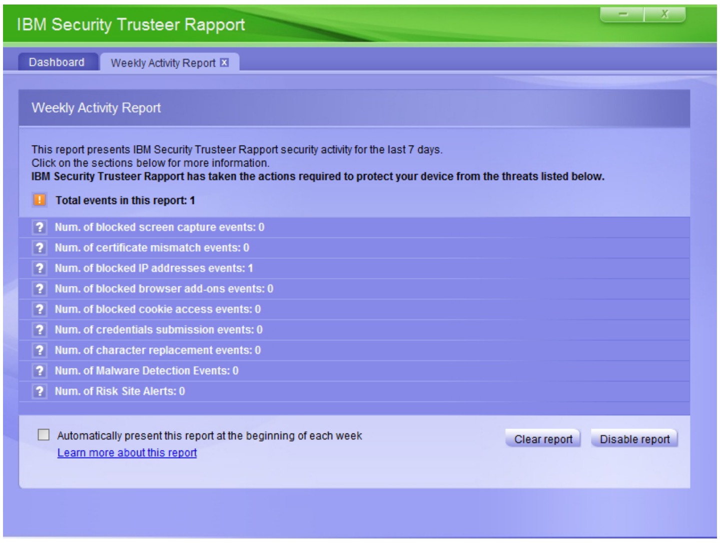
Blocked IP Addresses: 1

Blocked Screen Capture: 0

Certificate Mismatch: 0

Full Report

By clicking on the “Full Report” link on the lower part of this frame, you can access more detailed information about Trusteer activity. You will also have the choice of enabling automatic reporting each week or deactivating reporting (not recommended).



This report presents IBM Security Trusteer Rapport security activity for the last 7 days.
Click on the sections below for more information.
IBM Security Trusteer Rapport has taken the actions required to protect your device from the threats listed below.

Total events in this report: 1

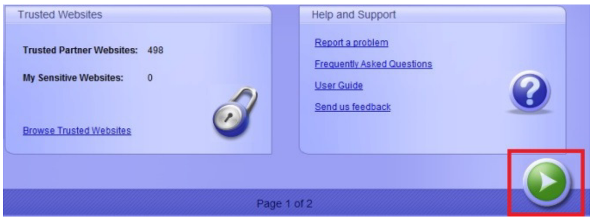
- **Num. of blocked screen capture events: 0**
- **Num. of certificate mismatch events: 0**
- **Num. of blocked IP addresses events: 1**
- **Num. of blocked browser add-ons events: 0**
- **Num. of blocked cookie access events: 0**
- **Num. of credentials submission events: 0**
- **Num. of character replacement events: 0**
- **Num. of Malware Detection Events: 0**
- **Num. of Risk Site Alerts: 0**

□ Automatically present this report at the beginning of each week

/!\ Please be advised to periodically check both reports (general and detailed) to detect possible suspect behavior.

3.3.4. Trusteer console: security policy.

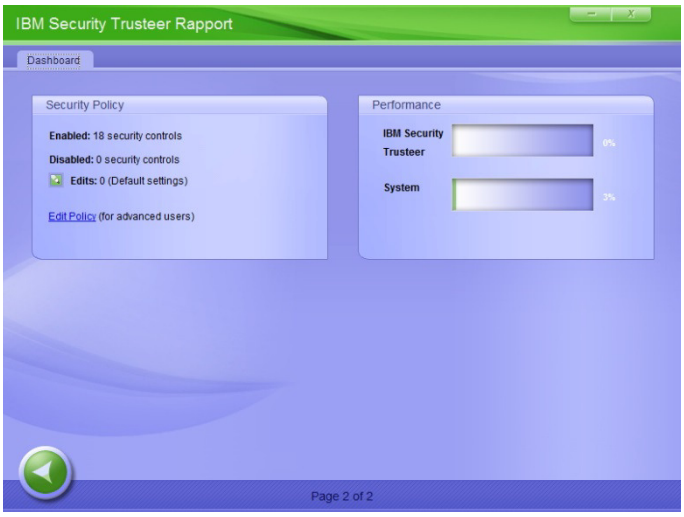
The security policy screen is located on the second screen of the Trusteer console. You access it by clicking the green icon on the lower right part of the first console screen.



Trusted Partner Websites: 498

My Sensitive Websites: 0

This screen will give you some information about the Trusteer application’s security policy (number of activated and deactivated security rules) and allow you to change some of them.



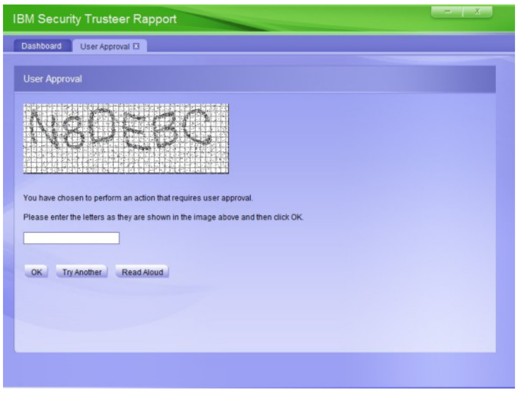
Enabled: 18 security controls

Disabled: 0 security controls

Edits: 0 (Default settings)

Edit Policy (for advanced users)

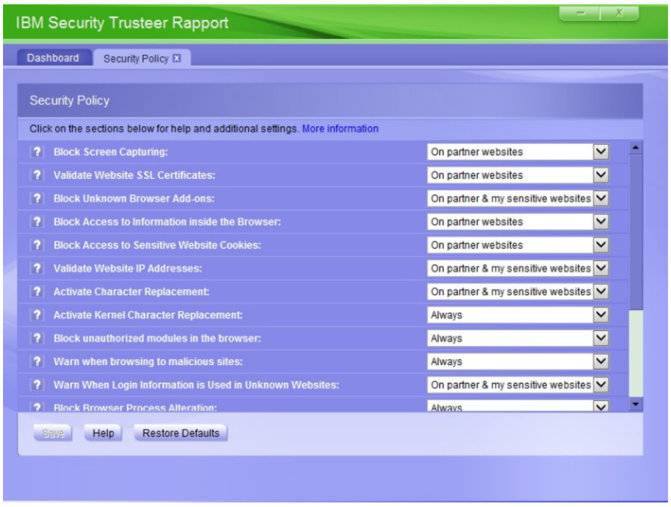
You can access the modification screen by clicking the “Edit Policy” link located on the lower part of the security policy frame and entering the exact captcha you receive from the application.



You have chosen to perform an action that requires user approval.

Please enter the letters as they are shown in the image above and then click OK.

/!\ Modification of the rules is NOT recommended and is done at your own risk. Any security breaches occurring due to security policy modification will be under your sole responsibility.

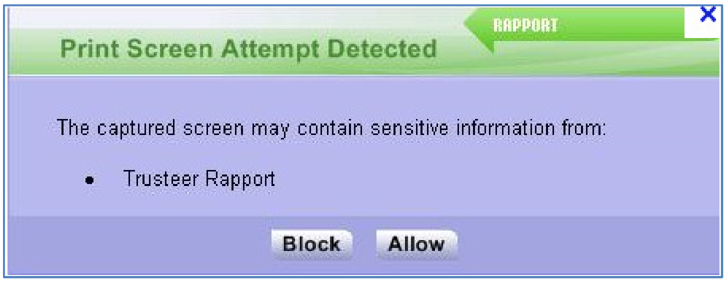


Click on the sections below for help and additional settings. More information

Block Screen Capturing:	On partner websites
Validate Website SSL Certificates:	On partner websites
Block Unknown Browser Add-ons:	On partner & my sensitive websites
Block Access to Information inside the Browser:	On partner websites
Block Access to Sensitive Website Cookies:	On partner websites
Validate Website IP Addresses:	On partner & my sensitive websites
Activate Character Replacement:	On partner & my sensitive websites
Activate Kernel Character Replacement:	Always
Block unauthorized modules in the browser:	Always
Warn when browsing to malicious sites:	Always
Warn When Login Information is Used in Unknown Websites:	On partner & my sensitive websites
Block Browser Process Alteration:	Always

3.4. IBM Security Trusteer: blocking message

When you navigate a Trusteer protected site (either from the Trusteer default list or the user added one), some actions like taking a screenshot of the internet protected site or remote access to your computer will give you Trusteer popup alert messages.



Print Screen Attempt Detected

The captured screen may contain sensitive information from:

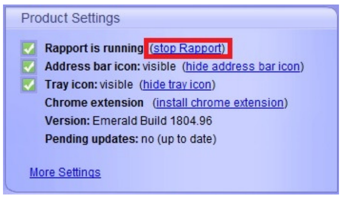
- Trusteer Rapport

If such a message appears, you have to accept or block the action regarding the context.

- If the action is not your own, click on the “Block” button to immediately stop the action. /!\ In such a case, be advised to do a complete and full security and virus scan of your computer as your computer can potentially be corrupted by malware and/or viruses. If needed, check for the procedure with your IT department.
- If the action is requested/done by you, you will have to click on the “Accept” button to allow execution of the action.

3.5. IBM Security Trusteer: deactivation

If needed, IBM Security Trusteer can be temporarily deactivated. This can be done from the console.

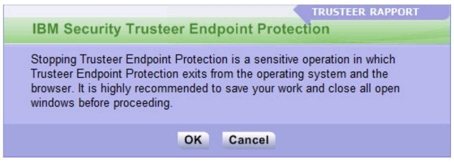


Product Settings

☑ **Rapport is running** (stop Rapport)
☑ **Address bar icon:** visible (hide address bar icon)
☑ **Tray icon:** visible (hide tray icon)
Chrome extension (install chrome extension)
Version: Emerald Build 1804.96
Pending updates: no (up to date)

More Settings

A warning message (to be validated) will show up, then a confirmation message.

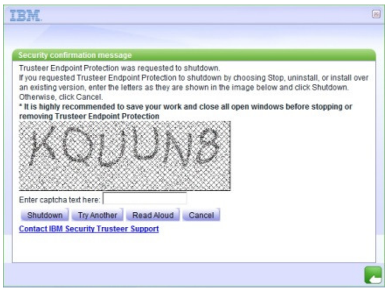


TRUSTEER RAPPORT

IBM Security Trusteer Endpoint Protection

Stopping Trusteer Endpoint Protection is a sensitive operation in which Trusteer Endpoint Protection exits from the operating system and the browser. It is highly recommended to save your work and close all open windows before proceeding.

The confirmation message has to be validated by entering the exact captcha given on the screen, then clicking on the “deactivate” button.



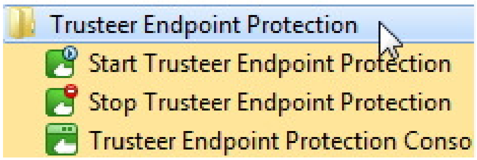
Security confirmation message

Trusteer Endpoint Protection was requested to shutdown.
If you requested Trusteer Endpoint Protection to shutdown by choosing Stop, uninstall, or install over an existing version, enter the letters as they are shown in the image below and click Shutdown. Otherwise, click Cancel.
*** It is highly recommended to save your work and close all open windows before stopping or removing Trusteer Endpoint Protection**

Enter captcha text here:

Trusteer will then be shut down and can be reactivated in the same manner.

Startup and shut down menus can also be found in the Windows Start menu.

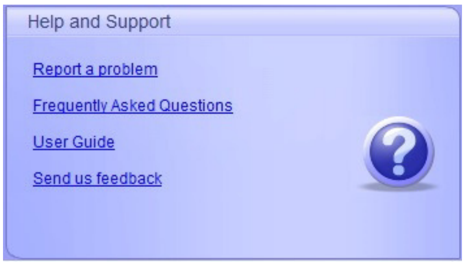


Trusteer Endpoint Protection
Start Trusteer Endpoint Protection
Stop Trusteer Endpoint Protection
Trusteer Endpoint Protection Conso

4. IBM Security Trusteer: more information

In the “Help and assistance” frame on the lower right part of the console screen, you have the option to:

- Inform a Trusteer engineer about a problem,
- Access the FAQ,
- Access the IBM Trusteer version of the User Guide
- Send your feedback about the application to a Trusteer Engineer.



Help and Support

Report a problem

Frequently Asked Questions

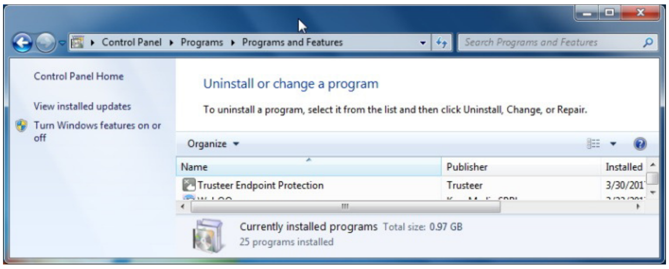
User Guide

Send us feedback

Just click on the corresponding link on the frame and follow the instructions or access the needed pages.

5. IBM Security Trusteer: uninstallation

The IBM Security Trusteer uninstall is done by going through the installed application list in the control panel, then selecting the Trusteer application and clicking on the “Uninstall/Change” menu.


Control Panel ▸ Programs ▸ Programs and Features
Search Programs and Features
Control Panel Home
View installed updates
Turn Windows features on or off
Organize ▾

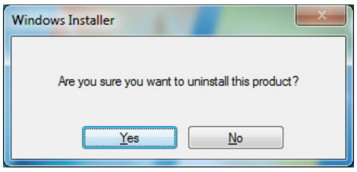
Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Name	Publisher	Installed
Trusteer Endpoint Protection	Trusteer	3/30/201

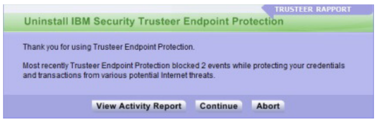
Currently installed programs Total size: 0.97 GB
25 programs installed

You have to confirm the uninstall request.


Windows Installer

Are you sure you want to uninstall this product?

An IBM Security Trusteer informational message about past Trusteer activity will be displayed and has to be accepted to continue, by clicking on the “Continue” button.

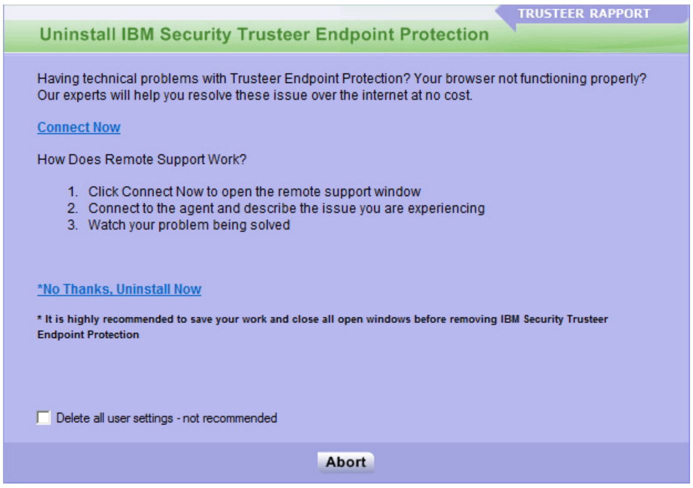


Uninstall IBM Security Trusteer Endpoint Protection

Thank you for using Trusteer Endpoint Protection.

Most recently Trusteer Endpoint Protection blocked 2 events while protecting your credentials and transactions from various potential Internet threats.

On the next screen, you have to select if you want remote help from a Trusteer engineer or just want to uninstall the product. Optionally, you can delete all the user preferences for the software before starting the uninstall.



Uninstall IBM Security Trusteer Endpoint Protection

Having technical problems with Trusteer Endpoint Protection? Your browser not functioning properly? Our experts will help you resolve these issue over the internet at no cost.

Connect Now

How Does Remote Support Work?

1. Click Connect Now to open the remote support window
2. Connect to the agent and describe the issue you are experiencing
3. Watch your problem being solved

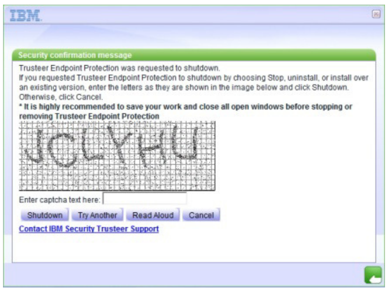
*No Thanks, Uninstall Now

* It is highly recommended to save your work and close all open windows before removing IBM Security Trusteer Endpoint Protection

□ Delete all user settings - not recommended

You have to choose “No Thanks, Uninstall Now” to process the uninstall of the IBM Security Trusteer application.

The confirmation message has to be validated by entering the exact captcha given on the screen, then clicking on the "Shutdown" button.



Security confirmation message

Trusteer Endpoint Protection was requested to shutdown.
If you requested Trusteer Endpoint Protection to shutdown by choosing Stop, uninstall, or install over an existing version, enter the letters as they are shown in the image below and click Shutdown.
Otherwise, click Cancel.
*** It is highly recommended to save your work and close all open windows before stopping or removing Trusteer Endpoint Protection**

Enter captcha text here:

It will just take a few seconds for IBM Security Trusteer to be uninstalled.

/!\ You have to restart your computer to fully remove Trusteer.