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

March 2017
Table of contents
1. MultiLine MSI: installation process ................................................................. 3
2. IBM Security Trusteer: installation process .................................................... 9
3. IBM Security Trusteer: usage ......................................................................... 12
   3.1. Validation of the protected site ............................................................... 12
   3.2. Add a site to the protected site list ......................................................... 12
   3.3. Open the Trusteer console ..................................................................... 13
         3.3.1. Trusteer console: configuration options ...................................... 14
         3.3.2. Trusteer console: trusted site list ................................................. 15
         3.3.3. Trusteer console: weekly reporting .............................................. 15
         3.3.4. Trusteer console: security policy ................................................ 16
   3.4. IBM Security Trusteer: blocking message ............................................. 18
   3.5. IBM Security Trusteer: deactivation ....................................................... 19
4. IBM Security Trusteer: more information ..................................................... 20
5. IBM Security Trusteer: uninstallation ............................................................ 21
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

![Welcome Screen](image1)

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.

![Requirements Screen](image2)
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.
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.

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.

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

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.
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.

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.

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:


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.

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

After the download, you’ll have to confirm that you want to run the application (RapportSetup-Full.msi).
You’ll see the IBM Security Trusteer Welcome screen

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.

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.
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.

/!/\ 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](image1)
![Unprotected site](image2)

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

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.
3.3. **Open the Trusteer console**

The Trusteer console can be accessed in multiple ways:

- **In the browser:**

- **In the taskbar:**

- **In the Windows start menu:**

The Trusteer console allows configuration and checking of the activity:
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:

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

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.
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).

⚠️ 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.
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.

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.

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

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.

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

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

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.
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.

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.

You have to confirm the uninstall request.

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.

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.

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.

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

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