MULTILINE

Installation de MultiLine et d'IBM Security Trusteer et guide d'utilisation d'IBM Security Trusteer

Mars 2017

MULTILINE

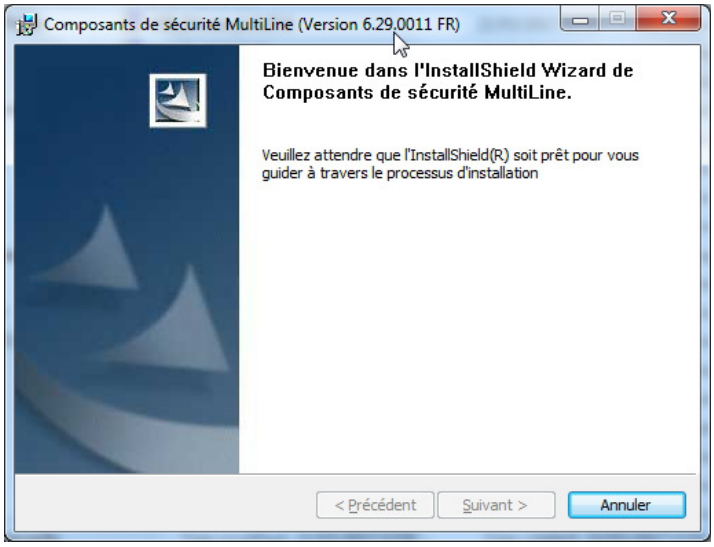
Table des matières

1. Processus d'installation de MSI MultiLine

Pour permettre la connexion et la sécurité des échanges avec MultiLine, il est obligatoire d'installer une couche applicative chargée de la gestion de la sécurité et des accès aux fonctionnalités LuxTrust, par exemple une authentification par Smartcard ou token USB, ainsi que la signature électronique des transactions.

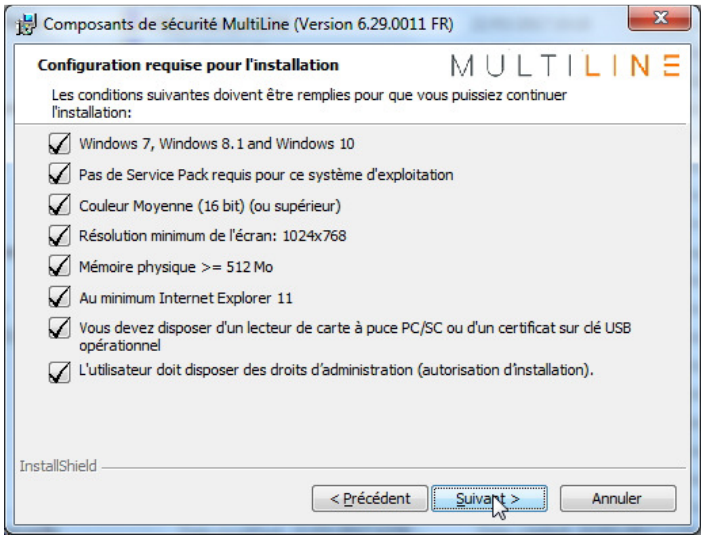
Pour ce faire, vous devez installer le MSI MultiLine en double cliquant sur le fichier téléchargé sur le site MultiLine à l'adresse : https://www.multiline.lu, cadre « Téléchargez » à droite, lien « Logiciels et documentation ».

Une fois le programme lancé, un écran de bienvenue s'affiche.



Lorsque les vérifications automatiques sont terminées, cliquez sur le bouton « Suivant » pour continuer l'**installation.**

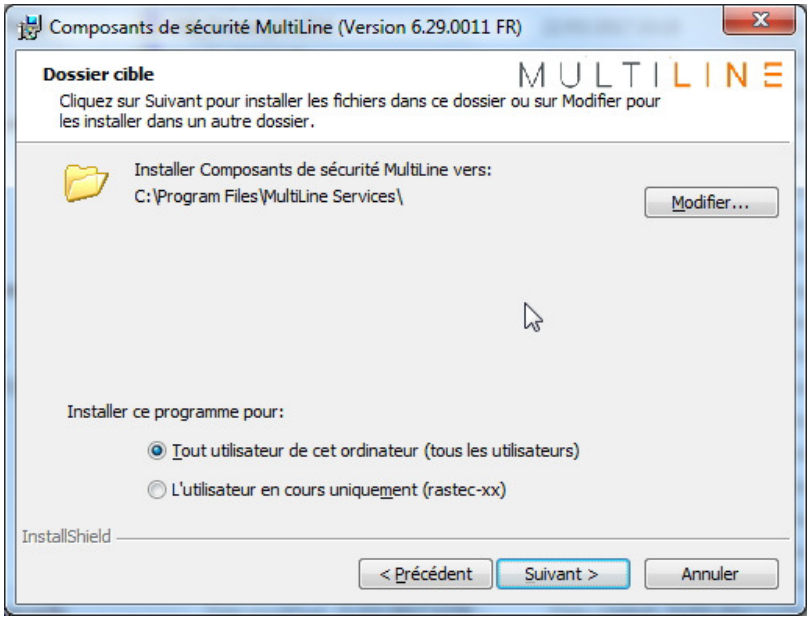
Un écran récapitulant le statut de tous les prérequis s'affiche.



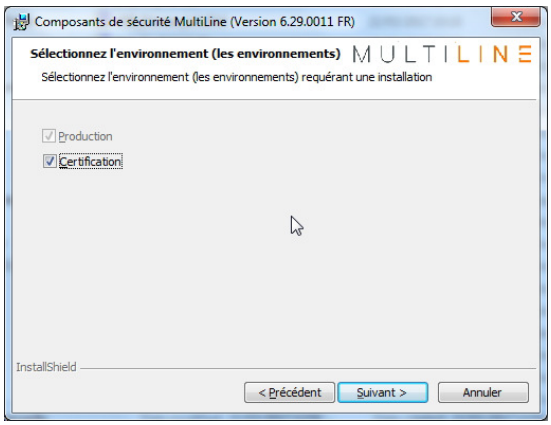
Si un prérequis n'est pas rempli, une croix rouge s'affiche dans la case associée. Vous devez corriger toutes les erreurs indiquées et redémarrer l'application de configuration (.msi) pour poursuivre le processus d'installation.

Lorsque tous les prérequis sont remplis, vous avez la possibilité de cliquer sur le bouton « Suivant » pour continuer l'installation.

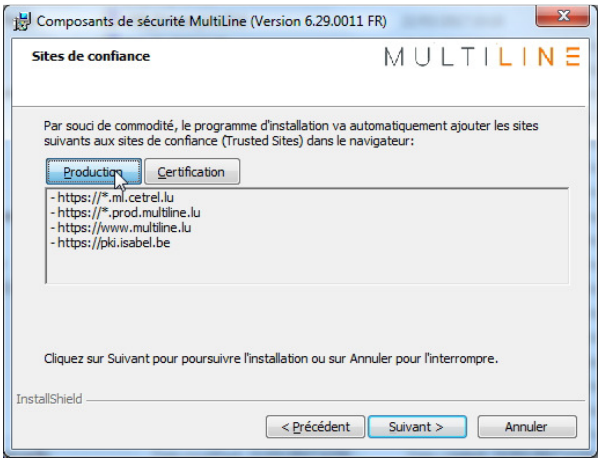
L'écran suivant, présenté ci-dessous, vous permet de changer le dossier de destination des fichiers de l'application installée (cette option n'est pas recommandée). Vous pouvez également choisir d'autoriser l'accès à l'application installée à vous seul ou à tous les utilisateurs de l'ordinateur. Par défaut, l'application est installée pour tous les utilisateurs (option recommandée).



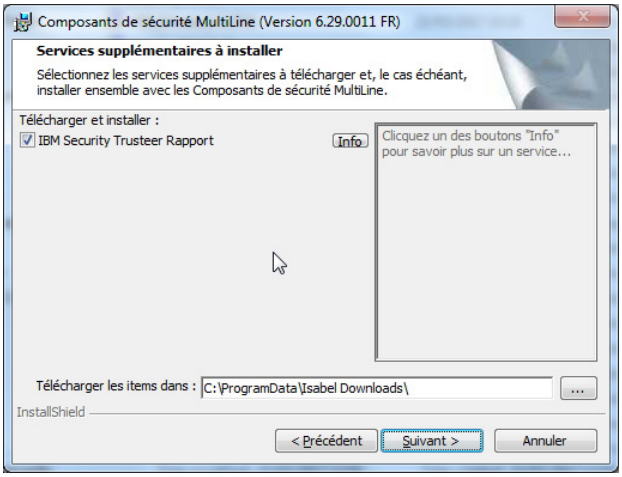
Sur l'écran suivant, si l'option est disponible, vous pouvez choisir les environnements installés pour accéder à MultiLine. La seule option obligatoire par défaut est l'installation de l'environnement de production. Cliquez sur le bouton « Suivant » pour continuer.



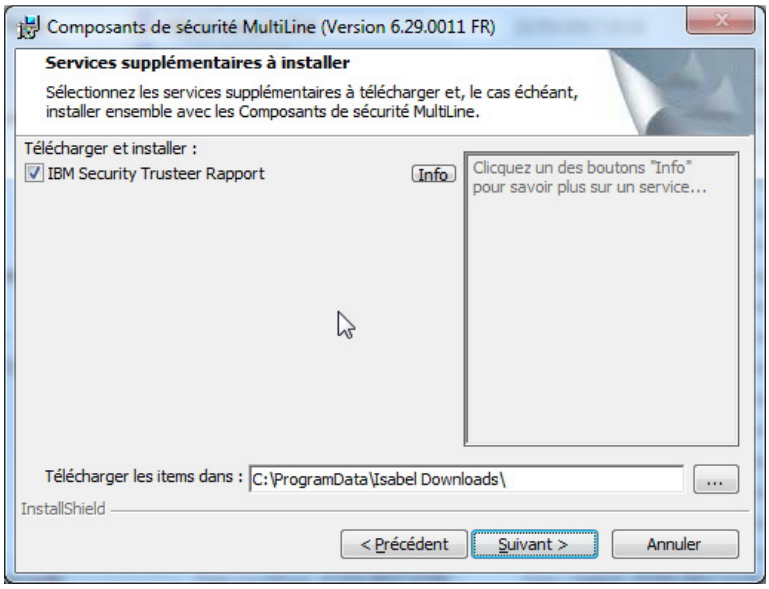
Si un environnement de certification est proposé et a été sélectionné dans l'écran précédent, vous devez choisir l'environnement qui sera actif par défaut. L'installation standard ne propose pas cet écran car l'environnement de production est généralement le seul choix.



L'écran suivant présente les sites de confiance qui sont automatiquement ajoutés à la configuration de votre navigateur (Internet Explorer). Comme pour l'environnement, seules les valeurs de production sont affichées dans le cadre d'une installation standard.

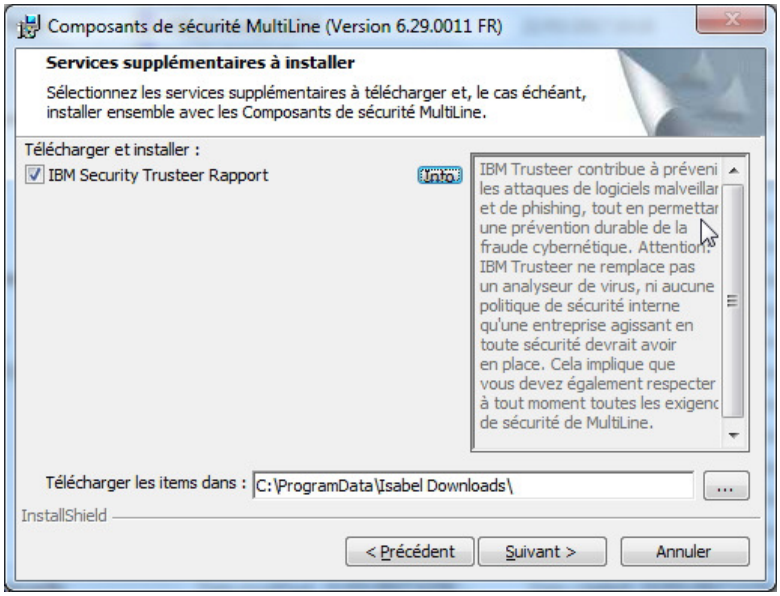


Sur l'écran suivant, vous pouvez choisir d'installer des services supplémentaires, le cas échéant. Par exemple IBM Security Trusteer, qui sécurise davantage l'accès à MultiLine.

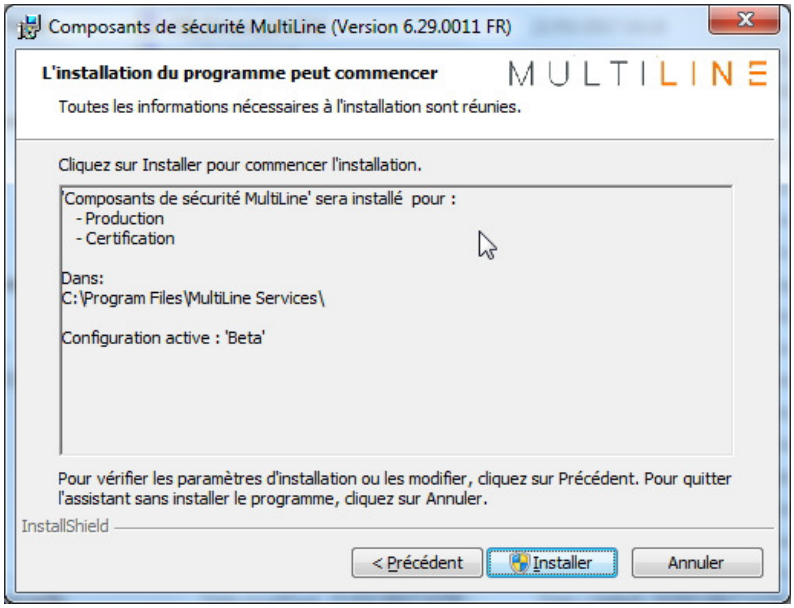


Les services facultatifs sont installés ultérieurement, si la case en regard du nom du service concerné est cochée. Par défaut, IBM Security Trusteer est sélectionné et installé.

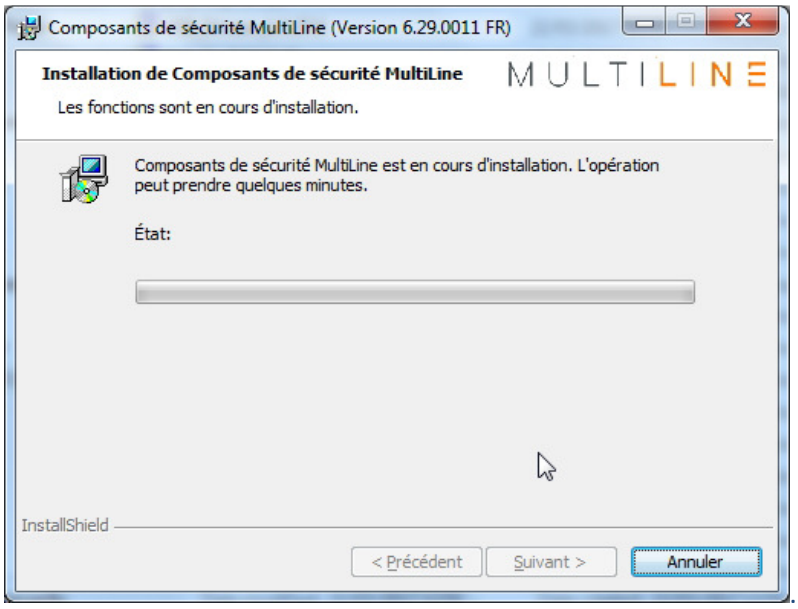
Le bouton « Info » fournit des informations sur les fonctions du service sélectionné :



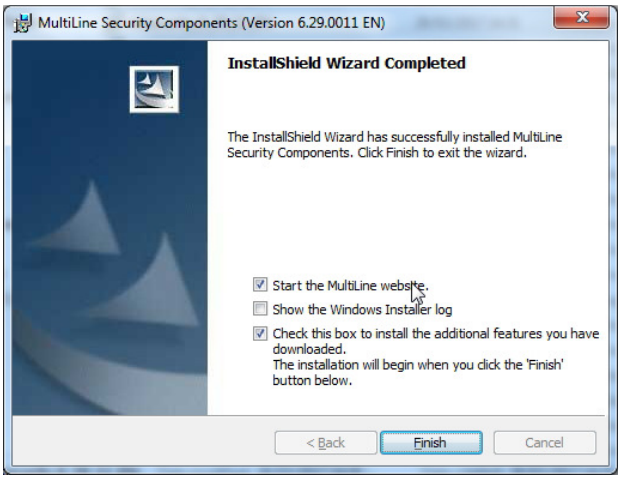
L'écran suivant affiche un récapitulatif des paramètres d'installation précédemment choisis.



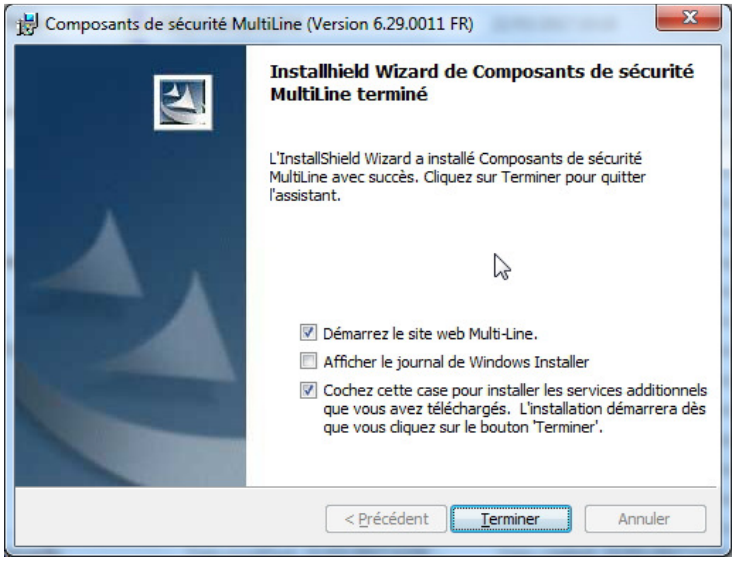
/!\ Lorsque vous cliquez sur le bouton « Installer », un écran vous demandant l'autorisation de modifier le système et l'accès aux droits d'administration s'affiche. Vous devez accepter la demande d'autorisation pour continuer l'installation et connaître la progression de la procédure.



A la fin de l'installation du MSI MultiLine, vous pouvez confirmer le téléchargement et l'installation des composants facultatifs (Trusteer, dans le cas présent) précédemment sélectionnés.



Pour Trusteer, comme le processus d'installation nécessite la mise à jour de certaines fonctionnalités d'Internet Explorer, vous devez décocher la case « Démarrer le site Web MultiLine » et garder la troisième case cochée. Il est également conseillé d'interrompre toutes les fonctions du navigateur en cours d'exécution avant de cliquer sur le bouton « Terminer ».



Si vous cliquez sur le bouton « Terminer » alors que la troisième case est cochée, le téléchargement des fichiers d'installation d'IBM Security Trusteer ou de tout autre service facultatif sélectionné démarre. Une fois le logiciel téléchargé, son installation est automatiquement lancée.

Vous trouverez ci-dessous des détails concernant le processus d'installation de Trusteer.

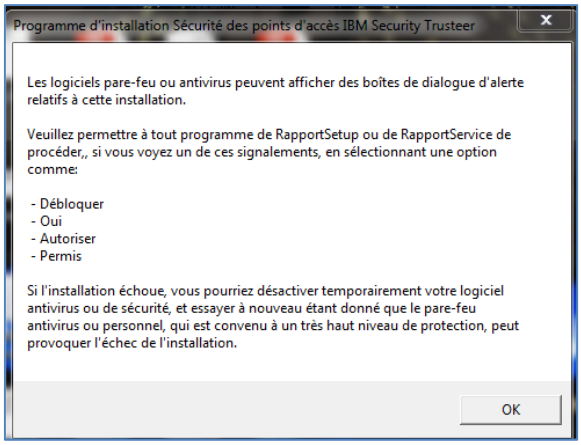
2. Processus d'installation d'IBM Security Trusteer

/!\ Vous devez être connecté à Internet pour pouvoir installer IBM Security Trusteer. Pour permettre le téléchargement et l'installation du logiciel, vous devez accéder aux adresses URL suivantes :

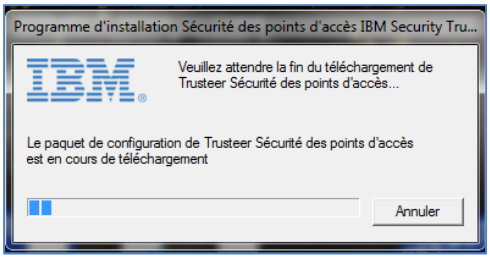
- *https://www.multiline.lu/fileadmin/media/downloads/FR/info2.txt*
- *https://www.multiline.lu/fileadmin/media/downloads/RapportSetup.exe*

Si vous ne parvenez pas à y accéder, vous serez invité à télécharger IBM Security Trusteer directement à partir du site Web d'IBM au cours du processus d'installation.

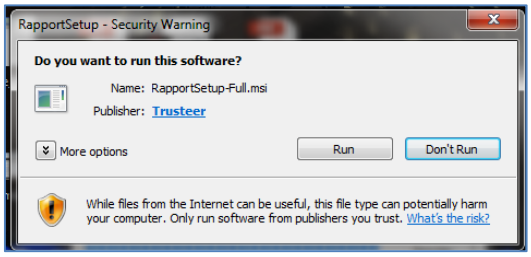
Lorsque la configuration est lancée, un message vous informe des éventuelles modifications de configuration à apporter à votre pare-feu et/ou à votre anti-virus. En cas de problème, vous pouvez désactiver temporairement votre anti-virus.



Le téléchargement d'IBM Security Trusteer démarre une fois le message validé.



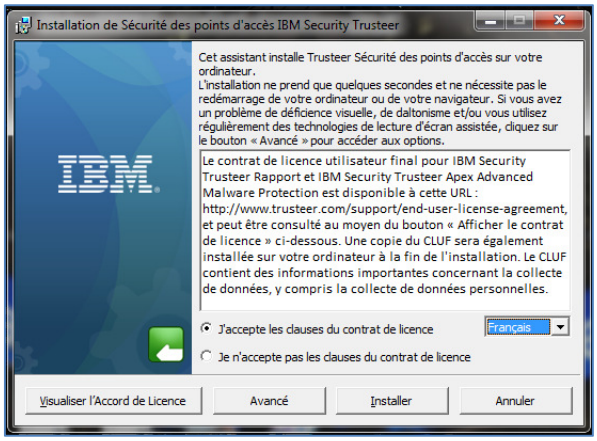
Lorsque le téléchargement est terminé, vous devez confirmer que vous souhaitez exécuter l'application (RapportSetup-Full.msi).



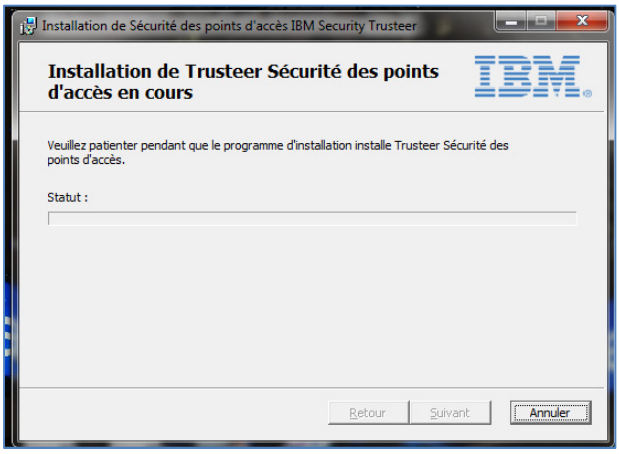
L'écran de bienvenue d'IBM Security Trusteer s'affiche.

Vous devez attendre quelques minutes, pour que le processus d'installation effectue des vérifications du système, avant de pouvoir cliquer sur « Suivant » pour poursuivre le processus d'installation. Lorsque le bouton est disponible, cliquez sur « Suivant » pour continuer.

Vous devez ensuite accepter le contrat de licence pour poursuivre l'installation.



Cliquez sur le bouton « Installer » pour lancer le processus d'installation. Le cas échéant, vous serez invité à autoriser la modification du système et passerez en mode Administrateur lors de l'installation.



A la fin de l'installation, cliquez sur le bouton « Terminer ». IBM Security Trusteer est désormais installé sur votre système.

/!\ Vous devez redémarrer votre système pour que toutes les modifications apportées par le processus d'installation soient prises en compte.

3. Utilisation d'IBM Security Trusteer

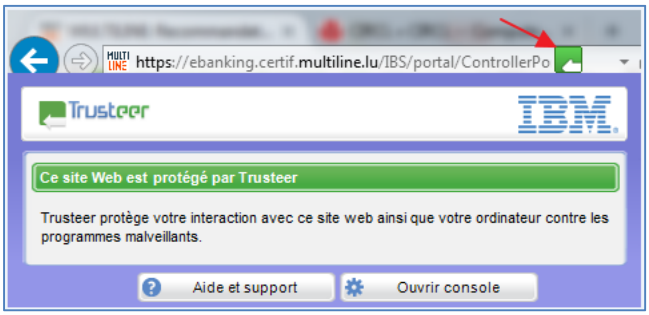
3.1. Valider le site protégé

L'icône Trusteer s'affiche dans votre navigateur une fois IBM Security Trusteer installé et le système redémarré. Une icône verte indique que le site est protégé par Trusteer ; une icône grise qu'il n'est pas protégé par Trusteer.

Site protégé

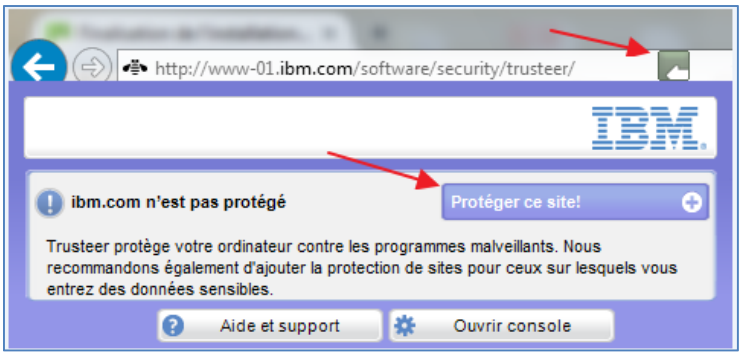
Site non protégé

Cliquez avec le bouton gauche de la souris pour afficher une fenêtre contenant des informations supplémentaires et accéder au menu Trusteer (bouton « Ouvrir console »).



3.2. Ajouter un site à la liste des sites protégés

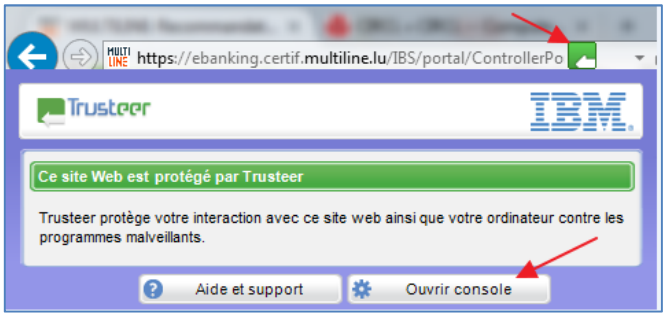
Trusteer utilise une liste prédéfinie de sites à protéger (non gérable par l'utilisateur) ainsi qu'une liste de sites à protéger définie par l'utilisateur (gérable par l'utilisateur). Lorsqu'un site n'est pas protégé par Trusteer (icône Trusteer grise), vous pouvez l'ajouter à la liste des sites protégés de l'utilisateur pour qu'il le devienne. Pour ce faire, cliquez sur l'icône Trusteer grise, puis cliquez sur le bouton « Protéger ce site ». L'icône Trusteer devient alors verte, vous indiquant que le site est protégé.



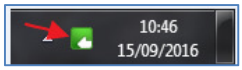
3.3. Ouvrir la console Trusteer

Vous pouvez accéder à la console Trusteer de plusieurs manières :

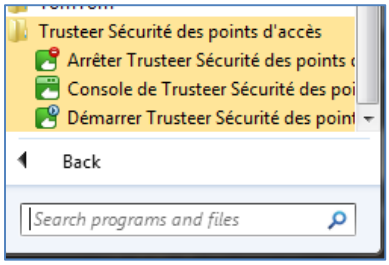
- Dans le navigateur :



- Dans la barre des tâches :



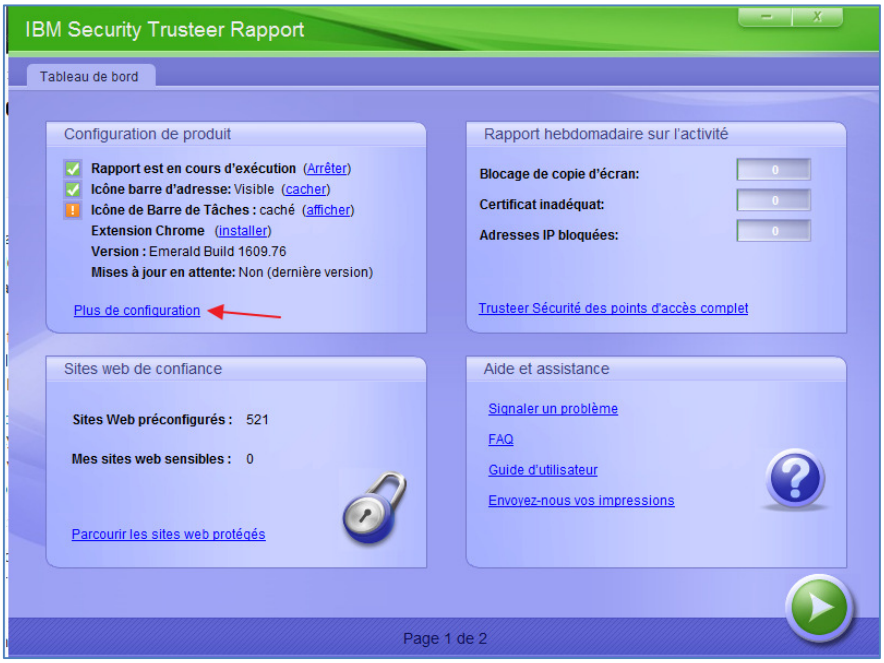
- Dans le menu Démarrer de Windows :



La console Trusteer permet de configurer et de contrôler l'activité :

3.3.1. Options de configuration de la console Trusteer

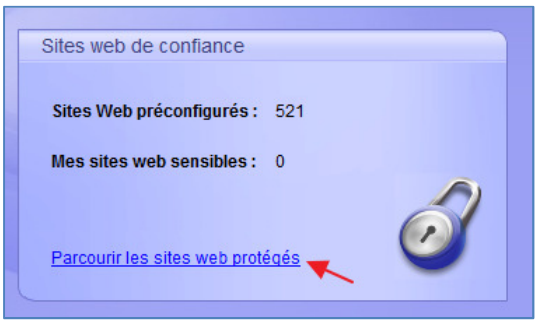
Les configurations ainsi que les informations générales sur Trusteer sont disponibles sur la page principale de la console. Vous pouvez accéder à des options de configuration supplémentaires en cliquant sur le lien « Plus de configuration » dans la partie inférieure du cadre supérieur droit de la console.



Par exemple, vous pouvez masquer l'icône Trusteer dans la barre des tâches, choisir la langue de l'interface ou le mode de mise à jour.

3.3.2. Liste des sites de confiance de la console Trusteer

Dans la partie « Sites Web de confiance », cadre inférieur gauche de la console, vous pouvez consulter la liste prédéfinie ainsi que la liste définie par l'utilisateur des sites de confiance.

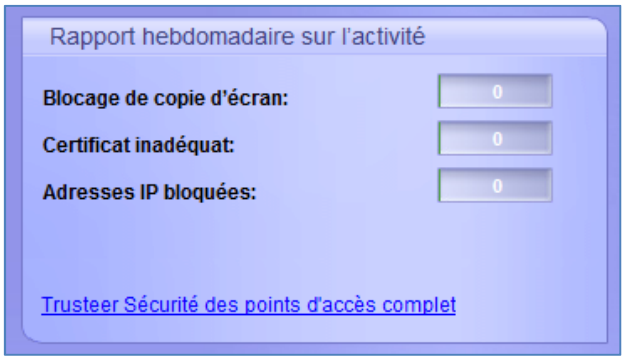


Vous avez la possibilité de consulter la liste prédéfinie de sites (non gérable par l'utilisateur) et de consulter ou de gérer la liste définie par l'utilisateur (par exemple, de supprimer des sites précédemment ajoutés manuellement).

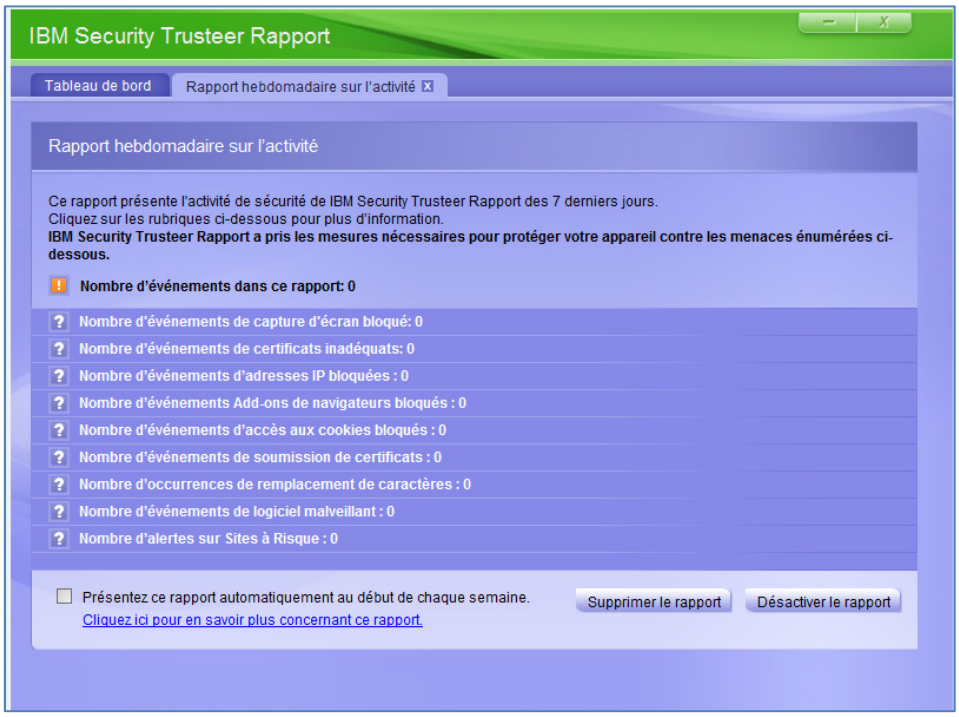
3.3.3. Rapport hebdomadaire dans la console Trusteer

La partie supérieure droite de la console est dédiée au rapport hebdomadaire sur l'activité de Trusteer. Le cadre contient les trois principaux compteurs de l'application :

- Blocage de copie d'écran ;
- Certificat inadéquat ;
- Adresses IP bloquées.



Cliquez sur le lien « Full Report » dans la partie inférieure de ce cadre pour accéder à des informations détaillées sur l'activité de Trusteer. Vous pouvez également choisir d'activer ou de désactiver (non recommandé) la génération automatique de rapports hebdomadaires.

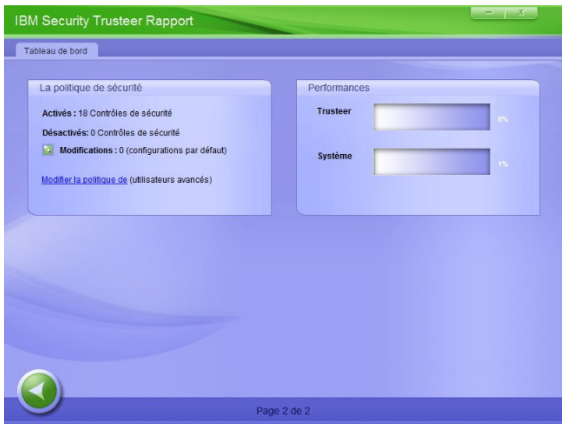


/!\ Veillez à consulter régulièrement les deux rapports (le rapport général et le rapport détaillé) afin de détecter d'éventuels comportements suspects.

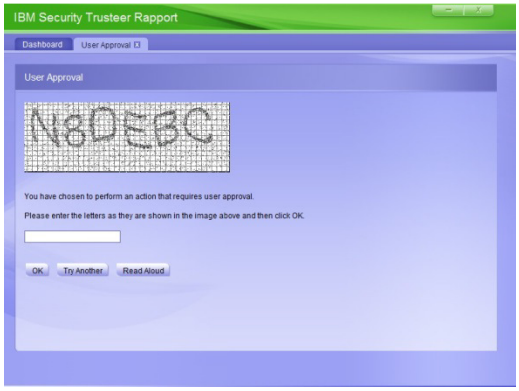
3.3.4. Politique de sécurité de la console Trusteer

L'écran Politique de sécurité se trouve sur le deuxième écran de la console Trusteer. Vous pouvez y accéder en cliquant sur l'icône verte située dans la partie inférieure droite du premier écran de la console.

Cet écran vous donne des informations sur la politique de sécurité de l'application Trusteer (nombre de règles de sécurité activées et désactivées) et vous permet de modifier certaines règles.



Vous pouvez accéder à l'écran de modification en cliquant sur le lien « Modifier la politique de » situé dans la partie inférieure du cadre de la politique de sécurité et en entrant le captcha exact reçu de l'application.



/!\ La modification des règles n'est PAS recommandée et s'effectue à vos propres risques. Les violations de la sécurité qui se produisent en raison d'une modification de la politique de la sécurité sont sous votre seule responsabilité.

3.4. **Message de blocage dans IBM Security Trusteer**

Lorsque vous parcourez un site protégé par Trusteer (contenu dans la liste par défaut de Trusteer ou dans celle ajoutée par l'utilisateur), certaines actions telles que la capture d'écran du site protégé ou l'accès distant à votre ordinateur déclenchent l'affichage de messages d'alerte contextuels de Trusteer.

Si un message de ce type s'affiche, vous devez accepter ou bloquer l'action concernée.

- Si vous n'êtes pas à l'origine de l'action, cliquez sur le bouton « Bloquer » pour arrêter immédiatement l'action.
  /!\ Dans ce cas, il est conseillé de faire une analyse et un contrôle anti-virus complets de votre ordinateur car il peut être corrompu par des logiciels malveillants et/ou des virus. Si nécessaire, renseignez-vous sur la procédure à suivre auprès de votre département informatique.
- Si vous êtes à l'origine de l'action, cliquez sur le bouton « Autoriser » pour permettre son exécution.

3.5. **Désactivation d'IBM Security Trusteer**

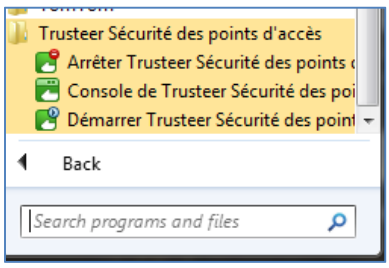
Vous pouvez temporairement désactiver IBM Security Trusteer si nécessaire. Cette opération peut être réalisée à partir de la console.

Un message d'avertissement (à valider) s'affiche alors, suivi d'un message de confirmation.

Vous devez valider le message de confirmation en entrant le captcha exact affiché sur l'écran, puis en cliquant sur le bouton « Désactiver ».

Trusteer est alors arrêté et peut être réactivé de la même manière.

Les menus de démarrage et d'arrêt sont également disponibles dans le menu Démarrer de Windows.



4. Informations complémentaires sur IBM Security Trusteer

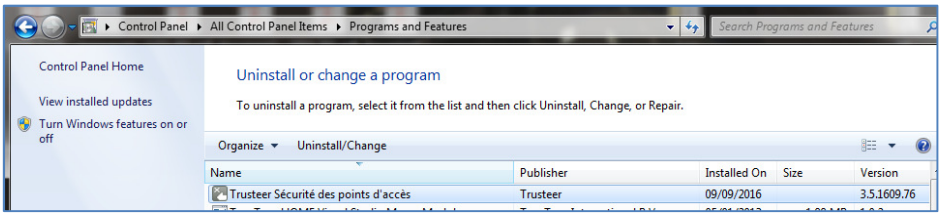
Dans le cadre « Aide et assistance » de la partie inférieure droite de l'écran de la console, vous pouvez :

- signaler un problème à un ingénieur Trusteer ;
- accéder à la FAQ ;
- accéder au guide d'utilisation d'IBM Trusteer ;
- envoyer vos commentaires sur l'application à un ingénieur Trusteer.

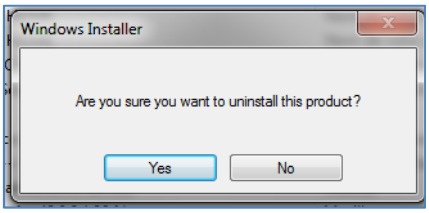
Cliquez simplement sur le lien correspondant dans le cadre et suivez les instructions ou accédez aux pages requises.

5. Désinstallation d'IBM Security Trusteer

Pour désinstaller IBM Security Trusteer, accédez à la liste des applications installées dans le panneau de configuration, puis sélectionnez l'application Trusteer et cliquez sur le menu « Uninstall/Change ».



Vous devez confirmer la demande de désinstallation.

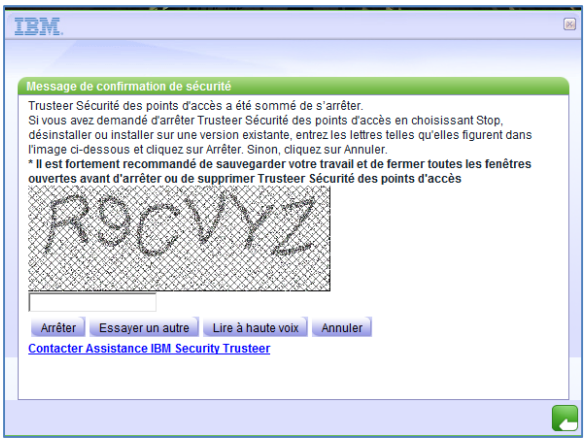


Un message d'information d'IBM Security Trusteer sur l'activité passée de Trusteer s'affiche. Vous devez l'accepter en cliquant sur le bouton « Continuer » pour pouvoir poursuivre.

Sur l'écran suivant, vous devez indiquer si vous souhaitez obtenir une aide à distance d'un ingénieur Trusteer ou si vous souhaitez seulement désinstaller le produit. Vous pouvez éventuellement supprimer toutes les préférences utilisateur pour le logiciel avant de lancer la désinstallation.

Vous devez choisir « Non merci, désinstaller maintenant » pour désinstaller l'application IBM Security Trusteer.

Vous devez valider le message de confirmation en entrant le captcha exact affiché sur l'écran, puis en cliquant sur le bouton « Arrêter ».



La désinstallation d'IBM Security Trusteer ne dure que quelques secondes.

/!\ Vous devez redémarrer votre ordinateur pour supprimer totalement Trusteer.