Trusteer

Trusteer Rapport

Manuel d'utilisation

Version 3.5.1207

Novembre 2012

nouvelles menaces, ***nouvelle approche***

Table des matières

À propos de ce guide

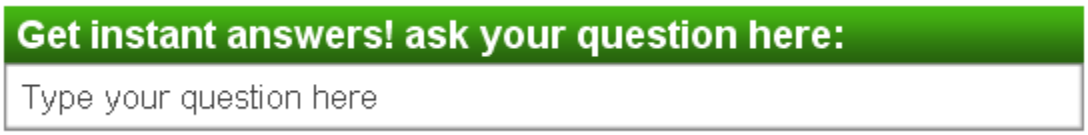
Ce guide explique comment utiliser Trusteer Rapport pour profiter au maximum de ce produit. Ce guide s'adresse aux:

- Clients des banques ou d'autres institutions financières qui offrent Trusteer Rapport en téléchargement gratuit en tant qu'outil de sécurité de protection de l'utilisation en ligne de comptes financiers.
- Membres d'entreprises qui utilisent Trusteer Rapport pour sécuriser leur accès Web à distance.
- Clients utilisant des cartes de paiement protégées par Trusteer Rapport qui se servent de Trusteer Rapport pour sécuriser leurs transactions en ligne au moyen de cette méthode de paiement.

Besoin de plus d'informations sur Trusteer Rapport?

Pour compléter ce guide d'utilisation, Trusteer fournit une FAQ complète (Foire aux questions) ici : http://www.trusteer.com/support/faq.

Sur la page Web de la FAQ, ce service nanoRep fournit immédiatement des réponses aux questions supplémentaires que vous pourriez avoir :



Saisissez simplement votre question et nanoRep affiche les réponses.

Nous envoyer des commentaires

Trusteer apprécie vos commentaires.

- Suggérez de nouvelles idées ou améliorations et exprimez votre opinion à propos de Trusteer Rapport.

Pour envoyer vos commentaires à propos de Trusteer Rapport, veuillez visiter visit http://www.trusteer.com/product-feedback.

- Suggérez de nouvelles idées ou améliorations et exprimez votre opinion à propos de ce guide d'utilisation.

➡ **Pour envoyer des commentaires à propos du guide d'utilisation:**

Cliquez sur le bouton Envoyer le commentaire (Submit Feedback) en haut de la page du guide d'utilisation de Trusteer Rapport. Ce bouton ouvre votre client de messagerie par défaut et vous permet de nous envoyer un e-mail avec vos commentaires.

1. Quelles Nouveautés?

Ces fonctionnalités sont nouvelles dans Trusteer Rapport 1207:

- Trusteer Rapport 1207 a été testé et certifié quant à sa compatibilité avec Windows 8.

Ces fonctionnalités étaient nouvelles dans Trusteer Rapport 1206:

- Trusteer Rapport 1206 propose un navigateur virtualisé, une nouvelle couche de protection des applications pour les sites Web protégés. Le navigateur virtualisé s'exécute au sein de sa propre machine virtuelle sur le SE de votre ordinateur Windows. Trusteer Rapport propose d'ouvrir des sites dans le navigateur virtualisé si Trusteer détecte un risque grave pour la sécurité de votre ordinateur ou si vous accédez à un site qui prend en charge le navigateur virtualisé. Vous pouvez installer le navigateur virtualisé en le téléchargeant depuis une alerte. Après l'installation à réaliser une seule fois, vous serez alerté lorsque vous aurez la possibilité d'ouvrir un site dans le navigateur et vous pourrez configurer des sites Web pour qu'ils s'ouvrent automatiquement dans le navigateur virtualisé. Pour plus d'informations à propos du navigateur virtualisé, veuillez consulter :These features are new in Trusteer Rapport 1207:

- Utiliser le navigateur virtualisé de Trusteer Rapport (on page 78)
- Répondre à une alerte forcée de téléchargement du navigateur virtualisé (on page 90)
- Répondre à une alerte forcée du navigateur virtualisé (on page 92)
- Répondre à une alerte facultative de téléchargement du navigateur virtualisé (on page 93)
- Répondre à une alerte facultative du navigateur virtualisé (on page 99)

- Trusteer Rapport 1206 offre aux partenaires un service de certificat logiciel (Soft Token) sécurisé pour l'attribution de mots de passe à usage unique. Le service de certificat logiciel sécurisé de Trusteer Rapport assure la protection contre les programmes malveillants qui se génèrent automatiquement ou qui procèdent à des vols de mots de passe à usage unique. Si votre banque ou votre entreprise vous demande d'utiliser le service de certificat logiciel sécurisé Trusteer Rapport, veuillez consulter Utiliser le service Token logiciel sécurisé de Trusteer Rapport (on page 82).

2. En quoi consiste Trusteer Rapport?

Trusteer Rapport est une application logicielle de sécurité qui est spécifiquement conçue pour vous protéger des fraudes basées sur un navigateur lorsque vous vous connectez à des sites sensibles tels que votre banque ou le réseau privé de votre entreprise. Trusteer Rapport vous protège contre les logiciels malveillants tels que Zeus qui contournent les méthodes d'authentification les plus rigoureuses et les antivirus en exploitant le navigateur afin de porter atteinte à vos données et opérations financières en ligne.

Trusteer Rapport vous protège contre les attaques qui prennent place au sein de votre navigateur, par exemple les téléchargements drive-by (involontaires), le phishing, le pharming, les enregistreurs de frappe, les attaques de l'homme du milieu, les attaques de l'homme dans le navigateur, les captures d'écran malveillantes et les attaques de piratage de session.

Vue d'ensemble

Les navigateurs Web constituent désormais le maillon faible de la chaîne de communication lorsque vous effectuez des opérations bancaires ou des achats en ligne ainsi que lorsque vous vous connectez à distance à votre bureau. Les antivirus, les pare-feu et autres logiciels de sécurité s'appuient sur des listes de comportements connus pour identifier et supprimer les logiciels malveillants. De récentes études révèlent un taux particulièrement faible de détection des programmes malveillants du secteur financier, y compris s'agissant des antivirus à la pointe du progrès. Dans le cas où un logiciel malveillant s'intègre de lui- même dans votre navigateur ou votre système d'exploitation sans être détecté, ces solutions ne combattent pas l'activité malveillante au moment de l'attaque.

Les entreprises qui fournissent un accès à distance aux employés, sous-traitants et clients sont vulnérables aux attaques basées sur le navigateur malgré l'utilisation de réseaux privés virtuels (VPN), de jetons, de contrôles d'accès réseau et d'autres méthodes d'authentification pour identifier les utilisateurs et protéger les données sensibles de l'entreprise ou les données personnelles. Les logiciels malveillants modernes contournent ces technologies d'authentification en attaquant le navigateur, en compromettant les sessions d'accès à distance et en volant les identifiants de connexion et les données ou bien en infectant les hôtes sur le réseau.

Là où d'autres solutions de sécurité se focalisent sur la recherche et la désactivation des logiciels malveillants, Trusteer Rapport protège votre navigateur en adoptant une approche basée sur les points d'attaque. Trusteer Rapport est doté d'une technique de fonctionnement qui reconnaît les tentatives des logiciels malveillants d'accéder aux informations sensibles, d'ordre privé ou financier, via le navigateur. En détectant un comportement malveillant au niveau du point d'attaque, Trusteer Rapport peut identifier rapidement et précisément les nouvelles variantes de logiciels malveillants. Trusteer Rapport fournit trois niveaux de protection :

- Empêche les applications malveillantes d'accéder aux informations sensibles avant même qu'elles soient reconnues.
- Identifie et supprime les logiciels malveillants dès que possible. Le fait de supprimer un logiciel malveillant empêche qu'il se transforme en une variante qui est soit plus difficile à bloquer ou soit attaque la solution de sécurité qui essaie de le bloquer. De plus, Trusteer Rapport peut détecter et supprimer plusieurs variantes du même logiciel malveillant indépendamment du fichier binaire utilisé par la variante.
- Vous empêche de télécharger inconsciemment des logiciels malveillants identifiés, y compris depuis des sites Web légitimes.

Quel est l'enjeu?

Les logiciels malveillants sont souvent téléchargés silencieusement vers votre ordinateur à partir de sites Web légitimes. Voici quelques faits alarmants à propos des logiciels malveillants et de votre PC :

- 2 millions de sites Web légitimes permettent de télécharger des logiciels malveillants sur votre PC sans qu'ils en aient conscience (Sophos, avril 2008).
- 15 000 nouvelles pages Web infectées sont identifiées chaque jour. 79 % d'entre elles se rapportent à des sites Web légitimes qui ont été piratés. Même des sites Web bien connus tels que Google et Yahoo ont été signalés comme ayant procuré des programmes malveillants aux utilisateurs par le biais d'annonces publicitaires. Même si vous faites preuve d'une grande prudence et ne visitez que des sites Web bien connus, les logiciels malveillants peuvent malgré tout trouver un moyen d'infecter silencieusement votre ordinateur (Sophos, avril 2008).
- D'après un récent test portant sur les meilleurs antivirus et filtres anti-hameçonnage pour navigateurs Web, plus de la moitié des logiciels malveillants et des menaces liées au phishing en activité sur Internet passe inaperçue, avec un taux moyen de détection de 37 % des logiciels malveillants et de 42 % pour le phishing (Cyveillance, février 2009).
- Un ordinateur personnel sur quatre aux États-Unis - soit 59 millions - est déjà infecté par un logiciel malveillant (Organisation de coopération et de développement économiques -OCDE-, juin 2008).
- Les programmes malveillants de dernière génération peuvent enregistrer silencieusement les frappes au clavier, capturer des images sur les écrans et voler des renseignements financiers confidentiels depuis votre ordinateur.

Les raisons pour lesquelles vous avez besoin de Trusteer Rapport

La protection de Trusteer Rapport est basée sur une technologie révolutionnaire qui est complètement différente de celles utilisées par les solutions de sécurité conventionnelles des ordinateurs de bureau. Trusteer Rapport fonctionne de manière autonome ou bien en partenariat avec votre solution de sécurité informatique. Il ne remplace pas votre antivirus et ne constitue pas une solution antivirus. Vous devriez utiliser Trusteer Rapport, même si votre ordinateur bénéficie de la protection antivirus la plus actualisée.

Les antivirus, pare-feu et autres logiciels de sécurité sont importants, mais, malheureusement, pas assez efficaces. Diverses études et de récentes incidents indiquent que ces outils ne sont pas toujours efficaces pour empêcher des malfaiteurs de vous voler de l'argent sur votre compte. Alors que la criminalité devient de plus en plus sophistiquée, votre banque recommande vivement des niveaux de protection supplémentaires sur votre ordinateur pour vous permettre d'effectuer des opérations bancaires en ligne de manière totalement sécurisée.

Les solutions classiques, telles que les logiciels antivirus, les antispywares, les pare-feu personnels et les barres d'outils anti-hameçonnage s'appuient sur une liste de mauvais comportements connus, tels que les signatures, les heuristiques ainsi que les listes noires. Ces solutions sont de moins en moins efficaces contre les techniques d'usurpation d'identité et de fraude financière les plus récentes. Ces attaques sont les plus dangereuses et peuvent vous causer d'importants préjudices financiers.

« D'après un récent test portant sur les meilleurs antivirus et filtres anti-hameçonnage pour navigateurs Web, plus de la moitié des logiciels malveillants et des menaces liées au phishing en activité sur Internet passe inaperçue, avec un taux moyen de détection de 37 % des logiciels malveillants et de 42 % pour le phishing. » Cyveillance, février 2009

Les programmes malveillants les plus récents sont capables de voler vos identifiants de connexion aux services en ligne bancaires, de courtage, d'achats, de commerce électronique, de messagerie et de réseaux sociaux. Même si le site est considéré comme sécurisé, les fraudeurs peuvent utiliser votre compte en ligne pour exécuter des transactions non autorisées, passer des commandes, envoyer des e-mails et bien plus encore.

Trusteer Rapport vous empêche d'envoyer votre nom d'utilisateur, votre mot de passe, ou d'autres identifiants de connexion sensibles vers des sites Web non sécurisés et évite que les logiciels malveillants et les sites Web frauduleux ne dérobent ces informations et piratent vos données transmises en ligne. Trusteer Rapport protège également vos communications en ligne et empêche les logiciels malveillants d'altérer vos transactions. Par exemple, Trusteer Rapport vous protège des logiciels qui peuvent transférer de l'argent depuis votre compte bancaire vers un compte frauduleux. Si vous effectuez des opérations bancaires, des transactions ou des achats en ligne, Trusteer Rapport peut considérablement réduire votre exposition à la menace croissante de la fraude financière et de l'usurpation d'identité.

En quoi Trusteer Rapport est-il différent des suites de sécurité pour Internet?

Trusteer Rapport is very different from Internet Security suites. An Internet Security suite consists of databases of malicious software and hostile websites which it uses to detect and remove threats from your computer. Internet Security suite vendors constantly look for new malicious software and hostile websites in order to update their databases. Trusteer Rapport uses a completely different technology.

Trusteer Rapport can tell when you are accessing your bank's website and can also tell when you are executing transactions, submitting login information, and reading sensitive bank statements. During that time Trusteer Rapport applies access control layers around your sensitive information and prevents malicious software and hostile websites from accessing or tampering with your sensitive information and transactions. An unauthorized access attempt, such as an attempt to read your password, or alter your transactions, is immediately blocked. Trusteer Rapport's access control policies are set by your bank.

Banks that work with Trusteer build and maintain policies that define which information is sensitive and which operations on this information should be restricted. Unlike Internet Security Suites, Trusteer Rapport does not need to maintain a database of malicious software and websites and can therefore block new threats and "under the radar" threats which Internet Security suites are not yet aware of. Your bank and Trusteer work hard to keep Trusteer Rapport effective against financial crimes that are currently targeting online bankers.

Contre quelles attaques Trusteer Rapport vous protège-t-il?

La technologie exclusive de verrouillage du navigateur de Trusteer Rapport empêche l'accès non autorisé aux informations qui circulent entre les clients et les sites Web quel que soit le logiciel malveillant spécifiquement à l'origine de la menace.

Trusteer Rapport permet de bloquer efficacement toutes ces techniques :

Phishing

Une attaque de *phishing* consiste pour le malfaiteur à mettre en place un site d'hameçonnage qui ressemble exactement à un site web que vous connaissez et qui vous inspire confiance (par exemple, le site Web de votre banque). Le malfaiteur vous convainc ensuite de visiter ce site Web (par exemple, en vous envoyant un e-mail frauduleux comportant un lien y menant). Lorsque vous arrivez sur le site Web frauduleux, vous pensez à tort qu'il s'agit du véritable site. Dès que vous essayez de vous connecter à ce site Web frauduleux, le malfaiteur s'empare vos identifiants de connexion et peut maintenant les utiliser pour ouvrir une session sur le véritable site en votre nom.

Pour vous protéger contre les attaques de phishing, Trusteer Rapport:

- Vous alerte si vous tentez d'accéder à un site Web qui est réputé pour être malveillant.
- Vous alerte lorsque vous venez de saisir un mot de passe sur un site qui ne traite pas les données de manière sécurisée. Les sites qui ne soumettent pas les données en toute sécurité sont considérés comme à haut risque et incluent les sites légitimes qui pourraient facilement être interceptés par des malfaiteurs.

Pharming ou usurpation de DNS

Une attaque par *pharming* ou usurpation de DNS se produit lorsqu'un malfaiteur force votre ordinateur à accéder à un site Web frauduleux chaque fois que vous saisissez l'adresse d'un site réel dans la barre d'adresse de votre navigateur. L'attaque parvient à ce résultat en utilisant diverses techniques telles que le fait d'infecter votre ordinateur de bureau avec des programmes malveillants ou en compromettant les serveurs du réseau de votre FAI. Une fois que vous arrivez sur le site Web frauduleux et essayez de vous connecter, le malfaiteur récupère vos identifiants de connexion et peut maintenant les utiliser pour ouvrir une session sur le site authentique, en usurpant votre identité et en effectuant des transactions frauduleuses. Pour vous protéger contre les attaques de pharming, Trusteer Rapport vérifie l'adresse IP et le certificat SSL du site Web à chaque fois que vous vous connectez à un site web protégé. Si la vérification échoue, Trusteer Rapport met fin à la connexion et en établit une nouvelle au véritable site.

Enregistreur de frappe

Un *keylogger* (enregistreur de frappe) est un programme malveillant qui réside indétectée dans votre ordinateur. L'enregistreur de frappe enregistre ce que vous saisissez au clavier puis envoie ces informations au malfaiteur. De cette façon, les enregistreurs de frapper peuvent récupérer des identifiants de connexion lorsque vous saisissez le mot de passe, les numéros de carte bancaire et d'autres informations sensibles pour les envoyer au malfaiteur qui peut les utiliser pour ouvrir une session sur vos comptes, en usurpant votre identité et en réalisant des transactions frauduleuses. Trusteer Rapport bloque les enregistreurs de frappe en cryptant ce que vous saisissez afin qu'ils ne puissent lire des informations sensibles.

Attaque de l'homme du milieu

Une attaque *Man-in-the-Middle* (de l'homme du milieu) constitue une variante avancée des attaques de phishing et de pharming. Dans cette attaque, vous vous connectez au site Web et commencez à travailler tout en n'ayant pas conscience que toutes les informations échangées entre vous et le site sont transférées au malfaiteur via un site intermédiaire qui peut accéder à toutes les informations privées et modifier vos transactions. Par exemple, si vous demandez de transférer une certaine somme d'argent à un bénéficiaire spécifique, le malfaiteur peut changer l'identité de ce dernier pour que l'argent soit transféré vers un autre compte.

Trusteer Rapport empêche le réacheminement malveillant par le navigateur vers des sites frauduleux en utilisant plusieurs niveaux de vérification, comme la vérification de la légitimité de l'adresse IP et du certificat du site.

Attaque de l'homme dans le navigateur

Une attaque *Man-in-the-Browser* (de l'homme dans le navigateur) consiste en un logiciel malveillant qui s'infiltre dans votre navigateur, parfois sous la forme d'une extension légitime, d'un objet d'aide du navigateur (BHO) ou d'un module. Ce logiciel malveillant contrôle tout ce qui se passe dans votre navigateur. Il est capable de lire des informations sensibles telles que vos identifiants de connexion et de les transmettre au malfaiteur. Il peut également effectuer des transactions en votre nom, telles que le fait de transférer de l'argent depuis votre compte vers celui du malfaiteur.

Trusteer Rapport empêche les logiciels malveillants d'accéder aux données au sein du navigateur par le biais de plusieurs mécanismes :

- Empêche les applications malveillantes d'accéder aux informations sensibles avant même qu'elles soient reconnues.

- Identifie et supprime les logiciels malveillants dès que possible. Le fait de supprimer un logiciel malveillant empêche qu'il se transforme en une variante qui est soit plus difficile à bloquer ou soit attaque la solution de sécurité qui essaie de le bloquer. De plus, Trusteer Rapport peut détecter et supprimer plusieurs variantes du même logiciel malveillant indépendamment du fichier binaire utilisé par la variante.
- Vous empêche de télécharger inconsciemment des logiciels malveillants identifiés, y compris depuis des sites Web légitimes.

Capture d'écran

Les logiciels malveillants peuvent inclure des mécanismes de capture d'écran qui enregistrent ce qui s'affiche sur votre moniteur pour en envoyer le contenu au malfaiteur. Les captures d'écran peuvent afficher les détails de votre compte, le solde et même les identifiants de connexion si le site utilise un clavier virtuel sur la page de connexion. Trusteer Rapport désactive les mécanismes de capture d'écran alors que vous êtes connecté aux sites Web protégés.

Piratage de session

Un programme malveillant de *piratage de session* vole les paramètres de votre session avec un site Web spécifique et envoie ces informations au malfaiteur. Le malfaiteur utilise ensuite ces paramètres de session pour prendre le contrôle de votre session sur le site et contourner le processus d'authentification qui est requis pour s'y connecter. Trusteer Rapport empêche l'accès aux paramètres de session alors que vous êtes connecté aux sites Web protégés.

Téléchargement drive-by

Lors d'un téléchargement drive-by, vous téléchargez sans le savoir des programmes malveillants en visitant simplement un site Web. Le site peut être légitime, mais être infecté afin qu'il charge de manière invisible un logiciel malveillant sur votre ordinateur.

Comment fonctionne l'application Trusteer Rapport?

Lorsqu'il est installé sur votre ordinateur, Trusteer Rapport protège automatiquement les sites qui appartiennent aux entreprises partenaires travaillant avec Trusteer pour fournir le niveau de sécurité le plus élevé pour leur entreprise et leurs clients. Trusteer Rapport vous permet également d'appliquer manuellement la protection de Rapport à tous les autres sites Web que vous

utilisez et sur lesquels vous vous connectez et échangez des informations sensibles, telles que des informations financières personnelles ou autres.

Lorsque vous vous connectez à un site Web protégé, Trusteer Rapport accomplit trois choses en arrière-plan pour rendre extrêmement difficile aux malfaiteurs de vous viser :

- Trusteer Rapport vérifie que vous êtes vraiment connecté au site authentique et non à un site factice créé par des malfaiteurs. De manière étonnante, il n'est pas banal d'atteindre un véritable site web lorsque vous saisissez son adresse dans votre navigateur.
- Une fois que la vérification est terminée, Trusteer Rapport verrouille la communication entre votre ordinateur et le site web protégé. Ceci empêche les malfaiteurs de pirater votre connexion en ligne avec la banque.
- Trusteer Rapport protège votre ordinateur et votre connexion internet en créant un tunnel de communication sécurisé avec votre banque ou entreprise, en empêchant les malfaiteurs d'utiliser des logiciels malveillants pour dérober vos données de connexions et falsifier des transactions financières ou échanges d'informations.

Trusteer Rapport ajoute un niveau unique et très important de sécurité qui permet à nos partenaires de mieux protéger vos informations sensibles et de réagir promptement aux menaces vous visant directement.

Ce sont là certaines des façons dont Trusteer Rapport protège vos communications, données et informations financières.

- Communication sécurisée avec des sites protégés (on page 16)

Communication sécurisée avec des sites protégés

Lorsque vous vous connectez à un site web protégé, Trusteer Rapport empêche tout processus sur votre ordinateur d'y accéder. Vous pouvez communiquer en toute sécurité avec le site Web, à l'abri de toute tentative d'accès hostile par des logiciels malveillants. Même si vous avez des logiciels malveillants non détectés et cachés dans votre ordinateur, ils ne peuvent pas lire des informations sensibles depuis le site Web ou falsifier vos transactions.

Protection de la connexion

Lorsque vous vous connectez à un site Web protégé, celui-ci vous authentifie avec des identifiants de connexion sécurisés tels qu'un nom d'utilisateur et un mot de passe. Le problème est que les malfaiteurs disposent de plusieurs méthodes pour saisir vos identifiants de connexion et les utiliser pour se connecter à votre compte en ligne.

Une méthode est appelée le phishing (hameçonnage). Dans une attaque de type phishing, vous êtes dirigé vers une réplique factice du véritable site Web de sorte que vous saisirez inconsciemment vos identifiants de connexion sur un site frauduleux. Les fraudeurs disposent désormais de vos identifiants de connexion et peuvent les utiliser pour se connecter à votre compte en ligne au lieu de vous.

Trusteer Rapport vous protège des attaques de phishing en vous avertissant si vous essayez d'accéder à un site Web qui est connu pour être malveillant et si, par mégarde, vous saisissez vos identifiants de connexion sur un site qui ne traite pas les données de façon sécurisée.

Protection de la session de navigation

Lorsque vous vous connectez à un site web, celui-ci conserve un fichier texte appelé un cookie de session dans la mémoire temporaire pour toute la durée de la session. Le cookie de session identifie votre session authentifiée et vous permet à plusieurs reprises d'échanger des informations sensibles avec le serveur du site sans avoir à vous connecter de nouveau.

Les logiciels malveillants peuvent récupérer les cookies de session et les utiliser pour contourner l'authentification et prendre le contrôle de votre session sur le site. Pour vous protéger contre ce type d'attaque, Trusteer Rapport empêche les applications d'accéder aux cookies de session sur les sites web partenaires.

Remarque: Cette fonctionnalité est uniquement prise en charge pour les partenaires qui travaillent avec Trusteer pour protéger les communications en ligne de leurs clients.

Protection de la saisie sur clavier

Trusteer Rapport crypte vos saisies au cours de leur transfert vers le navigateur et les cache des programmes malveillants connus comme les enregistreurs de frappe ainsi que des composants des logiciels malveillants à l'intérieur du système d'exploitation. Cela empêche les logiciels malveillants de lire ce que vous saisissez et de capturer des informations sensibles telles que votre mot de passe ou votre numéro de carte de paiement.

Protection des cartes de paiement

Trusteer Rapport vous avertit lorsque vous soumettez des informations de carte de paiement vers des sites locaux et non sécurisés. L'avertissement apparaît dans une boîte de dialogue qui vous permet d'interrompre l'envoi. Rapport active également une protection contre les enregistreurs de frappe lorsque vous saisissez un numéro de carte de paiement soit sur un site protégé par Rapport, soit sur tout site sécurisé (https) qui contient un mot clé relatif à une carte de paiement, comme Visa, Mastercard ou Amex. La protection contre les enregistreurs de frappe empêche également que des programmes malveillants disposant de telles fonctions ne puissent capturer les informations de votre carte de paiement.

Remarque: Cette fonctionnalité est uniquement prise en charge pour les cartes de paiement émises par les marques participantes desdites cartes.

Blocage des captures d'écran

Trusteer Rapport désactive toutes les tentatives de capture de l'écran tandis qu'un site Web protégé est affiché dans votre navigateur. Cela empêche les logiciels malveillants de récupérer des informations sensibles au moyen d'une capture d'écran.

Validation de site Web

Même lorsque vous saisissez l'adresse correcte du site de votre banque ou de votre entreprise, les logiciels malveillants peuvent utiliser plusieurs méthodes, appelées attaques de pharming, pour rediriger votre navigateur vers un site web frauduleux.

Pour vous protéger contre les attaques de pharming, Trusteer Rapport vérifie l'adresse IP et le certificat SSL chaque fois que vous vous connectez à un site web protégé. Si le certificat SSL est périmé, incorrect ou signé par un émetteur inconnu, Rapport vous avertit et vous permet d'éviter de vous connecter au site. Si l'adresse IP n'est pas trouvée dans les tableaux d'adresses IP de confiance relatives à ce site Web, Rapport remplace celle-ci par une autre valide pour le site.

Blocage des extensions de navigateur

Lorsque vous vous connectez à un site Web protégé, Trusteer Rapport bloque toutes les extensions de navigateur qu'il ne reconnaît pas comme étant des logiciels légitimes et sûrs. Les extensions de navigateur sont de petits logiciels (généralement tiers) qui s'intègrent à votre navigateur et peuvent contrôler sa manière de communiquer. Cela vous protège des extensions de navigateur malveillantes qui peuvent voler vos identifiants de connexion ou pirater vos communications.

Blocage des modifications de processus

Trusteer Rapport analyse les tentatives de modification des processus du navigateur et bloque celles qui semblent suspectes. Modifier les processus du navigateur (également connu sous le nom de function patching) est une technique qui permet de prendre le contrôle du navigateur et d'obtenir l'accès à vos informations sensibles.

Avertissements relatifs aux sites malveillants

Trusteer Rapport vous alerte si vous tentez d'accéder à un site Web qui est réputé pour être malveillant.

Signalement d'accès non autorisés

Trusteer Rapport communique avec les sites partenaires de Trusteer, procurant des informations sur le niveau de sécurité et signalant toute tentative non autorisée d'accéder à votre compte en ligne. Cela permet à votre banque ou entreprise de prendre des mesures immédiates contre les menaces.

Remarque:	Cette fonctionnalité est uniquement prise en charge pour les partenaires qui travaillent avec Trusteer pour protéger les communications en ligne de leurs clients.

L'expérience utilisateur

Trusteer Rapport est extrêmement facile à utiliser. Vous n'avez pas besoin de connaissances techniques pour utiliser Trusteer Rapport. Trusteer Rapport ne nécessite pas de configuration, ne change pas la façon dont vous travaillez, ne modifie pas le comportement du navigateur, et ne vous pose pas de questions techniques lorsqu'il rencontre une menace pour la sécurité.

La plupart des activités protectrices de Trusteer Rapport fonctionnent en mode silence et ne vous importunent pas, ni ne nécessitent votre participation. Rapport enregistre toutes les mesures qu'il prend pour vous protéger dans un Afficher les activités de Trusteer Rapport (on page 156) que vous pouvez afficher chaque fois que vous le souhaitez. Les détails à propos des niveaux de risque se trouvent dans le rapport d'activité. Lorsque Rapport rencontre des niveaux de menace élevés, vous en êtes informé. Certaines actions protectrices, dans ces cas, requièrent des Répondre aux alertes et avertissements (on page 90), qui sont faciles à comprendre.

Il est facile de voir quels sont les sites web protégés par Trusteer Rapport. Une icône affichée sur ou près du côté droit de la barre d'adresse de votre navigateur indique par sa couleur si le site actuel est protégé.

L'icône de Rapport ( ) apparaît dans la barre d'état système de Windows lorsque Trusteer Rapport est en cours d'exécution. Le fait de cliquer sur l'icône ouvre la console Trusteer Rapport grâce à laquelle vous pouvez accéder à diverses fonctionnalités et informations.

Lorsque vous utilisez de nouveaux identifiants de connexion sur un site protégé, une boîte de dialogue Répondre à une offre de protection du Mot de passe (on page 104). Cette boîte de dialogue s'affiche uniquement la première fois que vous utilisez les identifiants de connexion.

Tirer le meilleur profit de Trusteer Rapport

En plus de la protection dont vous bénéficiez automatiquement lorsque vous vous connectez aux sites partenaires de Trusteer, vous pouvez manuellement ajouter la protection de Trusteer Rapport à tous les autres sites sensibles que vous utilisez. Consultez les détails relatifs à la protection de sites Web et d'identifiants de connexion supplémentaires.

Au-delà de la protection de sites Web, Trusteer Rapport vous offre d'autres fonctionnalités de sécurité qui sont toutes incluses gratuitement :

- Consultez les Analyser votre ordinateur pour améliorer la sécurité (on page 160) pour savoir comment améliorer davantage la sécurité de votre ordinateur.
- Générez des Afficher les activités de Trusteer Rapport (on page 156) quant aux tentatives visant à pirater votre compte bancaire en ligne.
- Recevez des Recevoir des infos en matière de sécurité (on page 164) directement depuis Trusteer vers une boîte de réception dédiée et sans spam au sein même de la console Rapport.

Informations pour les utilisateurs avancés

Trusteer Rapport est un logiciel prenant peu de place. Pour obtenir des détails spécifiques à propos de l'espace occupé par Rapport, consultez les Traces laissées sur le Traces laissées sur le PC par Trusteer Rapport (on page 22).

Trusteer Rapport ne compromet en aucune façon votre vie privée. Consultez Trusteer Rapport et votre vie privée (on page 22).

Trusteer Rapport comprend un mécanisme de protection pour empêcher les logiciels malveillants de supprimer l'exécution du logiciel ou de l'éliminer. En conséquence, vous ne pouvez pas utiliser le gestionnaire des tâches pour interrompre ses processus. Pour plus d'informations sur la manière d'arrêter Trusteer Rapport, veuillez consulter Arrêter Trusteer Rapport (on page 194).

Traces laissées sur le PC par Trusteer Rapport

Les traces laissées par Trusteer Rapport incluent ce qui suit :

- Exécutables : Program Files\Trusteer\Rapport\bin\RapportService.exe, Program Files\Trusteer\Rapport\bin\RapportMgmtService.exe
- Processus : RapportService.exe, RapportMgmtService.exe
- Services : Rapport Management Service (pour les comptes non-administrateurs sur les systèmes d'exploitation en 64 bits : RapportInjService_x64.exe)
- Pilotes:
  - « RapportPG.sys » (sur les systèmes d'exploitation en 64 bits: « RapportPG64.sys »)
  - « RapportKELL.sys » (sur les systèmes d'exploitation en 64 bits: « RapportKE64.sys »)
  - « RapportEI.sys » (RapportEI64.sys pour les systèmes d'exploitation en 64 bits)
- Attendez-vous en moyenne à 15 Mo d'espace de profil d'utilisateur pour les journaux et les paramètres (selon le nombre de navigateurs différents utilisés sur l'ordinateur, ce chiffre peut être plus important).
- La taille du programme est de 15 Mo en plus de l'espace de profil d'utilisateur.

Trusteer Rapport et votre vie privée

Trusteer Rapport creates an encrypted signature of your credentials on your computer. This information cannot be used to retrieve your credentials and is used by Trusteer Rapport to identify any unauthorized leakage of your credentials. Trusteer Rapport sends anonymous reports about security events and internal errors to a Service central de Trusteer Rapport: Blocage puissant des manœuvres frauduleuses (on page 23). This information is used to improve the product and the policy.

Trusteer Rapport crée une signature cryptée pour vos identifiants de connexion sur votre ordinateur. Cette information ne peut pas être utilisée pour récupérer vos identifiants de connexion et est utilisée par Trusteer Rapport pour identifier toute divulgation non autorisée de vos informations d'identification. Trusteer Rapport envoie des rapports anonymes sur les événements de sécurité et les erreurs internes vers un Service central de Trusteer Rapport: Blocage puissant des manœuvres frauduleuses (on page 23). Cette information est utilisée pour améliorer le produit et les règles.

Service central de Trusteer Rapport: Blocage puissant des manœuvres frauduleuses

Le service central de Trusteer Rapport est offert par Trusteer aux partenaires pour leur permettre de prendre des mesures immédiates pour empêcher les manœuvres frauduleuses sur votre compte.

Chaque fois que Trusteer Rapport détecte une activité sur le site ou un logiciel suspect, il génère un événement de sécurité et l'envoie au service central de Trusteer Rapport pour qu'il y soit analysé. Le service central exécute des tests afin de déterminer si l'activité est frauduleuse. En cas d'activité frauduleuse, le service central ordonne à Trusteer Rapport de bloquer plus agressivement la menace.

Remarque: le service central de Trusteer Rapport est disponible pour votre banque, uniquement si vous ne désactivez pas l'envoi des événements de sécurité pour analyse. Ce paramètre se trouve dans l'assistant de configuration de Trusteer Rapport et est activé par défaut. Votre anonymat[1] le plus complet est garanti lorsque ce paramètre est activé.

Trusteer Rapport vous protège même si vous choisissez de ne pas envoyer d'événements de sécurité pour analyse. Toutefois, en envoyant des événements pour analyse, Rapport est capable de détecter des menaces plus sophistiquées, voire même inconnues.

[1] Toutes les informations envoyées à partir de votre ordinateur vers le service central de Trusteer Rapport sont anonymes et incluent les détails techniques, pas les données privées. Quand Trusteer Rapport suspecte que vos informations personnelles ont été mises en danger, il envoie à votre banque

Quelques exemples d'événements de sécurité que Trusteer Rapport envoie pour analyse sont :

- Un site Web suspect
- Des tentatives visant à s'emparer de vos identifiants
- Des tentatives visant à interférer avec vos communications à caractère sensible
- Des logiciels suspects

L'un des grands avantages du service central de Trusteer Rapport consiste en un système d'alerte qui prévient votre banque lorsque votre nom d'utilisateur et votre mot de passe sont en danger. Le service central est capable de détecter des menaces qui ont échappé aux antivirus et autres logiciels de sécurité.

En plus des événements de sécurité, Trusteer Rapport envoie de temps en temps des informations sur les erreurs internes du logiciel. Ces informations peuvent aider Trusteer à identifier et résoudre les problèmes logiciels.

Puis-je désactiver l'envoi des événements de sécurité et des journaux d'erreurs à Trusteer?

Votre anonymat[2] le plus complet est garanti lorsque l'envoi des événements de sécurité et des journaux d'erreurs à Trusteer est activé. Vous pouvez désactiver cette fonction si vous le souhaitez, même si nous ne le recommandons pas.

Pour désactiver l'envoi des événements de sécurité et des journaux d'erreurs à Trusteer, utilisez les instructions de Modifier les règles de sécurité (on page 178) pour modifier **Send Security Events and Errors for Analysis (Envoyer les événements de sécurité et les erreurs pour analyse)** de **Always (toujours)** à **Never (jamais)**.

ou entreprise un avertissement qui comprend un identificateur lui permettant d'associer l'incident avec votre compte. Trusteer n'est pas exposé à cet identificateur ou à toute autre information privée.

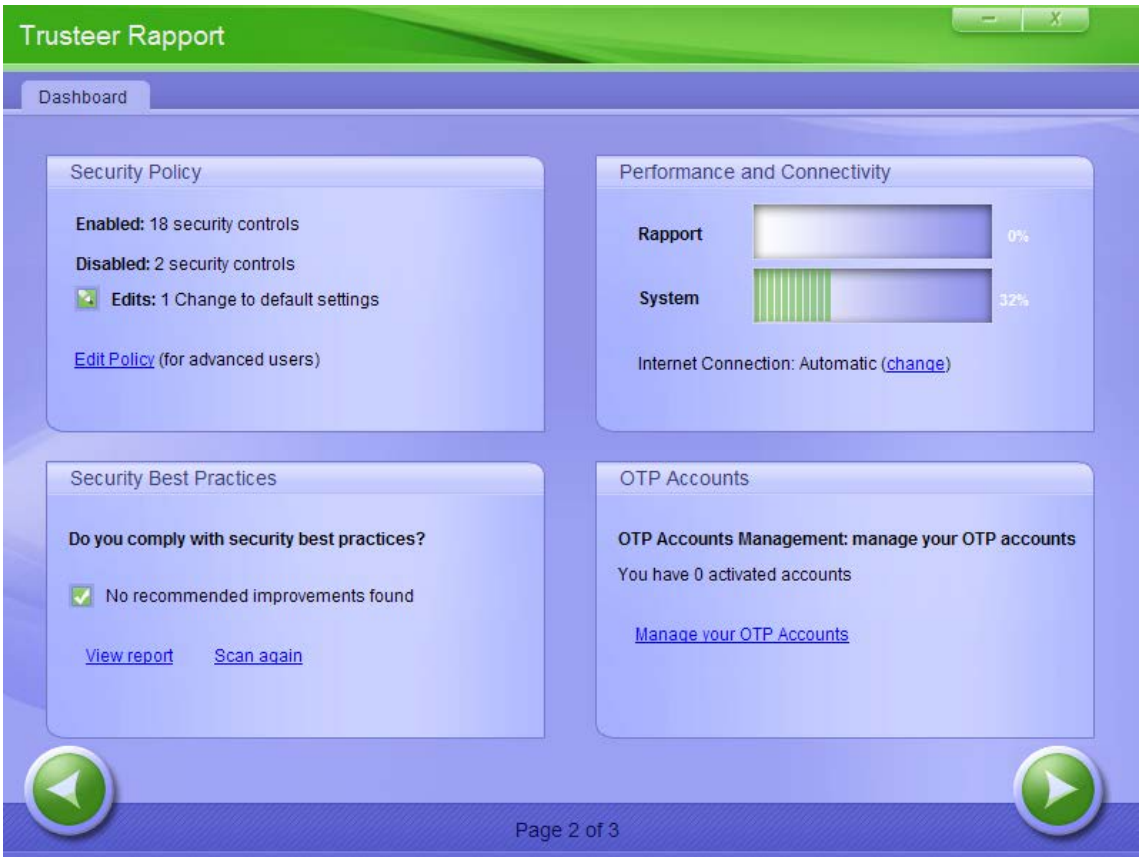
[2] Toutes les informations envoyées à partir de votre ordinateur vers le service central de Trusteer Rapport sont anonymes et incluent les détails techniques, pas les données privées. Quand Trusteer Rapport suspecte que vos informations personnelles ont été mises en danger, il envoie à votre banque ou entreprise un avertissement qui comprend un identificateur lui permettant d'associer l'incident avec votre compte. Trusteer n'est pas exposé à cet identificateur ou à toute autre information privée.

Enabling Sending of Security Events and Error Logs to Trusteer

If you unchecked the *Send security events and error logs anonymously to Trusteer* box in the setup wizard during installation, you can enable this important feature in the Rapport console.

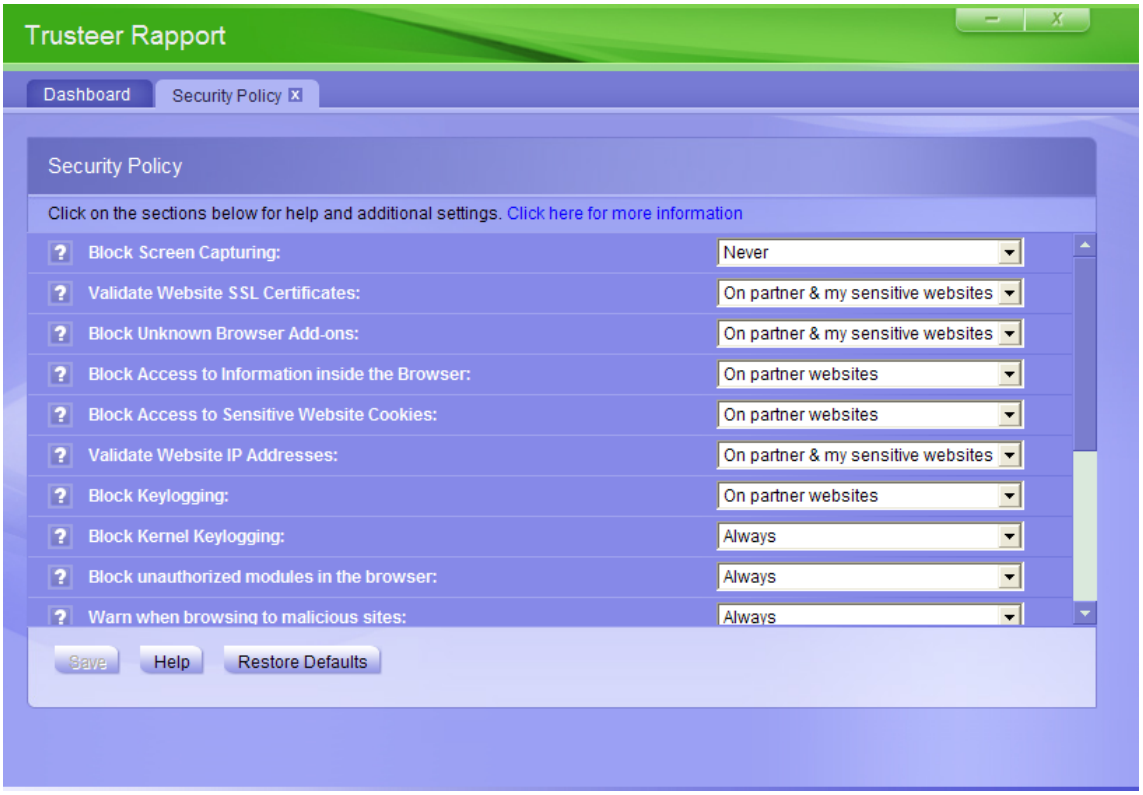
➡ **To enable the sending of security events and error logs to Trusteer:**

1. Ouvrir la console Rapport (on page 72).
2. Dans le tableau de bord, cliquez sur  . Le second écran du tableau de bord apparaît.



3. Dans la zone de la politique de sécurité, cliquez sur Modifier la politique. Un écran Approbation de l'utilisateur apparaît. L'écran vous montre l'image d'un mot pour que vous le saisissiez. Ceci est destiné à empêcher les logiciels malveillants d'accéder à la console et de désactiver Trusteer Rapport de manière efficace.

4. Saisissez le mot que vous voyez dans l'image.
5. Cliquez sur OK. L'écran Politique de sécurité apparaît, affichant tous les contrôles de sécurité.



6. Scroll down to **Send Security Events and Errors for Analysis**.
7. From the drop-down list next to **Send Security Events and Errors for Analysis**, select **Always**.
8. Click **Save**. This control is now enabled and Rapport will now send security events and errors to Trusteer for analysis.

3. Installer Trusteer Rapport

Installer Trusteer Rapport est rapide et facile. Il vous suffit de télécharger le fichier d'installation à partir du site de votre banque ou de votre entreprise, de l'exécuter et de suivre une procédure classique pour l'installer.

Si vous avez besoin d'instructions exactes pour savoir comment télécharger et installer l'application Trusteer Rapport, consultez la rubrique correspondante dans cette section.

Remarque: Si vous installez l'application Trusteer Rapport depuis un compte administrateur Windows, les utilisateurs standard peuvent exécuter Trusteer Rapport depuis leurs comptes et ne peuvent l'interrompre, le démarrer, le désinstaller ou l'écraser, ni modifier certains paramètres des règles. Cette restriction est une fonction qui permet aux administrateurs d'installer l'application Trusteer Rapport à l'échelle d'une entreprise et d'empêcher les employés de désactiver ses fonctionnalités de sécurité ou de modifier les règles de sécurité pour tous les utilisateurs.
Il est fortement recommandé d'installer Trusteer Rapport depuis un compte administrateur, puisque cela permet d'étendre automatiquement la protection de Trusteer Rapport au bénéfice de tous les utilisateurs, et parce que les pilotes ne peuvent pas être installés lors de l'installation depuis un compte utilisateur standard, étant donné que les mécanismes de protection les plus importants (prévention et suppression des logiciels malveillants) sont installés par les pilotes. Si vous installez Trusteer Rapport depuis un compte utilisateur standard, Trusteer Rapport ne fonctionnera pas sur tout autre compte utilisateur et ne pourra pas être installé sur un autre compte, sauf s'il est d'abord désinstallé.

Comment puis-je basculer vers un compte administrateur?

- Basculer vers un compte d'administrateur (Windows 7) (on page 143)
- Basculer vers un compte d'administrateur (XP) (on page 144)
- Basculer vers un compte d'administrateur (Vista) (on page 146)

Où puis-je télécharger Trusteer Rapport?

Si vous êtes un client d'une banque ou d'une autre organisation qui propose Trusteer Rapport, vous pouvez télécharger Rapport à partir du site Web de votre banque. Votre banque peut :

- Afficher une section relative à la sécurité sur le site Web de la banque (habituellement au bas de la page) avec un lien vers Trusteer Rapport ou vers « protégez-vous ».
- Vous proposer de télécharger Trusteer Rapport en tant que partie du processus de connexion à votre compte en ligne ou immédiatement après une ouverture de session réussie

L'application Trusteer Rapport est-elle compatible avec mon système d'exploitation et mon navigateur?

Trusteer Rapport est compatible avec ces systèmes d'exploitation et navigateurs: http://www.trusteer.com/supported-platforms.

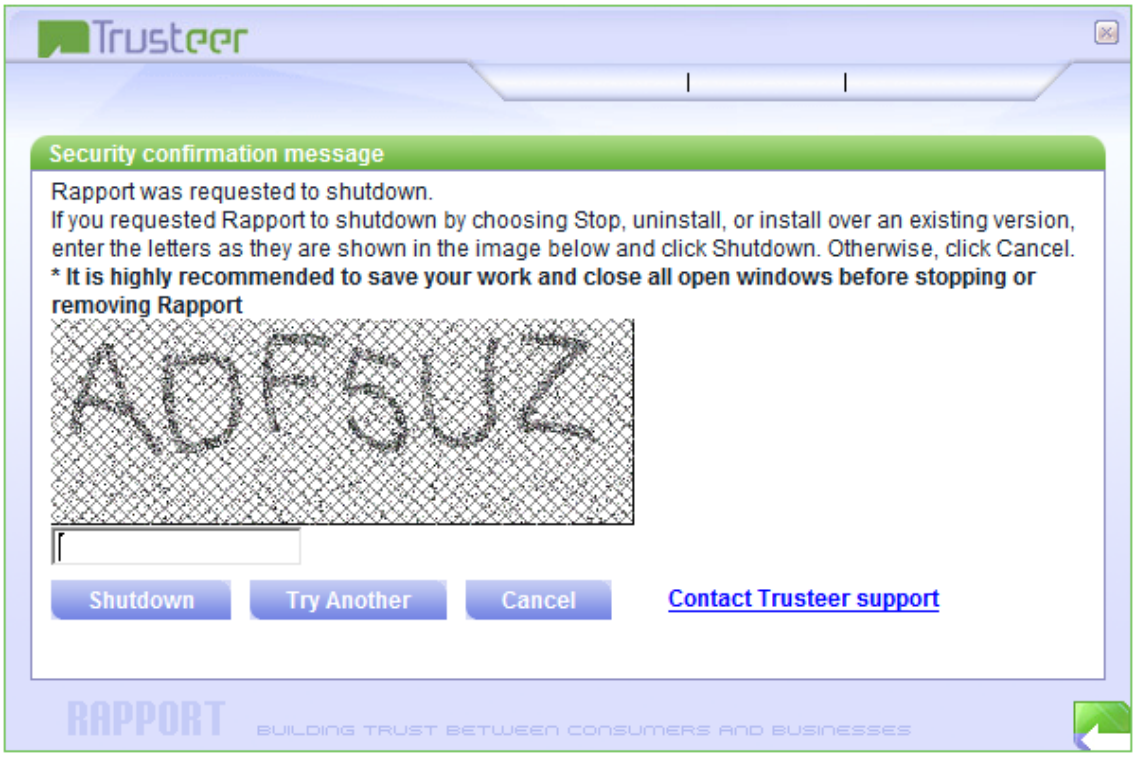
Pourquoi m'indique-t-on que Trusteer Rapport figure déjà sur mon ordinateur?

Si une version de Trusteer Rapport existe déjà sur votre ordinateur lorsque vous l'installez, la boîte de dialogue suivante s'affiche pendant le processus d'installation:

Si vous voyez cet écran durant l'installation, cela signifie qu'il existe déjà une version de Trusteer Rapport installée sur votre ordinateur. La réinstallation de Rapport est une opération totalement sure (tant que vous n'installez pas une version plus ancienne sur une plus récente).

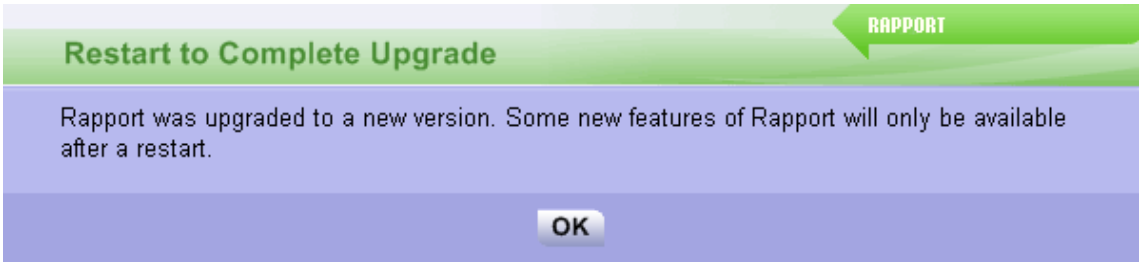
➡ **Pour installer Trusteer Rapport sur une version préexistante:**

1. Sélectionnez l'option qui décrit le mieux la raison pour laquelle vous souhaitez installer Trusteer Rapport de nouveau.
2. Cliquez sur **Next** (Suivant). Le processus d'installation commence et s'interrompt de lui-même pour arrêter Trusteer Rapport. Avant l'arrêt de Rapport, un message de sécurité de confirmation s'affiche. Le message présente une image contenant un mot que vous devez saisir. Cela vise à empêcher qu'un logiciel malveillant ne désactive Rapport.



3. ESaisissez le mot qui apparait dans l'image. (la saisie n'est pas sensible à la casse.)

4. Cliquez sur **Shutdown** (Arrêter). Le message suivant s'affiche pendant que Rapport s'arrête : « Please wait while Rapport shuts down » (Veuillez patienter alors que Rapport s'arrête) Lorsque le message disparaît, Rapport a cessé de fonctionner. Le processus d'installation se poursuit ensuite comme d'habitude. Ce message peut s'afficher après l'installation:



Votre ordinateur est protégé, même après l'apparition de ce message. Néanmoins, il est préférable de redémarrer votre ordinateur dès que possible.

Comment puis-je installer Trusteer Rapport dans un environnement de partage de bureau virtuel?

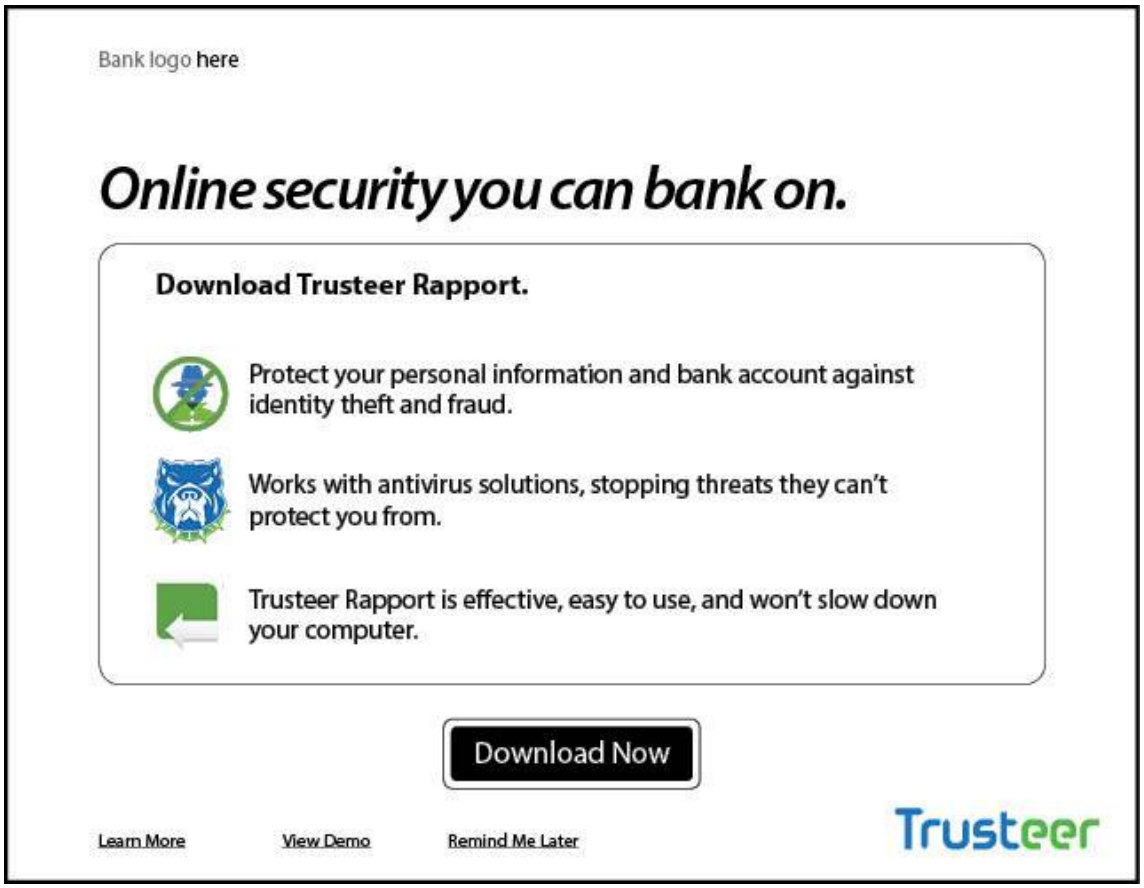
Si vous installez Trusteer Rapport sur Windows Server (2003 ou 2008), l'assistant d'installation détecte le système d'exploitation et installe la version serveur de Trusteer Rapport. Cette version prend en charge plusieurs sessions. Pour plus d'informations, consultez Installer Trusteer Rapport sous Windows Server (2003 ou 2008) (on page 67).

Installation de Trusteer Rapport sur Windows 7 utilisant Internet Explorer

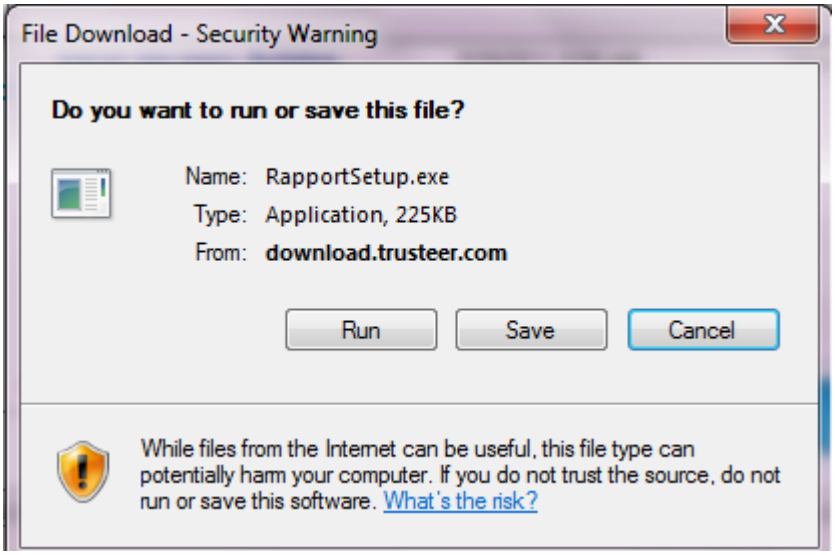
Cette procédure explique comment télécharger et installer Trusteer Rapport si vous êtes sous Windows 7 et utilisez Microsoft Internet Explorer comme navigateur.

➡ **Pour installer Trusteer Rapport:**

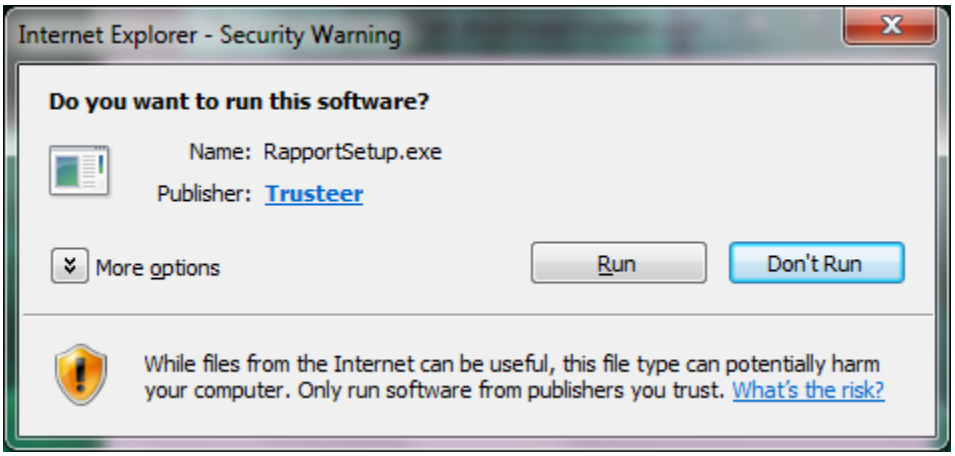
1. Accédez à la page de connexion de votre entreprise. Si celle-ci propose Trusteer Rapport au téléchargement, vous verrez un message montrant un bouton « **Download Now** » (Télécharger maintenant). Par exemple :



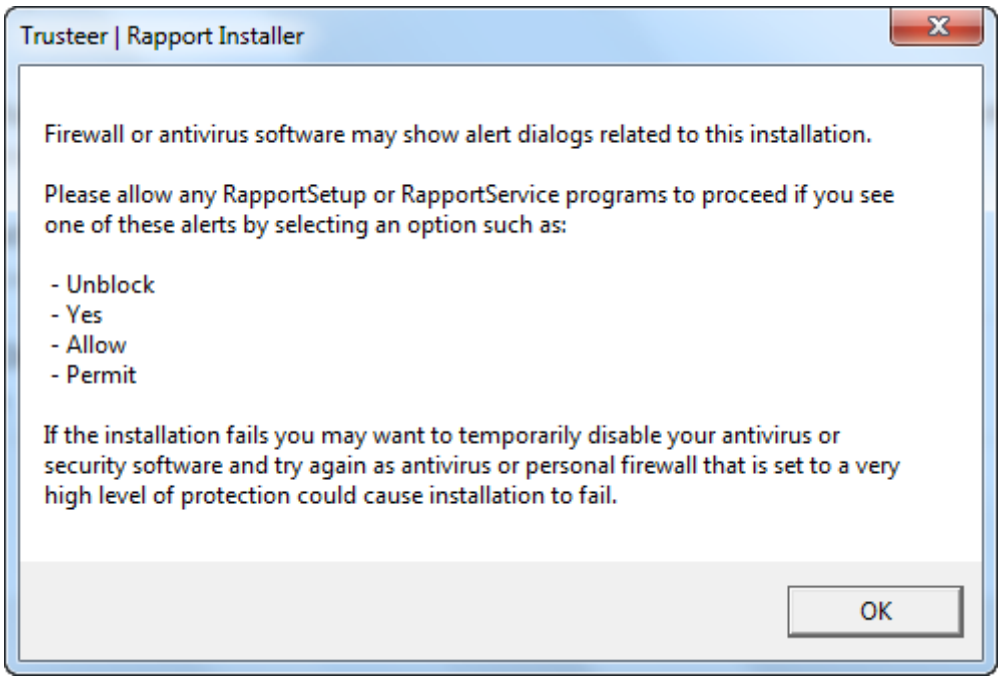
2. Cliquez sur **Download Now**. (Télécharger maintenant) La boîte de dialogue **File Download Now - Security Warning** (Télécharger le fichier maintenant - alerte de sécurité) s'afficher en vous demandant si vous souhaitez exécuter ou enregistrer le fichier RapportSetup.exe.



3. Cliquez sur **Run**. (Exécuter) Une autre boîte de dialogue s'affiche quelques secondes plus tard et vous demande « Do you want to run this software? » (Voulez-vous exécuter ce logiciel ?)

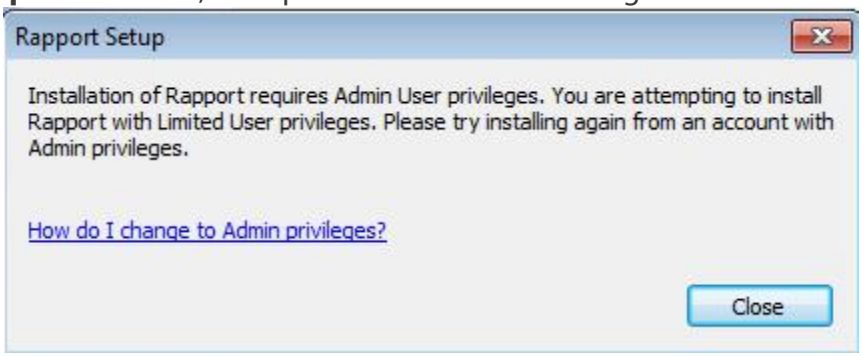


4. Cliquez sur **Run** (Exécuter) de nouveau. La boîte de dialogue suivante apparaît.



5. Cliquez sur **OK**. Trusteer Rapport se télécharge.

Remarque: à ce stade, vous pouvez recevoir ce message:

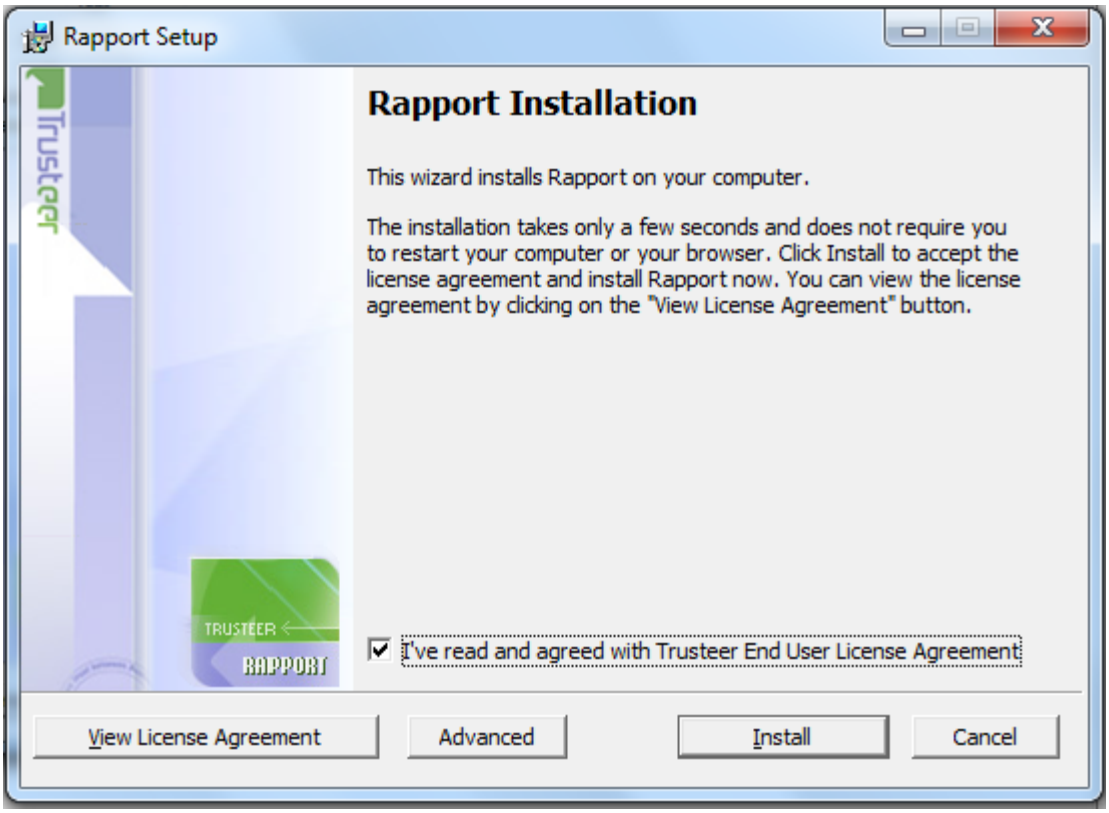


Cela signifie que votre fournisseur ne vous permet pas d'installer Trusteer Rapport depuis un compte utilisateur standard Windows. Si vous recevez ce message, basculez vers un compte administrateur, puis exécutez de nouveau l'installation.

Comment puis-je basculer vers un compte administrateur?

Basculer vers un compte d'administrateur (Windows 7) (on page 143)
Basculer vers un compte d'administrateur (XP) (on page 144)
Basculer vers un compte d'administrateur (Vista) (on page 146)

L'assistant d'installation de Rapport s'affiche.

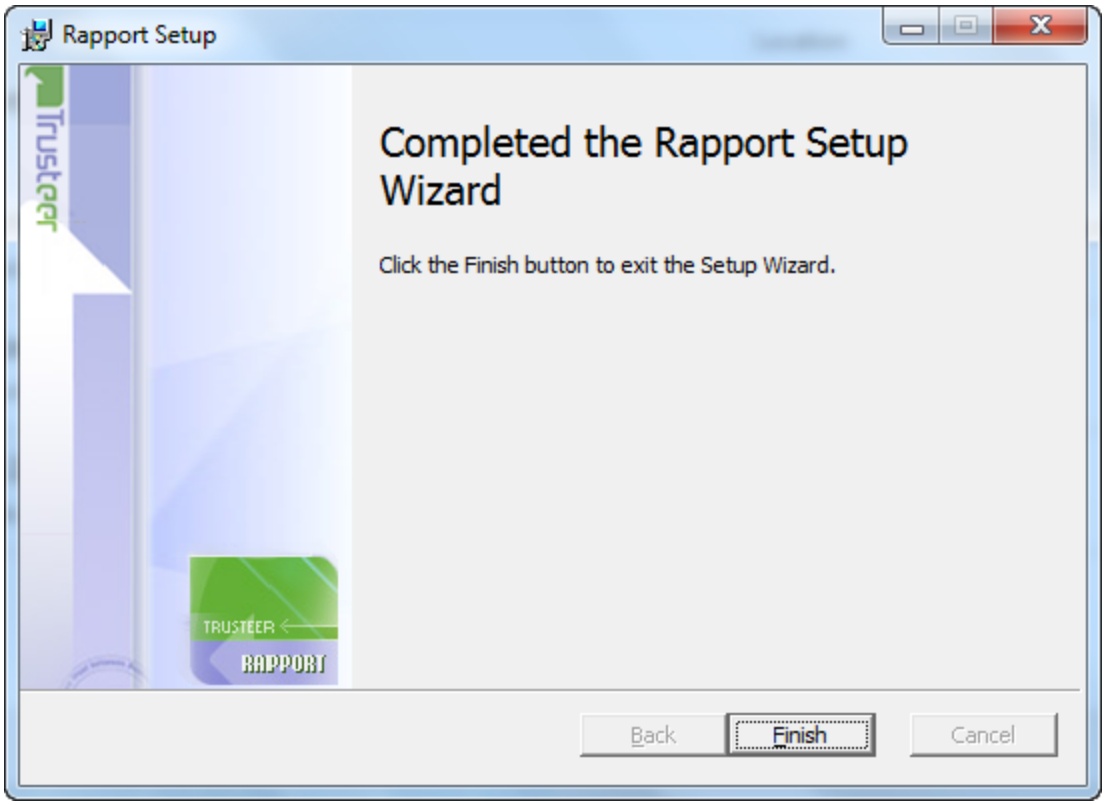


6. Si vous avez besoin que Trusteer Rapport soit compatible avec les lecteurs d'écran, cliquez sur **Advanced** (Avancé). L'écran des Options Avancées s'affiche. Cochez **I am visually impaired and regularly use assistive screen reader technologies** (je suis malvoyant et j'utilise régulièrement des technologies de lecture d'écran) et cliquez sur **Continue** (Continuer). Cela permet d'assurer la compatibilité avec les lecteurs d'écran pour narrer ce qu'indiquent les menus de Trusteer Rapport et garantit que Trusteer Rapport n'empêche pas les lecteurs d'écran de narrer les contenus affichés par le navigateur. Cela désactive également les boîtes de dialogue de codes visuels qui s'affichent lorsque vous arrêtez ou désinstallez Trusteer Rapport et qui sont requises pour plusieurs actions telles que l'arrêt et désinstallation de Rapport.

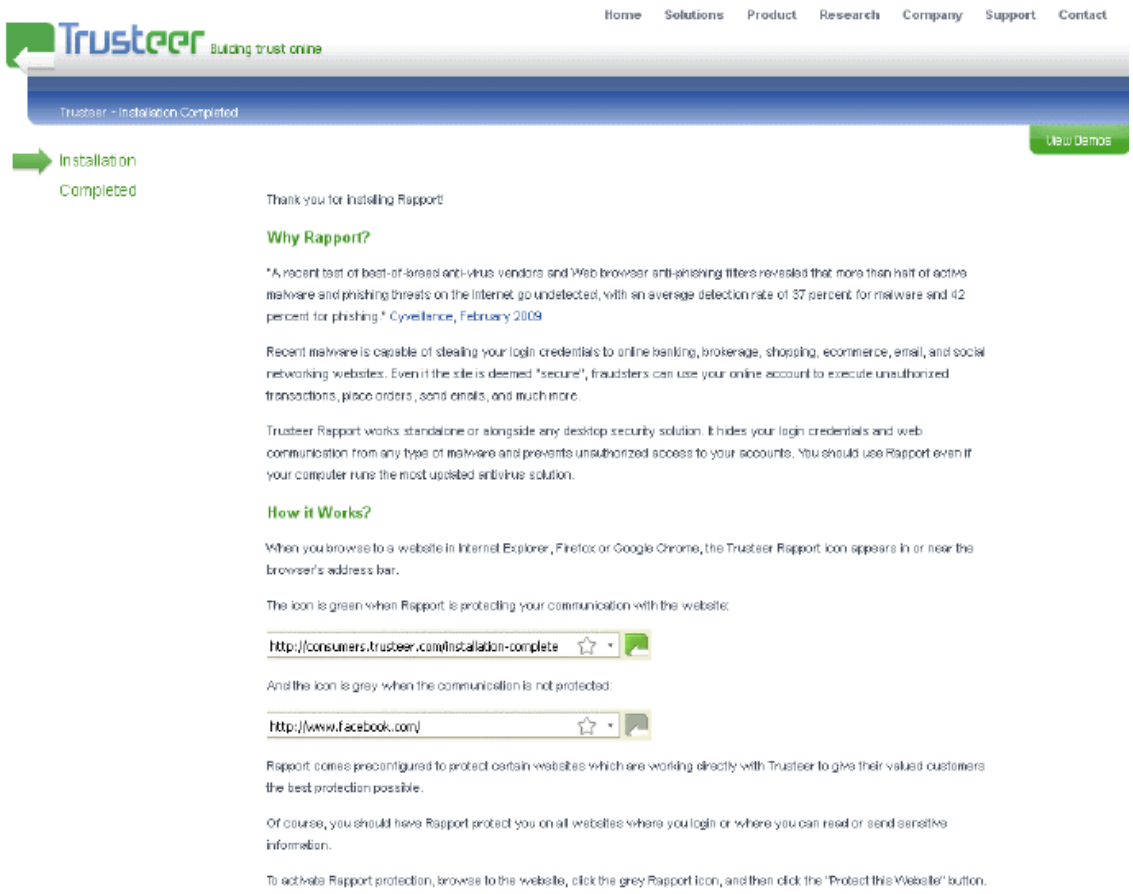
Remarque: ne cochez pas **I am visually impaired and regularly use assistive screen reader technologies** (je suis malvoyant et j'utilise régulièrement des technologies de lecture d'écran) à moins d'installer Trusteer Rapport sur un ordinateur pour lequel l'utilisation d'un logiciel de lecture d'écran est nécessaire. Ce paramètre désactive certaines fonctions de sécurité.

7. Cochez **I've read and agreed with Trusteer End User License Agreement** (J'ai lu et j'accepte le contrat de licence utilisateur final de Trusteer).

8. Cliquez sur **Install** (Installer). L'installation s'effectue. Lorsque l'installation est terminée, le bouton Finish (Terminer) s'affiche dans l'assistant.



9. Cliquez sur **Finish** (Terminer). Après quelques secondes, Trusteer Rapport ouvre une nouvelle fenêtre de navigateur pour effectuer un bref test de compatibilité. Lorsque le test est terminé, Trusteer Rapport ouvre la page de remerciement dans votre navigateur.



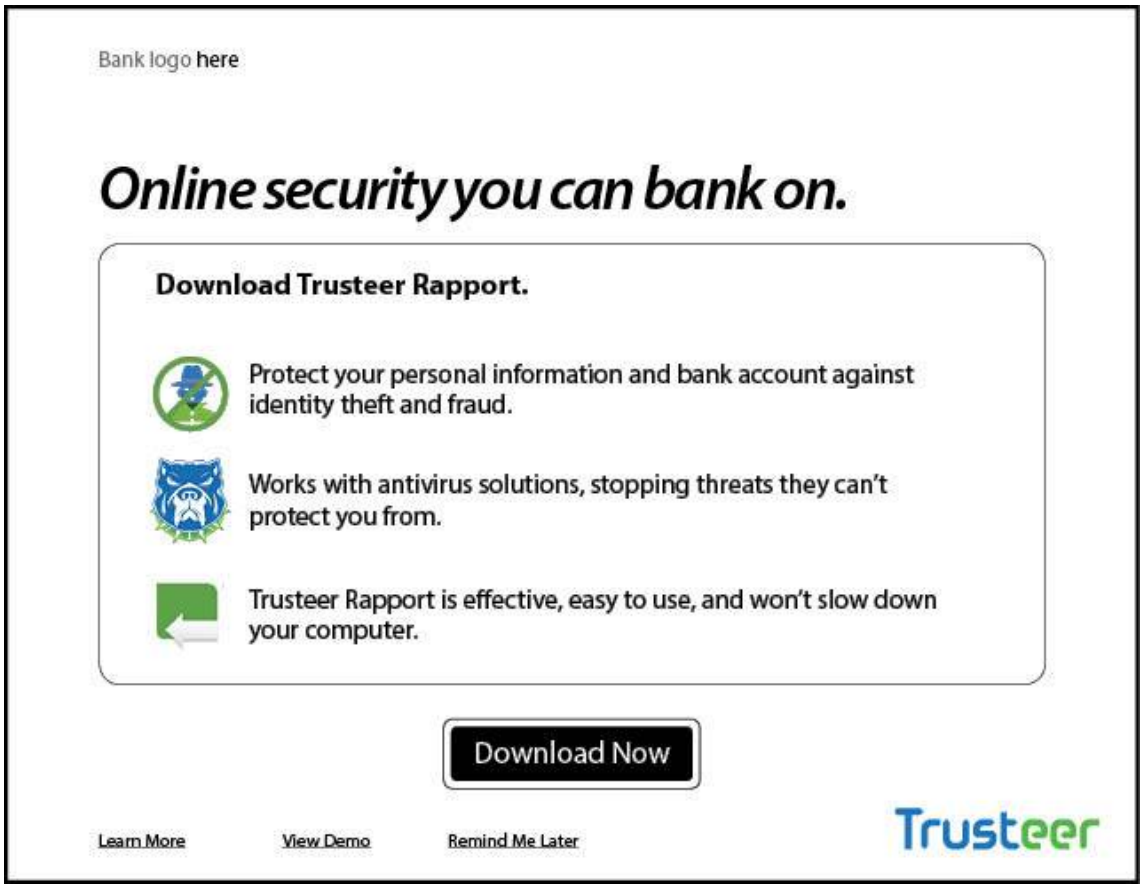
L'installation est terminée.

Installation de Trusteer Rapport sur Windows XP utilisant Internet Explorer

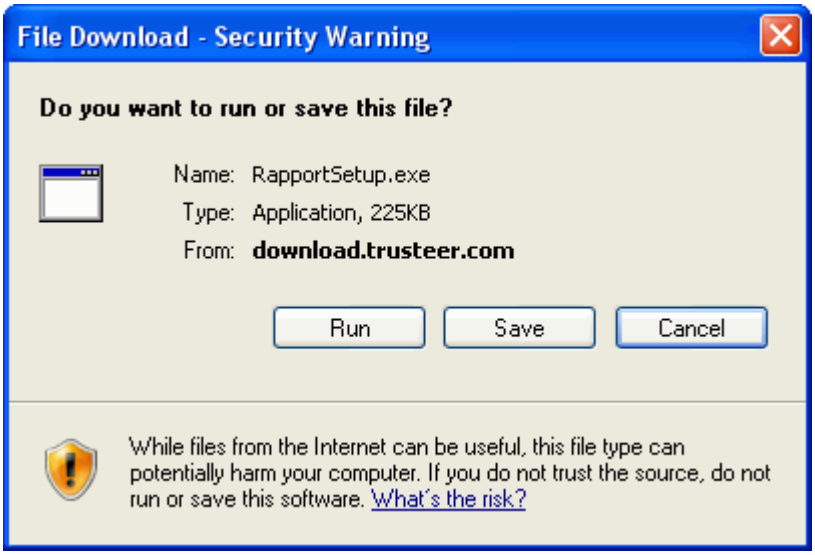
Cette procédure explique comment télécharger et installer Trusteer Rapport si vous êtes sous Windows XP et utilisez Microsoft Internet Explorer comme navigateur.

➡ **Pour installer Trusteer Rapport:**

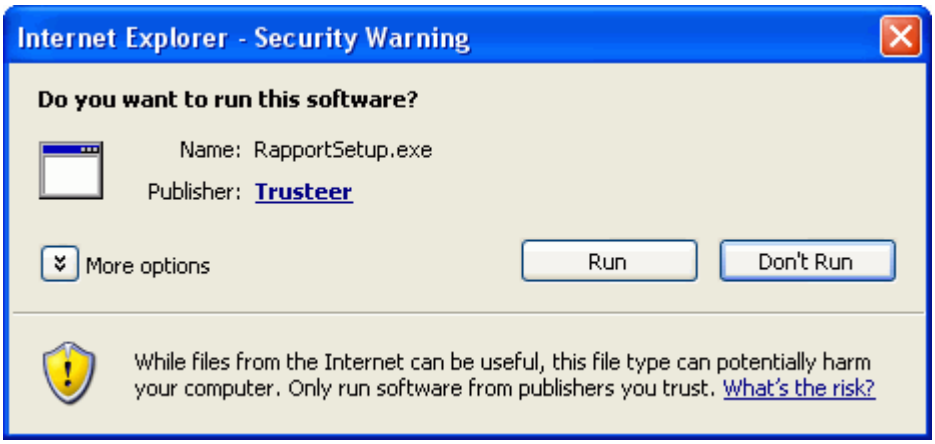
1. Accédez à la page de connexion de votre entreprise. Si celle-ci propose Trusteer Rapport au téléchargement, vous verrez un message montrant un bouton « **Download Now** » (Télécharger maintenant). Par exemple:



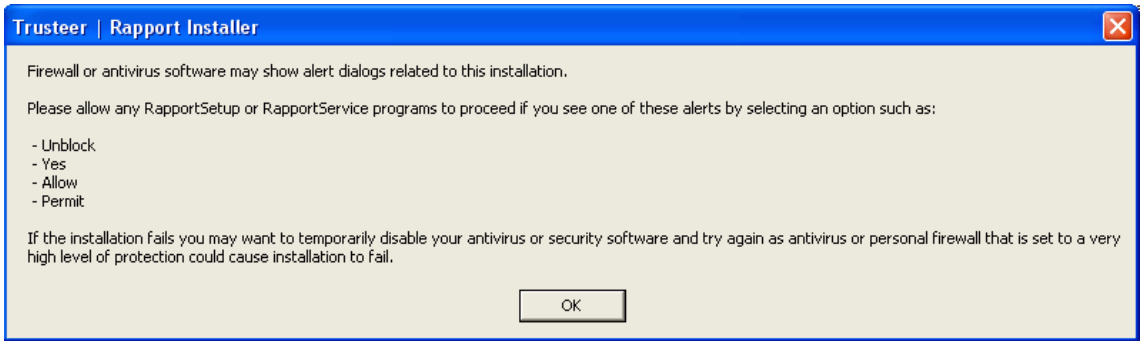
2. Cliquez sur **Download Now** (Télécharger maintenant). La boîte de dialogue **File Download Now - Security Warning** (Télécharger le fichier maintenant - alerte de sécurité) s'afficher en vous demandant si vous souhaitez exécuter ou enregistrer le fichier RapportSetup.exe.



3. Cliquez sur **Run** (Exécuter). Une autre boîte de dialogue s'affiche quelques secondes plus tard et vous demande « Do you want to run this software? » (Voulez-vous exécuter ce logiciel ?)

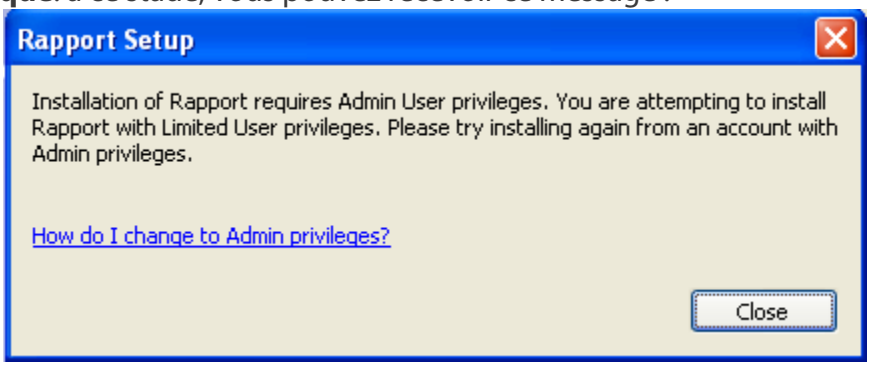


4. Cliquez sur **Run** (Exécuter) de nouveau. La boîte de dialogue suivante apparaît.



5. Cliquez sur **OK**. Trusteer Rapport se télécharge.

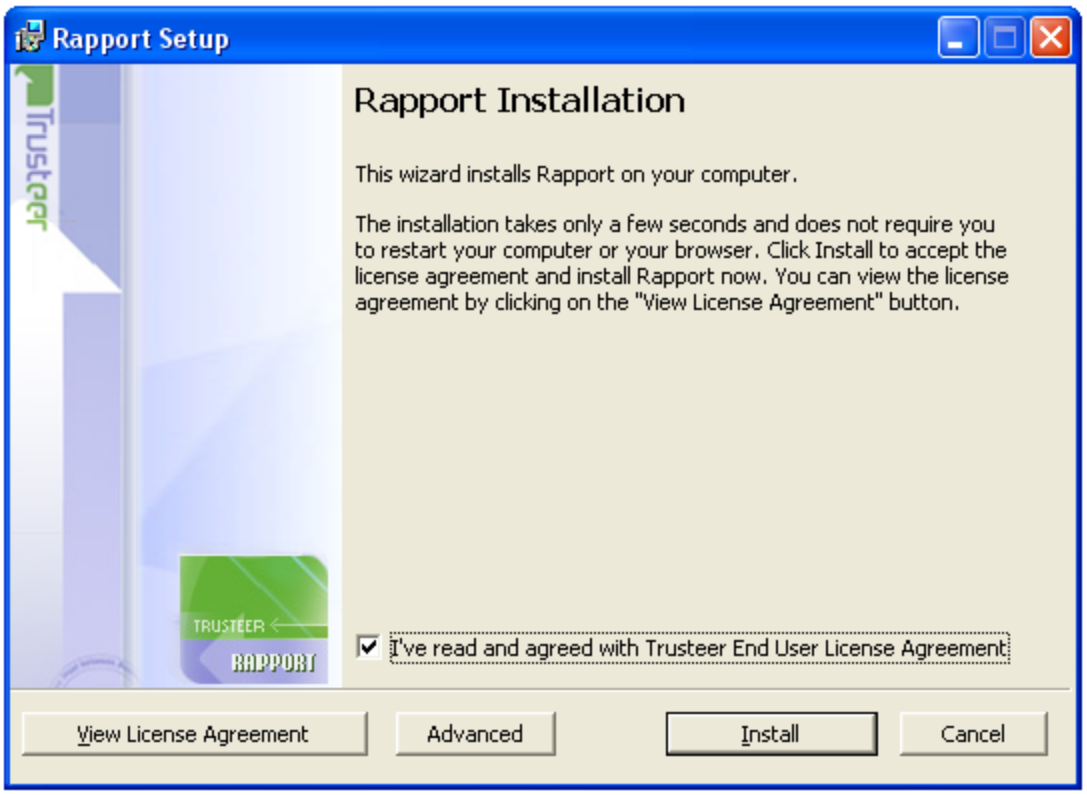
Remarque: à ce stade, vous pouvez recevoir ce message :



Cela signifie que votre fournisseur ne vous permet pas d'installer Trusteer Rapport depuis un compte utilisateur standard Windows. Si vous recevez ce message, basculez vers un compte administrateur, puis exécutez de nouveau l'installation.
Comment puis-je basculer vers un compte administrateur?

- Basculer vers un compte d'administrateur (Windows 7) (on page 143)
- Basculer vers un compte d'administrateur (XP) (on page 144)
- Basculer vers un compte d'administrateur (Vista) (on page 146)

L'assistant d'installation de Rapport s'affiche.

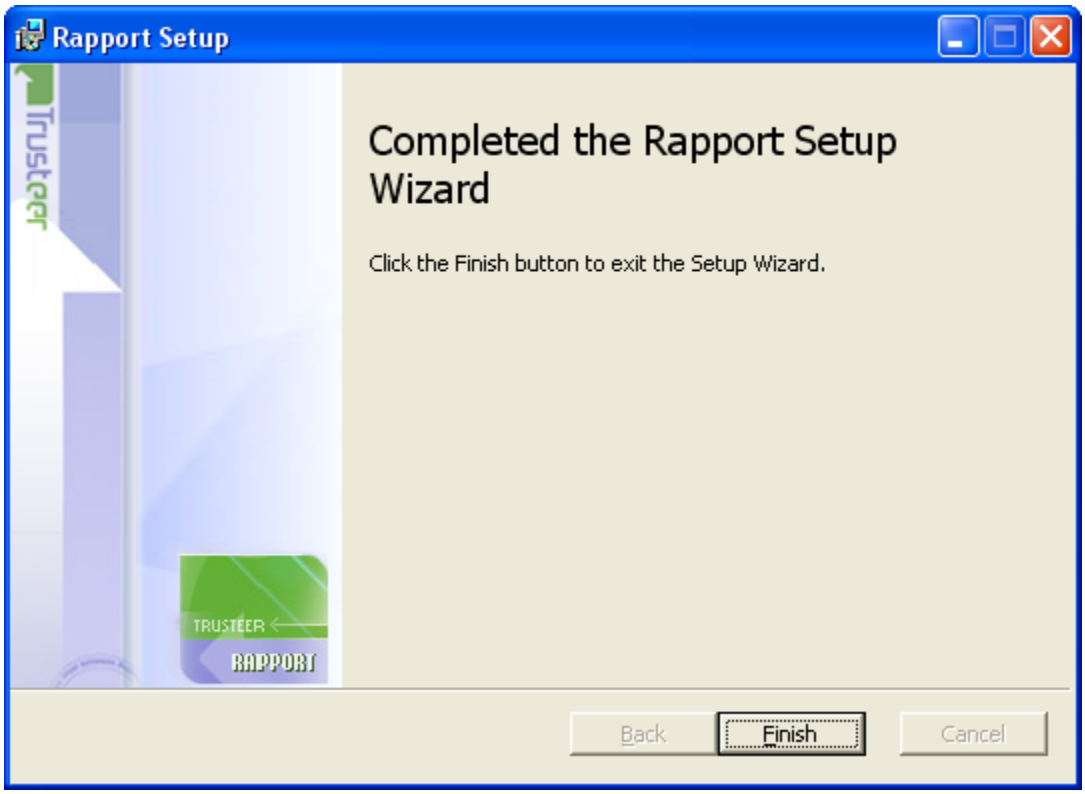


6. Si vous avez besoin que Trusteer Rapport soit compatible avec les lecteurs d'écran, cliquez sur **Advanced** (Avancé). L'écran des Options Avancées s'affiche. Cochez **I am visually impaired and regularly use assistive screen reader technologies** (je suis malvoyant et j'utilise régulièrement des technologies de lecture d'écran) et cliquez sur **Continue** (Continuer). Cela permet d'assurer la compatibilité avec les lecteurs d'écran pour narrer ce qu'indiquent les menus de Trusteer Rapport et garantit que Trusteer Rapport n'empêche pas les lecteurs d'écran de narrer les contenus affichés par le navigateur. Cela désactive également les boîtes de dialogue de codes visuels qui s'affichent lorsque vous arrêtez ou désinstallez Trusteer Rapport et qui sont requises pour plusieurs actions telles que l'arrêt et désinstallation de Rapport.

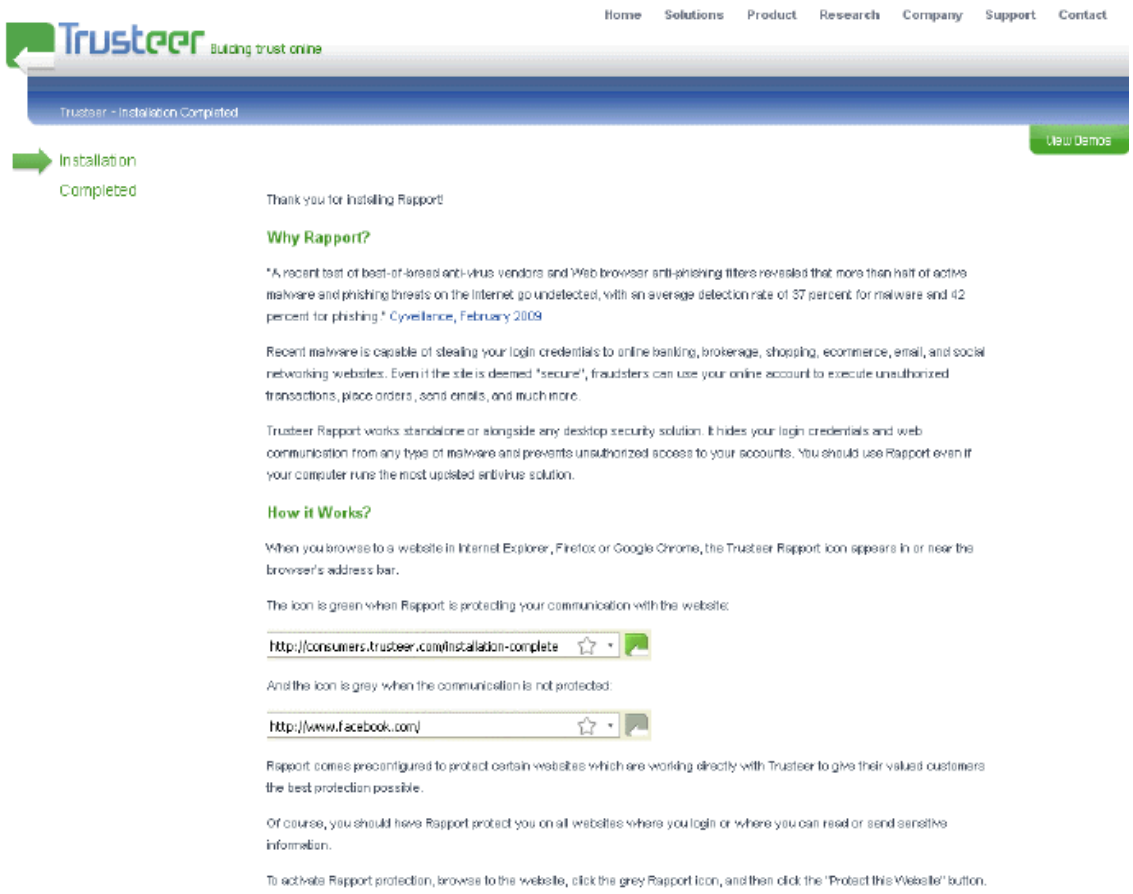
Remarque: ne cochez pas **I am visually impaired and regularly use assistive screen reader technologies** (je suis malvoyant et j'utilise régulièrement des technologies de lecture d'écran) à moins d'installer Trusteer Rapport sur un ordinateur pour lequel l'utilisation d'un logiciel de lecture d'écran est nécessaire. Ce paramètre désactive certaines fonctions de sécurité.

7. Cochez **I've read and agreed with Trusteer End User License Agreement** (J'ai lu et j'accepte le contrat de licence utilisateur final de Trusteer).

8. Cliquez sur **Install** (Installer). L'installation s'effectue. Lorsque l'installation est terminée, le bouton Finish (Terminer) s'affiche dans l'assistant.



9. Cliquez sur **Finish** (Terminer). Après quelques secondes, Trusteer Rapport ouvre une nouvelle fenêtre de navigateur pour effectuer un bref test de compatibilité. Lorsque le test est terminé, Trusteer Rapport ouvre la page de remerciement dans votre navigateur.



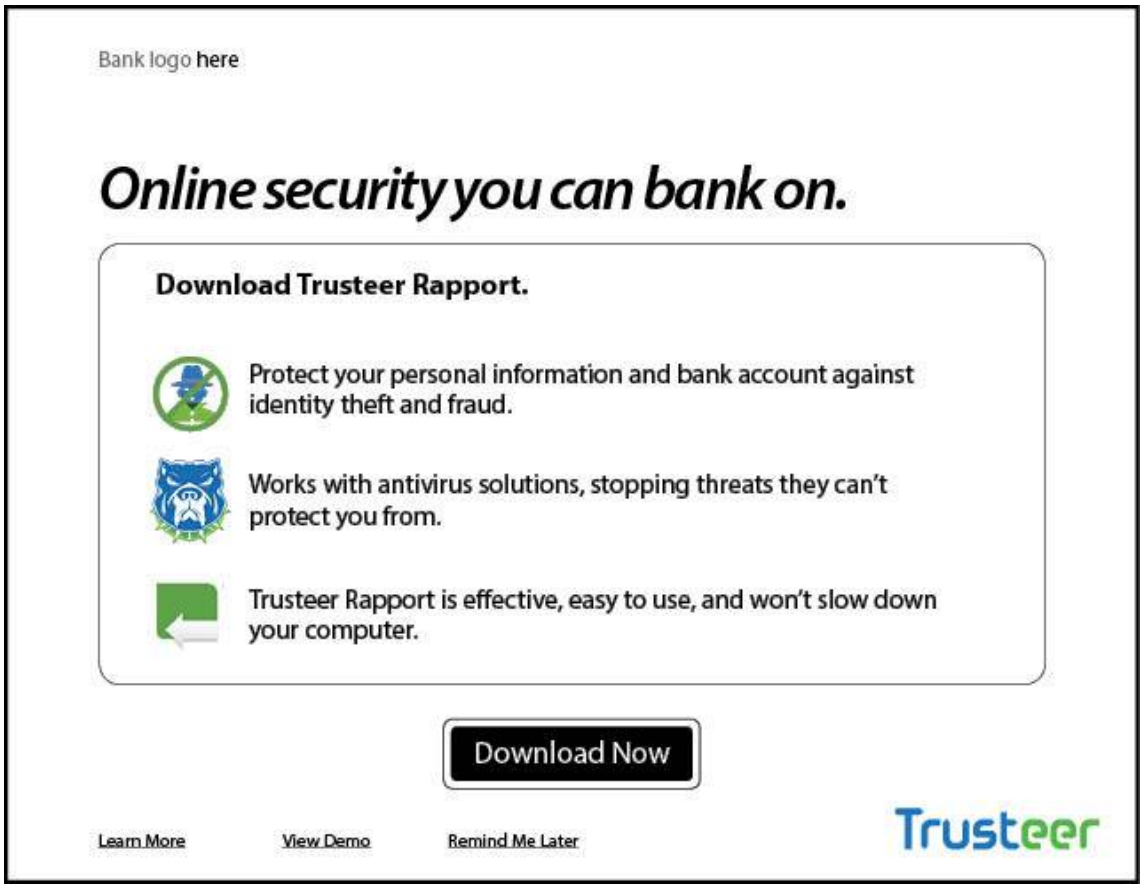
L'installation est terminée.

Installation de Trusteer Rapport sur Windows 7 utilisant Firefox

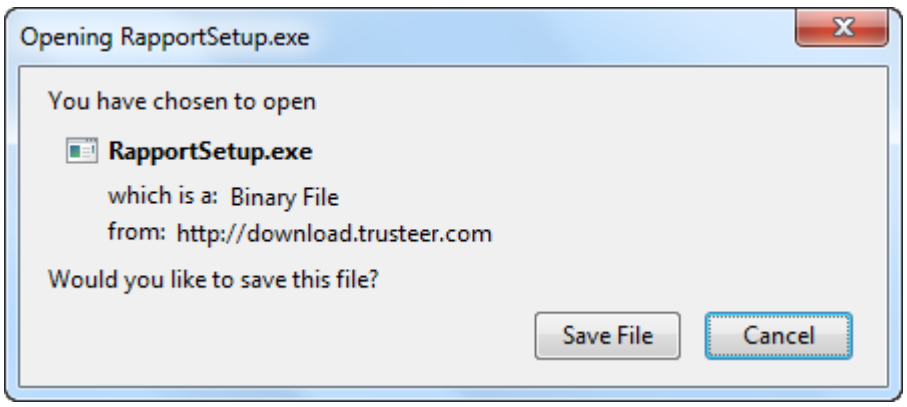
Cette procédure explique comment télécharger et installer Trusteer Rapport si vous êtes sous Windows 7 et utilisez Mozilla Firefox comme navigateur.

➡ **Pour installer Trusteer Rapport :**

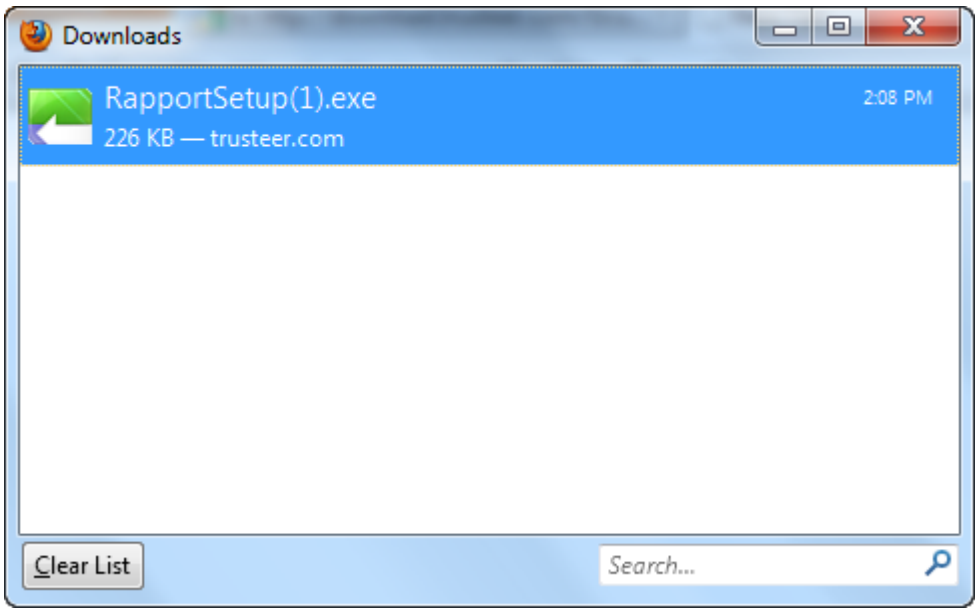
1. Accédez à la page de connexion de votre entreprise. Si celle-ci propose Trusteer Rapport au téléchargement, vous verrez un message montrant un bouton **Download Now** (Télécharger maintenant). Par exemple :



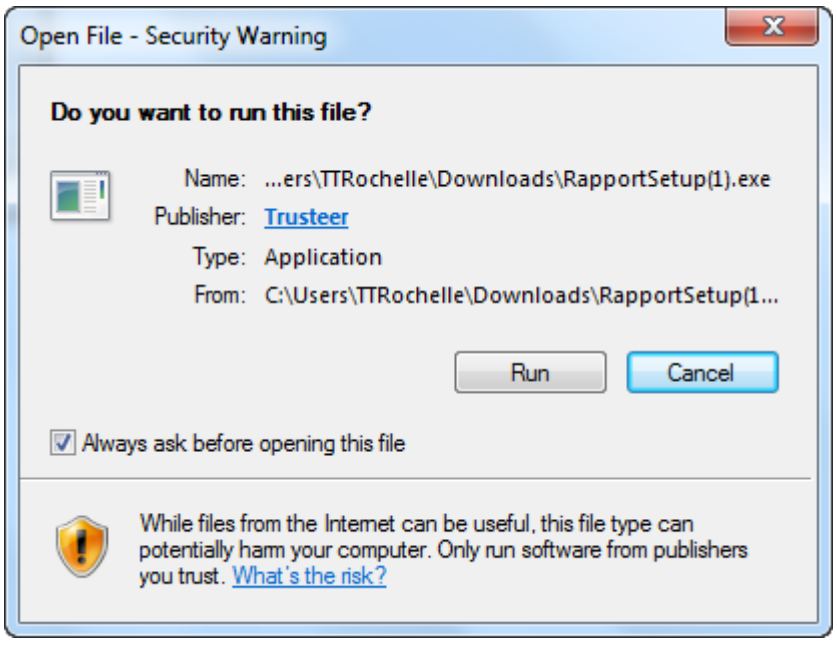
2. Cliquez sur **Download Now**. (Télécharger maintenant)



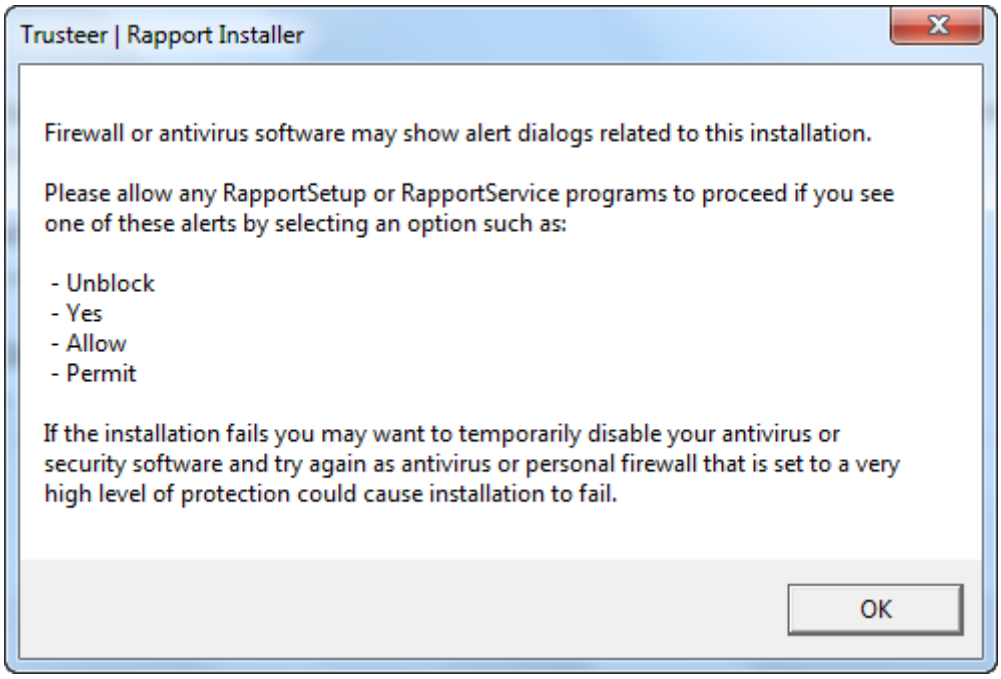
3. Cliquez sur **Save File** (Enregistrer le fichier). La liste de vos derniers téléchargements s'affiche.



4. Double-cliquez sur le fichier RapportSetup.exe en haut de la liste. Un avertissement de sécurité apparaît.

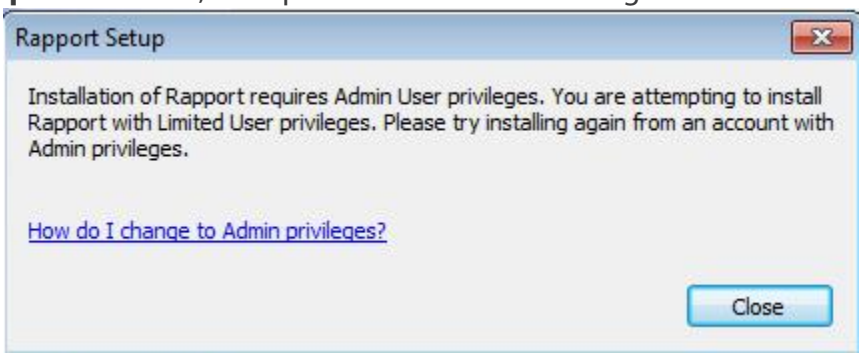


5. Cliquez sur **Run** (Exécuter) et la boîte de dialogue suivante apparaît.



6. Cliquez sur **OK**. Trusteer Rapport se télécharge.

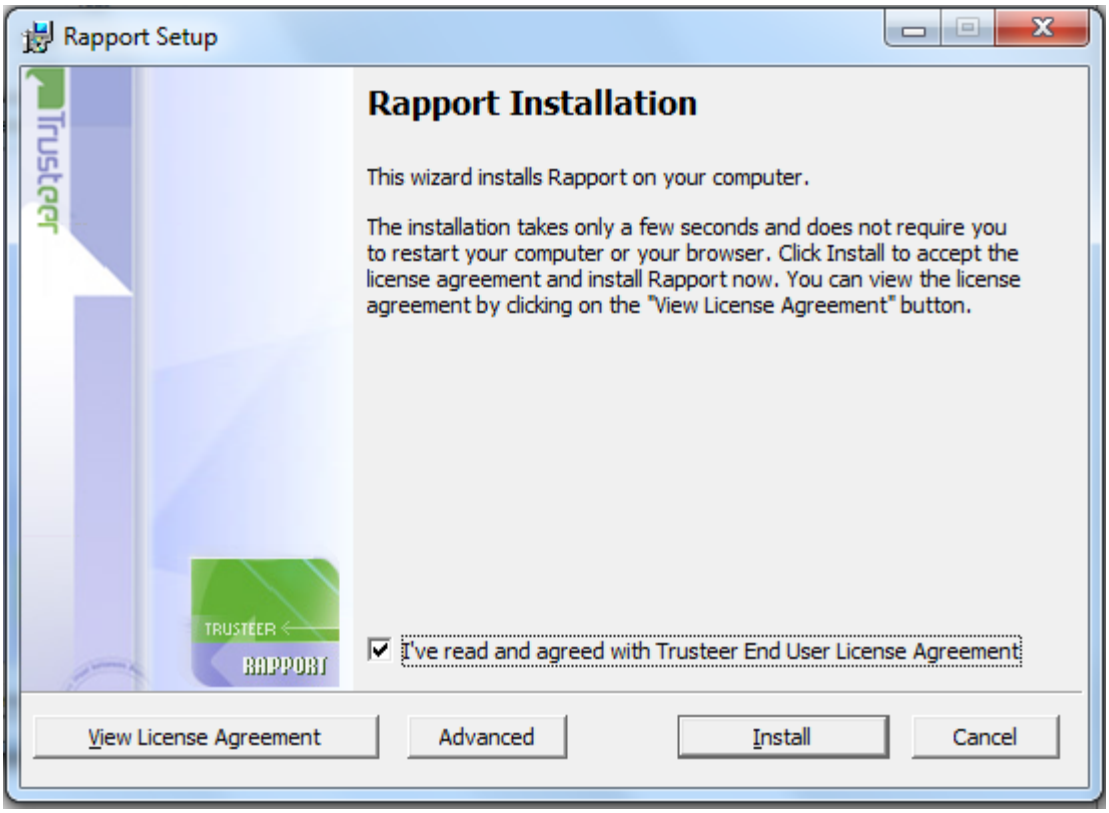
Remarque: à ce stade, vous pouvez recevoir ce message :



Cela signifie que votre fournisseur ne vous permet pas d'installer Trusteer Rapport depuis un compte utilisateur standard Windows. Si vous recevez ce message, basculez vers un compte administrateur, puis exécutez de nouveau l'installation.
Comment puis-je basculer vers un compte administrateur?

- Basculer vers un compte d'administrateur (Windows 7) (on page 143)
- Basculer vers un compte d'administrateur (XP) (on page 144)
- Basculer vers un compte d'administrateur (Vista) (on page 146)

L'assistant d'installation de Rapport s'affiche.

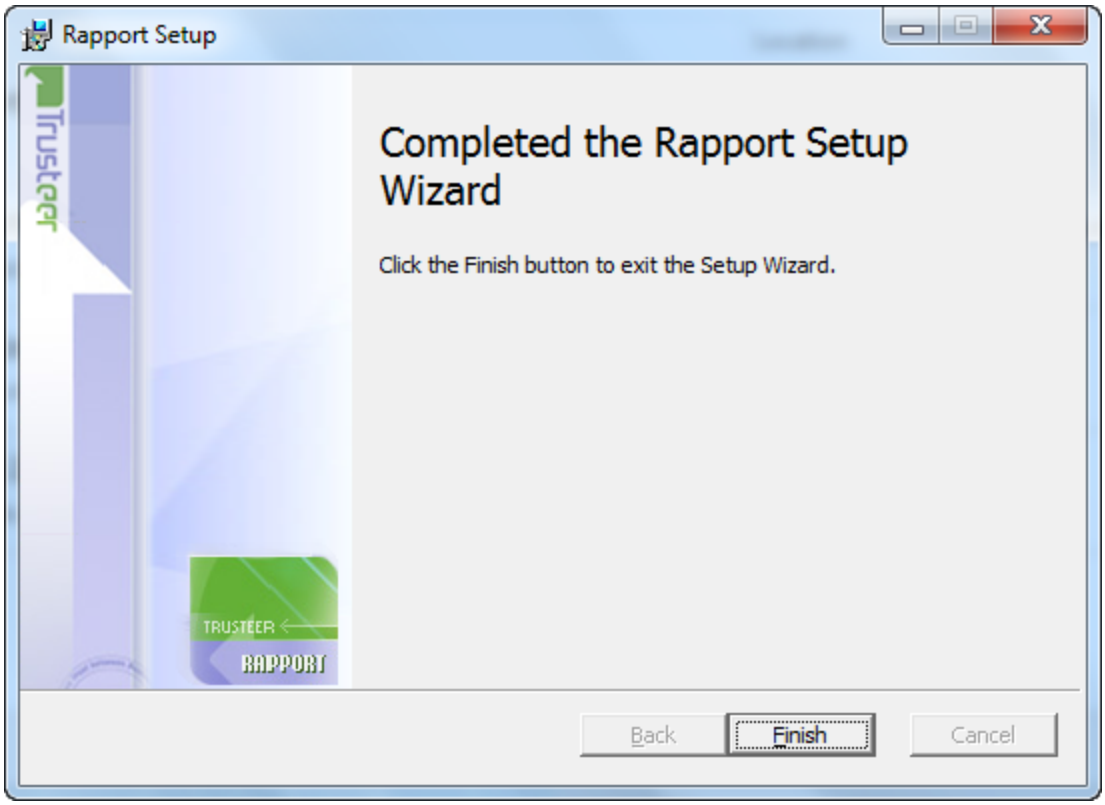


7. Si vous avez besoin que Trusteer Rapport soit compatible avec les lecteurs d'écran, cliquez sur **Advanced** (Avancé). L'écran des Options Avancées s'affiche. Cochez **I am visually impaired and regularly use assistive screen reader technologies** (je suis malvoyant et j'utilise régulièrement des technologies de lecture d'écran) et cliquez sur **Continue** (Continuer). Cela permet d'assurer la compatibilité avec les lecteurs d'écran pour narrer ce qu'indiquent les menus de Trusteer Rapport et garantit que Trusteer Rapport n'empêche pas les lecteurs d'écran de narrer les contenus affichés par le navigateur. Cela désactive également les boîtes de dialogue de codes visuels qui s'affichent lorsque vous arrêtez ou désinstallez Trusteer Rapport et qui sont requises pour plusieurs actions telles que l'arrêt et désinstallation de Rapport.

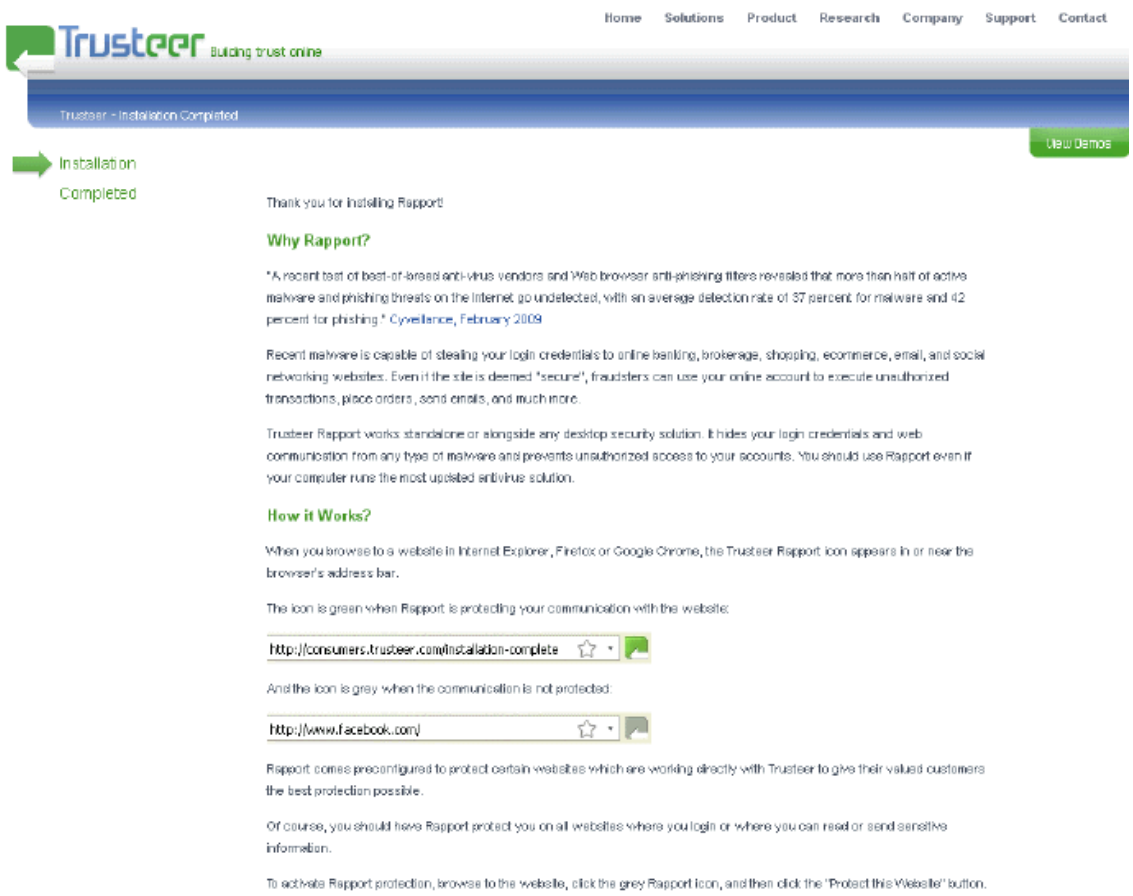
Remarque: ne cochez pas **I am visually impaired and regularly use assistive screen reader technologies** à moins d'installer Trusteer Rapport sur un ordinateur pour lequel l'utilisation d'un logiciel de lecture d'écran est nécessaire. Ce paramètre désactive certaines fonctions de sécurité.

8. Cochez **I've read and agreed with Trusteer End User License Agreement** (J'ai lu et j'accepte le contrat de licence utilisateur final de Trusteer).

9. Cliquez sur **Install** (Installer). L'installation s'effectue. Lorsque l'installation est terminée, le bouton Finish (Terminer) s'affiche dans l'assistant.



10. Cliquez sur Finish (Terminer). Après quelques secondes, Trusteer Rapport ouvre une nouvelle fenêtre de navigateur pour effectuer un bref test de compatibilité. Lorsque le test est terminé, Trusteer Rapport ouvre la page de remerciement dans votre navigateur.



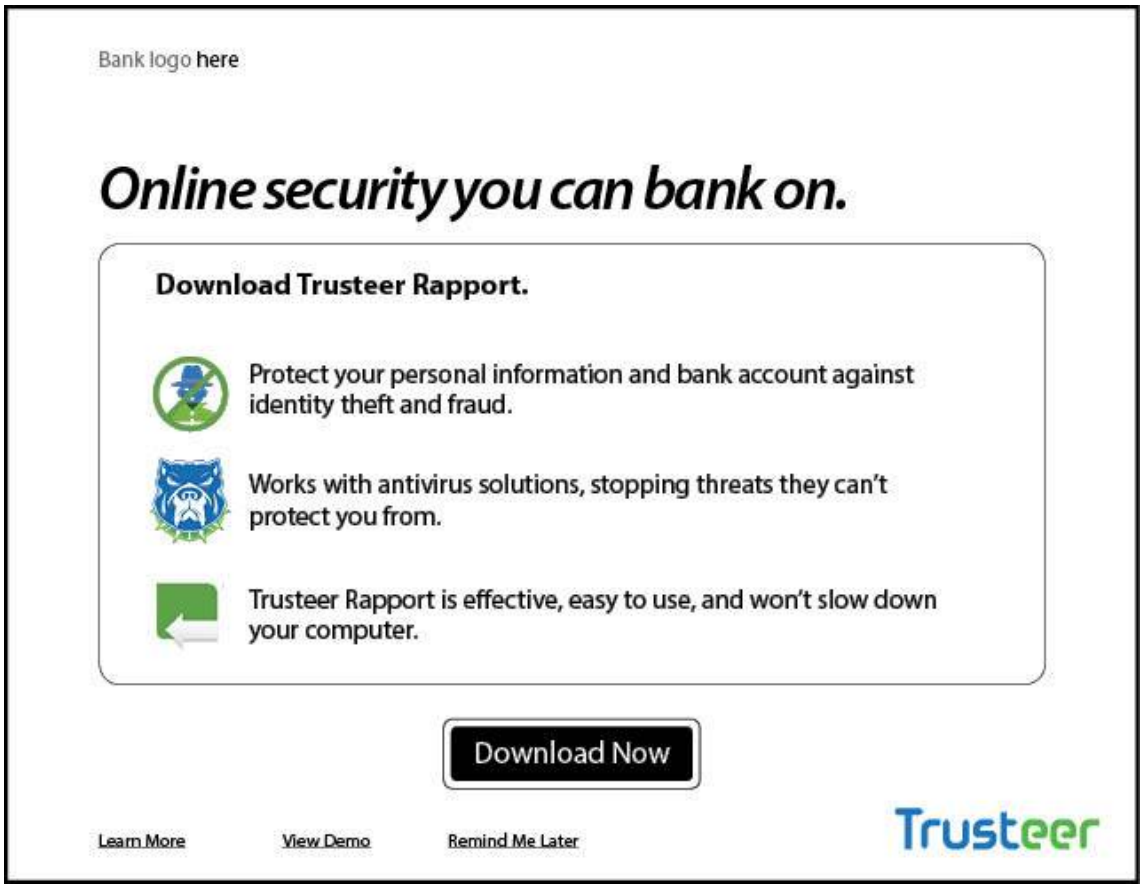
L'installation est terminée.

Installation de Trusteer Rapport sur Windows 7 utilisant Google Chrome

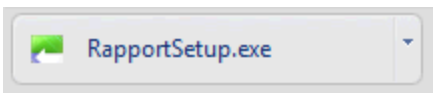
Cette procédure explique comment télécharger et installer Trusteer Rapport si vous êtes sous Windows 7 et utilisez Google Chrome comme navigateur.

➡ **Pour installer Trusteer Rapport :**

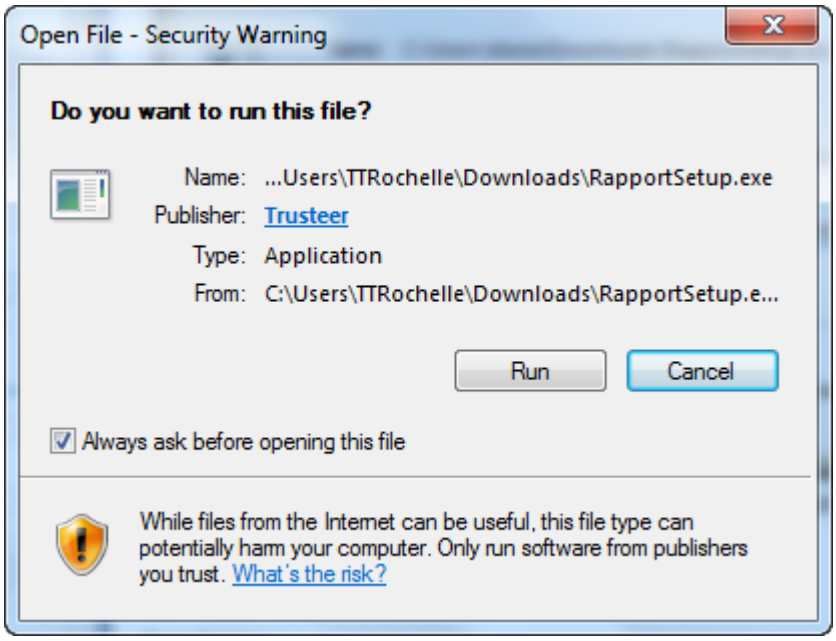
1. Accédez à la page de connexion de votre entreprise. Si celle-ci propose Trusteer Rapport au téléchargement, vous verrez un message montrant un bouton **Download Now** (Télécharger maintenant). Par exemple :



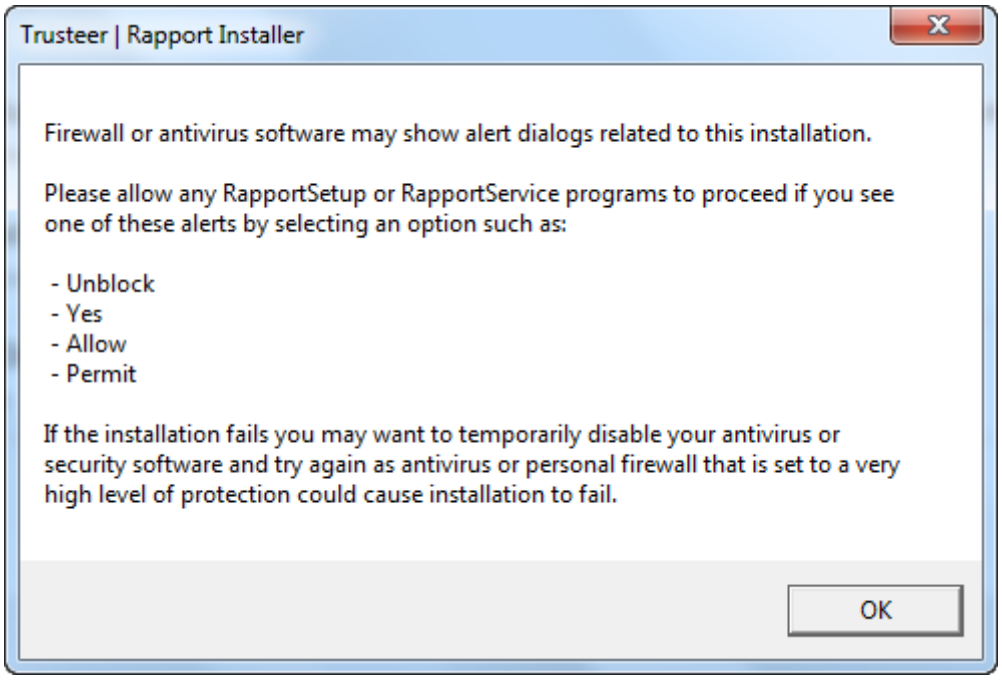
2. Cliquez sur **Download Now**. (Télécharger maintenant)
3. Selon les paramètres de votre navigateur, un message de sécurité peut apparaître au bas de la fenêtre de votre navigateur, vous demandant si vous souhaitez télécharger RapportSetup.exe. Cliquez sur **Save** (Enregistrer). Le fichier se télécharge et un bouton apparaît en bas à gauche de votre fenêtre de navigateur, affichant le nom du fichier téléchargé.



4. Cliquez sur le bouton. Un avertissement de sécurité apparaît, vous demandant si vous souhaitez exécuter le fichier.

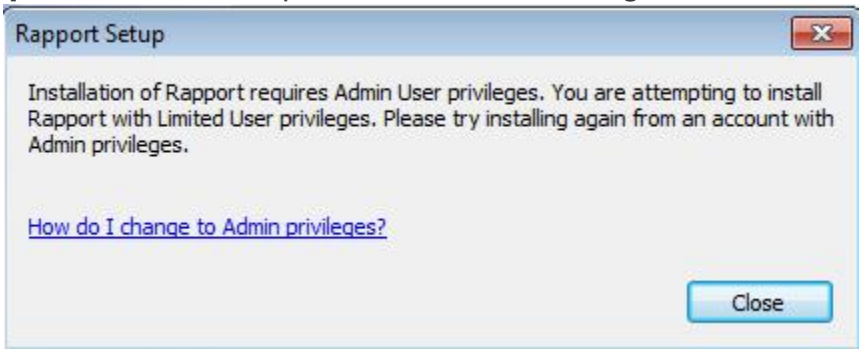


5. Cliquez sur **Run**. (Exécuter) La boîte de dialogue suivante apparaît.



6. Cliquez sur OK. Trusteer Rapport se télécharge.

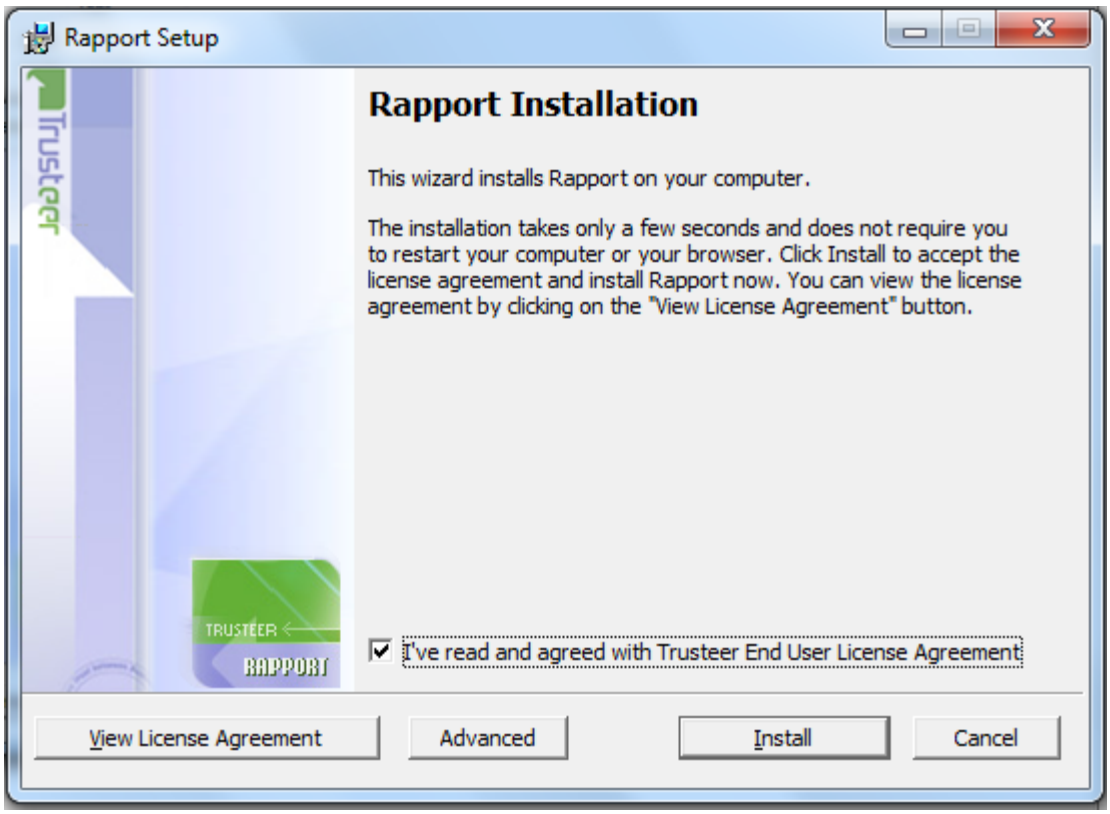
Remarque: à ce stade, vous pouvez recevoir ce message:



Cela signifie que votre fournisseur ne vous permet pas d'installer Trusteer Rapport depuis un compte utilisateur standard Windows. Si vous recevez ce message, basculez vers un compte administrateur, puis exécutez de nouveau l'installation.
Comment puis-je basculer vers un compte administrateur?

- Basculer vers un compte d'administrateur (Windows 7) (on page 143)
- Basculer vers un compte d'administrateur (XP) (on page 144)
- Basculer vers un compte d'administrateur (Vista) (on page 146)

L'assistant d'installation de Rapport s'affiche.

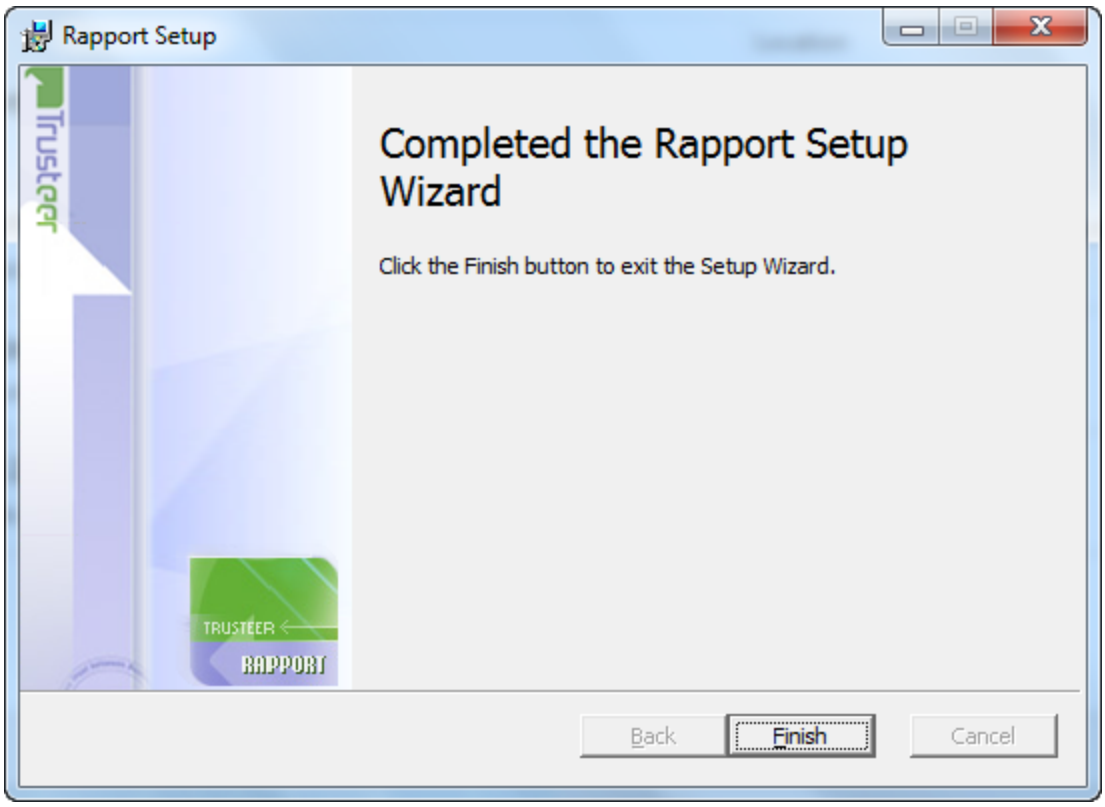


7. Si vous avez besoin que Trusteer Rapport soit compatible avec les lecteurs d'écran, cliquez sur **Advanced** (Avancé). L'écran des Options Avancées s'affiche. Cochez **I am visually impaired and regularly use assistive screen reader technologies** (je suis malvoyant et j'utilise régulièrement des technologies de lecture d'écran) et cliquez sur **Continue** (Continuer). Cela permet d'assurer la compatibilité avec les lecteurs d'écran pour narrer ce qu'indiquent les menus de Trusteer Rapport et garantit que Trusteer Rapport n'empêche pas les lecteurs d'écran de narrer les contenus affichés par le navigateur. Cela désactive également les boîtes de dialogue de codes visuels qui s'affichent lorsque vous arrêtez ou désinstallez Trusteer Rapport et qui sont requises pour plusieurs actions telles que l'arrêt et désinstallation de Rapport.

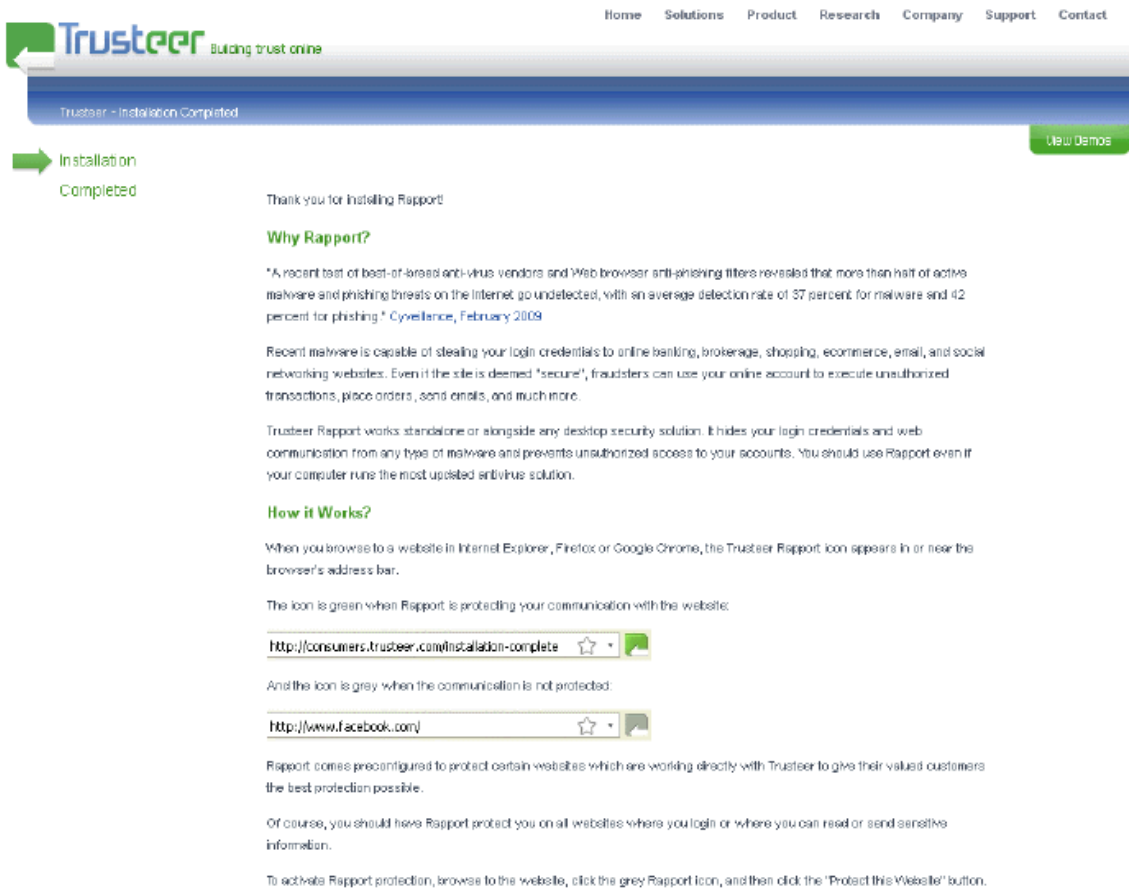
Remarque: ne cochez pas **I am visually impaired and regularly use assistive screen reader technologies** (je suis malvoyant et j'utilise régulièrement des technologies de lecture d'écran) à moins d'installer Trusteer Rapport sur un ordinateur pour lequel l'utilisation d'un logiciel de lecture d'écran est nécessaire. Ce paramètre désactive certaines fonctions de sécurité.

8. Cochez **I've read and agreed with Trusteer End User License Agreement** (J'ai lu et j'accepte le contrat de licence utilisateur final de Trusteer).

9. Cliquez sur **Install** (Installer). L'installation s'effectue. Lorsque l'installation est terminée, le bouton Finish (Terminer) s'affiche dans l'assistant.



10. Cliquez sur **Finish** (Terminer). Après quelques secondes, Trusteer Rapport ouvre une nouvelle fenêtre de navigateur pour effectuer un bref test de compatibilité. Lorsque le test est terminé, Trusteer Rapport ouvre la page de remerciement dans votre navigateur.



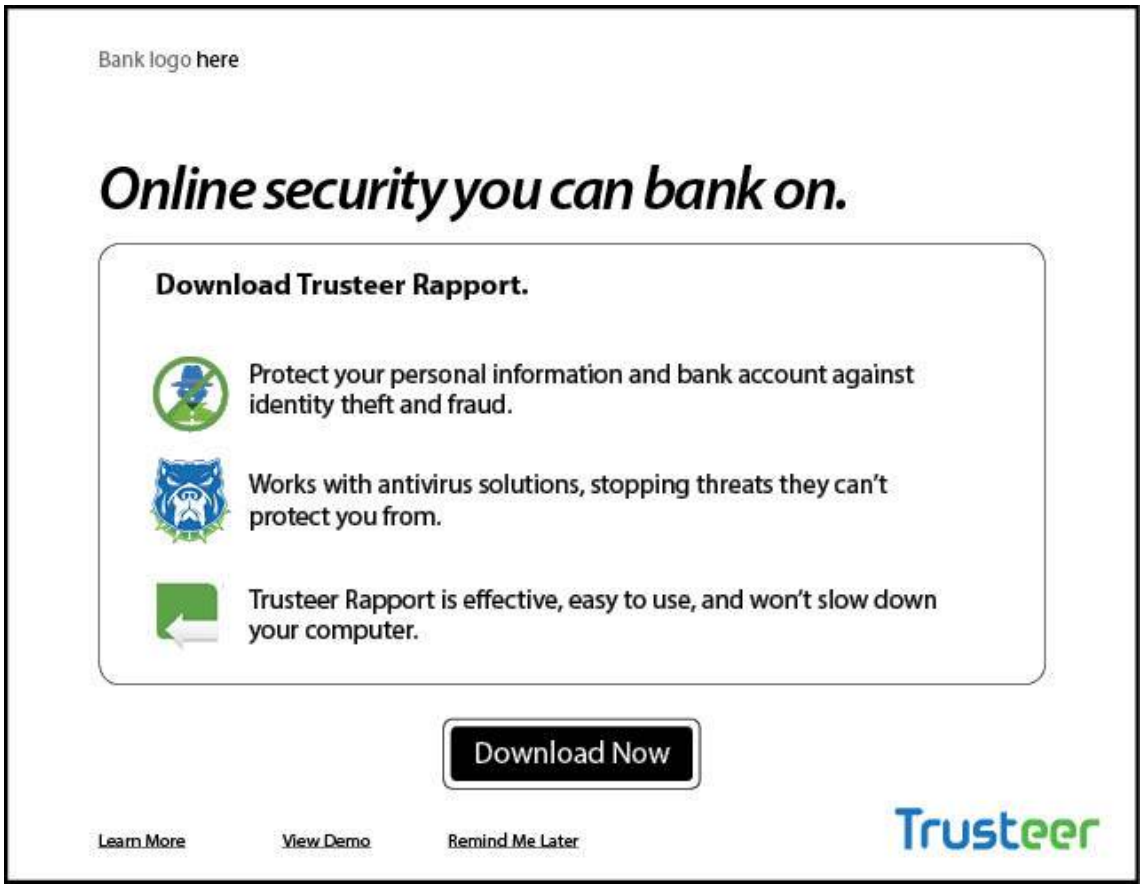
L'installation est terminée.

Installation de Trusteer Rapport sur Windows XP utilisant Firefox

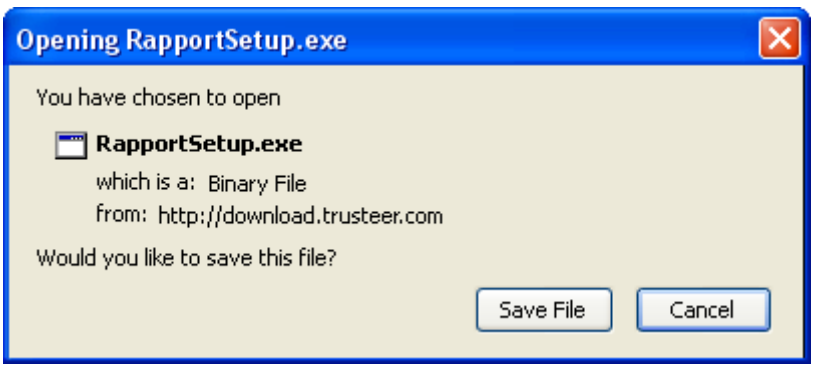
Cette procédure explique comment télécharger et installer Trusteer Rapport si vous êtes sous Windows XP et utilisez Mozilla Firefox comme navigateur.

➡ **Pour installer Trusteer Rapport:**

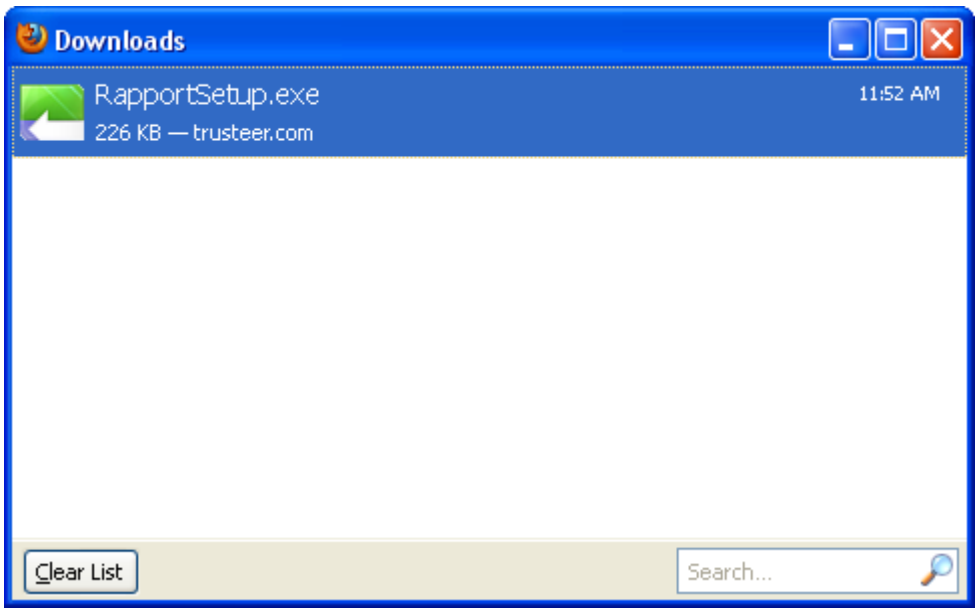
1. Accédez à la page de connexion de votre entreprise. Si celle-ci propose Trusteer Rapport au téléchargement, vous verrez un message montrant un bouton **Download Now** (Télécharger maintenant). Par exemple :



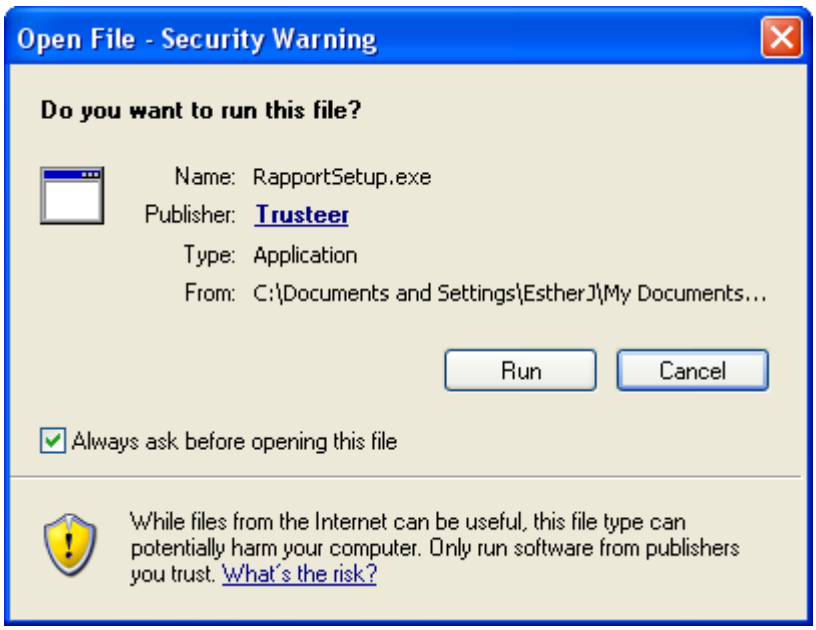
2. Cliquez sur **Download Now**. (Télécharger maintenant)



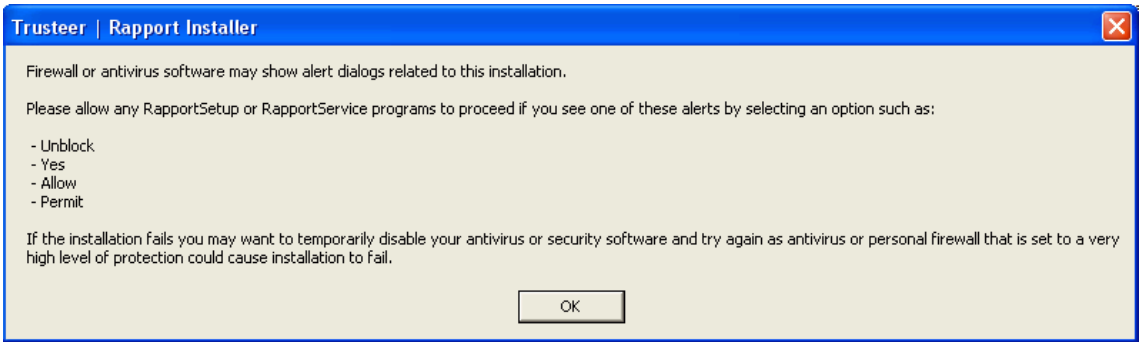
3. Cliquez sur **Save File** (Enregistrer le fichier). La liste de vos derniers téléchargements s'affiche.



4. Double-cliquez sur le fichier RapportSetup.exe en haut de la liste. Un avertissement de sécurité apparaît.

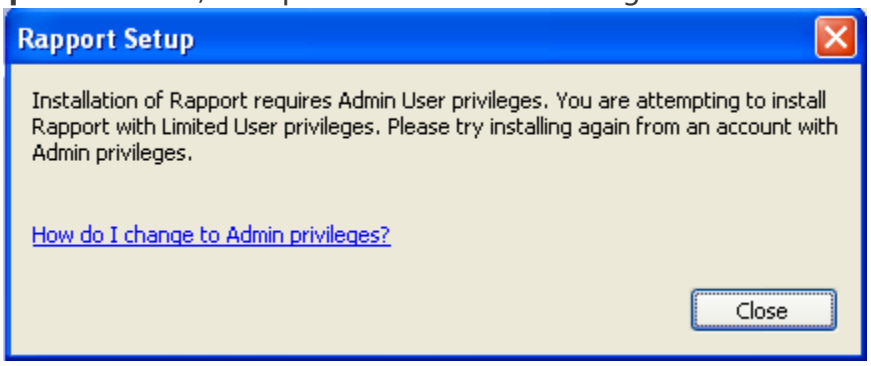


5. Cliquez sur **Run** (Exécuter). La boîte de dialogue suivante apparaît.



6. Cliquez sur **OK**. Trusteer Rapport se télécharge.

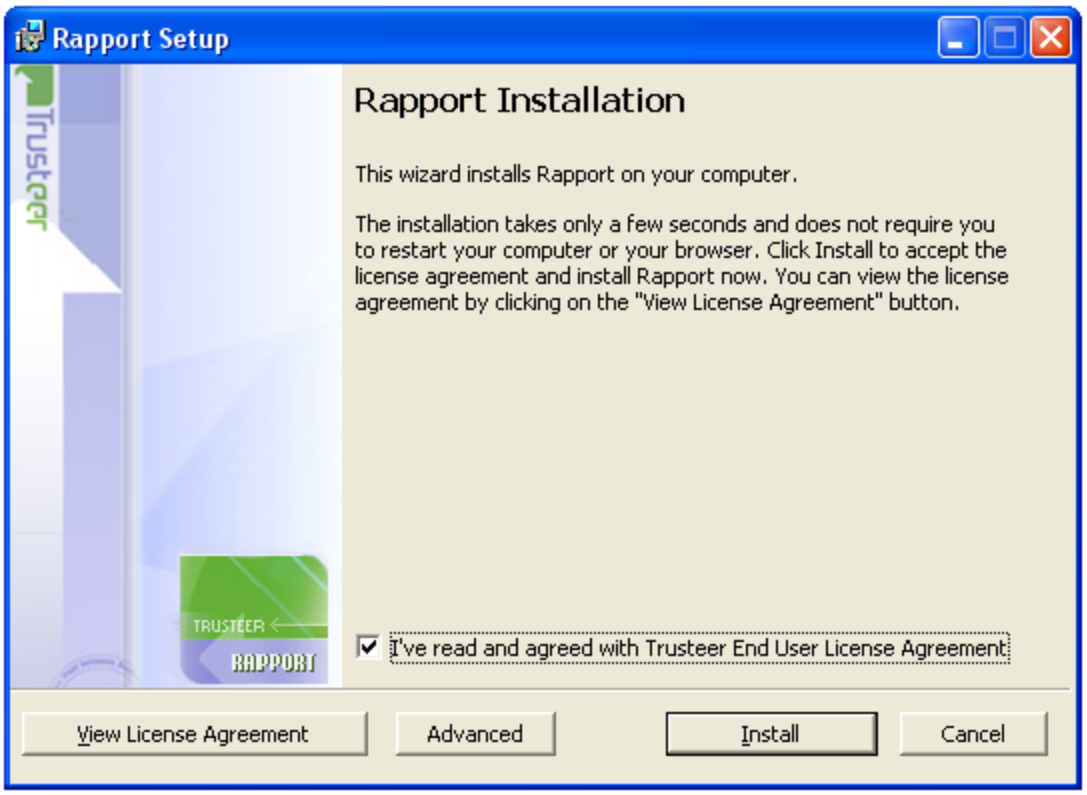
Remarque: à ce stade, vous pouvez recevoir ce message :



Cela signifie que votre fournisseur ne vous permet pas d'installer Trusteer Rapport depuis un compte utilisateur standard Windows. Si vous recevez ce message, basculez vers un compte administrateur, puis exécutez de nouveau l'installation.
Comment puis-je basculer vers un compte administrateur?

- Basculer vers un compte d'administrateur (Windows 7) (on page 143)
- Basculer vers un compte d'administrateur (XP) (on page 144)
- Basculer vers un compte d'administrateur (Vista) (on page 146)

L'assistant d'installation de Rapport s'affiche.

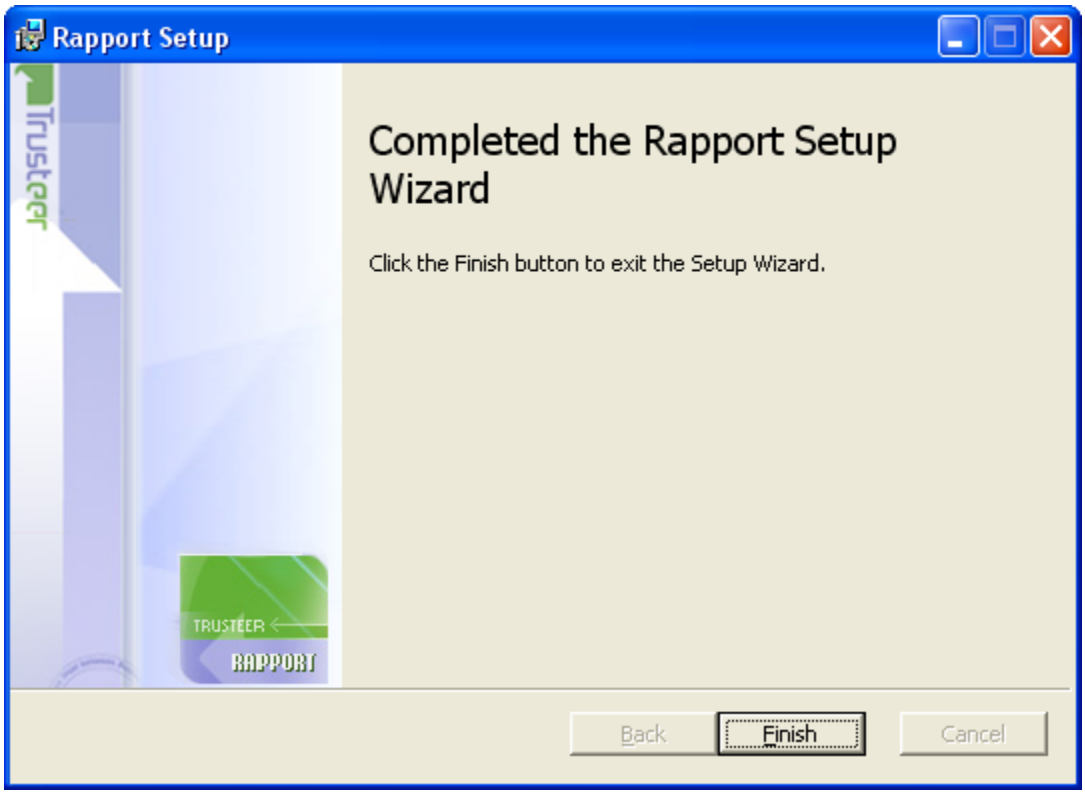


7. Si vous avez besoin que Trusteer Rapport soit compatible avec les lecteurs d'écran, cliquez sur **Advanced** (Avancé). L'écran des Options Avancées s'affiche. Cochez **I am visually impaired and regularly use assistive screen reader technologies** (je suis malvoyant et j'utilise régulièrement des technologies de lecture d'écran) et cliquez sur **Continue** (Continuer). Cela permet d'assurer la compatibilité avec les lecteurs d'écran pour narrer ce qu'indiquent les menus de Trusteer Rapport et garantit que Trusteer Rapport n'empêche pas les lecteurs d'écran de narrer les contenus affichés par le navigateur. Cela désactive également les boîtes de dialogue de codes visuels qui s'affichent lorsque vous arrêtez ou désinstallez Trusteer Rapport et qui sont requises pour plusieurs actions telles que l'arrêt et désinstallation de Rapport.

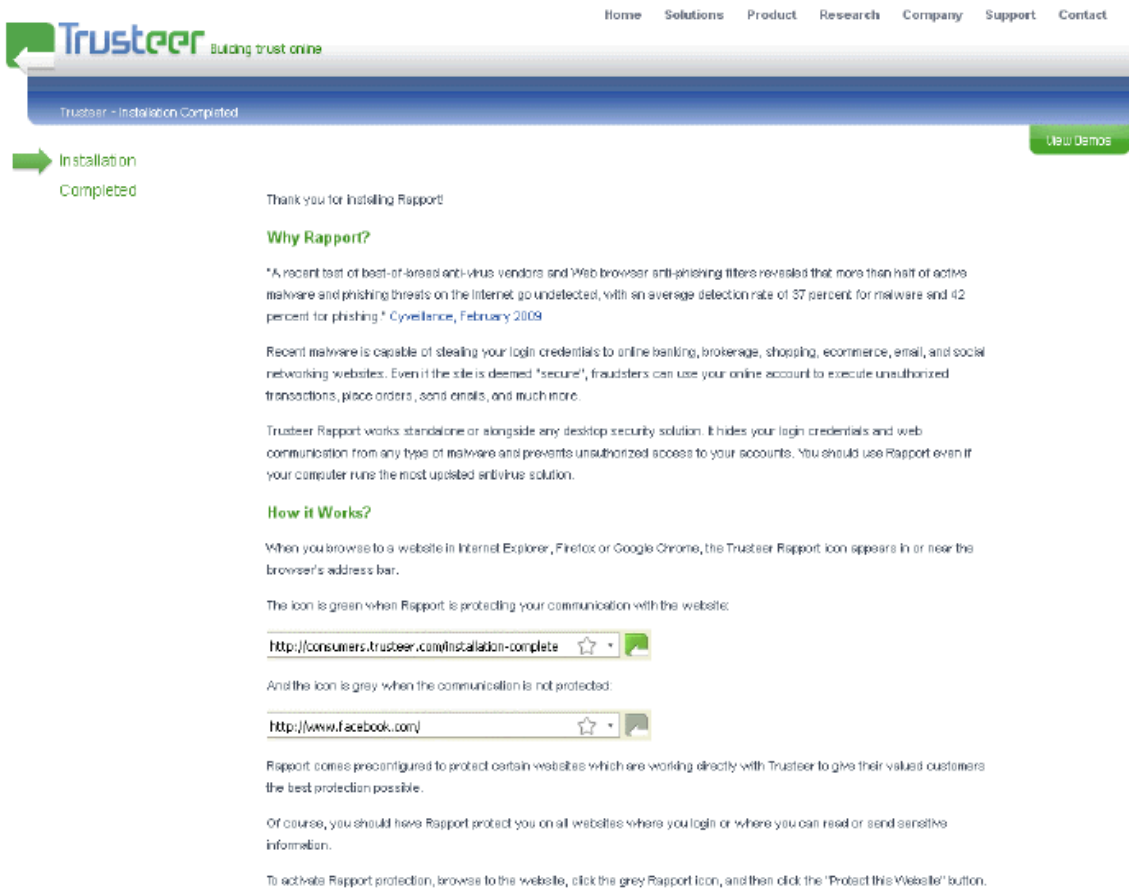
Remarque: ne cochez pas **I am visually impaired and regularly use assistive screen reader technologies** (je suis malvoyant et j'utilise régulièrement des technologies de lecture d'écran) à moins d'installer Trusteer Rapport sur un ordinateur pour lequel l'utilisation d'un logiciel de lecture d'écran est nécessaire. Ce paramètre désactive certaines fonctions de sécurité.

8. Cochez **I've read and agreed with Trusteer End User License Agreement** (J'ai lu et j'accepte le contrat de licence utilisateur final de Trusteer)

9. Cliquez sur **Install** (Installer). L'installation s'effectue. Lorsque l'installation est terminée, le bouton Finish (Terminer) s'affiche dans l'assistant.



10. Cliquez sur **Finish** (Terminer). Après quelques secondes, Trusteer Rapport ouvre une nouvelle fenêtre de navigateur pour effectuer un bref test de compatibilité. Lorsque le test est terminé, Trusteer Rapport ouvre la page de remerciement dans votre navigateur.



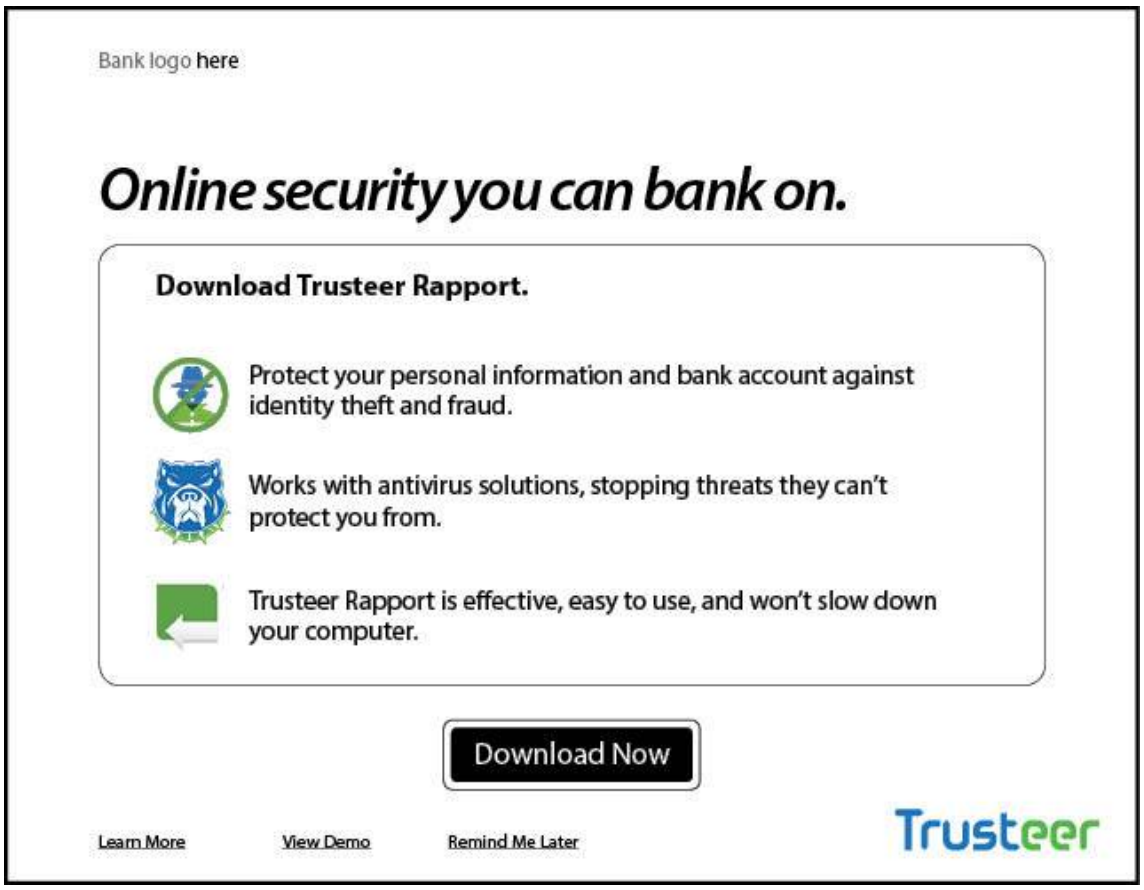
L'installation est terminée.

Installer Trusteer Rapport sous Windows XP en utilisant Google Chrome

Cette procédure explique comment télécharger et installer Trusteer Rapport sous Windows XP si vous utilisez Google Chrome comme navigateur.

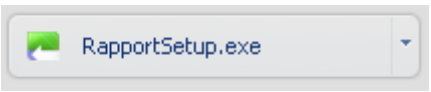
➡ **Pour installer Trusteer Rapport:**

1. Accédez à la page de connexion de votre société. Si votre société vous propose le téléchargement de Trusteer Rapport, vous verrez un écran d'accueil affichant un bouton Télécharger Maintenant. Par exemple:

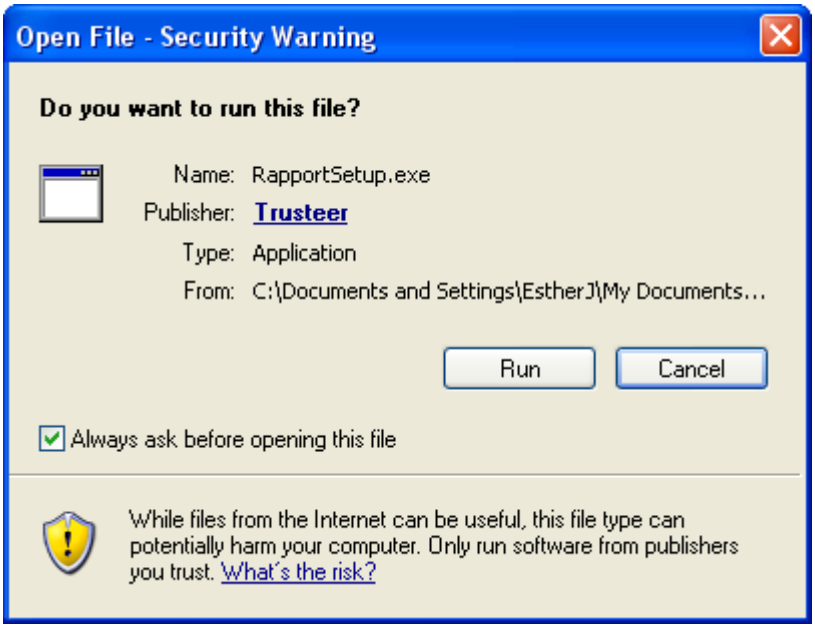


2. Cliquez sur **Download Now**. (Télécharger maintenant)

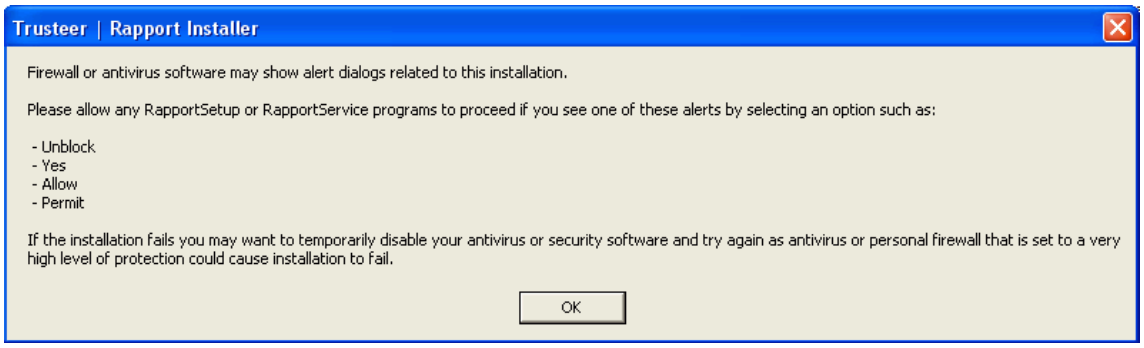
3. Selon les paramètres de votre navigateur, un message de sécurité peut apparaître en bas de la fenêtre de votre navigateur, vous demandant si vous souhaitez télécharger RapportSetup.exe. Cliquez sur **Save** (Enregistrer). Le fichier est téléchargé et un bouton apparaît en bas à gauche de la fenêtre de votre navigateur, affichant le nom du fichier téléchargé.



4. Cliquez sur le bouton. Un avertissement de sécurité s'affiche, vous demandant si vous voulez exécuter le fichier.

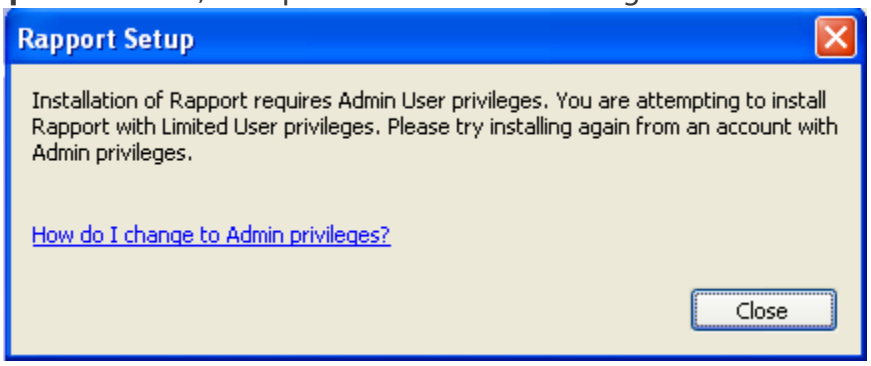


5. Cliquez sur **Run** (Exécuter). La boîte de dialogue suivante apparaît.



6. Cliquez sur **OK**. Trusteer Rapport est téléchargé.

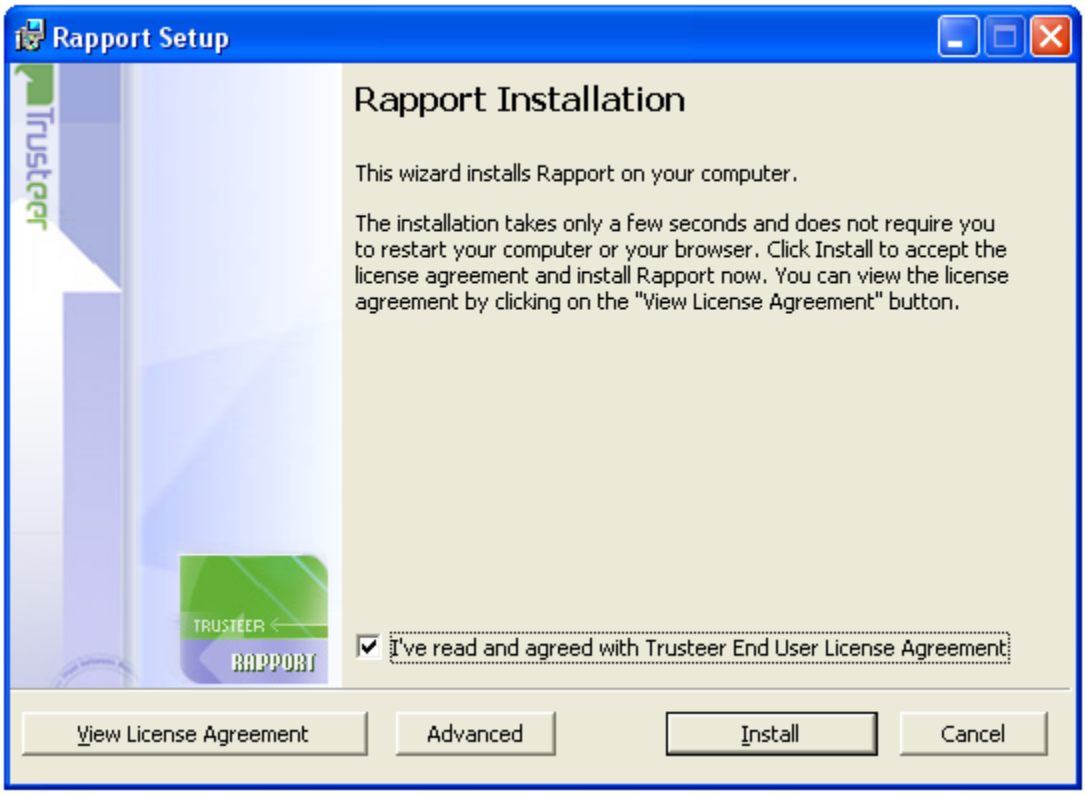
Remarque: à ce stade, vous pouvez recevoir ce message:



Cela signifie que votre fournisseur ne vous permet pas d'installer Trusteer Rapport depuis un compte utilisateur standard Windows. Si vous recevez ce message, basculez vers un compte administrateur, puis exécutez de nouveau l'installation.
Comment puis-je basculer vers un compte administrateur?

- Basculer vers un compte d'administrateur (Windows 7) (on page 143)
- Basculer vers un compte d'administrateur (XP) (on page 144)
- Basculer vers un compte d'administrateur (Vista) (on page 146)

L'assistant d'installation de Rapport apparaît.

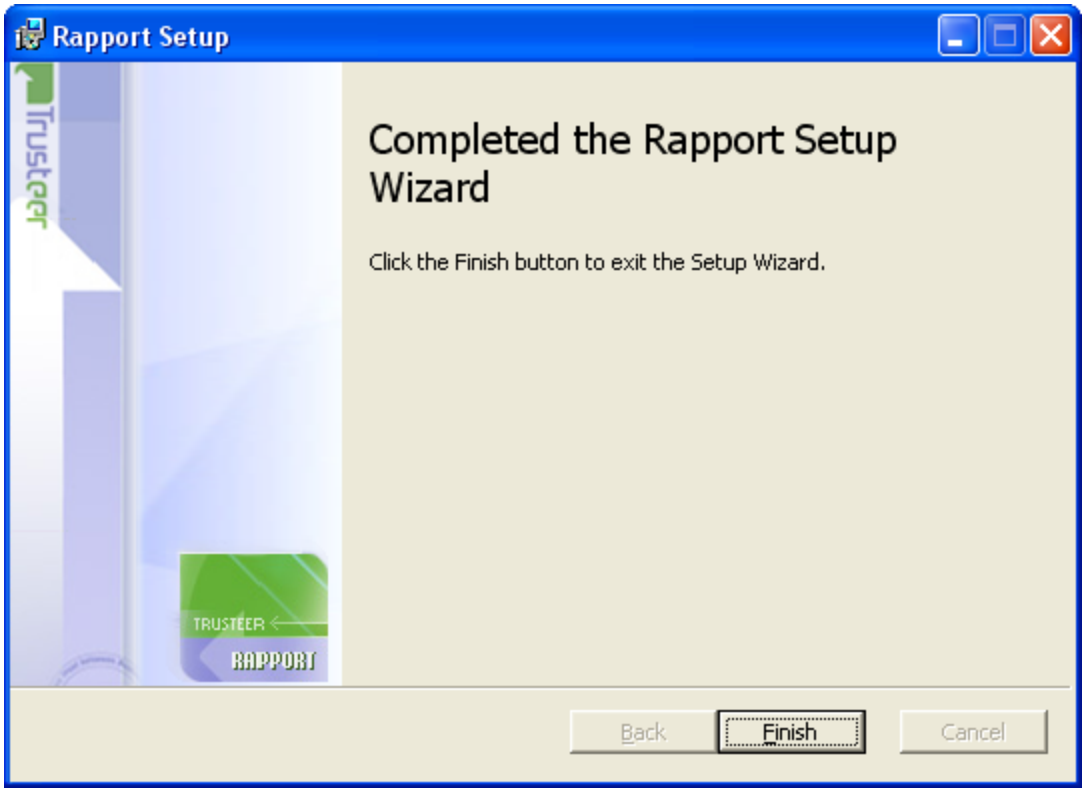


7. Si vous avez besoin que Trusteer Rapport soit compatible avec les lecteurs d'écran, cliquez sur **Advanced** (Avancé). L'écran des Options Avancées s'affiche. Cochez **I am visually impaired and regularly use assistive screen reader technologies** (je suis malvoyant et j'utilise régulièrement des technologies de lecture d'écran) et cliquez sur **Continue** (Continuer). Cela permet d'assurer la compatibilité avec les lecteurs d'écran pour narrer ce qu'indiquent les menus de Trusteer Rapport et garantit que Trusteer Rapport n'empêche pas les lecteurs d'écran de narrer les contenus affichés par le navigateur. Cela désactive également les boîtes de dialogue de codes visuels qui s'affichent lorsque vous arrêtez ou désinstallez Trusteer Rapport et qui sont requises pour plusieurs actions telles que l'arrêt et désinstallation de Rapport.

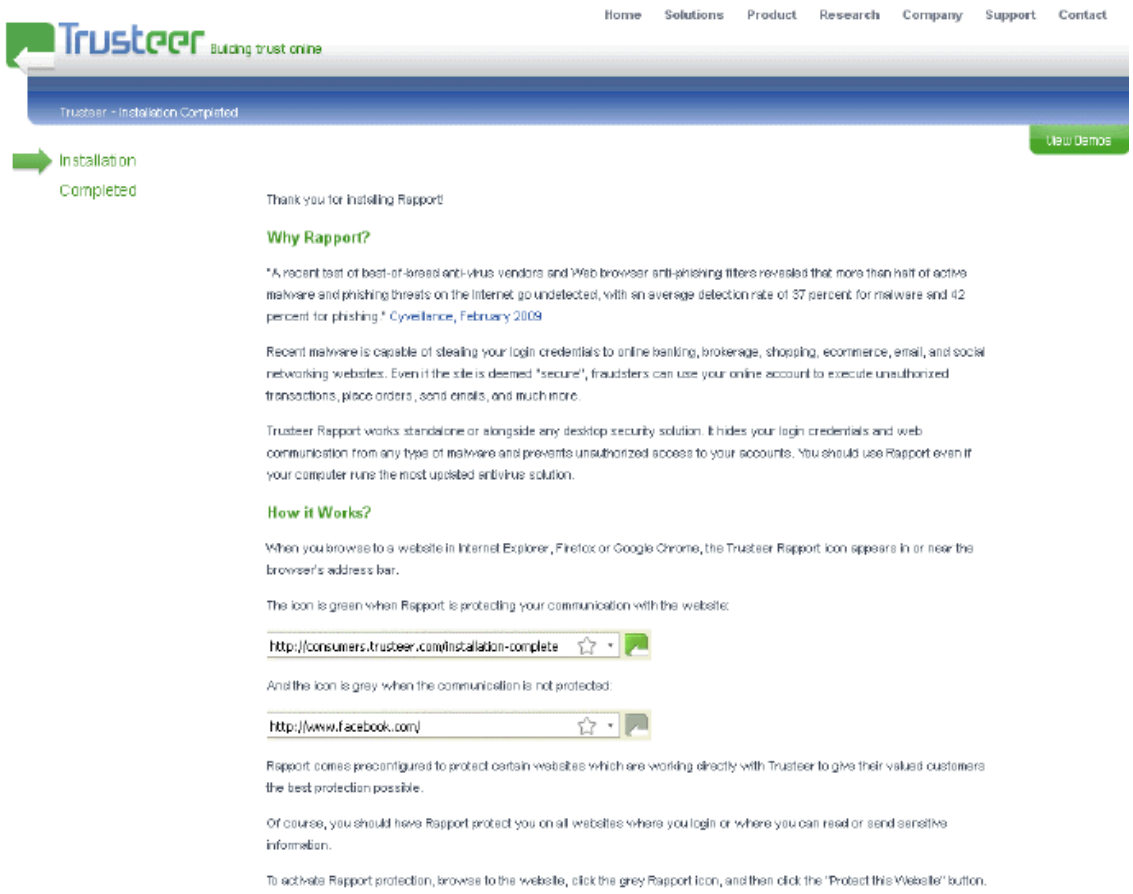
Remarque: ne cochez pas **I am visually impaired and regularly use assistive screen reader technologies** (je suis malvoyant et j'utilise régulièrement des technologies de lecture d'écran) à moins d'installer Trusteer Rapport sur un ordinateur pour lequel l'utilisation d'un logiciel de lecture d'écran est nécessaire. Ce paramètre désactive certaines fonctions de sécurité.

8. Cochez **I've read and agreed with Trusteer End User License Agreement** (J'ai lu et j'accepte le contrat de licence utilisateur final de Trusteer).

9. Cliquez sur **Install** (Installer). L'installation s'effectue. Lorsque l'installation est terminée, le bouton Finish (Terminer) s'affiche dans l'assistant.



Cliquez sur **Finish** (Terminer). Après quelques secondes, Trusteer Rapport ouvre une nouvelle fenêtre de navigateur pour effectuer un bref test de compatibilité. Lorsque le test est terminé, Trusteer Rapport ouvre la page de remerciement dans votre navigateur.



L'installation est terminée.

Installer Trusteer Rapport sous Windows Server (2003 ou 2008)

Trusteer Rapport prend en charge Windows Server (2003 et 2008). Trusteer Rapport prend aussi en charge plusieurs sessions utilisateur, ce qui permet une installation unique pour gérer plusieurs profils, telle que l'exige une infrastructure de bureaux virtuels partagés. Lorsque vous exécutez le processus d'installation sous Windows Server (2003 ou 2008), Trusteer Rapport détecte et installe une version serveur qui inclut la possibilité de désactiver l'envoi de requêtes de redémarrage aux utilisateurs, afin d'éviter une situation où un utilisateur redémarre le système pour tous les utilisateurs en cours d'exécution sur le système. Pour plus d'informations sur la manière de désactiver les requêtes de redémarrage, voir *Trusteer Rapport Virtual Environment Best Practices*.

Pour Installer Trusteer Rapport sous Windows Server (2003 ou 2008):

1. Exécutez le fichier RapportSetup.exe. Vous pouvez obtenir la version standard de ce fichier à partir de http://www.trusteer.com/support/rapport-installation-links. Si vous êtes un client professionnel, vous pouvez obtenir votre version personnalisée de ce fichier d'installation de votre chef de projet Trusteer.

2. Lancer le processus d'installation qui téléchargera le package complet d'installation et lance l'assistant d'installation. L'assistant d'installation détecte le système d'exploitation du serveur et affiche l'écran Hôte Windows Server détecté.

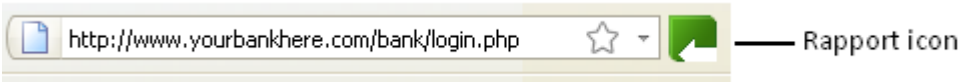
3. Lorsque vous voyez cet écran, cliquez sur Afficher les documents. Votre navigateur ouvre une page d'assistance aux entreprises de Trusteer Rapport (http://www.trusteer.com/support/business/main), Qui explique comment Trusteer Rapport aide à protéger les entreprises. Sur la page d'assistance aux entreprises, nous vous recommandons de cliquer sur le lien pour afficher le document Scénarios de mise en œuvre virtuelle de Trusteer Rapport, qui fournit des informations importantes sur la mise en œuvre de Rapport Trusteer dans un environnement de bureaux virtuels.

4. Lorsque vous aurez lu le document, cochez la case j'ai lu le document et continuez l'installation.

À part l'écran Hôte Windows Server détecté, l'installation est identique aux installations sous d'autres systèmes d'exploitation.

4. Mise en route

Immédiatement après l'installation, Trusteer Rapport est exécuté, protégeant vos communications avec les sites des partenaires. L'icône de Trusteer Rapport apparaît sur ou près du côté droit de la barre d'adresse de votre navigateur. Si vous accédez au site Web de votre banque ou de votre entreprise, l'icône Trusteer Rapport est verte, indiquant que le site est déjà protégé.



La première fois que vous vous connectez à votre compte en ligne, vous pouvez voir Répondre à une offre de protection du Mot de passe (on page 104).

Lorsque vous accédez à un site qui n'est pas protégé par Trusteer Rapport, l'icône de Rapport est grise et lorsque vous cliquez sur l'icône grise de Rapport, une boîte de dialogue déroulante (l'indicateur d'état de Rapport) vous indique que le site n'est pas protégé:

Vous aimeriez peut-être:

- Protecting Additional Websites sur lesquels vous vous connecter ou lisez ou envoyez des informations sensibles.
- Ouvrir la console Rapport (on page 72). Beaucoup de procédures dans ce guide commencent par l'ouverture de la console.
- Parcourez les titres des sujets pour obtenir les informations qui vous intéressent.

- SCommencez à vous sentir plus en sécurité lorsque vous effectuez votre travail, vos opérations bancaires et vos achats sur Internet.

Protecting Additional Websites

Remarque: Dans certaines installations de Trusteer Rapport, cette fonction est désactivée.

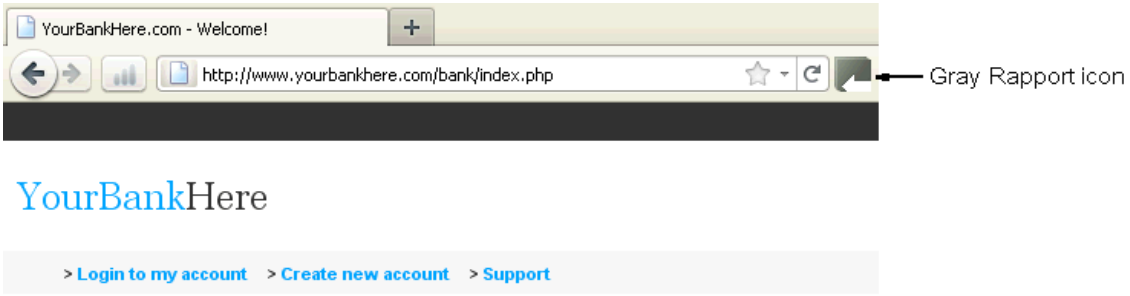
Par défaut, Trusteer Rapport protège les sites Web des partenaires tels que la société qui vous a offert Trusteer Rapport. Nos partenaires encouragent leurs clients à installer Trusteer Rapport. Cependant, toutes les banques et les autres entreprises ne collaborent pas avec Trusteer.

Vous pouvez facilement étendre la protection de Trusteer Rapport à d'autres sites Web. Il n'y a pas de limite quant au nombre de sites que vous pouvez protéger. Trusteer vous recommande d'activer la protection Trusteer Rapport sur tous les autres sites Web sur lesquels vous échangez des informations privées et personnelles ou tout autre type d'informations sensibles. Exemples de sites Web que vous voudriez peut-être protéger incluent:

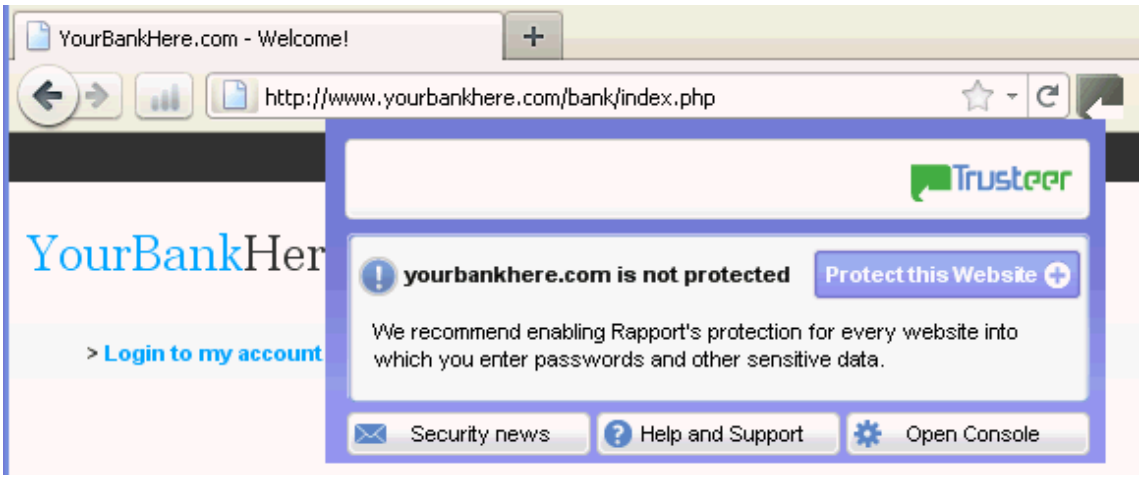
- Les comptes bancaires en ligne
- Les comptes de fonds de placement
- Les Comptes de courtage en ligne
- Les commerçants en ligne
- Les sites de messagerie sur le Web (tels que Hotmail, Yahoo! Mail et Gmail)
- Les sites de réseaux sociaux (tels que Myspace, Orkut, et Linkedin)
- Les demandes d'assurance
- Les sites d'informations médicales personnelles
- Les commerçants en ligne (tels que eBay, Amazon, Walmart.com, et Target.com)

➡ **Pour protéger un autre site:**

1. Accédez au site Web que vous souhaitez protéger. Si Trusteer Rapport n'est pas encore activé pour protéger ce site, l'icône de Rapport dans la barre d'adresse est grise.



2. Cliquez sur l'icône grise de Rapport sur la barre d'adresse. Une boîte de dialogue déroulante apparaît.



3. Dans la boîte de dialogue déroulante, cliquez sur Protéger ce site Web. L'icône de Rapport sur de la barre d'adresse devient verte, indiquant que ce site est désormais protégé par Trusteer Rapport.

L'icône s'affiche par défaut. Vous pouvez choisir de Masquer et rétablir l'icône de Trusteer Rapport dans la barre d'adresse (on page 150).

Pourquoi l'icône de Trusteer Rapport n'apparaît pas dans mon navigateur?

Si l'icône de Trusteer Rapport n'apparaît pas dans votre navigateur, il y a trois raisons possibles:

- Vous avez choisi de masquer l'icône de la barre d'adresse. Trusteer Rapport vous protège toujours, mais l'icône est masquée. Vous pouvez restaurer l'icône. Pour plus d'informations sur la manière de masquer et de restaurer l'icône de Trusteer Rapport, voir Masquer et rétablir l'icône de Trusteer Rapport dans la barre d'adresse (on page 150).
- Trusteer Rapport ne prend pas en charge votre navigateur. Pour une liste des navigateurs actuellement pris en charge, voir http://www.trusteer.com/support/faq/supported-platforms.
- Trusteer Rapport a été arrêté et n'est pas en cours d'exécution. Vous pouvez Redémarrer Trusteer Rapport. Voir Démarrer Trusteer Rapport (on page 195).

Ouvrir la console Rapport

La console de Trusteer Rapport est un portail vers diverses fonctions et informations de Trusteer Rapport.

➡ **Pour ouvrir la console de Rapport:**

- Cliquez sur l'icône de Rapport ( ) dans la barre d'état. La console de rapport s'affiche.

Je ne vois pas l'icône de Rapport dans la barre d'état.

L'icône de Rapport dans la barre d'état ( ) s'affiche par défaut lorsque Rapport est en cours d'exécution. Il est possible de masquer l'icône (voir Masquer et rétablir l'icône de la barre d'état système (on page 152).) L'icône indique que les protections indépendantes du navigateur de Trusteer Rapport fonctionnent correctement. Cela inclut la prévention, l'analyse et la suppression de logiciels malveillants. Si l'icône ne s'affiche pas et n'a pas été masqué via la console de Rapport, Trusteer Rapport n'est pas en cours d'exécution. Trusteer Rapport peut avoir été arrêté ou désinstallé. Pour démarrer Trusteer Rapport s'il a été arrêté, sélectionnez **Programmes** > **Trusteer Rapport** > **Démarrer**.

5. Protéger vos opérations bancaires en ligne

Si votre banque est un partenaire de Trusteer, vous pouvez télécharger Trusteer Rapport sur le site Web de votre banque et profiter d'une protection totale des services bancaires en ligne dès que vous installez Trusteer Rapport.

Trusteer Rapport identifie les risques de sécurité et neutralise les menaces sans avoir à vous en informer. Dans certains des cas où Trusteer Rapport détecte un certain niveau de risque, Rapport peut vous demander votre confirmation avant de neutraliser la menace. Pour plus d'informations sur les réponses aux alertes et avertissements de Trusteer Rapport, voir Répondre aux alertes et avertissements (on page 90).

6. Protéger l'accès Web à l'entreprise

Si vous accédez à votre réseau d'entreprise ou au portail de l'entreprise sur le Web, installer Trusteer Rapport sur votre ordinateur vous aide à protéger votre identité et à éviter de causer des atteintes à la sécurité de votre entreprise à travers vos informations d'identification utilisateur. Si vous appartenez à une entreprise partenaire de Trusteer Rapport, votre protection d'accès Web à l'entreprise commence dès que vous installez Trusteer Rapport.

Trusteer Rapport identifie les risques de sécurité et neutralise les menaces sans avoir à vous en informer. Dans certains des cas où Trusteer Rapport détecte un certain niveau de risque, Rapport peut vous demander votre confirmation avant de neutraliser la menace. Pour plus d'informations sur les réponses aux alertes et avertissements de Trusteer Rapport, voir Répondre aux alertes et avertissements (on page 90).

7. Utiliser les cartes de paiement en ligne en toute sécurité

Trusteer Rapport vous protège contre le vol de cartes de paiement lorsque vous utilisez vos cartes de paiement en ligne.

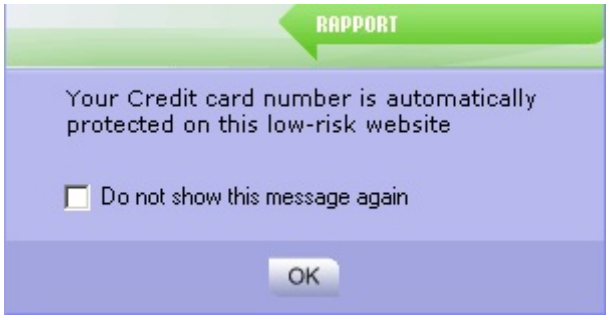
Trusteer Rapport fournit les fonctions de protection suivantes pour les cartes émises par des marques de cartes participantes:

- Détecte le moment où vous entrez le BIN (Numéro d'identification bancaire) d'une marque de carte participante dans une page Web.
- Active le blocage des enregistreurs de frappe immédiatement après avoir tapé le BIN, afin d'éviter que les logiciels malveillants d'enregistrement de frappe ne capturent votre numéro de carte de paiement.
- Vous avertit lorsque le blocage des enregistreurs de frappe est activé.
- Vous avertit lorsque vous entrez votre numéro de carte de paiement sur un site suspect ou non sécurisé, vous permettant de choisir de faire confiance au site ou annuler l'envoi de votre numéro de carte.

Remarque: Trusteer Rapport ne connait pas et ne mémorise pas vos numéros de cartes de paiement personnelles. Trusteer Rapport reconnaît la séquence des chiffres au début du numéro de votre carte qui identifie la marque émettrice. Ceci est connu comme le numéro d'identification bancaire (BIN).

Lorsque vous entrez des numéros de cartes de paiement, un des messages suivants peut s'afficher:

Pour plus d'informations à propos de cet avertissement, voir Répondre à une alerte de détection d'envoi de carte de paiement (on page 123).



Pour plus d'informations sur ce message, voir Répondre à un message de protection des cartes de paiement (on page 124).

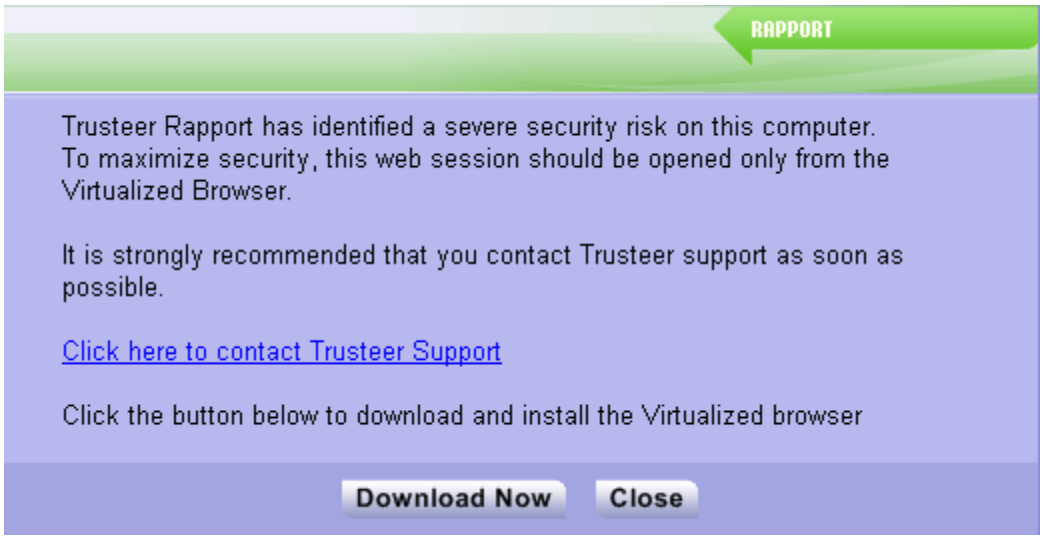
8. Utiliser le navigateur virtualisé de Trusteer Rapport

Le navigateur virtualisé de Trusteer Rapport fournit une couche supplémentaire de protection lors de la navigation des sites Web protégés. Cette couche de protection crée un environnement de navigation isolé qui protège contre des logiciels malveillants potentiels sur votre ordinateur.

Trusteer Rapport vous offre le téléchargement du navigateur virtualisé dans les situations suivantes:

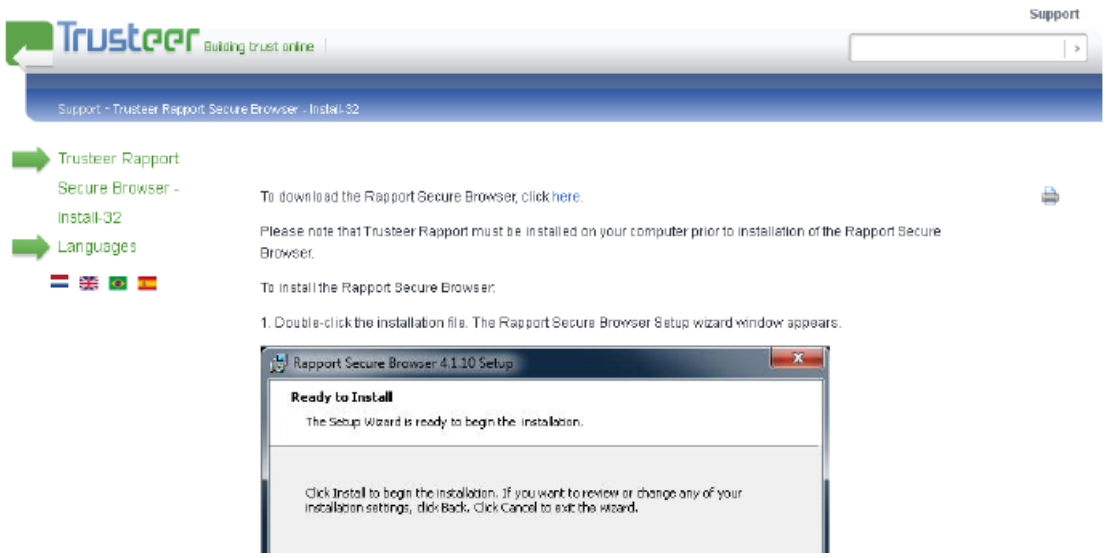
- Lorsque vous accédez à un site protégé. Si Trusteer Rapport détecte que vous courez un grave risque de sécurité de votre ordinateur. Dans ce cas, Trusteer Rapport vous empêche d'ouvrir le site dans le navigateur normal (voir Répondre à une alerte forcée de téléchargement du navigateur virtualisé (on page 90)).
- Lorsque vous accédez à un site qui prend en charge l'affichage facultatif dans le navigateur virtualisé (voir Répondre à une alerte facultative de téléchargement du navigateur virtualisé (on page 93)).

L'offre s'affiche avec un bouton **Download Now** (Télécharger maintenant). Par exemple:



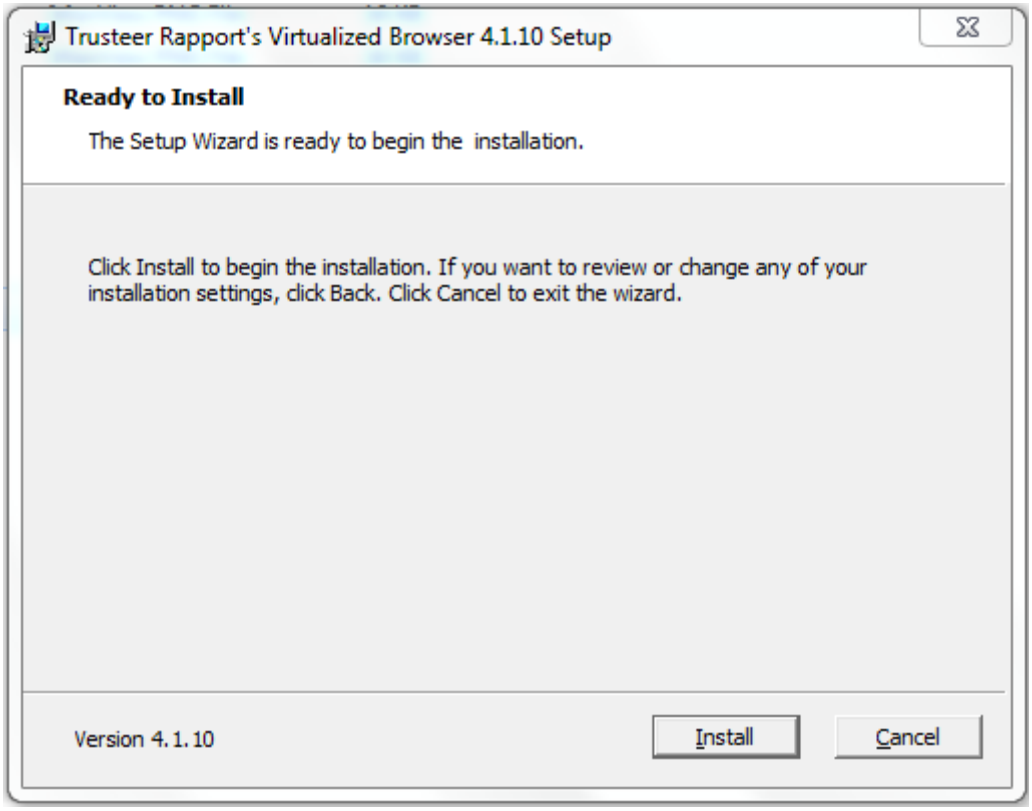
➡ **Pour installer le navigateur virtualisé:**

1. Lorsqu'une offre de téléchargement du navigateur virtualisé apparaît, cliquez sur le bouton Télécharger Maintenant. La page web suivante s'affiche dans votre navigateur.



2. Cliquez sur le lien ici. Votre navigateur démarre le téléchargement du fichier VirtualizedBrowserSetup.exe.

3. Lorsque le fichier VirtualizedBrowserSetup.exe est téléchargé, exécutez-le. Lorsque l'assistant d'installation est prêt à installer le navigateur virtualisé, cet écran apparaît.



4. Cliquez sur Installer. Le processus d'installation démarre. Lorsque l'installation est terminée, l'écran suivant apparaît.

5. Cliquez sur Terminer. Le navigateur virtualisé est installé. Vous pouvez maintenant ouvrir le site que vous consultiez au moment où l'offre de téléchargement vous a été annoncée. Une autre alerte vous offrira la possibilité d'ouvrir le site dans le navigateur virtualisé. Voir Répondre à une alerte facultative de téléchargement du navigateur virtualisé (on page 93) ou Répondre à une alerte facultative du navigateur virtualisé (on page 99).

9. Utiliser le service Token logiciel sécurisé de Trusteer Rapport

Certaines banques vous demandent de vous abonner à un service de Token logiciel sécurisé pour que chaque fois que vous vous connectez à la banque, vous vous connectez avec un mot de passe à usage unique (OTP) généré par le service. Trusteer Rapport fournit aux partenaires un service de Token logiciel sécurisé qui offre une protection supplémentaire pour empêcher les logiciels malveillants qui peuvent résider sur votre ordinateur de générer automatiquement ou de voler les OTP. Si votre banque s'abonne au service de Token logiciel sécurisé de Trusteer Rapport, suivez ces instructions pour activer le service, générer des OTPs au besoin, et gérer les OTPs générés.

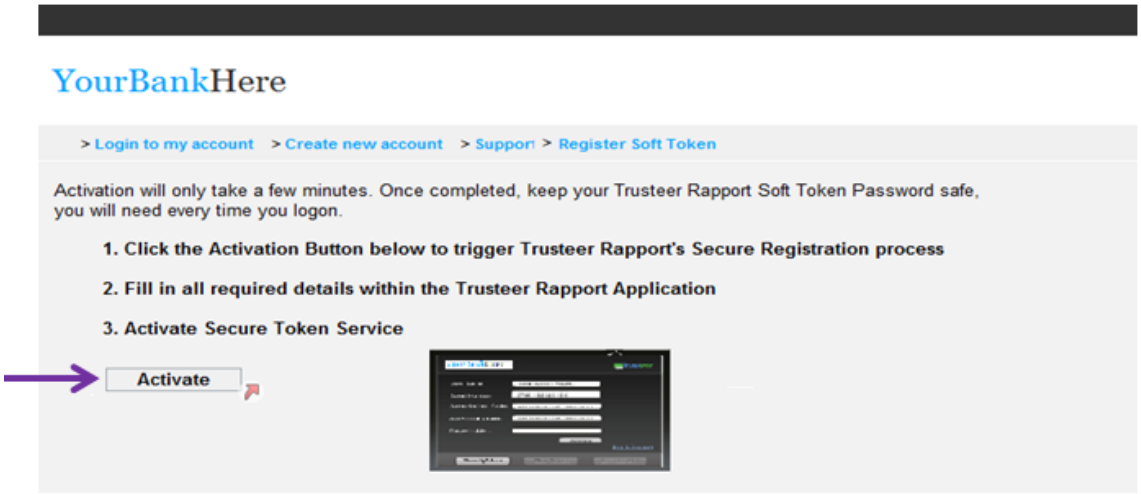
Activer le service de Token logiciel sécurisé

Pour pouvoir générer des mots de passe à usage unique, vous devez activer le service de Token logiciel sécurisé.

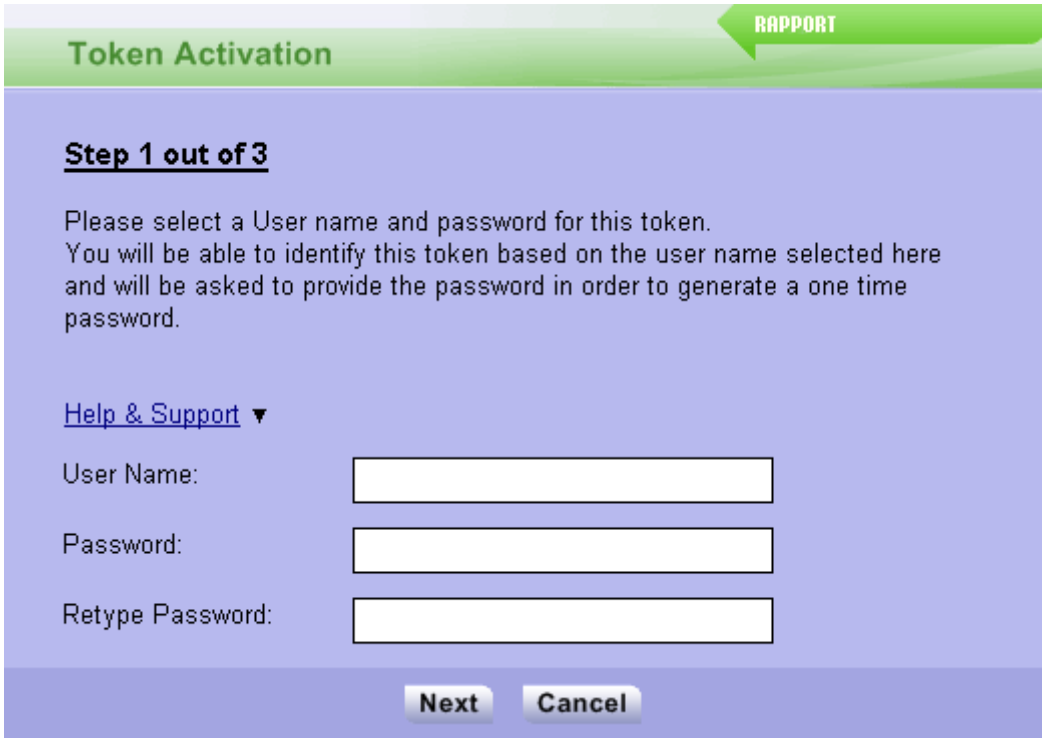
➡ **Pour activer le service de Token logiciel sécurisé de Trusteer Rapport:**

1. Après réception d'un numéro de série, un code d'autorisation et un code d'activation auprès de votre banque, accédez à la page de connexion sur le site Web de votre banque.

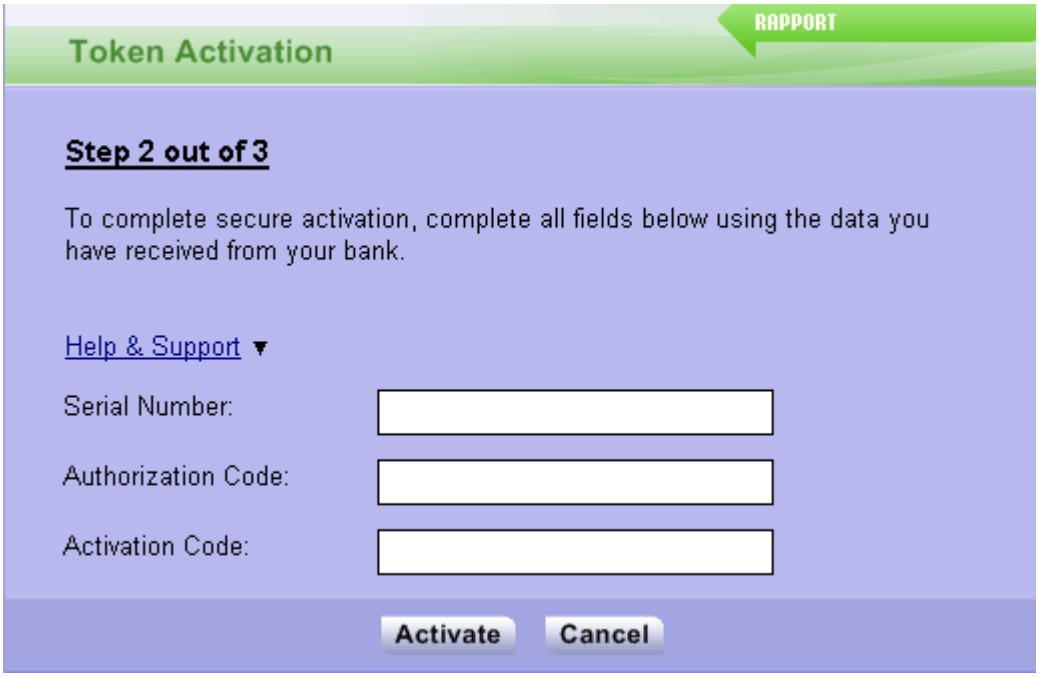
2. Suivez les instructions de votre banque pour démarrer le processus d'activation. Par exemple, vous devez peut-être cliquer sur un bouton Activer dans un écran comme celui-ci:



L'écran Activation du Token apparaît.

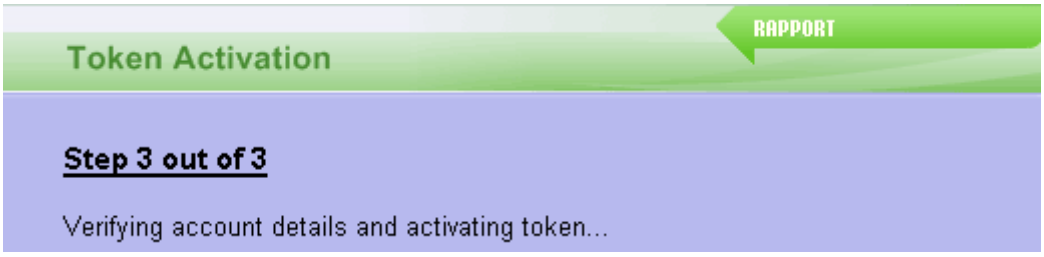


3. Saisissez un nom d'utilisateur et un mot de passe de votre choix et confirmer le mot de passe dans le champ prévu à cet effet. Ce sont le nom d'utilisateur et le mot de passe que vous utilisez pour vous connecter au service de Token logiciel à chaque fois que vous avez besoin de générer un mot de passe à usage unique.
4. Cliquez sur Suivant. L'écran suivant apparaît.

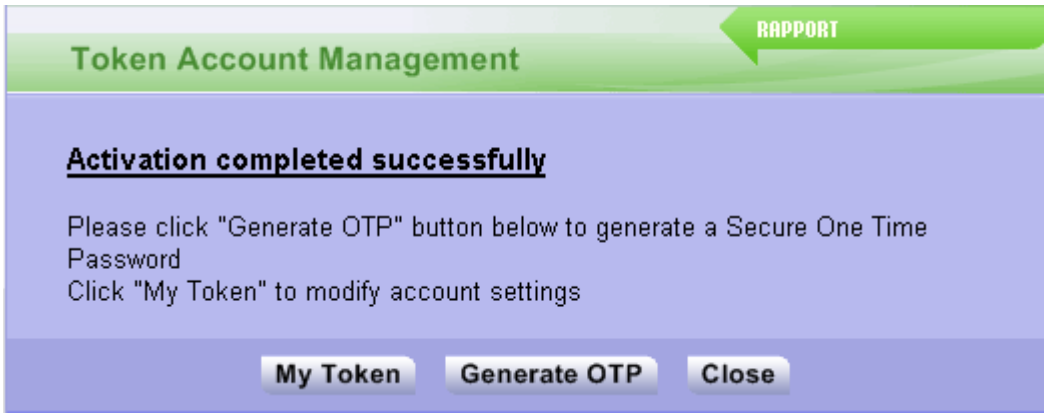


5. Dans les champs disponibles, entrez les informations d'activation fournies par votre banque.
6. Cliquez sur Activer. L'écran suivant apparaît.

Remarque: Veuillez vérifier que les informations saisies dans les champs sont exactement les mêmes que celles qui vous ont été envoyées par votre banque avant de cliquer sur Activer. Si les informations sont incorrectes, la génération d'un mot de passe à usage unique peut être bloquée jusqu'à ce que vous contactiez l'assistance clientèle de votre banque.



Une fois vos informations vérifiées, l'écran suivant apparaît.

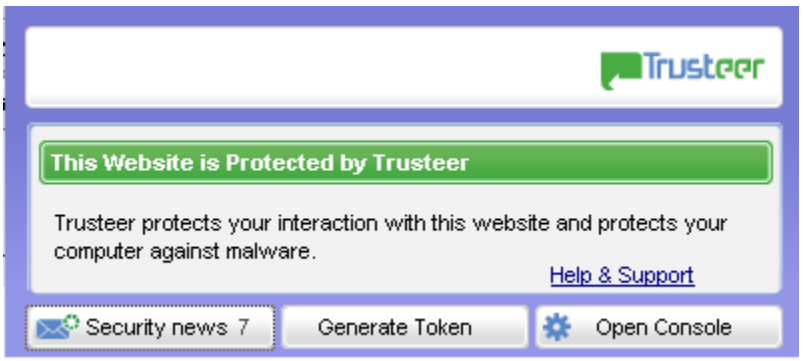


Vous pouvez générer immédiatement des mots de passe en utilisant le bouton Générer un OTP.

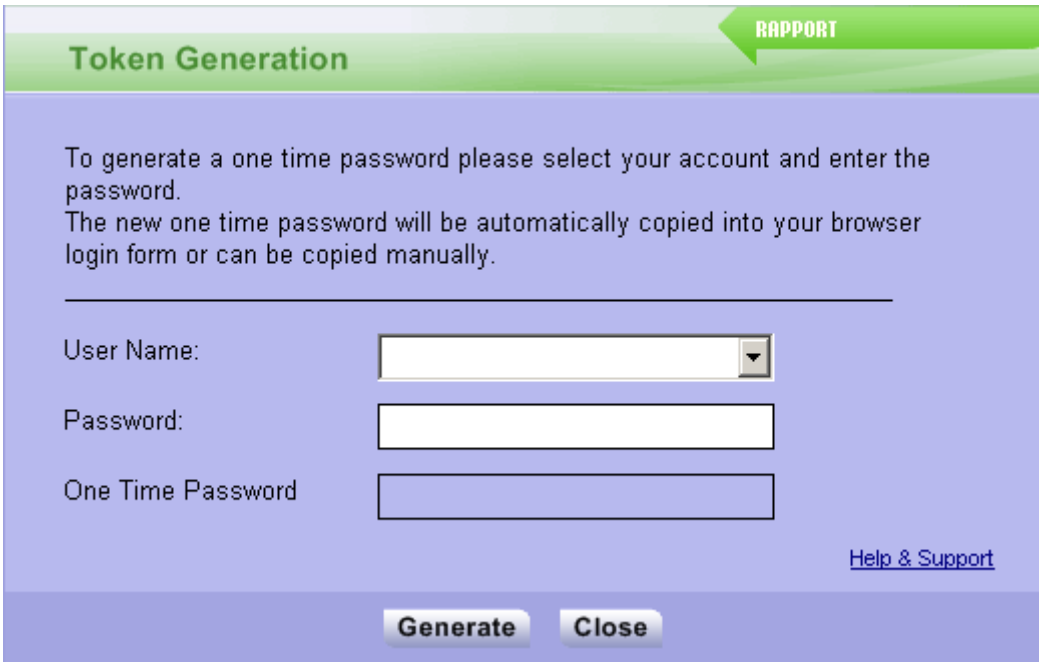
Générer des OTPs

➡ **Pour générer un mot de passe à usage unique:**

1. Accédez à la page de connexion sur le site de votre banque.
2. Si vous êtes invité à générer un Token, suivez les instructions du message d'invite.
3. Si vous n'êtes pas invité à générer un Token, cliquez sur l'icône de Trusteer Rapport. L'indicateur d'état de Rapport apparaît avec un bouton Générer un Token.



4. Cliquez sur Générer un Token. L'écran de génération de Token apparaît.



5. Dans la liste déroulante Nom d'utilisateur, sélectionnez le nom d'utilisateur que vous avez créé lorsque vous avez activé le service de Token logiciel pour le compte auquel vous voulez vous connecter (voir Activer le service de Token logiciel sécurisé (on page 82).)
6. Dans le champ Mot de passe, saisissez le mot de passe pour le même compte de Token que celui que vous avez sélectionné dans le champ Nom d'utilisateur.
7. Cliquez sur Générer. Un nouveau mot de passe à usage unique est généré et s'affiche dans le champ Mot de passe à usage unique. Copiez le mot de passe dans le presse- papier.
8. Cliquez sur Fermer. L'écran de génération de Token se ferme. Le nouveau mot de passe à usage unique est automatiquement copié dans le formulaire de connexion de votre banque.
9. Dans l'écran de connexion de votre banque, vérifiez que votre mot de passe unique a été copié automatiquement dans le champ Mot de passe. Sinon, collez le mot de passe dans le champ et utilisez-le pour vous connecter à votre compte.

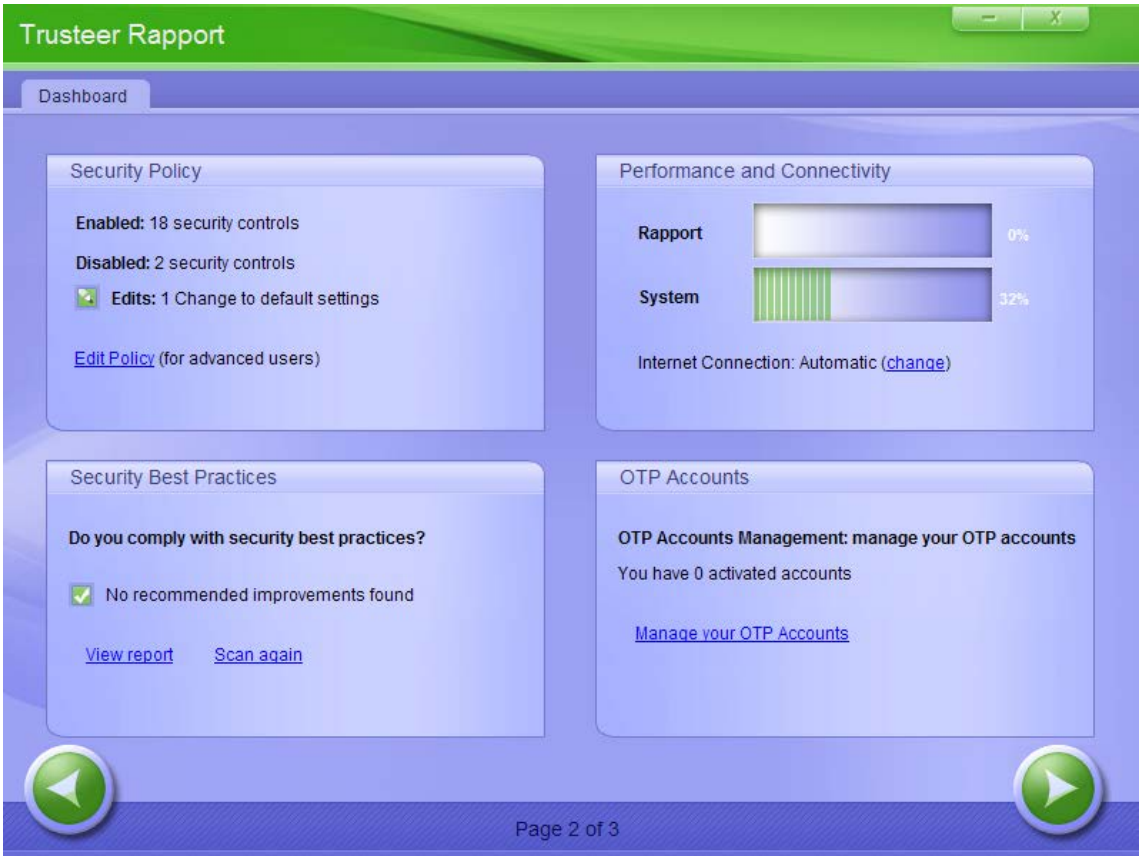
Gestion des comptes OTP

Lorsque vous activez le service OTP de Trusteer Rapport sur le site de votre banque, un compte OTP est créé. Vous pouvez avoir plus d'un compte OTP si vous êtes titulaires de plus d'un compte bancaire auprès d'une banque abonnée au service de Token logiciel sécurisé de Trusteer Rapport. Vous pouvez Renommer des comptes OTP (on page 87) et Supprimer des comptes OTP (on page 88) via la console de Rapport.

Renommer des comptes OTP

➡ **Pour renommer un compte OTP:**

1. Ouvrir la console Rapport (on page 72).
2. Dans le tableau de bord, cliquez sur . Le second écran du tableau de bord apparaît.



3. Dans la zone des comptes OTP, cliquez sur Gérez vos comptes OTP. L'onglet Gestion des comptes de Token s'affiche.
4. Dans le champ Nom d'utilisateur, sélectionnez le nom d'utilisateur pour le compte que vous souhaitez renommer.
5. Dans le champ Nouveau nom d'utilisateur, saisissez le nom du nouvel utilisateur.
6. Cliquez sur Renommer. Un message de confirmation apparaît.
7. Cliquez sur Oui. Le compte est renommé.

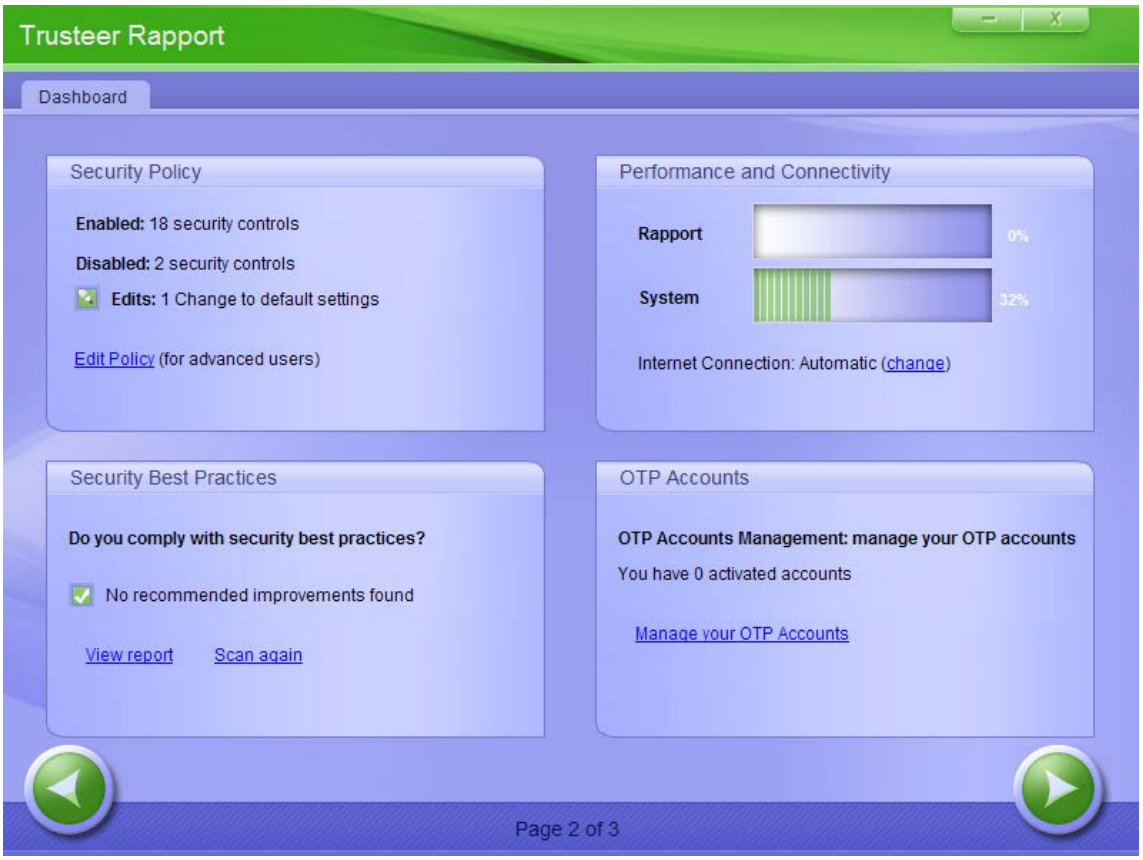
Supprimer des comptes OTP

Nous vous conseillons de supprimer un compte OTP existant si vous avez fermé le compte bancaire qui y est associé, ou si la banque émet de nouvelles informations d'activation du Token.

➡ **Pour supprimer un compte OTP:**

1. Ouvrir la console Rapport (on page 72).

2. Dans le tableau de bord, cliquez sur . Le second écran du tableau de bord apparaît.



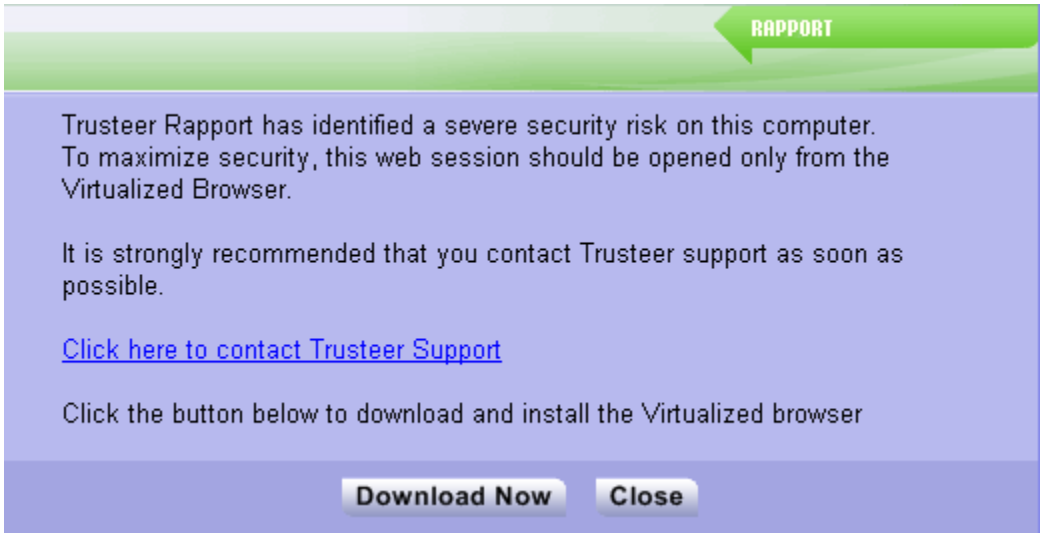
3. Dans la zone des comptes OTP, cliquez sur Gérez vos comptes OTP. L'onglet Gestion des comptes de Token s'affiche.
4. Dans le champ Nom d'utilisateur, sélectionnez le nom d'utilisateur pour le compte que vous souhaitez supprimer.
5. Cliquez sur Supprimer. Un message de confirmation apparaît.
6. Cliquez sur Oui. Le compte est supprimé.

10. Répondre aux alertes et avertissements

Trusteer Rapport affiche parfois des alertes et des avertissements qui requièrent votre réponse. Lorsque vous voyez une boîte de dialogue de Trusteer Rapport, lisez-le attentivement et sélectionnez la réponse appropriée. La prise des mesures nécessaires pourrait être cruciale pour votre sécurité. Voici quelques boîtes de dialogue que vous pouvez voir et la manière dont vous devez répondre.

Répondre à une alerte forcée de téléchargement du navigateur virtualisé

Ceci est un exemple d'une alerte forcée de téléchargement du navigateur virtualisé :



Cette alerte peut s'afficher lorsque vous accédez à un site Web protégé. Cette alerte indique que Trusteer Rapport a détecté un risque de sécurité sur votre ordinateur et vous empêche d'afficher le site dans le navigateur normal. Si vous souhaitez afficher le site, vous devez télécharger et installer le navigateur virtualisé de Trusteer Rapport. Le navigateur virtualisé de Trusteer Rapport est un environnement de navigation isolé qui fournit une couche supplémentaire de protection.

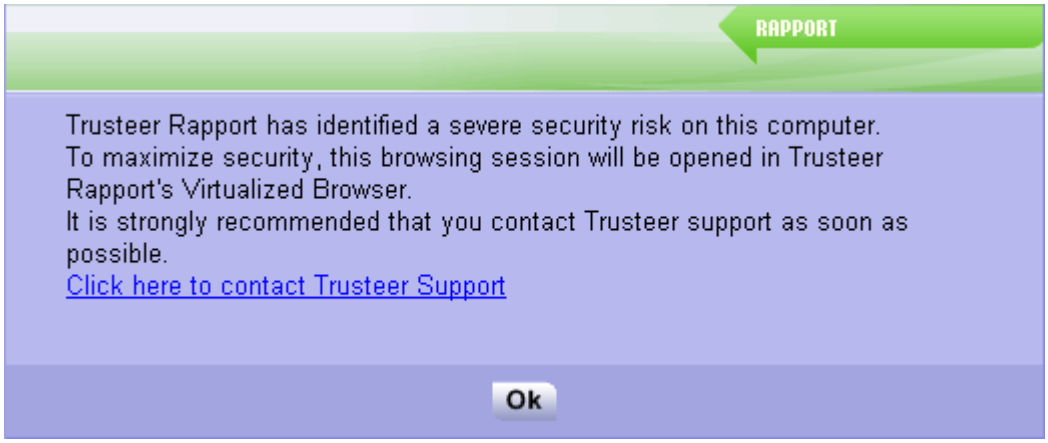
Lorsque vous voyez cette alerte, choisissez l'une des options suivantes:

- Cliquez sur Télécharger maintenant. Ceci télécharge le fichier d'installation du navigateur virtualisé de Trusteer Rapport. Une fois que vous aurez téléchargé et exécuté ce fichier, vous pourrez accéder à nouveau au site et l'afficher correctement dans le navigateur virtualisé. Il est également recommandé de contacter l'assistance de Trusteer (Voir Envoyer le signalement d'un problème d'utilisation (on page 220)) et nous informer que vous avez reçu cette alerte. Nous serons ainsi en mesure de vous guider pour prendre les mesures nécessaires pour lutter contre les risques de sécurité sur votre ordinateur.
- Cliquez sur Cliquez ici pour contacter l'assistance de Trusteer. Cela ouvre le formulaire Signaler un problème dans la console de Rapport. Utilisez ce formulaire pour informer Trusteer que vous avez reçu cette alerte. Nous serons ainsi en mesure de vous guider pour prendre des mesures pour lutter contre les risques de sécurité sur votre ordinateur. Voir Envoyer le signalement d'un problème d'utilisation (on page 220) si vous avez besoin d'aide sur la façon de signaler le problème.
- Cliquez sur Fermer. Ceci ferme l'alerte et le site web.

Pour plus d'informations sur le téléchargement et l'installation du navigateur virtualisé de Trusteer Rapport, voir Utiliser le navigateur virtualisé de Trusteer Rapport (on page 78).

Répondre à une alerte forcée du navigateur virtualisé

Ceci est un exemple d'une alerte forcée du navigateur virtualisé.



Cette alerte peut s'afficher lorsque vous accédez à un site Web protégé. Cette alerte indique que Trusteer Rapport a détecté un risque de sécurité sur votre ordinateur et vous empêche d'afficher le site dans le navigateur normal. Si vous souhaitez afficher le site, vous devez ouvrir le site dans le navigateur virtualisé de Trusteer Rapport, qui a déjà été installé sur votre ordinateur. Le navigateur virtualisé de Trusteer Rapport est un environnement de navigation isolé qui fournit une couche supplémentaire de protection.

Lorsque vous voyez cette alerte, sélectionnez l'une des options suivantes:

- Cliquez sur Cliquez ici pour contacter l'assistance de Trusteer. Cela ouvre le formulaire Signaler un problème dans la console de Rapport. Utilisez ce formulaire pour informer Trusteer que vous avez reçu cette alerte. Nous serons ainsi en mesure de vous guider pour prendre des mesures pour lutter contre les risques de sécurité sur votre ordinateur. Voir Envoyer le signalement d'un problème d'utilisation (on page 220) si vous avez besoin d'aide sur la façon de signaler le problème.
- Cliquez sur OK. Le site s'ouvre dans le navigateur virtualisé de Trusteer Rapport.

Répondre à une alerte facultative de téléchargement du navigateur virtualisé

Ceci est un exemple d'une alerte facultative de téléchargement du navigateur virtualisé:

Cette alerte s'affiche lorsque vous accédez à un site Web qui prend en charge le navigateur virtualisé de Trusteer Rapport. Le navigateur virtualisé de Trusteer Rapport est un environnement de navigation isolé qui fournit une couche supplémentaire de protection contre des logiciels malveillants potentiels sur votre ordinateur.

Lorsque vous voyez cette alerte, choisissez l'une des options suivantes :

- Cliquez sur Télécharger maintenant. Ceci téléchargera le fichier d'installation du navigateur virtualisé de Trusteer Rapport. Une fois que vous aurez téléchargé et exécuté ce fichier, vous serez en mesure de naviguer à nouveau sur le site et l'afficher correctement dans le navigateur virtualisé
- Cliquez sur Ne plus demander pour ce site. Ceci ferme l'alerte sans télécharger le navigateur virtualisé et empêche l'offre de s'afficher lorsque vous revisitez ce site. Le site s'ouvre dans le navigateur normal.
- Cliquez sur Ne plus afficher cette alerte. Ceci ferme l'alerte sans télécharger le navigateur virtualisé et empêche l'offre de s'afficher lorsque vous revisitez des sites qui prennent en charge le navigateur virtualisé. Le site s'ouvre dans le navigateur normal.

- Cliquez sur Fermer. Ceci ferme l'alerte et le site s'ouvre dans le navigateur normal.

Pour plus d'informations sur le téléchargement et l'installation du navigateur virtualisé de Trusteer Rapport, voir Utiliser le navigateur virtualisé de Trusteer Rapport (on page 78).

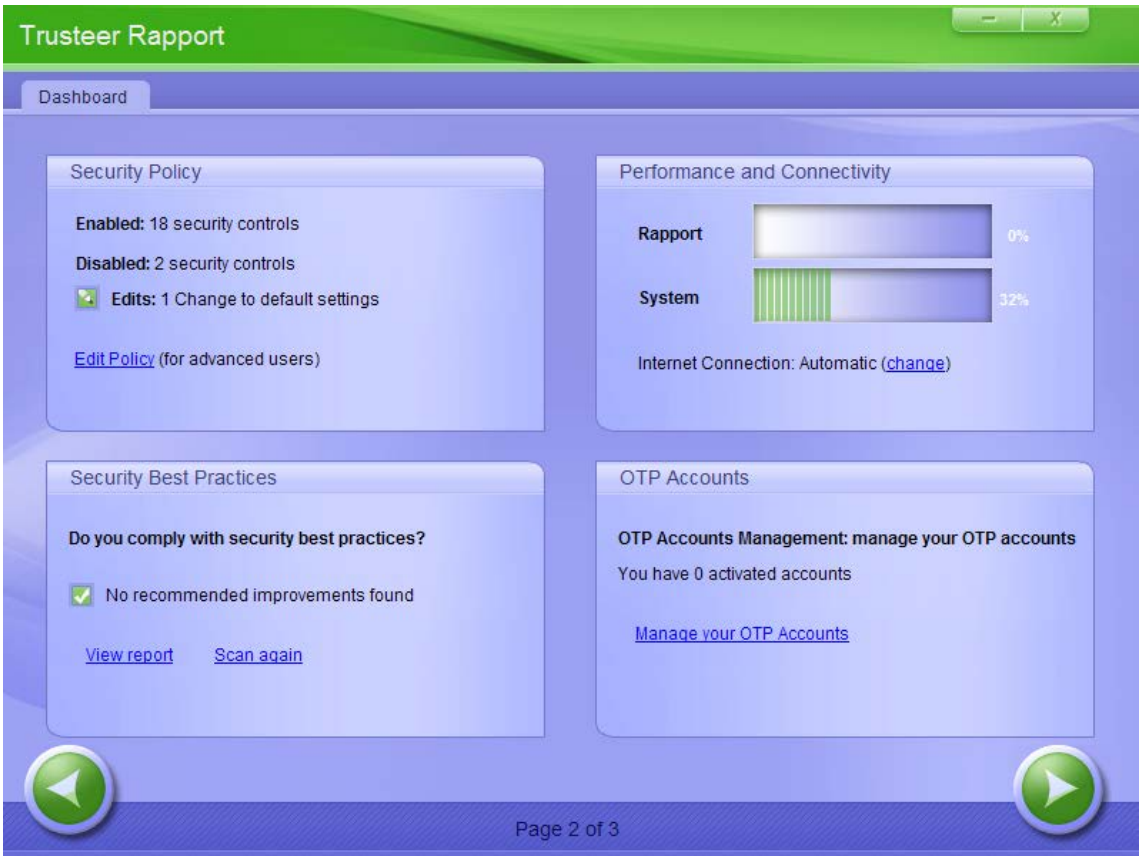
J'ai cliqué sur Ne plus afficher cette alerte par erreur. Serais-je toujours en mesure d'ouvrir des sites dans le navigateur virtualisé?

Lorsque vous avez cliqué sur Ne plus afficher cette alerte suite à une Répondre à une alerte facultative de téléchargement du navigateur virtualisé (on page 93) ou à une Répondre à une alerte facultative du navigateur virtualisé (on page 99), la politique de sécurité a été modifiée de sorte que vous ne soyez plus alerté lorsque vous accédez à un site qui prend en charge le navigateur virtualisé. Vous pouvez réinitialiser cette politique en utilisant la procédure suivante.

Pour réinitialiser la politique d'alerte du navigateur virtualisé:

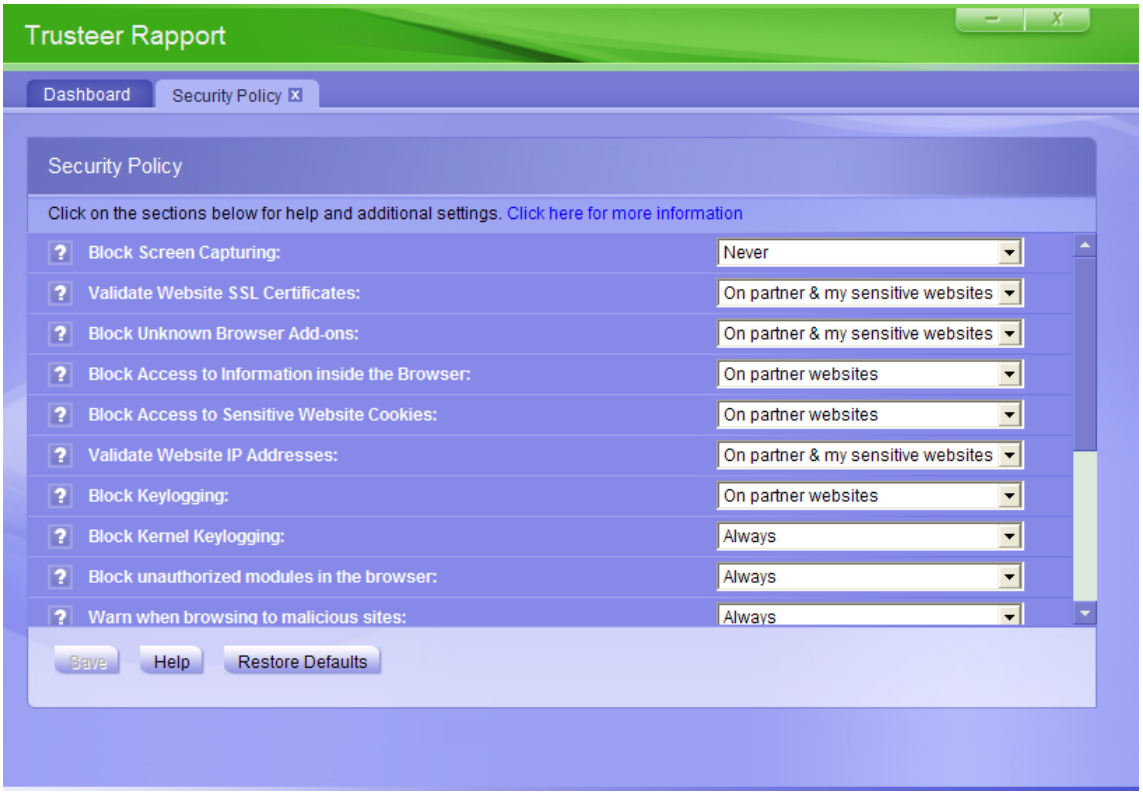
1. Ouvrir la console Rapport (on page 72).

2. Dans le tableau de bord, cliquez sur . Le second écran du tableau de bord apparaît.



3. Dans la zone de la politique de sécurité, cliquez sur Modifier la politique. Un écran Approbation de l'utilisateur apparaît. L'écran vous montre l'image d'un mot pour que vous le saisissiez. Ceci est destiné à empêcher les logiciels malveillants d'accéder à la console et de désactiver Trusteer Rapport de manière efficace.
4. Saisissez le mot que vous voyez dans l'image.

5. Cliquez sur OK. L'écran Politique de sécurité apparaît, affichant tous les contrôles de sécurité.



6. Faites défiler jusqu'au contrôle appelé Proposer l'utilisation du navigateur virtualisé de Trusteer Rapport sur les sites pris en charge. Dans le menu déroulant sur la droite de cette commande, sélectionnez Toujours pour réinitialiser la politique à sa valeur par défaut.
7. Cliquez sur Enregistrer. Votre modification de la politique est enregistrée. Désormais, lorsque vous accédez à des sites qui prennent en charge le navigateur virtualisé, Trusteer Rapport proposera d'ouvrir ces sites dans le navigateur virtualisé.

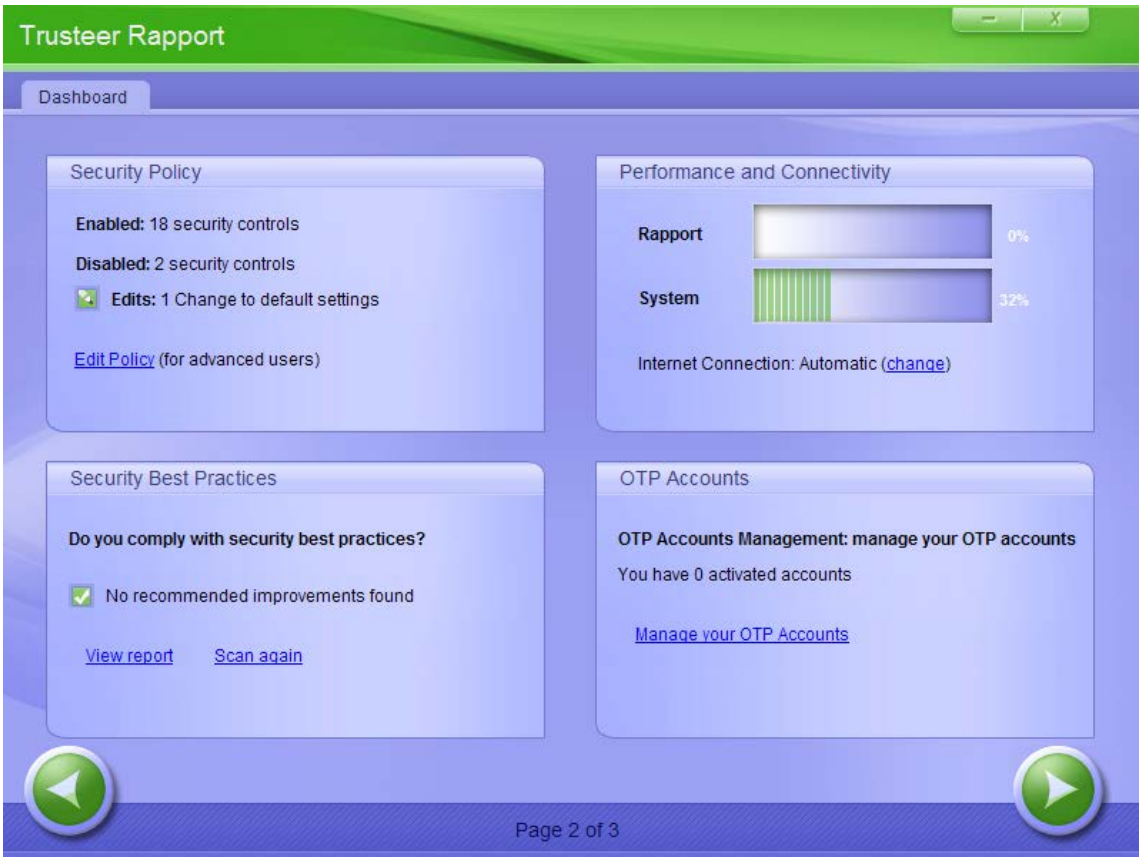
J'ai cliqué sur Ne plus demander pour ce site. Maintenant je souhaite afficher ce site dans le navigateur virtualisé. Que dois-je faire?

Lorsque vous avez cliqué sur Ne plus afficher cette alerte suite à une Répondre à une alerte facultative de téléchargement du navigateur virtualisé (on page 93), la politique de sécurité a été modifiée de sorte que vous ne soyez plus alerté à propos du navigateur virtualisé lorsque vous accédez à ce site. Vous pouvez réinitialiser cette politique.

Pour modifier la politique du navigateur virtualisé pour un site:

1. Ouvrir la console Rapport (on page 72).

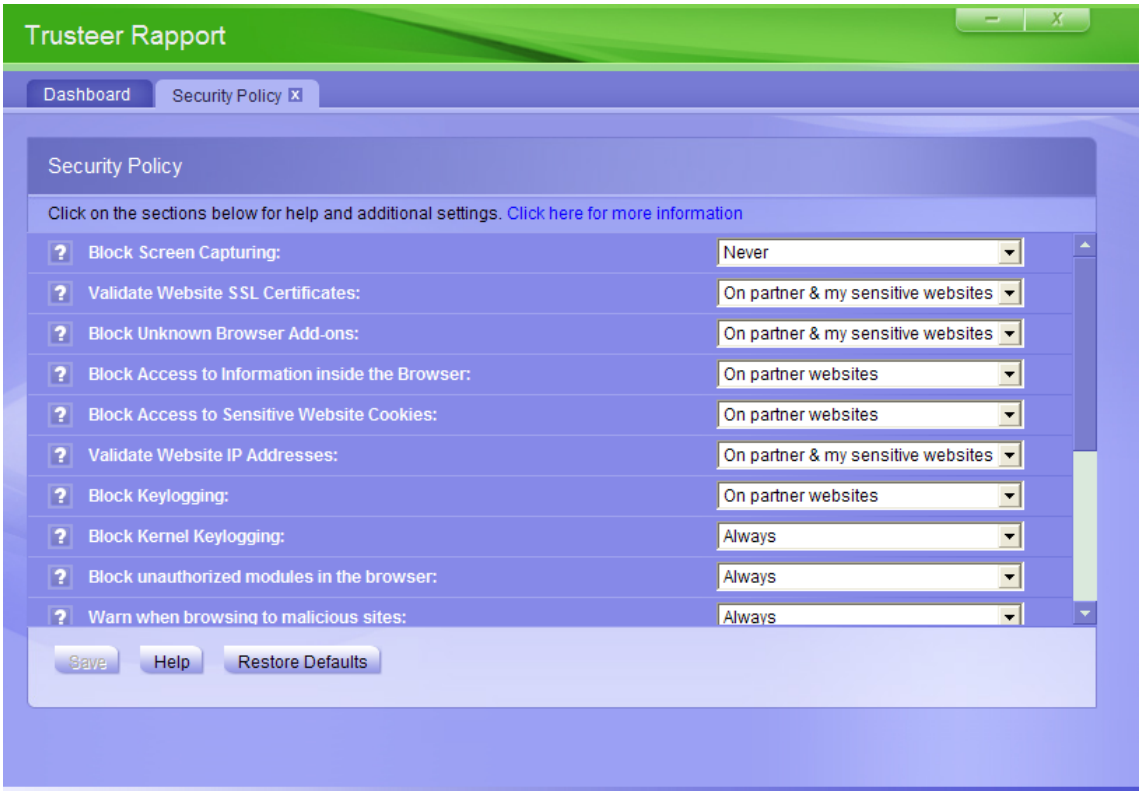
2. Dans le tableau de bord, cliquez sur . Le second écran du tableau de bord apparaît.



3. Dans la zone de la politique de sécurité, cliquez sur Modifier la politique. Un écran Approbation de l'utilisateur apparaît. L'écran vous montre l'image d'un mot pour que vous le saisissiez. Ceci est destiné à empêcher les logiciels malveillants d'accéder à la console et de désactiver Trusteer Rapport de manière efficace.

4. Saisissez le mot que vous voyez dans l'image.

5. Cliquez sur OK. L'écran Politique de sécurité apparaît, affichant tous les contrôles de sécurité.



6. Faites défiler jusqu'à la commande appelée Proposer l'utilisation du navigateur virtualisé de Trusteer Rapport sur les sites pris en charge. Sous Vous avez choisi de ne pas voir les alertes du navigateur virtualisé pour les sites suivants, cliquez sur le bouton Supprimer le site pour le site concerné.
7. Cliquez sur Enregistrer. Votre modification de la politique est enregistrée. Désormais, lorsque vous accédez au site, Trusteer Rapport affichera une alerte du navigateur virtualisé.

Répondre à une alerte facultative du navigateur virtualisé

Ceci est un exemple d'une alerte facultative du navigateur virtualisé.

Cette alerte s'affiche si le navigateur virtualisé de Trusteer Rapport est déjà installé sur votre ordinateur et que vous accédez à un site qui prend en charge le navigateur virtualisé de Trusteer Rapport. L'alerte vous offre la possibilité d'ouvrir le site dans le navigateur virtualisé.

Lorsque vous voyez cette alerte, sélectionnez l'une des options suivantes:

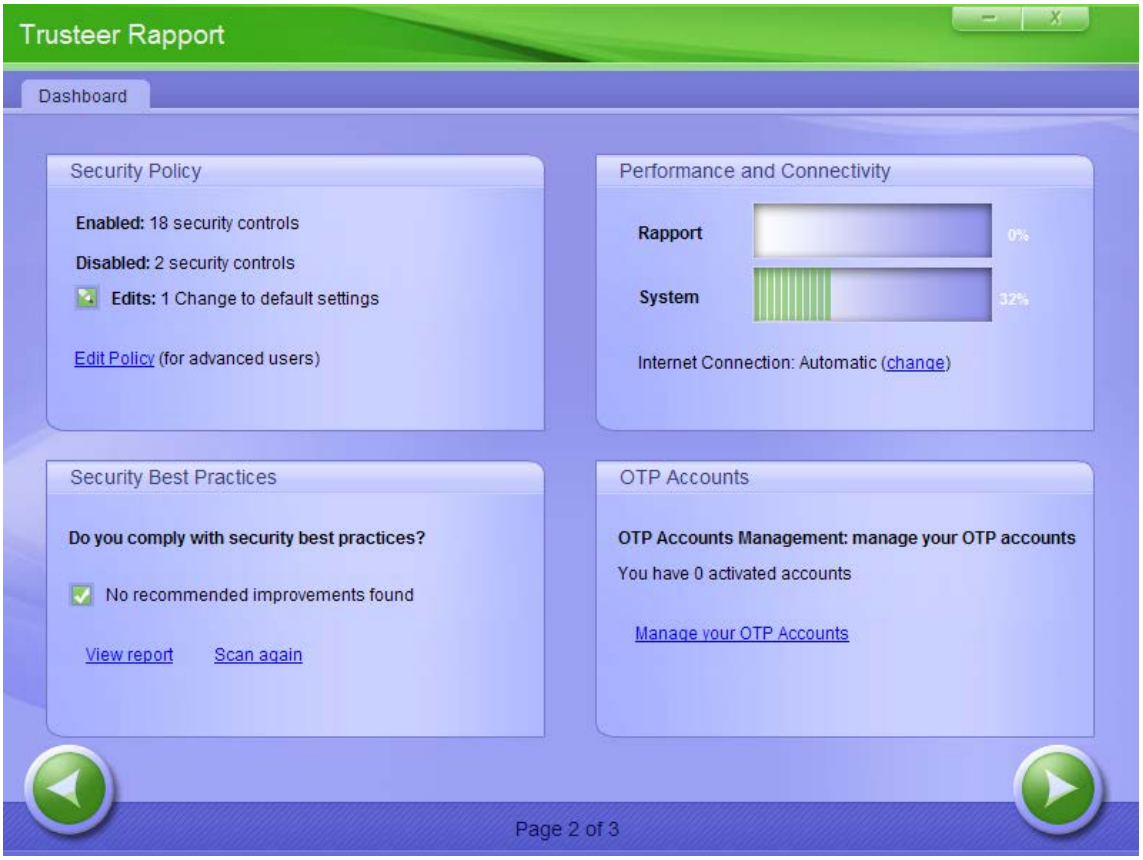
- Cliquez sur Oui pour ouvrir le site dans le navigateur virtualisé de Trusteer Rapport. Si vous cochez aussi la case Se souvenir de mon choix pour ce site, ce site sera automatiquement ouvert dans le navigateur virtualisé chaque fois que vous le visitez.
- Cliquez sur Qu'est-ce que le navigateur virtualisé ? Pour en savoir plus sur le navigateur virtualisé de Trusteer Rapport
- Cliquez sur Non pour ouvrir le site dans le navigateur normal. Si vous cochez la case Se souvenir de mon choix pour ce site, cette alerte ne s'affichera plus pour ce site, et le site s'ouvrira automatiquement dans le navigateur normal.
- Cliquez sur Ne plus afficher cette alerte pour modifier la politique de Trusteer Rapport de sorte que les sites qui prennent en charge le navigateur virtualisé s'ouvrent désormais par défaut dans le navigateur normal sans afficher cette alerte. Le site s'ouvre dans le navigateur normal.

J'ai cliqué sur Ne plus afficher cette alerte par erreur. Serais-je toujours en mesure d'ouvrir des sites dans le navigateur virtualisé?

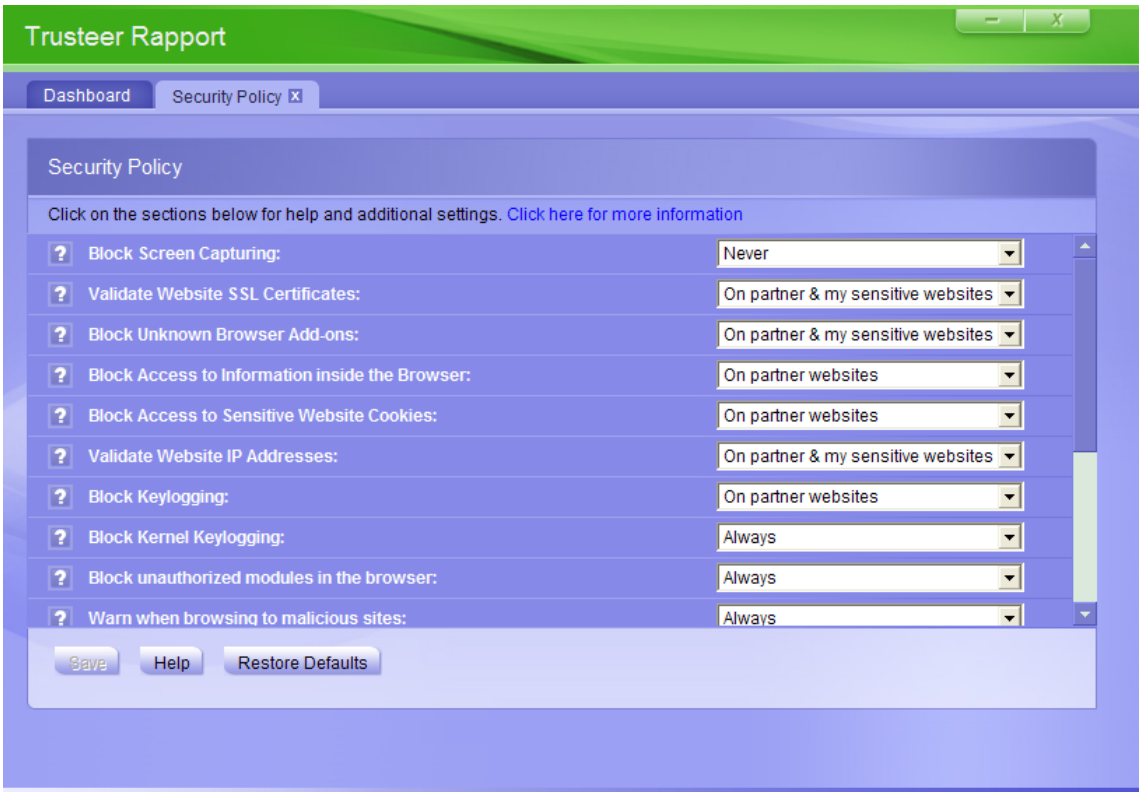
Lorsque vous avez cliqué sur Ne plus afficher cette alerte suite à une Répondre à une alerte facultative de téléchargement du navigateur virtualisé (on page 93) ou à une Répondre à une alerte facultative du navigateur virtualisé (on page 99), la politique de sécurité a été modifiée de sorte que vous ne soyez plus alerté lorsque vous accédez à un site qui prend en charge le navigateur virtualisé. Vous pouvez réinitialiser cette politique en utilisant la procédure suivante.

Pour réinitialiser la politique d'alerte du navigateur virtualisé:

1. Ouvrir la console Rapport (on page 72).
2. Dans le tableau de bord, cliquez sur . Le second écran du tableau de bord apparaît.



3. Dans la zone de la politique de sécurité, cliquez sur Modifier la politique. Un écran Approbation de l'utilisateur apparaît. L'écran vous montre l'image d'un mot pour que vous le saisissiez. Ceci est destiné à empêcher les logiciels malveillants d'accéder à la console et de désactiver Trusteer Rapport de manière efficace.
4. Saisissez le mot que vous voyez dans l'image.
5. Cliquez sur OK. L'écran Politique de sécurité apparaît, affichant tous les contrôles de sécurité.



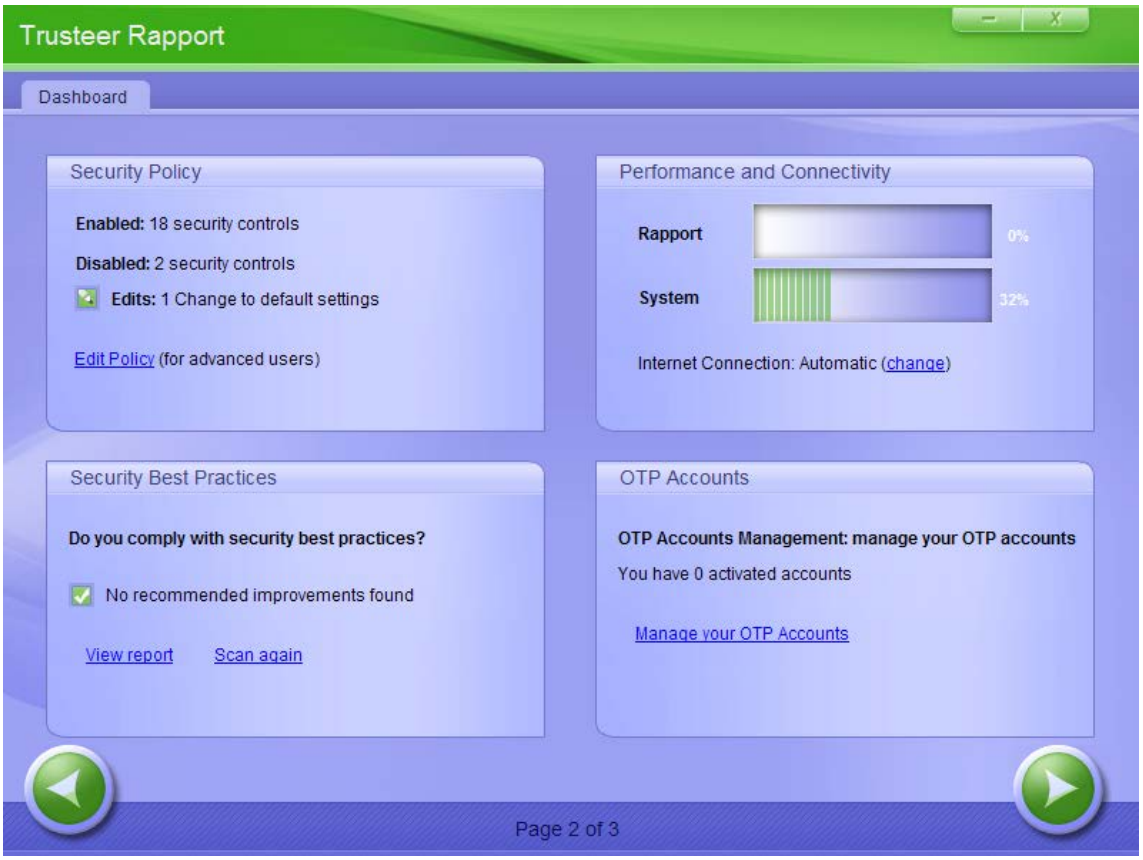
6. Faites défiler jusqu'au contrôle appelé Proposer l'utilisation du navigateur virtualisé de Trusteer Rapport sur les sites pris en charge. Dans le menu déroulant sur la droite de cette commande, sélectionnez Toujours pour réinitialiser la politique à sa valeur par défaut.
7. Cliquez sur Enregistrer. Votre modification de la politique est enregistrée. Désormais, lorsque vous accédez à des sites qui prennent en charge le navigateur virtualisé, Trusteer Rapport proposera d'ouvrir ces sites dans le navigateur virtualisé.

J'ai cliqué sur Oui et coché la case Se rappeler de ma décision pour ce site. Maintenant Je voudrais ouvrir le site dans le navigateur normal. Que dois-je faire?

Vous pouvez modifier la politique de sécurité pour rétablir la possibilité d'ouvrir le site dans le navigateur normal.

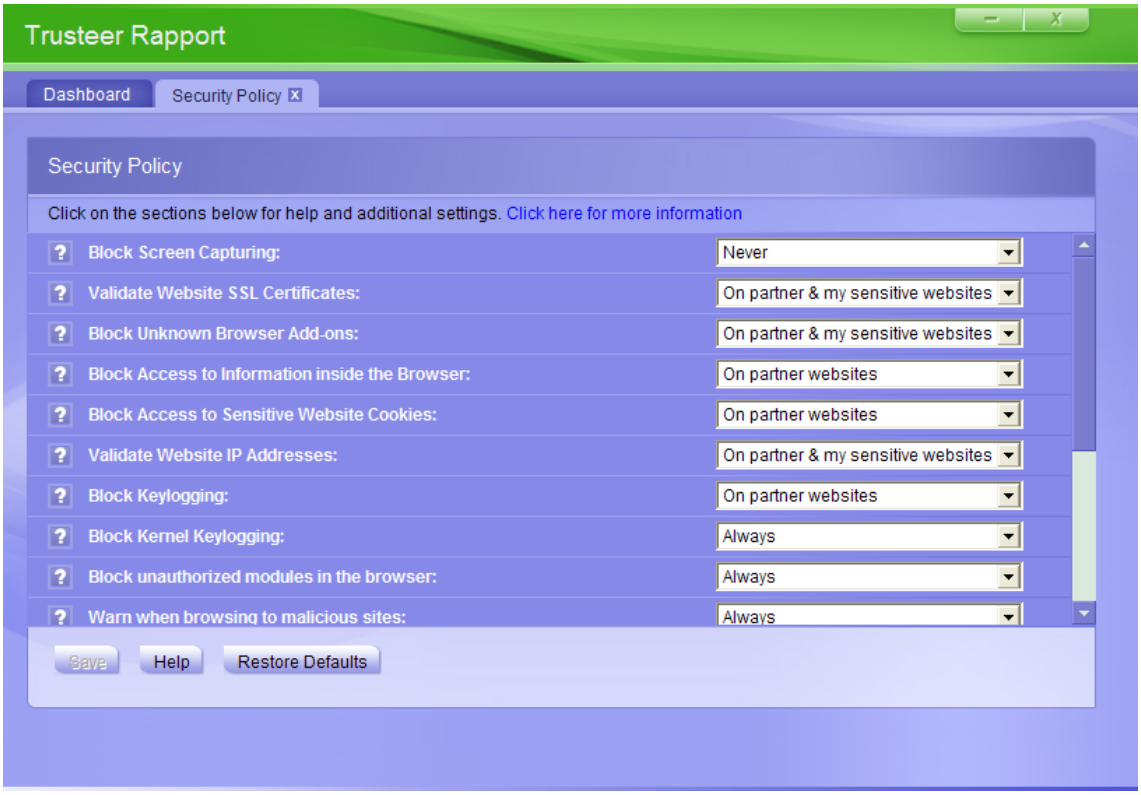
➡ **Pour modifier la politique du navigateur virtualisé pour un site:**

1. Ouvrir la console Rapport (on page 72).
2. Dans le tableau de bord, cliquez sur  . Le second écran du tableau de bord apparaît.



3. Dans la zone de la politique de sécurité, cliquez sur Modifier la politique. Un écran Approbation de l'utilisateur apparaît. L'écran vous montre l'image d'un mot pour que vous le saisissiez. Ceci est destiné à empêcher les logiciels malveillants d'accéder à la console et de désactiver Trusteer Rapport de manière efficace.
4. Saisissez le mot que vous voyez dans l'image.

5. Cliquez sur OK. L'écran Politique de sécurité apparaît, affichant tous les contrôles de sécurité.

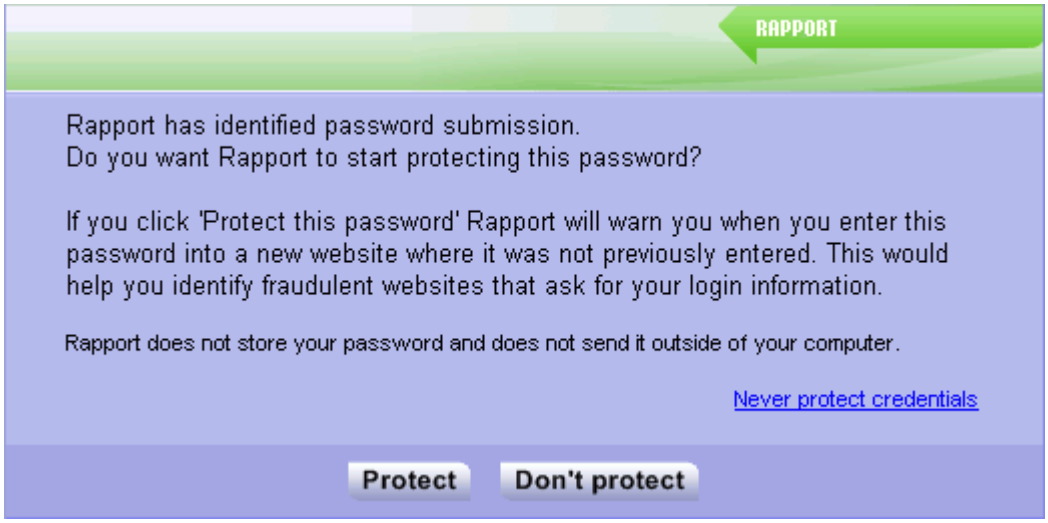


6. Faites défiler jusqu'à la commande appelée Proposer l'utilisation du navigateur virtualisé de Trusteer Rapport sur les sites pris en charge. Sous Vous avez choisi d'ouvrir les sites suivants en utilisant le navigateur virtualisé, Cliquez sur le bouton Supprimer le Site pour le site concerné.

7. Cliquez sur Enregistrer. Votre modification de la politique est enregistrée.

Répondre à une offre de protection du Mot de passe

Ceci est un exemple d'une offre de protection du Mot de passe:



Une offre de protection du mot de passe s'affiche une seule fois pour chaque site protégé. Cette offre apparaît la première fois que Trusteer Rapport détecte que vous avez saisi un mot de passe sur un site Web protégé. Par exemple, si vous avez récemment téléchargé Trusteer Rapport à partir du site Web de votre banque, et que par la suite vous vous êtes connecté à ce site, vous verrez cette boîte de dialogue. Autre exemple : si vous avez récemment protégé manuellement un site Web, et que par la suite vous vous êtes connecté à ce site Web.

Si vous entrez un mot de passe protégé sur un site Web que Trusteer Rapport ne reconnaît pas, Trusteer Rapport Responding to a Protected Information Warning que vous utilisez le mot de passe sur un autre site Web. Cet avertissement vous permet d'empêcher que votre mot de passe ne soit soumis à un site Web frauduleux. Cela vous aide à vous protéger contre les phishing attacks[3].

Lorsque vous voyez cette offre, choisissez l'une des options suivantes:

[3] Une attaque de phishing est une tentative pour vous inciter à visiter un faux site auquel vous faites confiance tel que votre banque, et à soumettre vos identifiants en ligne qui permettront à des criminels d'accéder en ligne à votre compte bancaire et de commettre une fraude, en transférant par exemple de l'argent depuis votre compte.

- Cliquez sur **Protéger**. À partir de ce moment, Trusteer Rapport protègera votre mot de passe pour ce site. Lorsque vous modifiez votre mot de passe, Trusteer Rapport protège automatiquement le nouveau mot de passe sans vous le demander.
- Cliquez sur **Ne pas protéger**. Si vous choisissez cette option, Trusteer Rapport ne protègera pas les mots de passe sur ce site et ne proposera plus de les protéger lorsque vous visitez ce site.
- Cliquez sur **Ne jamais protéger** les mots de passe. Ceci désactive la protection anti-hameçonnage de Trusteer Rapport sur tous les sites. Si vous cliquez dessus, Trusteer Rapport n'affichera plus d'avertissements liés à la soumission des mots de passe, et n'offrira plus de protéger les mots de passe sur des sites Web.

J'ai protégé le mauvais mot de passe! Que dois-je faire maintenant?

Il vous suffit de saisir le bon mot de passe. Trusteer Rapport le protégera.

J'ai saisi mon mot de passe de manière incorrecte et j'ai choisi de le protéger. Que dois-je faire?

Il vous suffit de ressaisir le mot de passe correctement. Trusteer Rapport protégera le bon mot de passe.

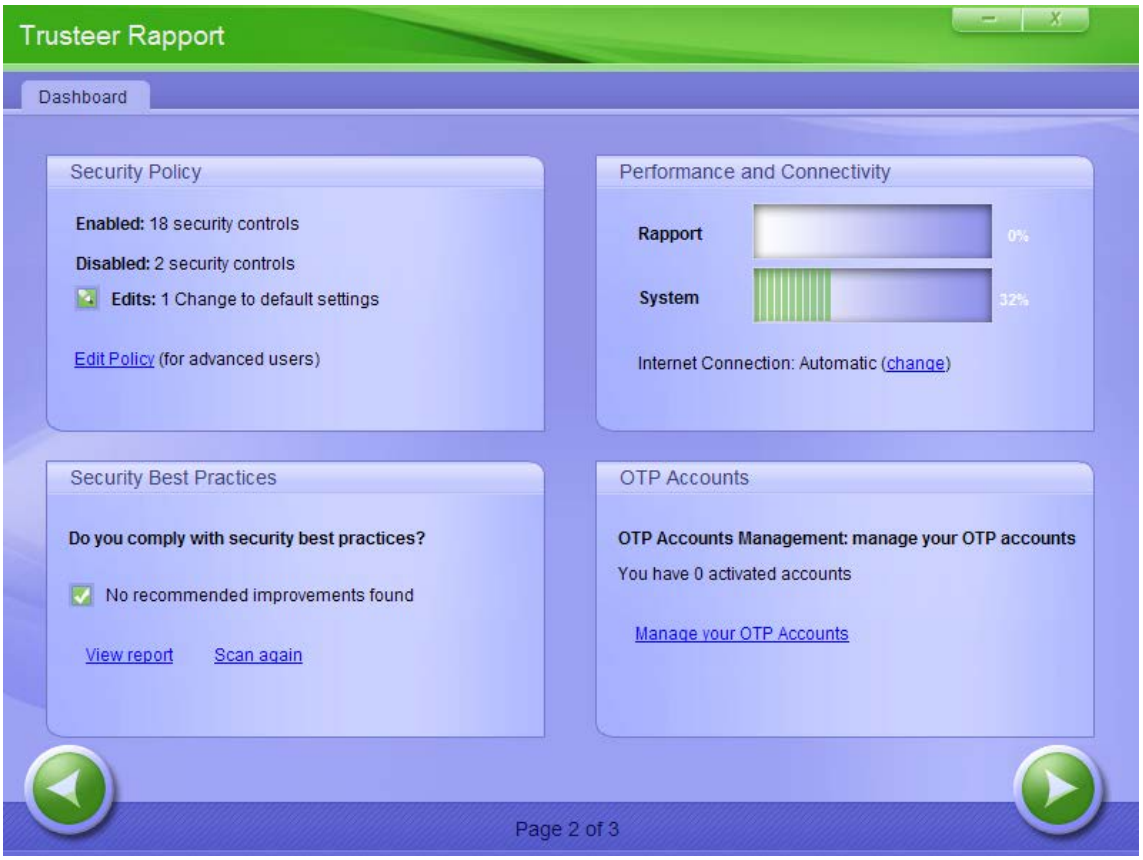
J'ai choisi de ne jamais protéger les mots de passe et maintenant je souhaite les protéger. Que dois-je faire?

Lorsque vous avez choisi de ne jamais protéger les mots de passe, une définition de politique a été définie dans la politique de sécurité de Trusteer Rapport. Vous pouvez modifier cette politique.

➡ **Pour modifier la politique de protection des mots de passe:**

1. Ouvrir la console Rapport (on page 72).

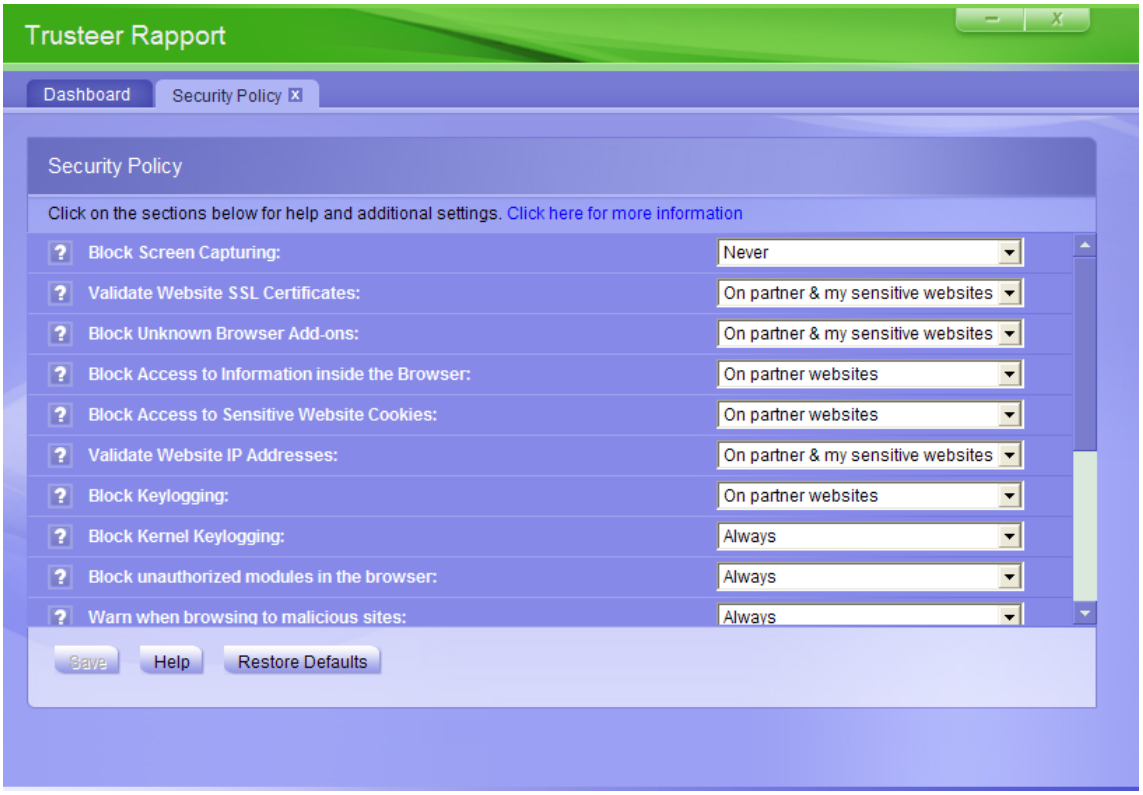
2. Dans le tableau de bord, cliquez sur . Le second écran du tableau de bord apparaît.



3. Dans la zone de la politique de sécurité, cliquez sur Modifier la politique. Un écran Approbation de l'utilisateur apparaît. L'écran vous montre l'image d'un mot pour que vous le saisissiez. Ceci est destiné à empêcher les logiciels malveillants d'accéder à la console et de désactiver Trusteer Rapport de manière efficace.

4. Saisissez le mot que vous voyez dans l'image.

5. Cliquez sur OK. L'écran Politique de sécurité apparaît, affichant tous les contrôles de sécurité.



6. Recherchez un contrôle appelé Avertir lorsque les identifiants de connexion sont utilisés sur des sites Web inconnus. Dans le menu déroulant à droite de cette commande, sélectionnez Sur les sites Web des partenaires et sur mes sites sensibles pour réinitialiser la politique à sa valeur par défaut ou sur les sites des partenaires, si vous bénéficiez d'une protection des mots de passe uniquement sur des sites de partenaires.
7. Cliquez sur Enregistrer. Votre modification de la politique est enregistrée.

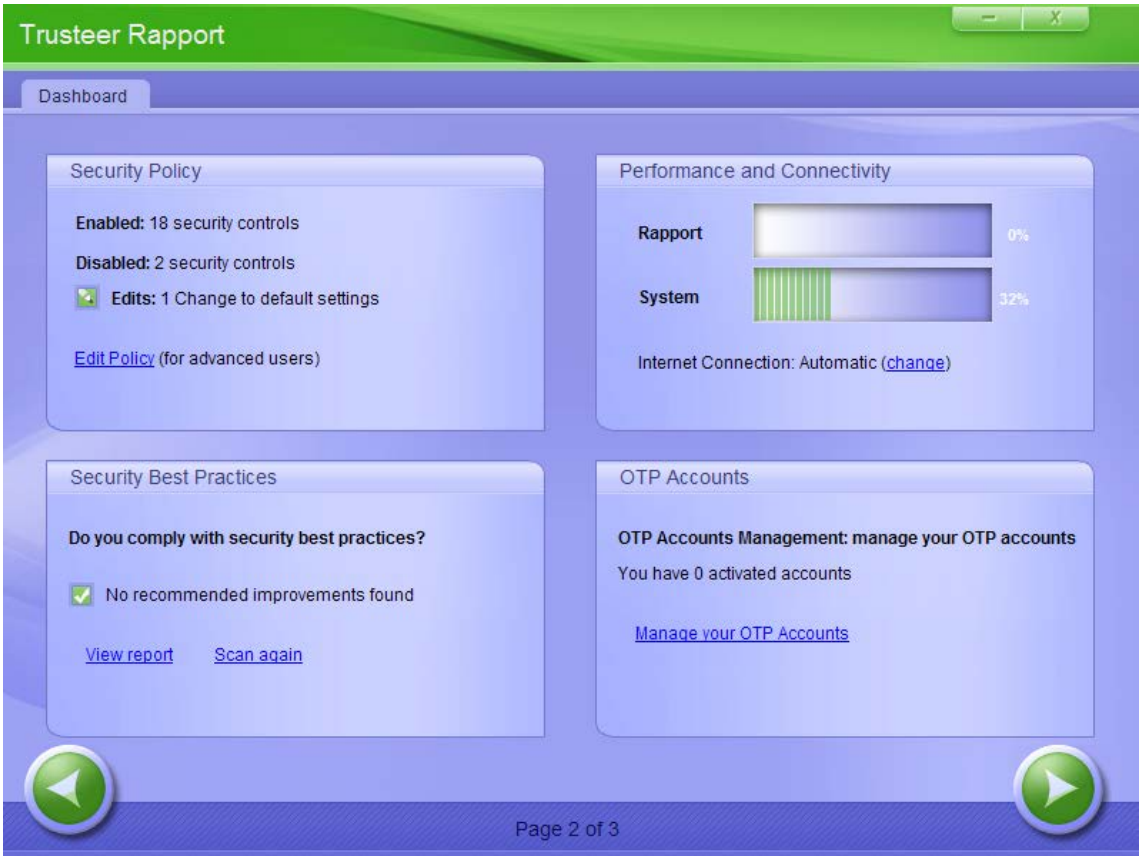
J'ai choisi « Ne pas protéger » et maintenant Je souhaite protéger mon mot de passe. Commentpuis-je le protéger?

Vous pouvez modifier la décision de protéger votre mot de passe pour ce site spécifique.

➡ **Pour activer la protection des mots de passe lorsqu'elle a été désactivée pour un site Web spécifique:**

1. Ouvrir la console Rapport (on page 72).

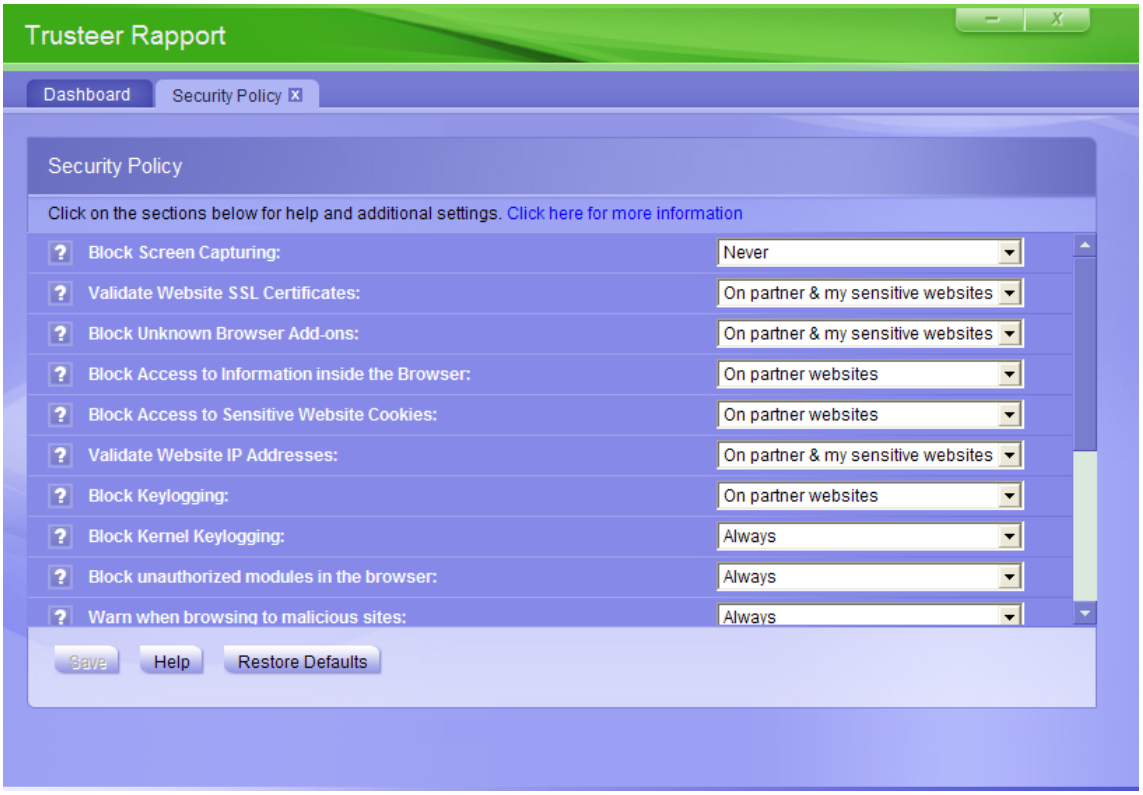
2. Dans le tableau de bord, cliquez sur . Le second écran du tableau de bord apparaît.



3. Dans la zone de la politique de sécurité, cliquez sur Modifier la politique. Un écran Approbation de l'utilisateur apparaît. L'écran vous montre l'image d'un mot pour que vous le saisissiez. Ceci est destiné à empêcher les logiciels malveillants d'accéder à la console et de désactiver Trusteer Rapport de manière efficace.

4. Saisissez le mot que vous voyez dans l'image.

5. Cliquez sur OK. L'écran Politique de sécurité apparaît, affichant tous les contrôles de sécurité.



6. Cliquez sur Avertir lorsque les identifiants de connexion sont utilisés sur des sites Web inconnus. La politique de protection des noms d'utilisateurs et des mots de passe sur chaque site est affichée.

7. Cochez la case Avertir si le mot de passe est utilisé ailleurs pour le site pour lequel vous souhaitez activer la protection des mots de passe. Trusteer Rapport protégera désormais votre mot de passe pour ce site.

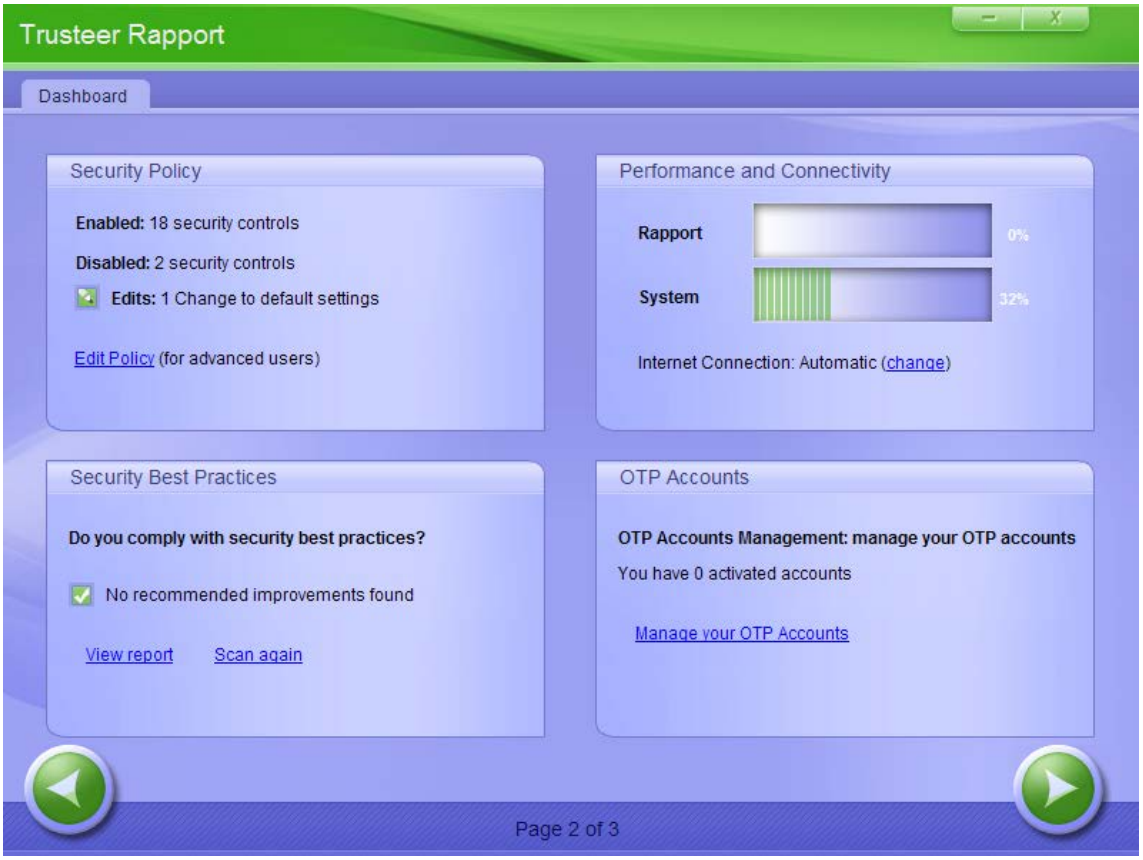
8. Cliquez sur Enregistrer. Votre modification de la politique est enregistrée.

J'ai reçu une alerte pour un mot de passe qui n'est plus utilisé. Comment puis-je arrêter cela?

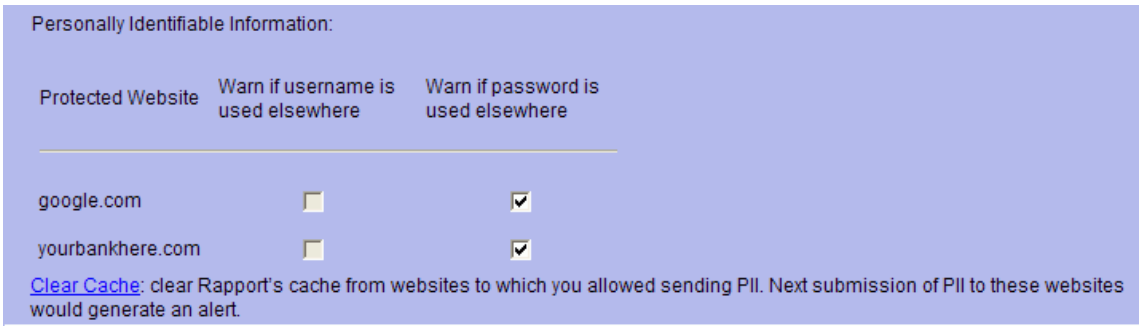
Selon notre accord avec les sites de nos partenaires, nous continuons souvent à protéger les mots de passe, même après les avoir remplacés. Ceci pose rarement de problèmes car les mots de passe sécurisés ne sont pas utilisés à d'autres fins. Si vous devez arrêter la protection de Trusteer Rapport d'un ancien mot de passe, vous pouvez effacer le cache des informations d'identification personnelle (PII) pour réinitialiser le mécanisme de protection des mots de passe. Cela arrêtera la protection de Trusteer Rapport de l'ancien mot de passe, mais celui-ci générera une nouvelle offre de protection des mots de passe la prochaine fois que vous visiterez chaque site Web protégé.

Pour effacer le cache des PII:

1. Ouvrir la console Rapport (on page 72).
2. Dans le tableau de bord, cliquez sur  . Le second écran du tableau de bord apparaît.



3. L'écran vous montre une image de caractères pour que vous les saisissiez. Ceci est destiné à empêcher les logiciels malveillants d'accéder à la console et de désactiver Trusteer Rapport de manière efficace.
4. Saisissez les caractères que vous voyez dans l'image.
5. Cliquez sur OK. L'écran de la politique de sécurité apparaît, affichant tous les contrôles de sécurité.
6. Faites défiler la liste des contrôles de sécurité jusqu'à ce que vous trouverez Avertir Lorsque les identifiants de connexion sont utilisés sur des sites Web inconnus.
7. Cliquez sur Avertir lorsque les identifiants de connexion sont utilisés sur des sites Web inconnus. La politique de protection des noms d'utilisateurs et des mots de passe sur chaque site est affichée.



8. Cliquez sur Effacer le cache. La protection de tous les mots de passe est effacée et toutes les politiques de protection des mots de passe sont réinitialisées, faisant en sorte que Trusteer Rapport affiche une offre de protection des mots de nouveau la prochaine fois que vous visitez chaque site.

J'ai saisi un mot de passe sur un site autre que celui pour lequel j'ai protégé le mot de passe, mais je n'ai pas reçu d'alerte. Pourquoi?

Certains sites légitimes ont déjà été identifiés par Trusteer Rapport comme légitimes. Puisque la saisie de votre mot de passe ne mènera pas à une éventuelle fraude, Trusteer Rapport ne génère pas d'avertissement pour ces sites.

Répondre à une alerte d'informations protégées

Ceci est un exemple d'un avertissement d'informations protégées:

Une alerte d'informations protégées apparaît lorsque vous saisissez du texte qui correspond à un nom d'utilisateur ou à un mot de passe protégé sur un site Web que Trusteer Rapport ne reconnaît pas. Le but de ce message est de vérifier que le site sur lequel vous êtes actuellement en train de soumettre vos identifiants n'est pas un site Web frauduleux qui essaie de voler vos informations d'identification sensibles. C'est ce qu'on appelle une attaque d'hameçonnage.

Dans l'exemple ci-dessus, Trusteer Rapport veut s'assurer que le site www.example-phishing.com (un faux site) ne fait pas semblant d'être google.com et qu'il ne cherche pas à vous inciter à y entrer vos informations d'identification de google.com.

Lorsque vous voyez cette alerte, choisissez l'une des options suivantes:

- Cliquez sur Faîtes confiance à ce site si vous êtes heureux d'envoyer vos identifiants de connexion à ce site, et si vous savez que le site ne demande pas d'informations d'identification d'un autre site Web. Après avoir cliqué sur ce bouton, vous ne serez pas averti à nouveau si vous entrez le nom d'utilisateur ou le mot de passe protégé sur ce site. Si le texte que vous avez saisi ne contient pas vos identifiants de connexion ou contient des identifiants de connexion que vous utilisez sur plusieurs sites et que vous souhaitez le saisir sans être alerté chaque fois que vous l'utilisez, vous pouvez aussi cocher l'option Ne protéger ces identifiants de connexion sur aucun site Web.

Remarque: La pratique de sécurité recommandée est de choisir des mots de passe qui contiennent des phrases uniques, difficiles à prédire et de ne pas utiliser le même mot de passe pour plusieurs sites Web. Si vous suivez cette pratique, il est peu probable que vous ayez besoin de cocher l'option Ne protéger ces identifiants de connexion sur aucun site web.

- Cliquez sur Sortez-moi de là ! Si vous ne souhaitez pas envoyer vos identifiants de connexion à ce site. Une boîte de dialogue vous invite à choisir le site vers lequel vous souhaitez être redirigé.

Pourquoi reçois-je tant d'avertissements d'informations protégées?

Si vous utilisez du texte que vous saisissez régulièrement comme mot de passe sur de nombreux sites différents, vous recevrez un avertissement d'informations protégées chaque fois que vous entrez ce mot sur un site autre que le site pour lequel le mot de passe a été protégé. Afin d'éviter tout agacement que cela peut causer, ne protégez pas les mots de passe de ce genre. Si vous utilisez ce type de mot de passe pour un site Web sur lequel vous échangez des informations confidentielles, nous vous conseillons fortement de changer votre mot de passe en un mot de passe plus sécurisé. Un mot de passe sécurisé est unique pour le site sur lequel vous l'utilisez, et se compose d'une séquence de caractères difficiles à prédire. Il est généralement composé d'une combinaison de lettres, de chiffres et de symboles.

J'ai saisi un mot de passe protégé sur un site Web qui n'est pas protégé par Trusteer Rapport, mais ce dernier ne m'a pas alerté. Pourquoi?

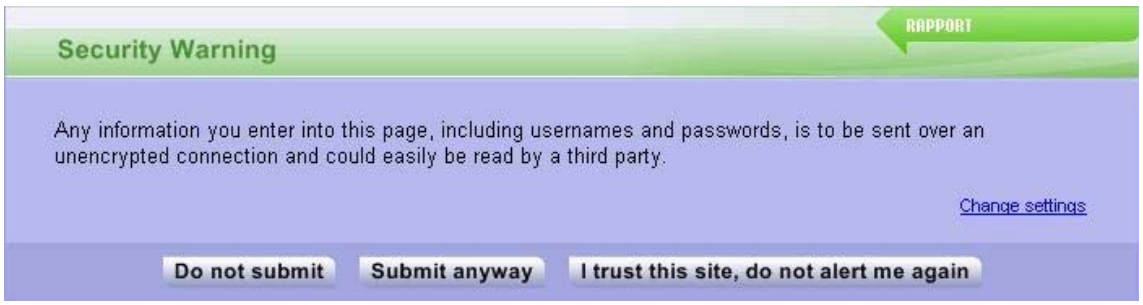
Trusteer Rapport utilise plusieurs méthodes pour reconnaître certains sites comme légitime. Si vous pensez que Trusteer Rapport aurait dû vous alerter et qu'il ne l'a pas fait, veuillez contacter le Getting Support (on page 196).

J'ai reçu une alerte d'informations protégées mais je n'ai pas saisi de mot de passe protégé. Pourquoi?

Pour certains sites protégés, Trusteer Rapport protège tous les mots de passe que vous avez déjà saisis sur ce site après l'installation de Trusteer Rapport. Cela inclut les anciens mots de passe et même des mots que vous y avez saisis par accident. Cela peut expliquer la raison pour laquelle vous avez reçu cette alerte.

Répondre à une alerte de soumission non sécurisée

Ceci est un exemple d'une alerte de soumission non sécurisée:



Cette alerte apparaît lorsque vous venez de saisir un mot de passe sur un site qui envoie les données de manière non sécurisée. Le but de cette alerte est de vous protéger contre l'envoi de données sensibles sur des sites à haut risque, y compris des sites légitimes qui pourraient facilement être interceptés par des personnes malveillantes.

Lorsque vous voyez ce message, effectuez l'une des actions suivantes :

- Cliquez sur Ne pas envoyer pour arrêter l'envoi. Votre navigateur est redirigé vers une page web de Trusteer qui vous explique le risque d'envoyer vos données sur des sites non sécurisés.
- Cliquez sur Envoyer quand même pour continuer l'envoi malgré l'avertissement.

- Cliquez sur J'ai confiance en ce site, ne plus m'alerter pour procéder à l'envoi malgré l'avertissement et pour demander à Trusteer Rapport de faire confiance à ce site à l'avenir. Si vous cliquez sur ce bouton, le site est ajouté à une liste de sites auxquels vous faites confiance et que vous ne souhaitez pas que Trusteer Rapport vous en alerte à l'avenir. Si vous décidez que vous voulez supprimer le site de la liste, voir Supprimer les sites de confiance pour les envois non sécurisés (on page 208).
- Cliquez sur Modifier les paramètres pour ouvrir l'écran Politique de sécurité de Trusteer Rapport et modifier la politique M'avertir lorsque j'envoie des données de sécurité sur des sites non sécurisés qui contrôle les alertes de ce type que vous recevez.

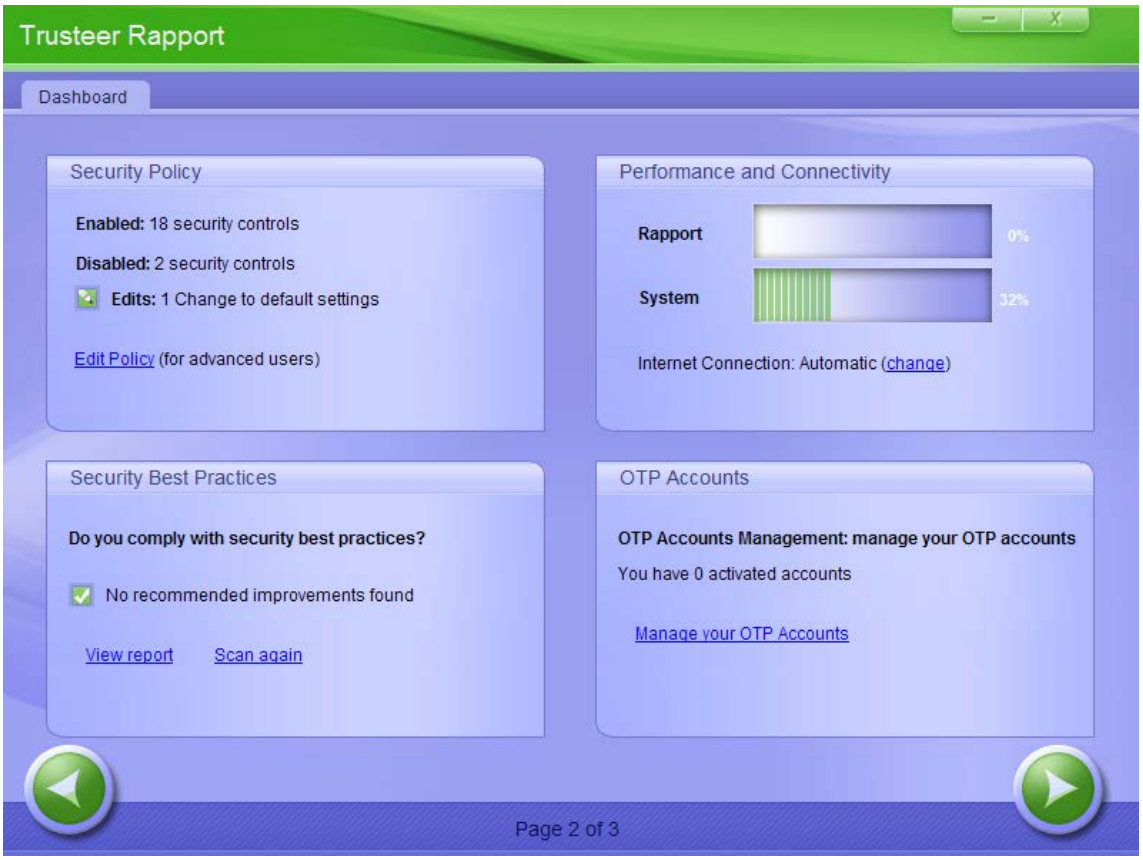
J'ai cliqué sur « J'ai confiance en ce site, ne plus m'alerter. » Puis-je supprimer le site de la liste des sites de confiance?

Oui, vous le pouvez le faire.

➡ **Pour supprimer un site de la liste des sites dont vous avez choisi de faire confiance:**

1. Ouvrir la console Rapport (on page 72).

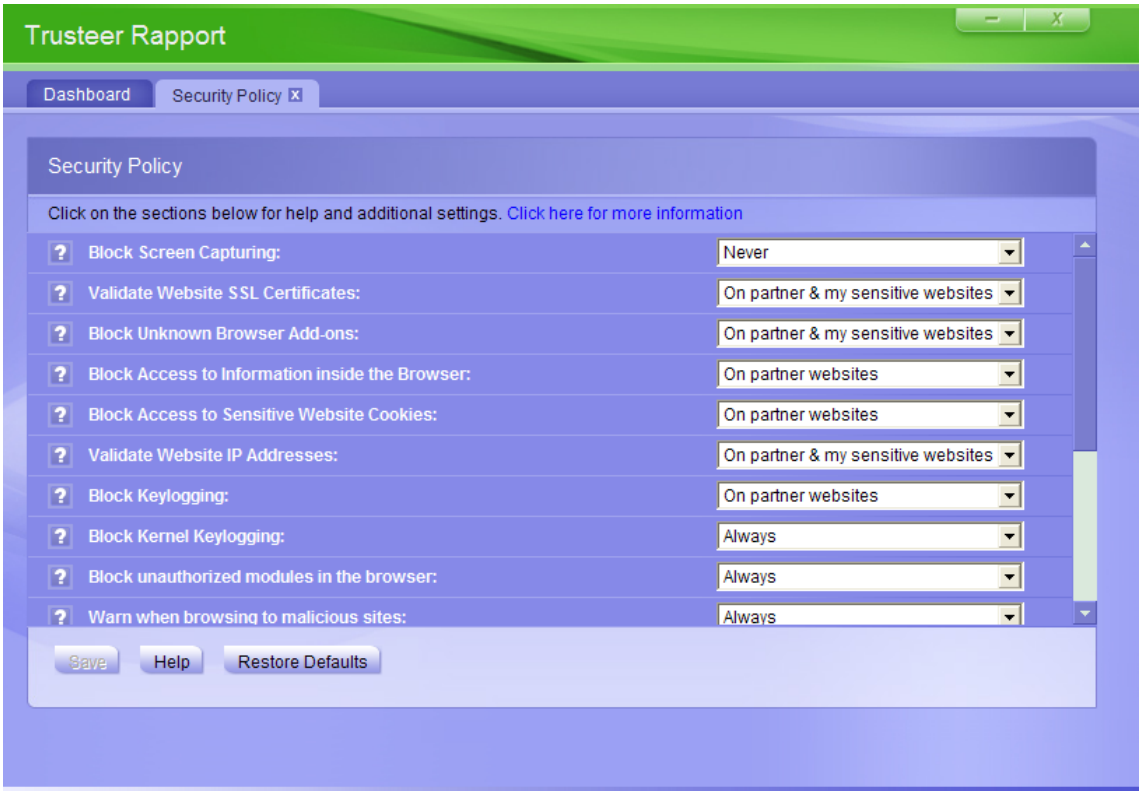
2. Dans le tableau de bord, cliquez sur . Le second écran du tableau de bord apparaît.



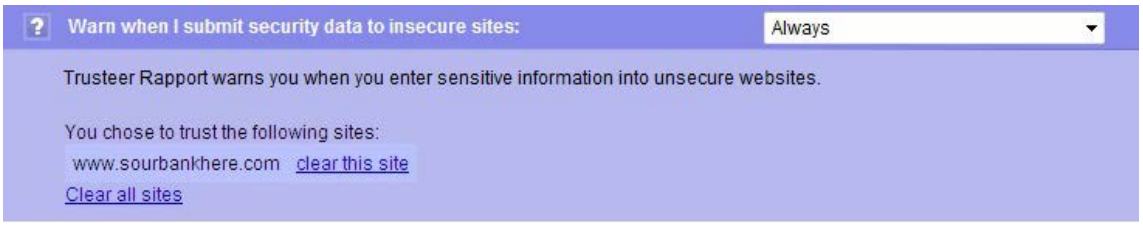
3. Dans la zone de la politique de sécurité, cliquez sur Modifier la politique. Un écran Approbation de l'utilisateur apparaît. L'écran vous montre l'image d'un mot pour que vous le saisissiez. Ceci est destiné à empêcher les logiciels malveillants d'accéder à la console et de désactiver Trusteer Rapport de manière efficace.

4. Saisissez le mot que vous voyez dans l'image.

5. Cliquez sur OK. L'écran Politique de sécurité apparaît, affichant tous les contrôles de sécurité.



6. Cliquez sur le contrôle de la politique appelé M'avertir lorsque j'envoie des données de sécurité sur des sites non sécurisés. La phrase « Vous avez choisi de faire confiance aux sites suivants : » apparait, suivies d'une liste des sites dont vous avez choisi de faire confiance.

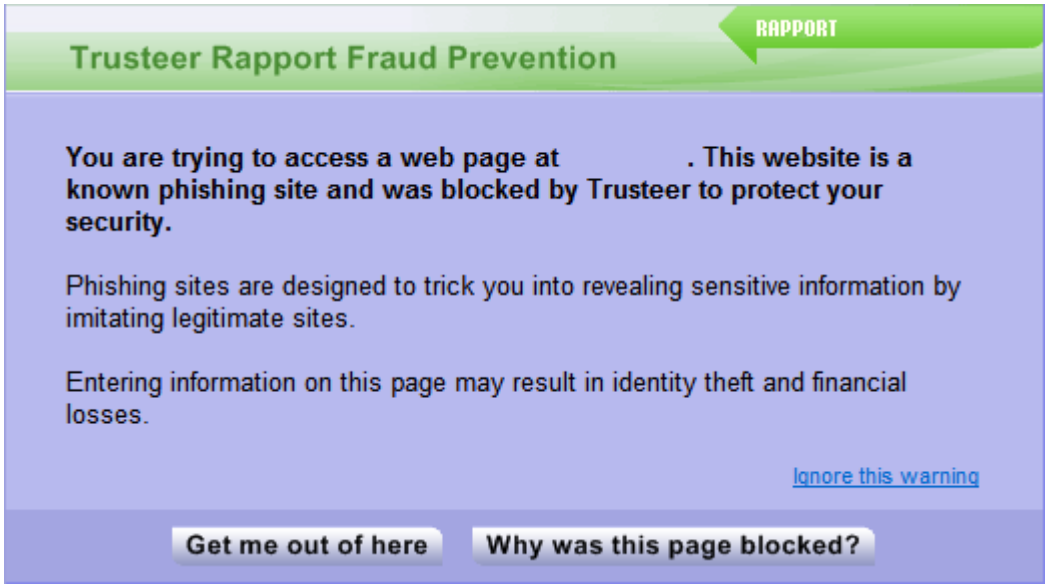


7. Trouvez le site que vous avez ajouté à la liste blanche et cliquez sur le bouton Effacer ce site qui apparaît à côté du site.

8. Cliquez sur Enregistrer. Votre modification de la politique est enregistrée.

Répondre à une alerte de site d'hameçonnage

Ceci est un exemple d'une alerte d'un site d'hameçonnage:



Cette alerte s'affiche lorsque Trusteer Rapport bloque un site Web que vous aviez l'intention de visiter, car Trusteer Rapport a vérifié que le site est faux, souvent connu comme un site d'hameçonnage. Trusteer Rapport dispose de grandes capacités pour détecter avec précision les sites d'hameçonnage. Cet avertissement qui apparaît lorsque vous visitez un site Web suspect est fourni pour vous empêcher d'être victime de fraude liée à l'hameçonnage. Si cet avertissement est apparu après avoir cliqué sur un lien vers un site web, il est très probable que le lien est frauduleux et le risque est plus grand.

Si vous voyez cet avertissement, choisissez l'une des options suivantes :

- Cliquez sur Sortez-moi de là ! Ceci redirige votre navigateur vers le site précédent que vous avez visité.
- Cliquez sur Pourquoi cette page a-t-elle été bloquée ? Ceci ouvre une page web qui explique la raison pour laquelle cet avertissement apparaît.

- Cliquez sur Ignorer cet avertissement. Ceci charge le site malgré les risques signalés. Vous accéderez à un site Web qui a été vérifié comme étant créé par des personnes malveillantes dans le but frauduleux de voler des identifiants confidentiels de connexion aux comptes. Dans certains sites Web d'hameçonnage, la saisie des données, même sans cliquer sur Envoyer, est suffisante pour que les personnes malveillantes les reçoivent et ensuite les utilisent pour commettre un vol d'identité. Nous vous conseillons fortement de ne pas choisir cette option.

Que dois-je faire si je pense qu'un site Web légitime a été marqué comme un site d'hameçonnage?

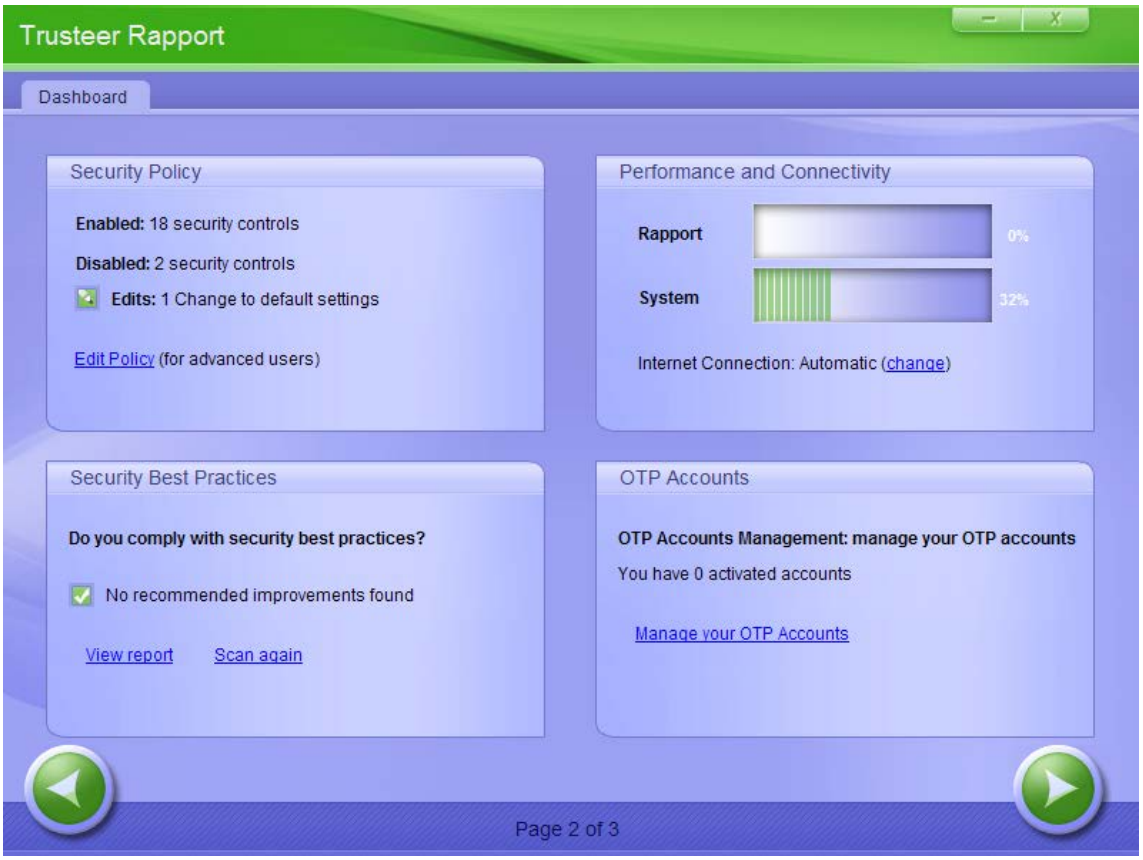
Si vous pensez qu'un site Web légitime a été marqué comme un site d'hameçonnage, veuillez envoyer une capture d'écran du site et de l'alerte que vous avez reçue à support@trusteer.com.

Comment puis-je désactiver les alertes de prévention des fraudes?

Pour désactiver les alertes de prévention des fraudes :

1. Ouvrir la console Rapport (on page 72).

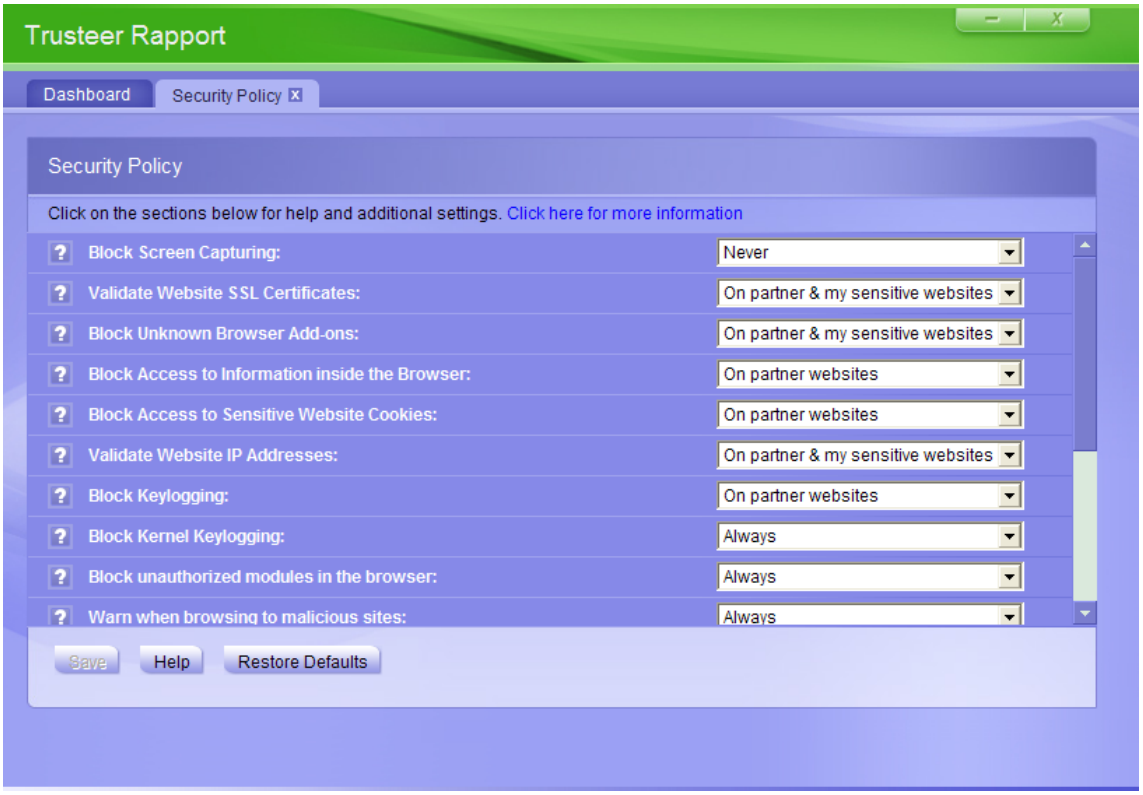
2. Dans le tableau de bord, cliquez sur . Le second écran du tableau de bord apparaît.



3. Dans la zone de la politique de sécurité, cliquez sur Modifier la politique. Un écran Approbation de l'utilisateur apparaît. L'écran vous montre l'image d'un mot pour que vous le saisissiez. Ceci est destiné à empêcher les logiciels malveillants d'accéder à la console et de désactiver Trusteer Rapport de manière efficace.

4. Saisissez le mot que vous voyez dans l'image.

5. Cliquez sur OK. L'écran Politique de sécurité apparaît, affichant tous les contrôles de sécurité.



6. Paramétrez le contrôle appelé Avertir lors de la navigation vers des sites malveillants sur jamais.

7. Cliquez sur Enregistrer. Votre modification de la politique est enregistrée.

Répondre à une alerte d'une page Web infectée

Ceci est un exemple d'une alerte d'une page Web infectée:

Cette boîte de dialogue s'affiche si Trusteer Rapport identifie la page que vous envisagiez de visiter comme une page qui pourrait infecter votre ordinateur par des logiciels malveillants. Trusteer Rapport fournit cette protection pour vous empêcher de devenir une victime de fraude en ligne.

Lorsque vous voyez cette boîte de dialogue, sélectionnez l'une des options suivantes:

- Cliquez sur Sortez-moi de là ! Ceci redirigera votre navigateur vers votre page d'accueil.
- Cliquez sur Pourquoi cette page a-t-elle été bloquée ? Ceci ouvre une page web qui explique la raison pour laquelle cet avertissement apparaît (https://www.trusteer.com/support/trusteer-fraud-prevention-infected-webpage).
- Cliquez sur Ignorer et signaler l'erreur. Ceci charge le site, malgré les risques signalés. Un rapport anonyme sera envoyé aux serveurs de Trusteer. Vous avez choisi de continuer vers le site malgré les risques signalés et votre ordinateur peut être infecté par des logiciels malveillants.

Répondre à une alerte de détection d'envoi de carte de paiement

Ceci est un exemple d'une alerte d'envoi de carte de paiement:

Cet avertissement apparaît lorsque vous entrez un numéro de carte de paiement protégé sur une page Web qui réside sur un disque local ou sur un site Web non sécurisé. Le but de ce message est de vous permettre d'éviter d'envoyer votre numéro de carte de paiement à un site d'hameçonnage ou à un site Web légitime non sécurisé.

Lorsque vous voyez cette alerte, effectuez l'une des actions suivantes :

- Cliquez sur Sortez-moi de là ! Si vous ne souhaitez pas envoyer les informations de votre carte à ce site. Votre navigateur quitte le site et charge à sa place votre page d'accueil.
- Cliquez sur Ignorer, j'ai confiance en ce site si vous êtes heureux d'envoyer les informations de votre carte à ce site. Les boîtes de dialogue se ferment, mais Trusteer Rapport continue de bloquer les enregistreurs de frappe pour qu'ils ne puissent pas capturer vos informations de carte de paiement. L'émetteur de votre carte de paiement reçoit une notification de cet envoi. Si vous décidez que vous voulez supprimer un site dont vous avez choisi d'avoir confiance, voir Supprimer les sites de confiance pour l'envoi d'informations de carte de paiement (on page 205).

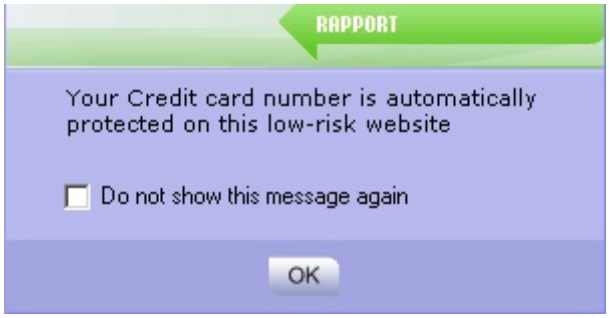
Remarque: En choisissant d'ignorer cet avertissement, vous envoyez vos informations de carte de paiement soit à un site malveillant connu, soit à un site qui ne les crypte pas, et elles risquent d'être interceptées par un tiers.

- Cliquez sur Toujours faire confiance à ce site. Désormais, Trusteer Rapport fait confiance à ce site et n'affiche plus cet avertissement lorsque vous entrez un numéro de carte de paiement sur ce site. Trusteer Rapport continue de bloquer les enregistreurs de frappe pour qu'ils ne puissent pas capturer vos informations de carte de paiement.
- Cliquez sur Arrêter de protéger les cartes. Cela désactive la fonction de protection des cartes de paiement. Si vous souhaitez réactiver cette fonction, changer la politique Protéger les numéros de cartes de paiement du vol de Jamais à Toujours. Pour obtenir des instructions sur la façon de modifier la politique de sécurité, voir Modifier les règles de sécurité (on page 178).

Remarque: La protection des cartes de paiement n'est activée que pour les marques de cartes de paiement participantes.

Répondre à un message de protection des cartes de paiement

Ceci est un exemple d'un message de protection des cartes de paiement:



Ce message vous informe que Trusteer Rapport a détecté que vous êtes en train d'envoyer un numéro de carte de paiement sur une page web, et il est en train de crypter vos frappes sur la page pour empêcher d'éventuels logiciels malveillants d'intercepter le numéro de votre carte de paiement. Ce message apparaît lorsque vous entrez un numéro de carte de paiement protégé sur un site protégé par Trusteer Rapport ou un site sécurisé (https) qui contient un mot clé lié à la carte de paiement tel que Visa, Mastercard, ou Amex.

Lorsque ce message s'affiche, vous n'avez pas besoin de faire quoi que ce soit. Vous pouvez éventuellement cliquer sur OK pour fermer le message. Si vous ne faites rien, il disparaîtra par lui-même après un court laps de temps.

Si vous ne voulez pas recevoir des notifications lorsque Trusteer Rapport active la protection contre les enregistreurs de frappe, cliquez sur Ne plus afficher ce message. Si vous souhaitez réactiver ces notifications, allez dans la politique de sécurité et cocher l'option Prévenez-moi lorsque Trusteer active la protection des cartes de paiement sous la politique protéger les numéros de cartes de paiement du vol. Pour obtenir des instructions sur la façon d'accéder à, et de modifier la politique de sécurité, voir Modifier les règles de sécurité (on page 178).

Remarque: La protection des cartes de paiement n'est activée que pour les marques de cartes de paiement participantes.

Répondre à une alerte de détection d'une tentative d'impression écran

Ceci est un exemple d'une alerte de détection d'une tentative d'impression écran:

Cette boîte de dialogue s'affiche si le bouton de commande d'impression écran sur votre ordinateur est enfoncé à un moment où votre navigateur affiche un site d'un partenaire. La boîte de dialogue vous permet de choisir si vous souhaitez bloquer ou autoriser le mécanisme de capture d'écran.

Le bouton de commande Impression écran sur votre clavier est utilisé légitimement pour capturer des écrans. Cependant, il est possible pour les logiciels malveillants d'activer le même mécanisme que ce bouton active, et de récupérer des informations sensibles à des fins frauduleuses.

Remarque: Cette alerte fait partie de la fonction de blocage des captures d'écran, activée par défaut sur les sites des partenaires. Découvrez avec plus de détails la fonction de blocage des captures d'écran de Trusteer Rapport dans Comprendre les règles de sécurité (on page 182).

Lorsque vous voyez cet avertissement, choisissez l'une des options suivantes:

- Cliquez sur Autoriser. Ceci permet au bouton de commande Impression écran de capturer votre écran. Sélectionnez cette option si vous avez volontairement appuyé sur le bouton de commande d'impression écran pour capturer l'écran.
- Cliquez sur Bloquer. Ceci empêche le bouton de commande Impression écran de capturer votre écran. Sélectionnez cette option si vous n'avez pas intentionnellement appuyé sur le bouton de commande Impression écran de votre clavier.

Je reçois la boite de dialogue même si je n'essaie pas de capturer un site sensible.

Réduisez ou fermez toutes les fenêtres du navigateur et essayez à nouveau.

Répondre à une alerte de protection du navigateur

Ceci est un exemple d'une alerte de protection du navigateur:

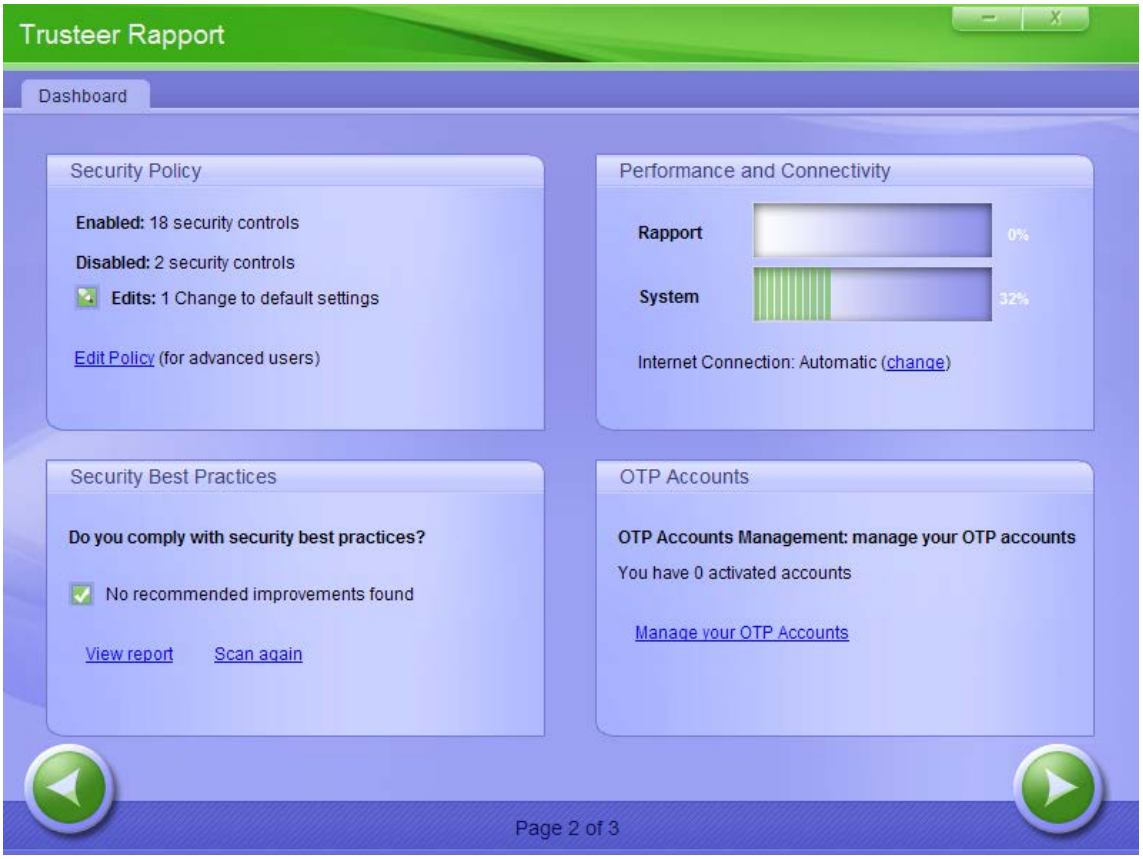
Cette boîte de dialogue s'affiche lorsqu'un module complémentaire du navigateur (barre d'outils, extension, ou autre) tente d'accéder à des informations appartenant à un site protégé en utilisant une méthode qui n'est pas actuellement surveillée par Trusteer Rapport.

Lorsque vous voyez cette boîte de dialogue, sélectionnez l'une des options suivantes :

- Cliquez sur Autoriser de façon permanente. Cela incite Trusteer Rapport à autoriser ce module complémentaire à fonctionner sur n'importe quel site Web. Choisissez cette option si vous connaissez la fonctionnalité de ce module complémentaire dans le navigateur, si vous l'utilisez, et si vous faites confiance à sa source.
- Cliquez sur bloquer de façon permanente. Cela incite Trusteer Rapport à bloquer l'exécution de ce module complémentaire sur n'importe quel site Web et envoie anonymement à Trusteer un rapport de sécurité sur le module qui a été bloqué afin que nos experts en sécurité puissent l'analyser. Cette soumission permet à Trusteer de bloquer le module de manière globale et permanente s'il est avéré malveillant.

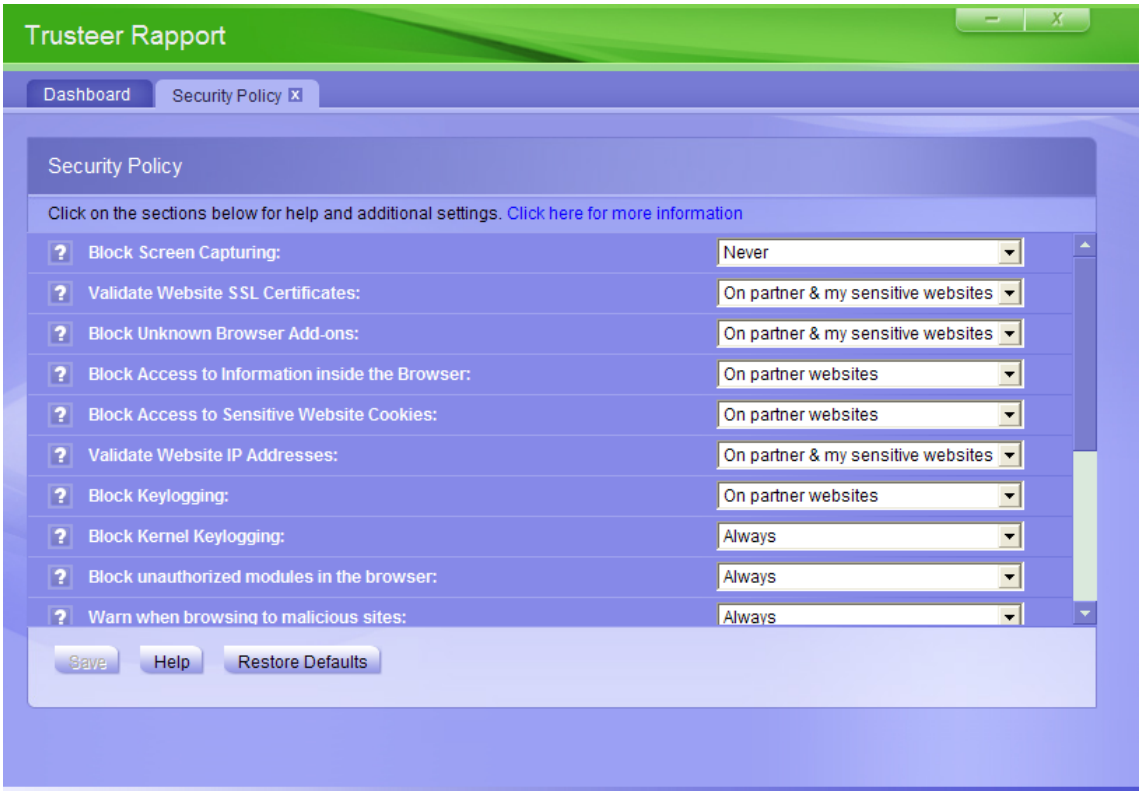
Pour modifier l'état du module que vous avez bloqué ou autorisé:

1. Ouvrir la console Rapport (on page 72).
2. Dans le tableau de bord, cliquez sur . Le second écran du tableau de bord apparaît.



3. Dans la zone de la politique de sécurité, cliquez sur Modifier la politique. Un écran Approbation de l'utilisateur apparaît. L'écran vous montre l'image d'un mot pour que vous le saisissiez. Ceci est destiné à empêcher les logiciels malveillants d'accéder à la console et de désactiver Trusteer Rapport de manière efficace.
4. Saisissez le mot que vous voyez dans l'image.

5. Cliquez sur OK. L'écran Politique de sécurité apparaît, affichant tous les contrôles de sécurité.



6. Cliquez sur bloquer le module du navigateur inconnu. Une liste de tous les modules que vous avez autorisés ou bloqués apparaît sous le nom de la politique.
7. Basculer entre les statuts Bloqué et Autorisé de chaque module, si nécessaire.
8. Cliquez sur Enregistrer. Vos modifications sont enregistrées.

Répondre à une alerte pour activer la suppression des logiciels malveillants

Ceci est un exemple d'une alerte pour activer la suppression des logiciels malveillants:

Cette alerte s'affiche lorsque la politique de suppression des logiciels malveillants est désactivée et lorsque Trusteer Rapport détecte et bloque des logiciels malveillants. Le but de cette alerte est de vous permettre d'activer la politique de suppression des logiciels malveillants pour que Trusteer Rapport puisse supprimer les logiciels malveillants. La suppression des logiciels malveillants est activée par défaut, mais peut avoir été désactivée dans la politique de sécurité de Rapport (voir Modifier la stratégie de sécurité de Trusteer Rapport (on page 176)).

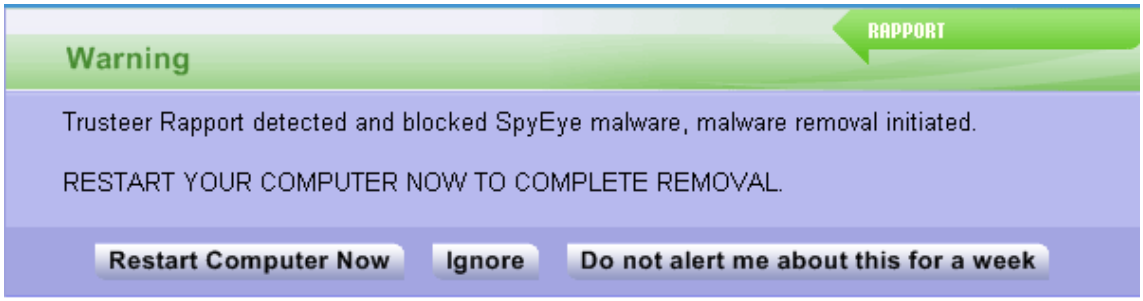
Lorsque vous voyez cette alerte, effectuez l'une des actions suivantes :

- Cliquez sur Activer la politique de suppression maintenant. La politique de suppression des logiciels malveillants est activée et Trusteer Rapport lance la suppression des logiciels malveillants bloqués. Une autre boîte de dialogue peut s'afficher pour vous demander de redémarrer votre ordinateur. Vous serez en mesure d'enregistrer et fermer les fichiers et les applications ouverts avant de cliquer sur Redémarrer l'ordinateur maintenant. Le redémarrage termine la suppression des logiciels malveillants.

- Cliquez sur Ignorer. L'alerte apparaît à nouveau la prochaine fois que Trusteer Rapport détectera à nouveau le logiciel malveillant. Le logiciel malveillant reste sur l'ordinateur, mais il est bloqué. Les logiciels malveillants bloqués résidant sur votre ordinateur présentent un risque, car ils peuvent devenir actifs à un moment donné si Trusteer Rapport est arrêté ou supprimé, ou si vous utilisez un navigateur qui ne prend pas en charge Rapport.

Répondre à une alerte pour lancer la suppression des logiciels malveillants

Ceci est un exemple d'une alerte pour lancer la suppression des logiciels malveillants:



Une alerte comme celle-ci apparaît lorsque Trusteer Rapport a détecté, bloqué, et lancé la suppression des logiciels malveillants de votre ordinateur. Pour terminer la suppression des logiciels malveillants, Trusteer Rapport nécessite le redémarrage de votre ordinateur.

Lorsque vous voyez cette alerte, effectuez l'une des actions suivantes:

- Cliquez sur Redémarrer l'ordinateur maintenant. Ceci redémarre l'ordinateur immédiatement, et termine la suppression des logiciels malveillants. Après le redémarrage, assurez-vous que l'icône Trusteer Rapport est verte lorsque vous vous connectez à votre compte sur un site Web protégé par Trusteer Rapport. La boîte de dialogue Alerte pour lancer la suppression des logiciels malveillants ne doit pas réapparaître après le redémarrage de votre ordinateur. Si elle réapparaît après le redémarrage de votre ordinateur, veuillez Envoyer le signalement d'un problème d'utilisation (on page 220) à partir de la console de Rapport.

- Cliquez sur Ignorer. Vous mettrez fin à la suppression des logiciels malveillants la prochaine fois que vous redémarrerez votre ordinateur. En attendant de redémarrer votre ordinateur, évitez les activités sensibles en ligne. Trusteer Rapport ne vous alertera plus sur cette suppression des logiciels malveillants.
- Cliquez sur Ne pas m'alerter pendant une semaine. Vous recevrez à nouveau cette alerte dans une semaine si le logiciel malveillant est toujours présent. Si, entre temps, vous redémarrez votre ordinateur, la suppression des logiciels malveillants sera terminée et l'alerte ne s'affichera plus.

Répondre à une alerte d'une infection par un logiciel malveillant lors de la désinstallation

Ceci est un exemple d'une alerte d'une infection par un logiciel malveillant lors de la désinstallation:

Cette boîte de dialogue apparaît si vous lancez le processus de désinstallation et Trusteer Rapport détecte un logiciel malveillant sur votre ordinateur. Cette boîte de dialogue vous permet de revenir sur votre décision de désinstaller Trusteer Rapport en raison de l'existence de logiciels malveillants résidant dans votre PC. Certains logiciels malveillants ne peuvent pas être supprimés sans risquer d'endommager le système d'exploitation et les données personnelles. Trusteer Rapport les bloque et les neutralise mais ne les supprime pas.

Remarque: Trusteer Rapport n'affiche actuellement pas le nom du logiciel malveillant bloqué. Le travail est en cours pour remédier à cela. Si vous souhaitez plus d'informations sur les logiciels malveillants bloqués, veuillez Envoyer le signalement d'un problème d'utilisation (on page 220) à partir de la console de Rapport.

Si vous voyez cette boîte de dialogue, sélectionnez l'une des options suivantes :

- Cliquez sur Continuer. Ceci reprend le processus de désinstallation.
- Cliquez sur Abandonner. Ceci met fin au processus de désinstallation.

Nous vous recommandons fortement d'abandonner le processus, et de ne pas désinstaller Trusteer Rapport. Si Trusteer Rapport perturbe d'autres programmes ou si vous pensez qu'il est à l'origine d'un problème, veuillez Arrêter Trusteer Rapport (on page 194) et utiliser le formulaire http://www.trusteer.com/support/submit-ticket pour nous envoyer une demande d'assistance. En attendant que ce problème soit résolu, nous vous recommandons de ne pas mener des activités sensibles en ligne tels que l'utilisation des services bancaires en ligne ou l'accès Web à l'entreprise.

Répondre à une alerte de Certificat non valide

Ceci est un exemple d'une alerte de Certificat non valide:

Cette boîte de dialogue apparaît lorsque vous naviguez sur un site Web protégé et Trusteer Rapport détecte que le certificat est non valide. Un certificat non valide peut-être obsolète, incorrect ou signé par un émetteur inconnu. Le but de cette boîte de dialogue est de vous protéger contre l'envoi d'informations à un site Web frauduleux.

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.

Remarque: Cette alerte peut souvent apparaître sur les sites Web avec des certificats valides si la date ou l'heure de l'ordinateur est mal réglée. Si cette alerte apparaît fréquemment, vérifiez la date et l'heure de votre ordinateur.

L'alerte de certificat non valide affiche les informations suivantes:

Champ Affichage	Description
Raison de l'erreur	La raison pour laquelle Trusteer Rapport a déclenché cette alerte. Valeurs possibles: • Les adresses ne correspondent pas : L'adresse à laquelle vous essayez d'accéder et l'adresse sur le certificat ne correspondent pas. Les adresses doivent être les mêmes pour que le certificat soit valide. Vérifiez les deux adresses. Si l'adresse sur le certificat paraît suspecte ou n'est pas apparentée au site Web auquel vous souhaitez accéder, choisissez de bloquer l'accès. • Signataire de certificat inconnu : L'autorité qui a signé le certificat est inconnue de Trusteer. Il ne faut pas faire confiance aux autorités inconnues pour émettre des certificats valides. Les banques et les institutions financières utilisent toujours des certificats émis par des signataires connus. • Certificat obsolète : Le certificat a expiré et il n'est plus valide. Un site Web qui utilise un certificat obsolète présente des normes de sécurité plutôt faibles. Les banques et les institutions financières n'utilisent jamais les certificats expirés. Vérifiez l'horloge de votre ordinateur pour vous assurer que la date sur votre ordinateur est correcte. Si la date sur votre ordinateur est en avance, ce message peut apparaître par erreur. • Mauvais certificat : Le format du certificat est incorrect.
Adresse sur le certificat	L'adresse qui apparait sur le certificat présenté par ce site Web. Chaque certificat est émis pour une adresse Web spécifique. Un site Web doit présenter un certificat qui affiche sa propre adresse.
Adresse dans la requête	L'adresse vers laquelle votre navigateur est dirigé. C'est l'adresse à laquelle vous avez tenté d'accéder
Date d'expiration du certificat	Chaque certificat est limité dans le temps. Un site Web qui utilise des certificats obsolètes présente des normes de sécurité plutôt faibles.
Signataire	L'autorité qui a émis ce certificat. Les certificats provenant d'autorités inconnus ne doivent pas être digne de confiance.

Si vous voyez cette boîte de dialogue, sélectionnez l'une des options suivantes:

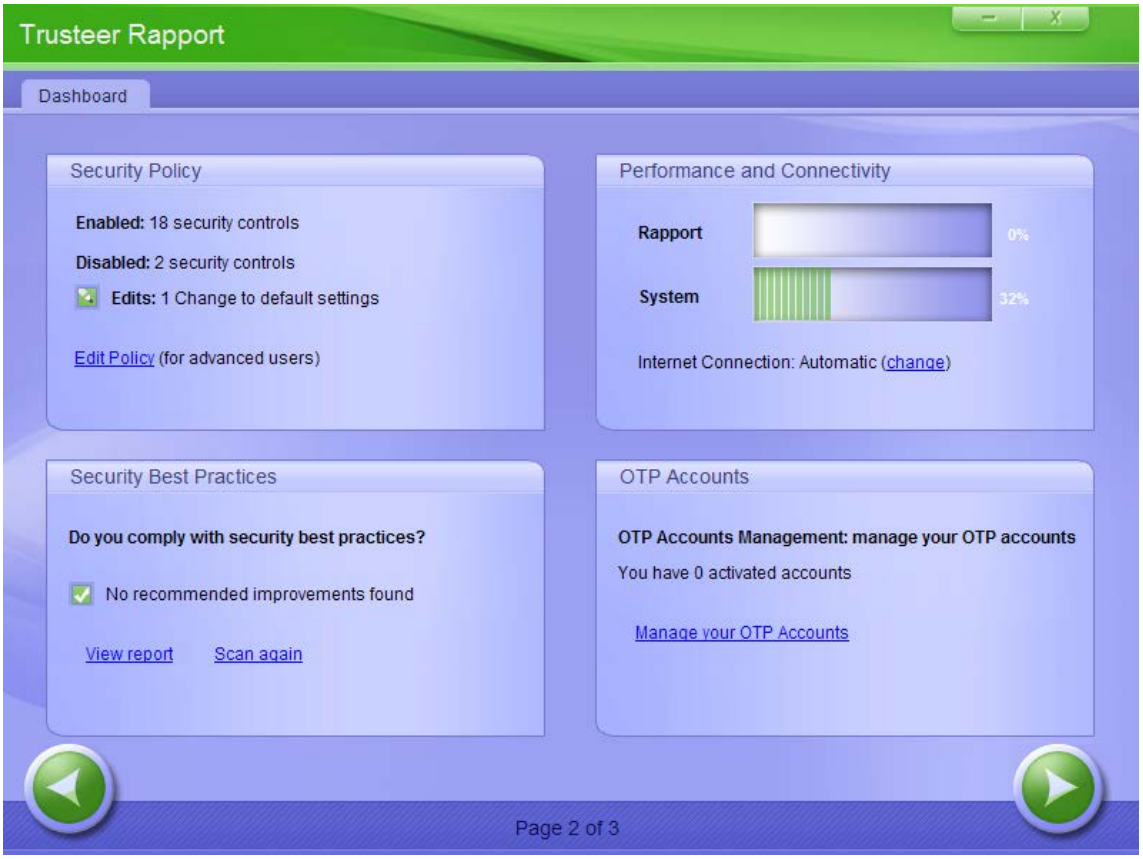
- Cliquez sur Bloquer l'accès. Ceci bloque l'accès au site. Sélectionnez cette option si le site est un site financier ou de commerce sur lequel les utilisateurs envoient des informations sensibles.
- Cliquez sur Autoriser l'accès. Ceci autorise l'accès au site. Vous pouvez choisir cette option si le site est sur votre réseau local (intranet) ou si le site ne traite pas les informations sensibles. Si vous autorisez l'accès, faites-le avec prudence et n'envoyez pas des informations sensibles sur le site. Ne cochez la case Ne me plus prévenir de ce site que si vous souhaitez éviter que Rapport de Trusteer ne vous alerte sur ce site à l'avenir.

Comment puis-je désactiver cette fonctionnalité?

La Console de Trusteer Rapport vous permet de désactiver la validation du certificat SSL, qui empêche Trusteer Rapport de vérifier la validité des certificats de sites Web, et empêche par conséquent, ces alertes de s'afficher.

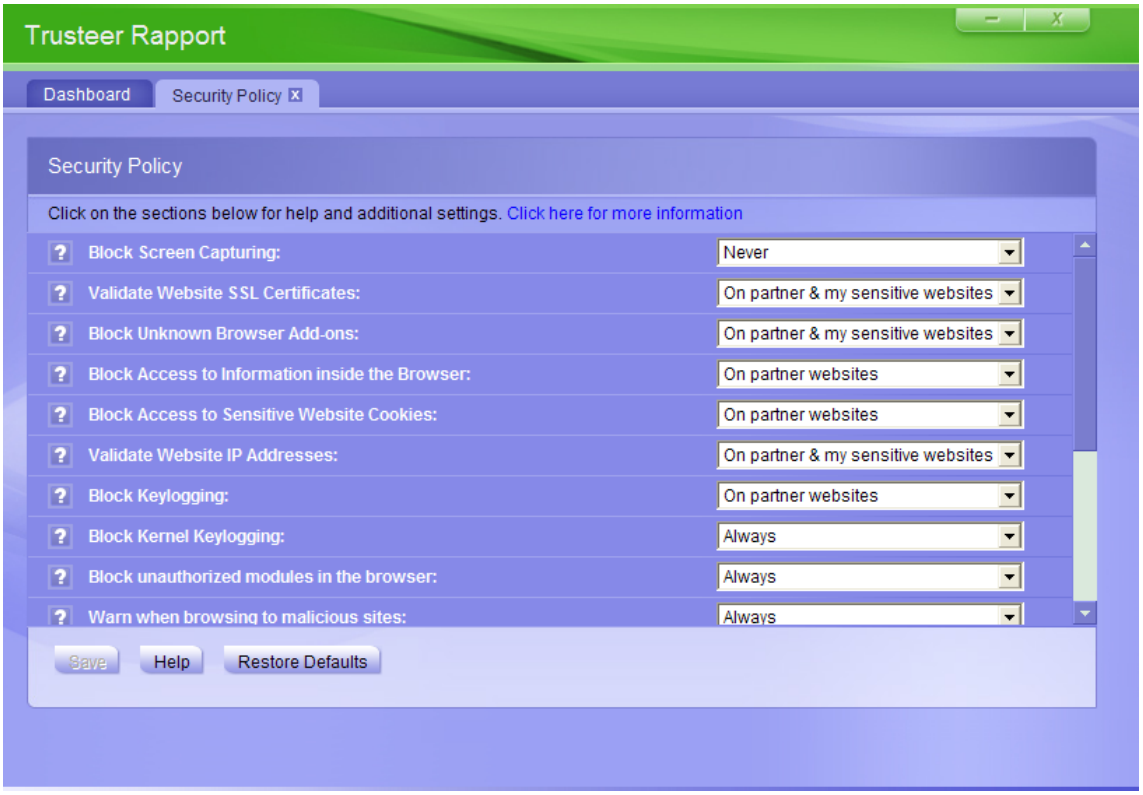
Pour désactiver la validation des certificats SSL:

1. Ouvrir la console Rapport (on page 72).
2. Dans le tableau de bord, cliquez sur . Le second écran du tableau de bord apparaît.



3. Dans la zone de la politique de sécurité, cliquez sur Modifier la politique. Un écran Approbation de l'utilisateur apparaît. L'écran vous montre l'image d'un mot pour que vous le saisissiez. Ceci est destiné à empêcher les logiciels malveillants d'accéder à la console et de désactiver Trusteer Rapport de manière efficace.
4. Saisissez le mot que vous voyez dans l'image.

5. Cliquez sur OK. L'écran Politique de sécurité apparaît, affichant tous les contrôles de sécurité.



6. Trouvez le contrôle appelé Valider les certificats SSL des Sites Web.
7. Dans le menu déroulant à droite de ce contrôle, sélectionnez Jamais.
8. Cliquez sur Enregistrer. La validation des certificats SSL est maintenant désactivée.

Répondre à une notification d'un rapport d'activité

Ceci est un exemple d'une notification hebdomadaire d'un rapport d'activité:

Cette boîte de dialogue apparaît chaque semaine si vous sélectionnez une option dans la console de Rapport pour Configurer le rapport des activités (on page 158).

Lorsque vous voyez cette notification, effectuez l'une des actions suivantes:

- Cliquez sur Ouvrir le rapport. Ceci ouvre la console de Rapport et affiche le rapport d'activité hebdomadaire.
- Cliquez sur Fermer. Ceci ferme l'alerte et n'affiche pas le rapport d'activité. Toutefois, vous pouvez Afficher le rapport des activités (on page 156) tout moment.

Cela fait plus d'une semaine que je n'ai pas reçu de notifications des activités de Rapport. Pourquoi?

Le rapport hebdomadaire des activités n'apparaît que s'il y a eu au moins un événement durant la dernière semaine. Il est possible qu'aucun événement n'ait été enregistré.

Répondre à une invite de mise à niveau de Trusteer Rapport

Ceci est un exemple d'une invite de mise à niveau de Trusteer Rapport:

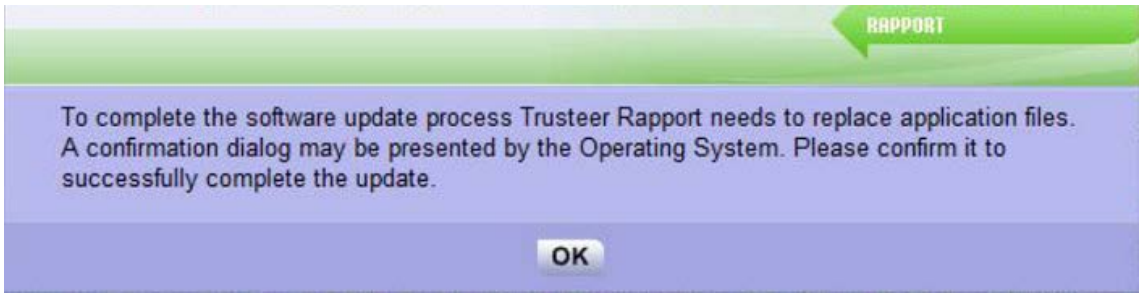
Cette boîte de dialogue s'affiche lorsque vous essayez de protéger manuellement un site Web, et lorsque l'ajout de ce site vous ferait dépasser le nombre maximum de sites protégés autorisé par votre licence. Cette boîte de dialogue vous permet de mettre à niveau votre licence de sorte que vous puissiez protéger un nombre illimité de sites.

Lorsque vous voyez cette boîte de dialogue, effectuez l'une des actions suivantes:

- Cliquez sur Mettre Rapport à niveau maintenant. Ceci ouvre le site Web de Trusteer et vous permet de mettre à niveau votre licence. La mise à niveau est gratuite.
- Cliquez sur Annuler. Ceci annule l'action de protéger le site que vous avez essayé de protéger et ne met pas à niveau votre licence.
- Supprimer un site protégé pour pouvoir ajouter un autre. Voir Gérer des sites Web protégés (on page 170).

Répondre à un message de confirmation de mise à jour du code

Si le contrôle de compte d'utilisateur (fonctionnalité de protection de Windows 7 et Windows Vista) est activé sur votre ordinateur, vous pouvez voir ce message de temps à autre lorsque Trusteer Rapport effectue automatiquement une mise à jour:

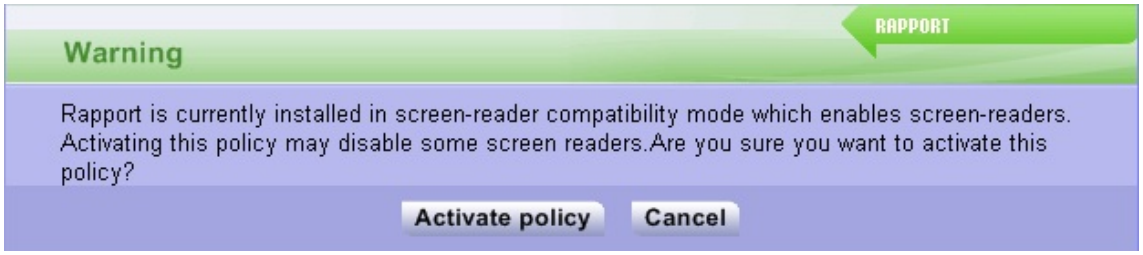


Si vous voyez ce message, cliquez sur OK. Vous pouvez alors voir une boîte de dialogue du Contrôle de compte d'utilisateur vous demandant votre autorisation pour continuer le processus de mise à jour de Trusteer Rapport. Si vous voyez un message du Contrôle de compte d'utilisateur, cliquez sur Continuer et la mise à jour sera terminée.

Remarque: Si le message de confirmation de mise à jour du code apparaît fréquemment, veuillez envoyer une demande au service d'assistance de Trusteer à http://www.trusteer.com/support/submit-ticket.

Répondre à une alerte de mode de compatibilité du lecteur d'écran

Ceci est un exemple d'une alerte de mode compatibilité du lecteur d'écran:



Une alerte de ce type apparaît si Trusteer Rapport est installé en mode compatibilité des lecteurs d'écran et que vous tentez d'activer l'une de ces politiques de sécurité (pour plus d'informations sur l'activation et la désactivation des politiques de sécurité, voir Modifier les règles de sécurité (on page 178)):

- **Bloquer la capture d'écran**
- **Bloquer l'accès aux informations dans le navigateur**

Ces politiques sont désactivés par défaut si Trusteer Rapport est installé en mode compatibilité des lecteurs d'écran. L'activation de l'une ou de l'autre de ces politiques peut interférer avec votre logiciel de lecture d'écran, l'empêchant de lire les pages Web et les menus et boîtes de dialogue de Trusteer Rapport.

Si vous voyez cette alerte, effectuez l'une des actions suivantes:

- Cliquez sur Activer la politique. Sélectionnez cette option si vous êtes sûr que vous souhaitez activer la politique, et si cela vous est égal si les lecteurs d'écran sur votre ordinateur ne peuvent pas accéder à Trusteer Rapport.

Remarque:	Si vous n'avez pas besoin d'exécuter des lecteurs d'écran, nous vous recommandons fortement de réinstaller Trusteer Rapport sans choisir le mode compatibilité des lecteurs d'écran.

- Cliquez sur Annuler. Choisissez cette option si vous souhaitez annuler l'activation des politiques.

Répondre à une alerte de mode réinstallation par un administrateur

Ceci est un exemple d'une alerte de Mode réinstallation par un administrateur:

Cette alerte indique que votre fournisseur de Trusteer Rapport a récemment limité l'installation de Rapport aux comptes d'administrateur Windows. Vous avez installé Trusteer Rapport à partir d'un compte d'utilisateur standard. Le fournisseur recommande maintenant de désinstaller Trusteer Rapport du compte d'utilisateur standard dans lequel vous avez installé Trusteer Rapport, et réinstaller Trusteer Rapport à partir d'un compte d'administrateur. Une fois Trusteer Rapport installé à partir d'un compte administrateur, il sera activé pour tous les comptes d'utilisateur Windows sur l'ordinateur.

Un compte d'administrateur Windows est un compte d'utilisateur Windows dans lequel vous pouvez apporter des modifications qui affectent tous les utilisateurs de l'ordinateur ou qui affectent certains utilisateurs. Ces modifications incluent les paramètres de sécurité, les installations de logiciels et l'accès aux fichiers. Bien que chaque ordinateur Windows possède un compte d'administrateur, la recommandation de Microsoft est d'utiliser un compte d'utilisateur standard pour la plupart des utilisations quotidiennes de l'ordinateur.

Si vous voyez cette alerte, effectuez l'une des actions suivantes:

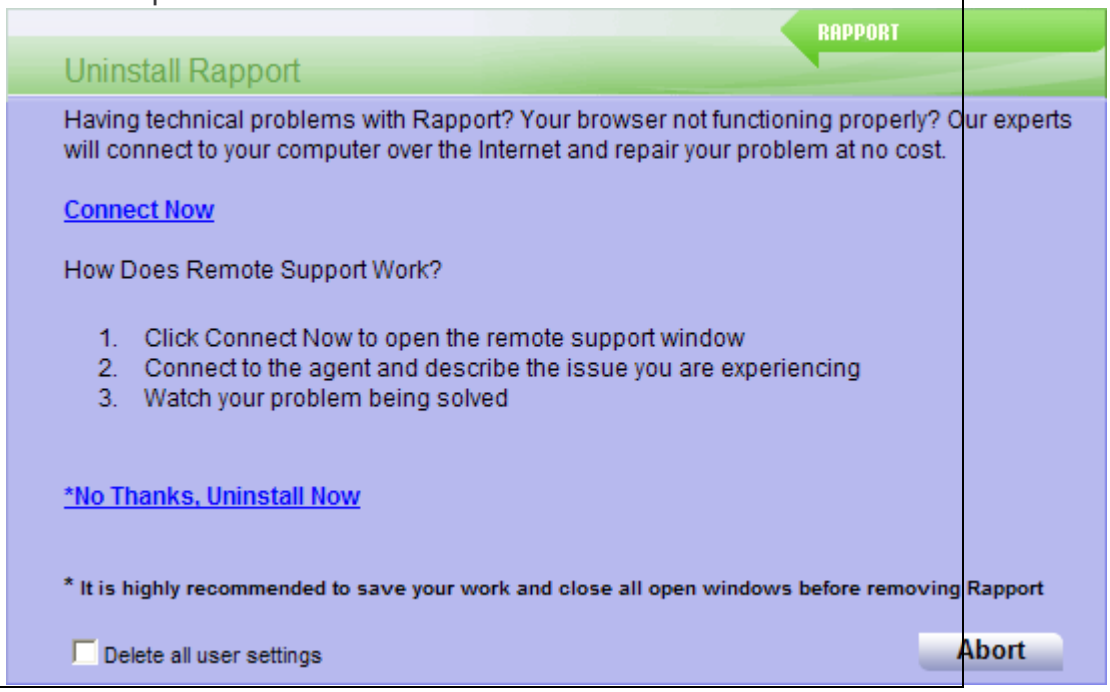
- Cliquez sur Fermer. L'alerte se ferme. Vous pouvez alors effectuer la réinstallation recommandée en utilisant la procédure ci-dessous.

- Cliquez sur M'alerter dans 7 jours. L'alerte se ferme et réapparaît 7 jours plus tard pour vous rappeler d'effectuer la réinstallation.

Pour effectuer la réinstallation recommandée:

1. Désinstaller Trusteer Rapport du compte d'utilisateur standard que vous avez utilisé pour installer Trusteer Rapport:
   - Uninstalling Trusteer Rapport (Windows 7) (on page 148)
   - Uninstalling Trusteer Rapport (Windows XP) (on page 148)

Remarque: Lors de la désinstallation, cochez la case Supprimer tous les paramètres utilisateur qui apparaît dans l'écran ci-dessous. Cela est nécessaire pour assurer une réinstallation en douceur.



2. Basculez vers un compte d'administrateur:
   - Basculer vers un compte d'administrateur (Windows 7) (on page 143)
   - Basculer vers un compte d'administrateur (XP) (on page 144)
   - Basculer vers un compte d'administrateur (Vista) (on page 146)
3. Télécharger la dernière version de Trusteer Rapport de votre fournisseur:
   a. Visitez http://www.trusteer.com/support/en/windows-operating-systems-xp-vista-windows-7.

b. Trouvez le lien de téléchargement correspondant à votre fournisseur (votre banque, entreprise, ou tout autre organisme qui vous a offert Trusteer Rapport).

c. Cliquez sur le lien du fournisseur pour télécharger le fichier d'installation.

d. À l'invite, enregistrez le fichier sur votre ordinateur.

e. Exécutez le fichier pour l'installer. Pour obtenir des instructions d'installation complètes, voir Installer Trusteer Rapport (on page 27).

Basculer vers un compte d'administrateur (Windows 7)

Pour basculer vers un compte d'administrateur, vous devez connaître le nom d'utilisateur et le mot de passe du compte utilisateur de l'administrateur. Si vous ne connaissez pas le nom d'utilisateur et le mot de passe d'un utilisateur administrateur, vous devez demander à votre administrateur de modifier votre type de compte, ou d'installer Trusteer Rapport.

➡ **Pour basculez vers un compte d'administrateur:**

1. Cliquez sur le bouton Démarrer.
2. Cliquez sur la flèche à côté du bouton Arrêter.
3. Cliquez sur Changer d'utilisateur.
4. Appuyez sur Ctrl+Alt+Supprimer, puis cliquez sur l'utilisateur vers lequel vous souhaitez basculer.

Je ne sais pas si le compte que j'utilise est un compte d'administrateur.

Si vous n'êtes pas sûr si un compte utilisateur est un compte d'administrateur ou un compte d'utilisateur standard, vous pouvez vérifier le type de compte en basculant vers ce compte, puis effectuez les actions suivantes.

➡ **Si votre ordinateur fait partie d'un domaine:**

1. Cliquez sur le bouton Démarrer.
2. Cliquez sur Panneau de configuration.

3. Cliquez sur Comptes d'utilisateurs.
4. Cliquez sur Comptes d'utilisateurs.
5. Cliquez sur Gérer les comptes d'utilisateurs.
6. Si vous êtes invité à fournir un mot de passe administrateur ou une confirmation, saisissez votre mot de passe ou fournissez la confirmation. (Si votre mot de passe n'est pas accepté, vous pouvez supposer que le compte que vous utilisez est un compte d'utilisateur standard.) Votre nom d'utilisateur est mis en surbrillance et le type de votre compte est indiqué dans la colonne Groupe.

➡ **Si votre ordinateur fait partie d'un groupe de travail :**

1. Cliquez sur le bouton Démarrer.
2. Cliquez sur Panneau de configuration.
3. Cliquez sur Comptes d'utilisateur et contrôle parental.
4. Cliquez sur Comptes d'utilisateurs.
5. Cliquez sur Gérer un autre compte. Si vous êtes invité à fournir un mot de passe administrateur ou une confirmation, saisissez le mot de passe ou fournissez la confirmation. (Si votre mot de passe n'est pas accepté, vous pouvez supposer que le compte que vous utilisez est un compte d'utilisateur standard.) Votre type de compte est affiché sous votre nom d'utilisateur.

Basculer vers un compte d'administrateur (XP)

Pour basculer vers un compte d'administrateur, vous devez connaître le nom d'utilisateur et le mot de passe du compte utilisateur de l'administrateur. Si vous ne connaissez pas le nom d'utilisateur et le mot de passe d'un utilisateur administrateur, vous devez demander à votre administrateur de modifier votre type de compte, ou d'installer Trusteer Rapport.

➡ **Pour basculer vers un compte d'administrateur:**

- Si le basculement rapide est activé (par défaut pour Windows XP Édition familiale et Professionnelle sur des ordinateurs avec plus de 64 Mo de RAM):
  1. Cliquez sur Démarrer.
  2. Cliquez sur Fermer la session.
  3. Cliquez sur Changer d'utilisateur. L'écran de connexion de Windows XP apparaît et affiche le nombre de programmes en cours d'exécution pour chaque utilisateur sous ce nom d'utilisateur.
  4. Cliquez sur l'utilisateur vers lequel vous souhaitez basculer.
  5. Entrez votre mot de passe, puis cliquez sur le bouton fléché pour ouvrir une session sur l'ordinateur.
- Si le basculement rapide est désactivé ou n'est pas pris en charge (Ordinateurs avec Windows XP Professionnel faisant partie d'un réseau avec domaine):
  1. Redémarrez votre ordinateur.
  2. Connectez-vous avec le nom d'utilisateur et le mot de passe d'un administrateur.

Je ne sais pas si le compte que j'utilise est un compte d'administrateur.

Si vous n'êtes pas sûr si un compte utilisateur est un compte d'administrateur ou un compte d'utilisateur standard, vous pouvez vérifier le type de compte en basculant vers ce compte, puis effectuez les actions suivantes.

Si votre ordinateur fait partie d'un domaine:

1. Cliquez sur le bouton Démarrer.
2. Cliquez sur Panneau de configuration.
3. Cliquez sur Comptes d'utilisateurs.
4. Cliquez sur Comptes d'utilisateurs.
5. Cliquez sur Gérer les comptes d'utilisateurs.

6. Si vous êtes invité à fournir un mot de passe administrateur ou une confirmation, saisissez votre mot de passe ou fournissez la confirmation. (Si votre mot de passe n'est pas accepté, vous pouvez supposer que le compte que vous utilisez est un compte d'utilisateur standard.) Votre nom d'utilisateur est mis en surbrillance et le type de votre compte est indiqué dans la colonne Groupe.

➡ **Si votre ordinateur fait partie d'un groupe de travail :**

1. Cliquez sur le bouton Démarrer.
2. Cliquez sur Panneau de configuration.
3. Cliquez sur Comptes d'utilisateur et contrôle parental.
4. Cliquez sur Comptes d'utilisateurs.
5. Cliquez sur Gérer un autre compte. Si vous êtes invité à fournir un mot de passe administrateur ou une confirmation, saisissez le mot de passe ou fournissez la confirmation. (Si votre mot de passe n'est pas accepté, vous pouvez supposer que le compte que vous utilisez est un compte d'utilisateur standard.) Votre type de compte est affiché sous votre nom d'utilisateur.

Basculer vers un compte d'administrateur (Vista)

Pour basculer vers un compte d'administrateur, vous devez connaître le nom d'utilisateur et le mot de passe du compte utilisateur de l'administrateur. Si vous ne connaissez pas le nom d'utilisateur et le mot de passe d'un utilisateur administrateur, vous devez demander à votre administrateur de modifier votre type de compte ou d'installer Trusteer Rapport.

➡ **Pour basculez vers un compte d'administrateur :**

1. Cliquez sur le bouton Démarrer.
2. Cliquez sur la flèche à côté du bouton Verrouiller.
3. Cliquez sur Changer d'utilisateur.

4. Cliquez sur l'utilisateur vers lequel vous souhaitez basculer.

Je ne sais pas si le compte que j'utilise est un compte d'administrateur.

Si vous n'êtes pas sûr si un compte utilisateur est un compte d'administrateur ou un compte d'utilisateur standard, vous pouvez vérifier le type de compte en basculant vers ce compte, puis effectuez les actions suivantes.

Si votre ordinateur fait partie d'un domaine:

1. Cliquez sur le bouton Démarrer.
2. Cliquez sur Panneau de configuration.
3. Cliquez sur Comptes d'utilisateurs.
4. Cliquez sur Comptes d'utilisateurs.
5. Cliquez sur Gérer les comptes d'utilisateurs.
6. Si vous êtes invité à fournir un mot de passe administrateur ou une confirmation, saisissez votre mot de passe ou fournissez la confirmation. (Si votre mot de passe n'est pas accepté, vous pouvez supposer que le compte que vous utilisez est un compte d'utilisateur standard.) Votre nom d'utilisateur est mis en surbrillance et le type de votre compte est indiqué dans la colonne Groupe.

Si votre ordinateur fait partie d'un groupe de travail :

1. Cliquez sur le bouton Démarrer.
2. Cliquez sur Panneau de configuration.
3. Cliquez sur Comptes d'utilisateur et contrôle parental.
4. Cliquez sur Comptes d'utilisateurs.
5. Cliquez sur Gérer un autre compte. Si vous êtes invité à fournir un mot de passe administrateur ou une confirmation, saisissez le mot de passe ou fournissez la confirmation. (Si votre mot de passe n'est pas accepté, vous pouvez supposer que le compte que vous utilisez est un compte d'utilisateur standard.) Votre type de compte est affiché sous votre nom d'utilisateur.

Uninstalling Trusteer Rapport (Windows 7)

➡ **To uninstall Trusteer Rapport:**

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

Uninstalling Trusteer Rapport (Windows XP)

➡ **To uninstall Trusteer Rapport:**

1. Open the Control Panel.
2. Click **Add/Remove Programs**.
3. Find Trusteer Rapport in the list of programs, and click the **Change/Remove** button for Trusteer Rapport. A confirmation message appears.
4. Click **Yes**. A Trusteer Rapport dialog box appears, showing you recent events Trusteer Rapport successfully prevented.

5. Click **Continue**. Another Trusteer Rapport dialog box appears, offering you assistance with technical problems you may have had with Trusteer Rapport. Before continuing with the uninstall, close any files and applications you may have open.
6. Click **No Thanks, Uninstall Now**. Trusteer Rapport completes the uninstall as requested. Once the uninstall is complete, a new browser window opens, asking for your feedback about Trusteer Rapport and a few basic questions.

Répondre à une alerte de Redémarrage nécessaire

Ceci est un exemple d'une alerte de Redémarrage nécessaire:

Cette boîte de dialogue apparaît lorsque certaines fonctionnalités de Trusteer Rapport ont été mises à jour et leur activation nécessite un redémarrage. Effectuez l'une des actions suivantes :

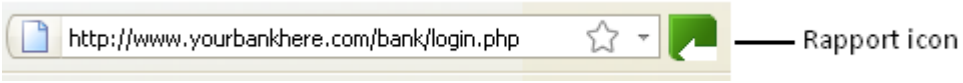
- Cliquez sur Redémarrer maintenant. Votre ordinateur redémarre immédiatement.
- Cliquez sur Me le rappeler ultérieurement. La boîte de dialogue se ferme. Vous recevrez un rappel pour redémarrer plus tard.
- Cliquez sur Annuler. La boîte de dialogue se ferme. Vous ne recevrez plus de rappels en relation avec cette mise à jour. La prochaine fois que vous redémarrerez votre ordinateur, la ou les fonctions de mise à jour seront activées.

11. Personnaliser Trusteer Rapport

Vous pouvez modifier la langue de la console et des boîtes de dialogue de Rapport, et vous pouvez masquer l'icône de Trusteer Rapport qui apparaît près de la barre d'adresse de votre navigateur, et vous pouvez masquer l'icône de Trusteer Rapport qui apparaît dans votre barre d'état système.

Masquer et rétablir l'icône de Trusteer Rapport dans la barre d'adresse

Par défaut, l'icône de Trusteer Rapport apparaît toujours sur ou près du côté droit de la barre d'adresse de votre navigateur. L'icône est verte lorsque le site internet affiché dans votre navigateur est protégé par Trusteer Rapport, et grise lorsque le site internet affiché dans votre navigateur n'est pas protégé par Trusteer Rapport.



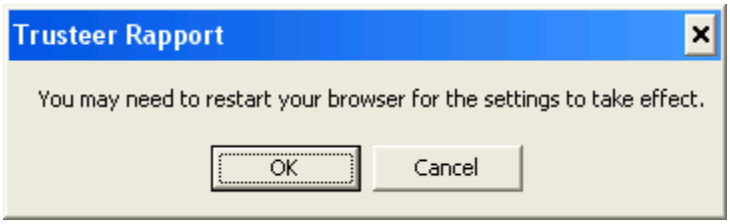
En plus d'indiquer les sites qui sont protégés, l'icône vous permet également de protéger un site non protégé (il suffit de cliquer sur l'icône Trusteer Rapport et sélectionner Protéger ce site Web).

Trusteer Rapport vous permet de masquer cette icône si vous préférez qu'elle soit masquée. Lorsque l'icône de Trusteer Rapport est masquée, Trusteer Rapport continue d'offrir la même protection aux sites protégés, mais vous ne pouvez pas voir lesquels de ces sites sont protégés et vous ne pouvez pas choisir de protéger un site non protégé.

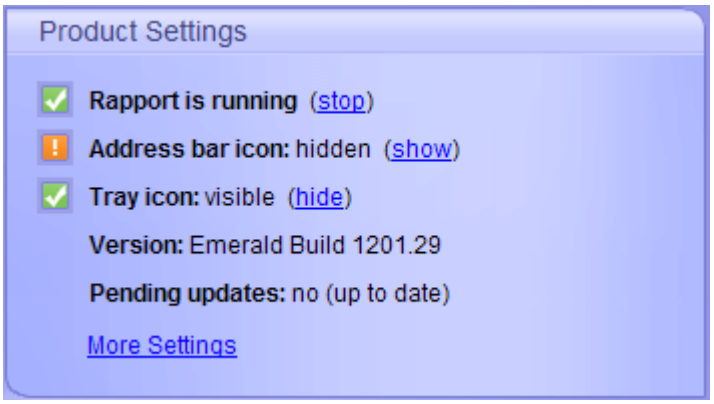
L'affichage ou le masquage de l'icône est contrôlé dans la console de Rapport. Lorsque l'icône est masquée, vous pouvez accéder à la console Rapport uniquement à partir du menu Démarrer de Windows.

➡ **Pour masquer l'icône de Trusteer Rapport:**

1. Ouvrir la console Rapport (on page 72).
2. Dans la zone Paramètres du produit du tableau de bord, à côté du statut de l'icône de la barre d'adresses, cliquez sur Masquer. Une boîte de message apparaît.



3. Cliquez sur OK. Le statut de l'icône de la barre d'adresse change en Masquée et un bouton Afficher apparaît.



L'icône est maintenant masquée dans le navigateur ou le sera après le redémarrage de votre navigateur.

Pour rétablir l'icône:

1. Cliquez sur Afficher.

Masquer et rétablir l'icône de la barre d'état système

Par défaut, l'icône de Trusteer Rapport ( ) apparaît toujours dans la barre d'état système lorsque Trusteer Rapport est en cours d'exécution.

Figure 1: Icône de la barre d'état système

L'icône indique que les protections indépendantes du navigateur de Trusteer Rapport fonctionnent correctement. Cela inclut la prévention, l'analyse et la suppression de logiciels malveillants. L'icône ouvre également la console de Rapport. (Il vous suffit de cliquer sur l'icône de Trusteer Rapport et la console de Rapport s'ouvre).

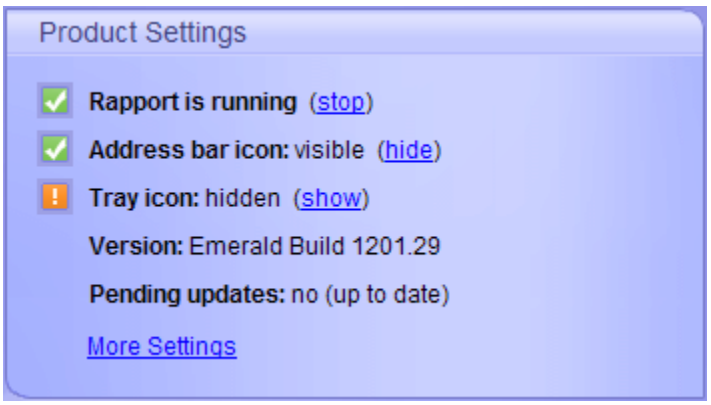
Trusteer Rapport vous permet de masquer cette icône si vous préférez qu'elle le soit. Lorsque l'icône de Trusteer Rapport est masquée dans la barre d'état système, Trusteer Rapport continue de fournir la même protection.

L'affichage ou le masquage de l'icône est contrôlé dans la console de Rapport. Lorsque l'icône est masquée, vous pouvez accéder à la console Rapport uniquement à partir du menu Démarrer de Windows.

➡ **Pour masquer l'icône de Rapport dans la barre d'état système:**

1. Ouvrir la console Rapport (on page 72).

2. Dans la zone Paramètres du produit du tableau de bord, à côté de l'icône de la barre d'état système, cliquez sur Masquer. Le statut de l'icône de la barre d'état change en Masquée et un bouton Afficher apparaît.



L'icône est maintenant masquée dans la barre d'état système.

➡ **Pour rétablir l'icône :**

1. Cliquez sur Afficher.

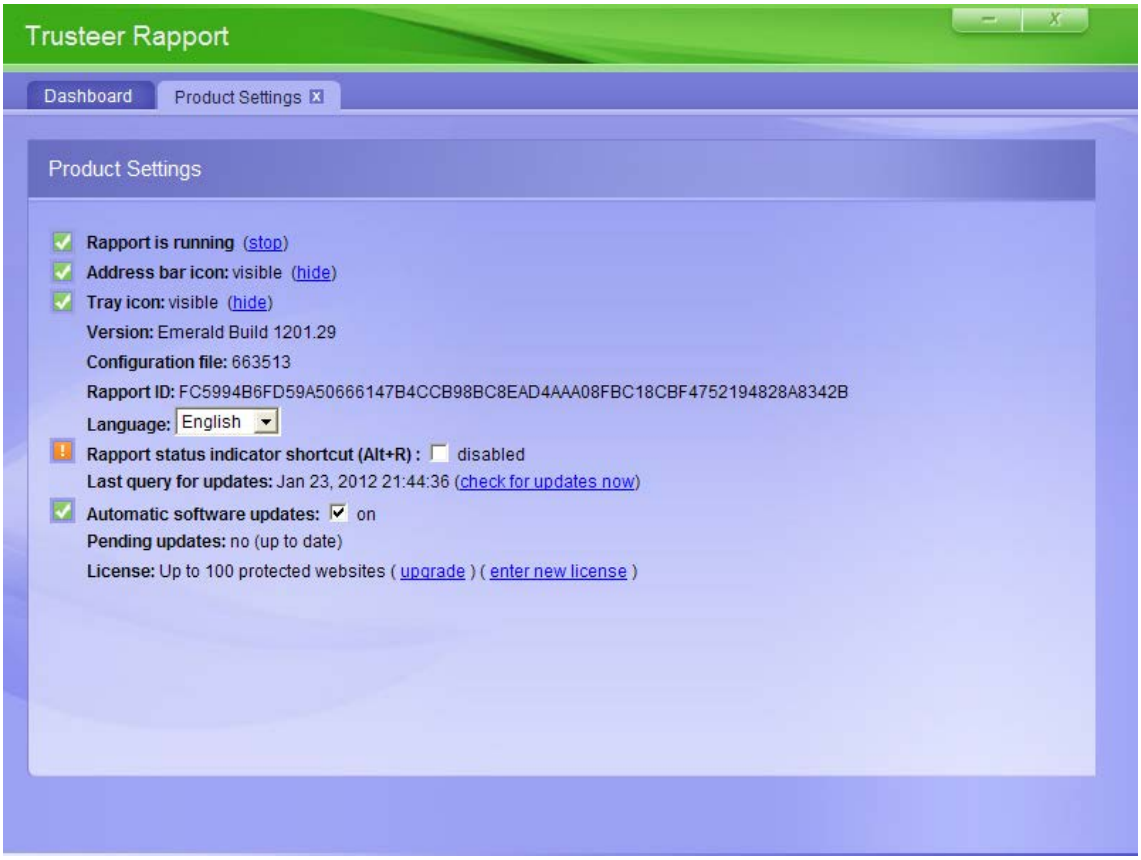
Modification de la langue de l'interface

Par défaut, Trusteer Rapport affiche la console de Rapport et toutes les autres boîtes de dialogue en langue anglaise. Vous pouvez modifier la langue utilisée dans la console de Rapport et toutes les autres boîtes de dialogue pour les afficher en espagnol, français ou allemand.

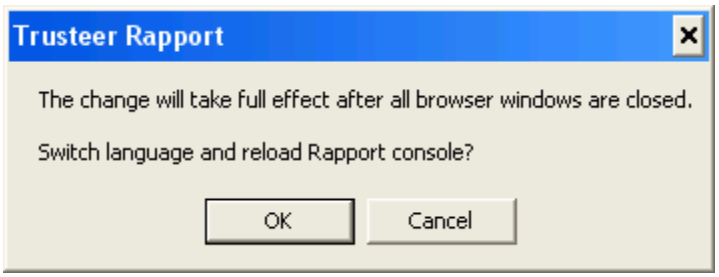
➡ **Pour modifier la langue de la console de Rapport:**

1. Ouvrir la console Rapport (on page 72).
2. Dans la zone Paramètres du produit du tableau de bord, Cliquez sur Autres paramètres.

L'onglet Paramètres du produit apparaît



3. Dans la liste déroulante Langue, sélectionnez une langue. Le message suivant apparaît.



4. Cliquez sur OK. La console de rapport est chargée dans la langue sélectionnée.

12. Afficher les activités de Trusteer Rapport

Les mécanismes de protection de Trusteer Rapport sont déclenchés par différents types d'événements. Certains de ces événements sont des événements légitimes qui ressemblent à des événements causés par des logiciels malveillants. D'autres événements peuvent être initiés par des logiciels malveillants résidant dans votre ordinateur. Chaque événement est compté et enregistré dans un rapport d'activités que vous pouvez consulter au besoin. Le rapport affiche les activités au cours des sept derniers jours. Vous pouvez réinitialiser le comptage ou arrêter le comptage et activer ou désactiver une boîte de dialogue qui s'affiche sur votre écran au début de chaque semaine, vous proposant d'afficher le rapport hebdomadaire des activités.

Afficher le rapport des activités

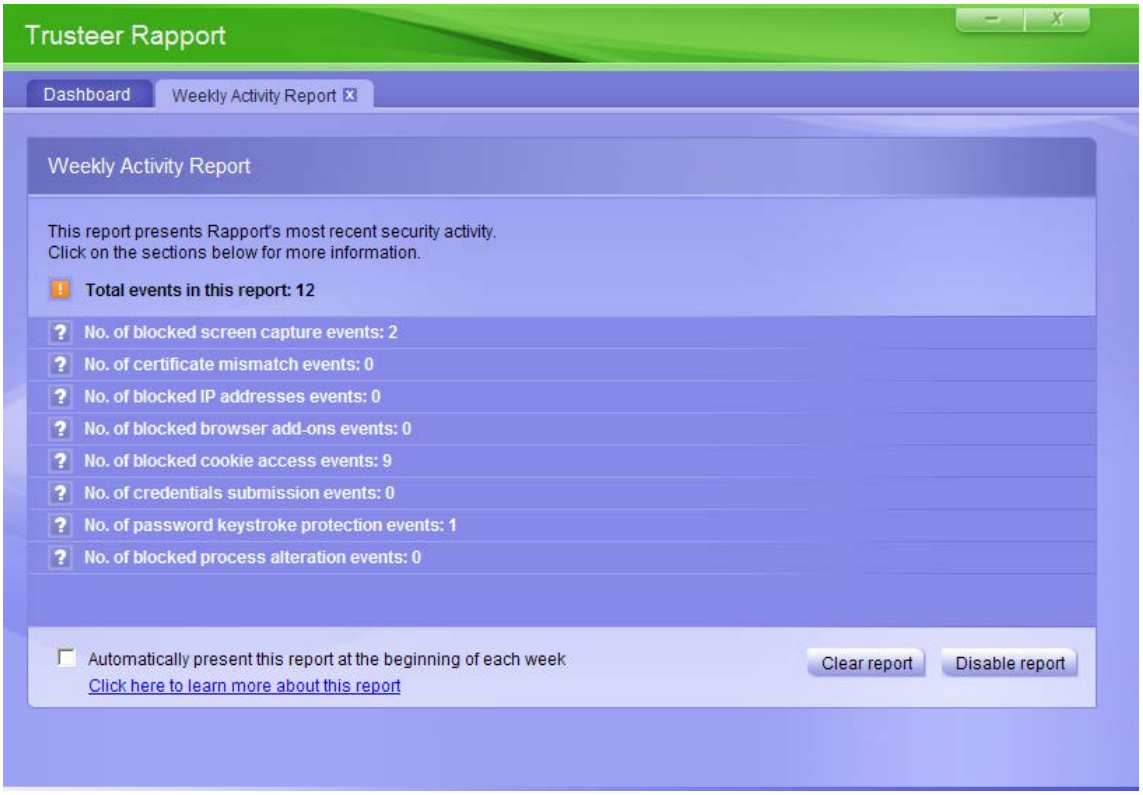
Le rapport hebdomadaire des activités vous indique combien d'événements ont déclenché chacun des mécanismes de protection de Trusteer Rapport durant les sept derniers jours. Ce rapport est pour votre information uniquement. Aucune action de votre part n'est nécessaire, car Trusteer Rapport bloque tous les événements de sécurité qui peuvent conduire à une violation des données. Le rapport des activités est affiché automatiquement 12 heures après l'installation de Trusteer Rapport.

Le fait que le rapport des activités comprend des événements ne signifie pas que vous avez des logiciels malveillants sur votre ordinateur ou que vous avez visité des sites Web frauduleux. Mais cela signifie que certains logiciels ou sites Web que vous avez visités ont violé la politique de sécurité définie par les propriétaires de vos sites Web protégées ou par Trusteer. Par exemple, il se peut qu'un logiciel ait essayé de prendre une capture d'écran de votre relevé de compte bancaire, ou qu'un logiciel ait essayé de lire les informations que vous avez saisies sur le site de votre banque en ligne. Cette violation de la politique a incité Trusteer Rapport à bloquer le logiciel pour qu'il ne puisse pas atteindre les informations sensibles.

➡ **Pour afficher le Rapport hebdomadaire des activités à tout moment:**

1. Ouvrir la console Rapport (on page 72).

2. Dans la zone Rapport hebdomadaire des activités du tableau de bord, cliquez sur Rapport complet. Le rapport hebdomadaire des activités apparaît.



Le rapport affiche huit compteurs pour huit catégories d'événements. Les catégories du rapport des activités énumèrent différents types d'événements que Rapport a rencontrés et atténués pendant que vous naviguiez sur Internet.

3. Cliquez sur le nom de chaque compteur pour afficher une description de l'événement de sécurité qu'il compte, ainsi qu'une liste des événements de cette catégorie qui ont été comptés.

Remarque: Ne vous inquiétez pas si vous ne comprenez pas une partie ou même la totalité des informations présentées dans ce rapport, car il est d'une nature un peu technique. Comme mentionné ci-dessus, ces informations ne nécessitent aucune action de votre part. Vous pouvez ignorer ce rapport en toute sécurité et ne jamais le consulter à nouveau. Il est là pour les utilisateurs qui veulent examiner l'activité de Trusteer Rapport avec le temps.

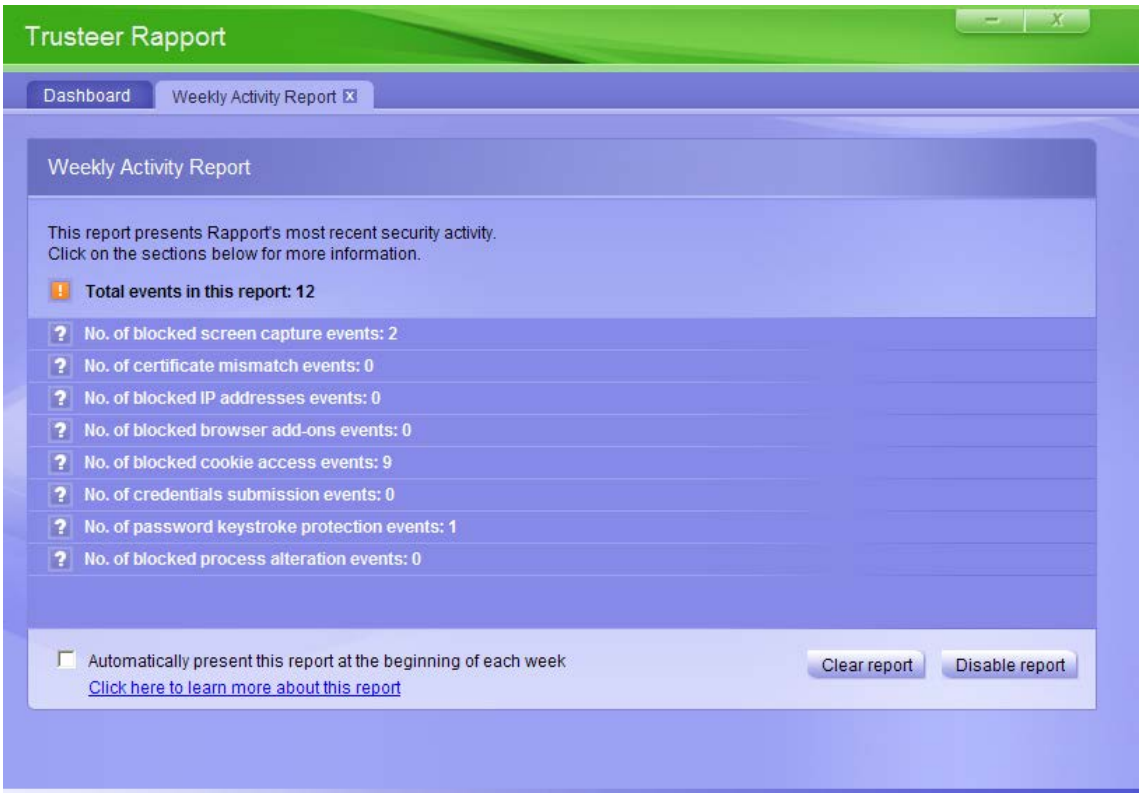
Configurer le rapport des activités

Il y a une option pour obtenir un rapport des activités qui s'affiche automatiquement tous les sept jours. Le rapport est d'abord affiché automatiquement 12 heures après l'installation de Trusteer Rapport. Par défaut, le rapport ne s'affiche pas chaque semaine, mais vous pouvez le consulter dans la console de Rapport quand vous le souhaitez.

« Effacer le rapport hebdomadaire des activités » efface tous les compteurs d'événements. Désactiver le rapport hebdomadaire des activités efface tous les compteurs d'événements.

➡ **Pour configurer le rapport des activités:**

1. Ouvrir la console Rapport (on page 72).
2. Dans la zone Rapport hebdomadaire des activités du tableau de bord, cliquez sur Rapport complet. Le rapport hebdomadaire des activités apparaît.



Vous pouvez maintenant :

- Activer le rapport hebdomadaire des activités en cochant la case Afficher ce rapport automatiquement au début de chaque semaine. Tous les sept jours, une boîte de dialogue s'affiche vous proposant d'afficher le rapport.
- Effacer le rapport.
- Désactiver le rapport.

13. Analyser votre ordinateur pour améliorer la sécurité

Maintenir le logiciel à jour sur votre ordinateur est important pour la sécurité. De nouvelles menaces émergent tout le temps et les développeurs de logiciels mettent régulièrement à jour leurs programmes pour inclure des correctifs contre les vulnérabilités de sécurité et autres bogues. Certains logiciels sont particulièrement vulnérables aux abus s'ils ne sont pas à jour.

Trusteer Rapport analyse votre ordinateur tous les trois jours pour vérifier que votre ordinateur dispose d'un logiciel antivirus installé, et que votre ordinateur exécute des versions à jour du logiciel antivirus et des divers autres logiciels tels qu'Adobe Flash, Adobe Reader, Java et Skype. Le rapport des Meilleures Pratiques de Sécurité vous indique les programmes que Trusteer Rapport a jugés obsolètes et la manière de les mettre à jour. Vous pouvez accéder au rapport des meilleures pratiques de sécurité à partir de la console de Rapport

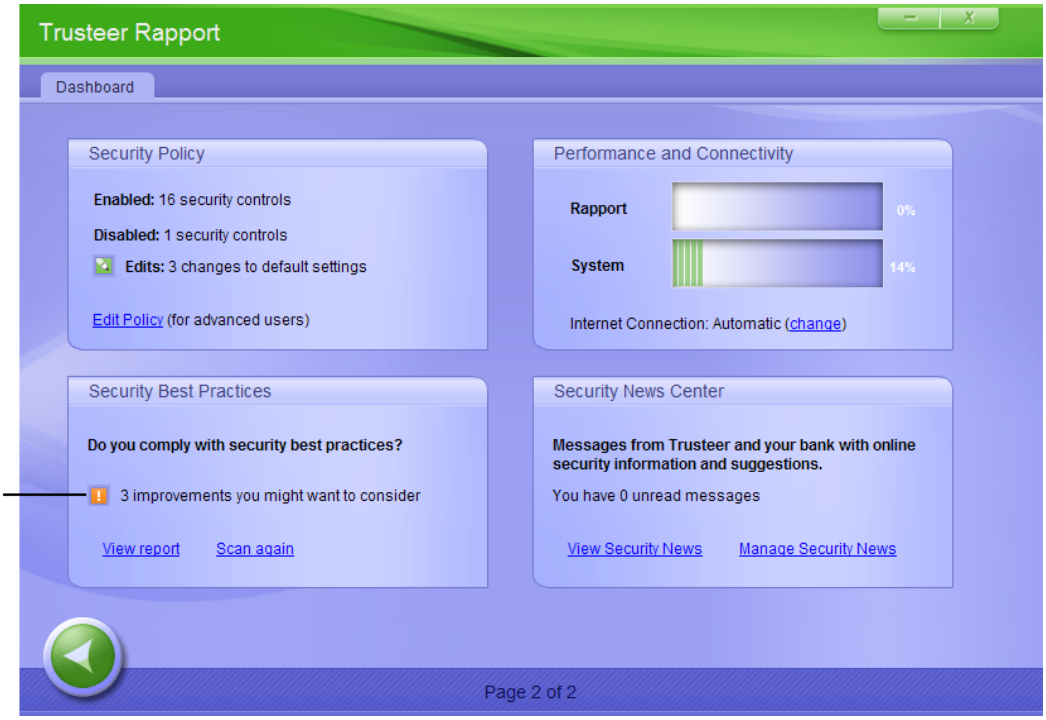
Exécuter une analyse manuelle

Bien que Trusteer Rapport effectue cette analyse régulièrement, vous pouvez analyser à nouveau votre ordinateur à chaque fois que vous le souhaitez.

➡ **Pour analyser votre ordinateur pour améliorer la sécurité:**

1. Ouvrir la console Rapport (on page 72).

2. Dans le tableau de bord, cliquez sur . Le second écran du tableau de bord apparaît, affichant le résumé des meilleures pratiques de sécurité en bas à gauche.



3. Dans la zone Meilleures pratiques du tableau de bord, Cliquez sur Analyser à nouveau. Pendant que l'analyse est en cours, le bouton Analyser à nouveau disparaît et les mots « Analyse en cours... » apparaissent. Lorsque l'analyse est terminée, le bouton Analyser à nouveau réapparaît et les résultats de l'analyse sont mis à jour.

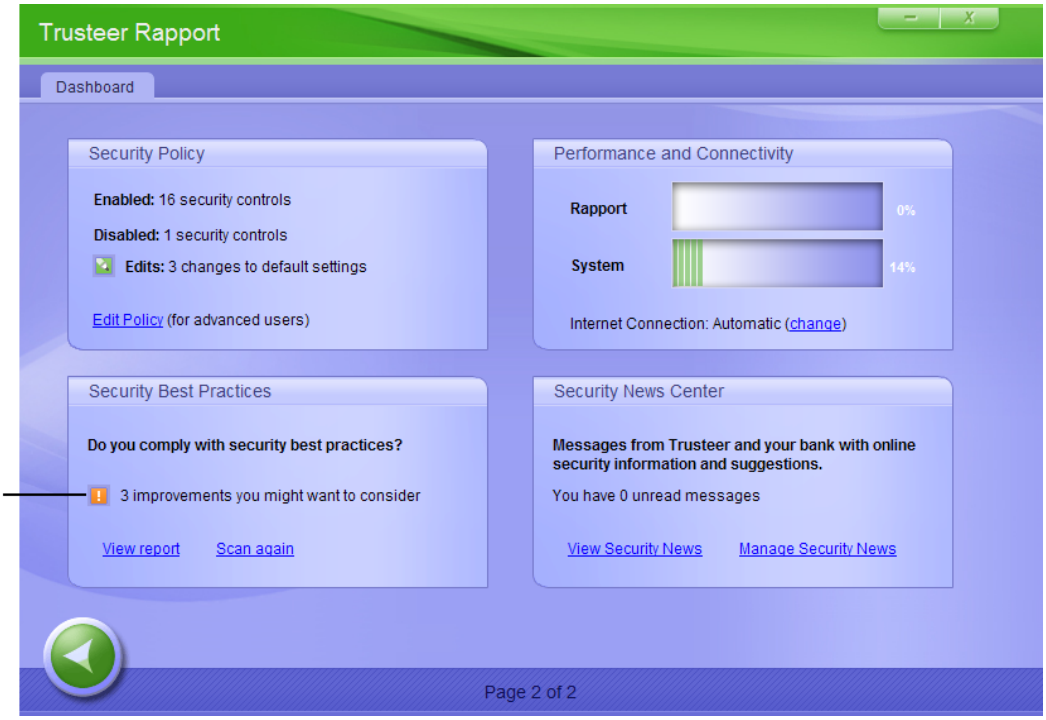
Afficher le rapport des meilleures pratiques de sécurité

Le rapport des meilleures pratiques de sécurité vous indique les programmes que Trusteer Rapport a jugés obsolètes et la manière de les mettre à jour.

➡ **Pour afficher le rapport des meilleures pratiques de sécurité:**

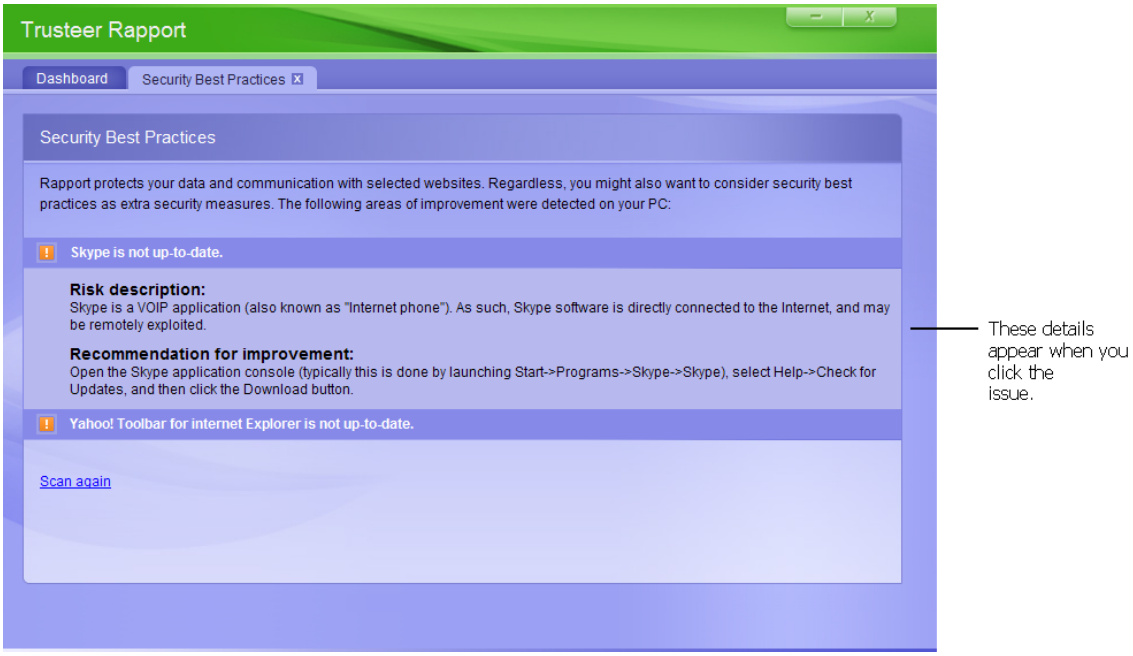
1. Ouvrir la console Rapport (on page 72).

2. Dans le tableau de bord, cliquez sur . Le second écran du tableau de bord apparaît, affichant le résumé des meilleures pratiques de sécurité en bas à gauche.



3. Cliquez sur Afficher le rapport. L'onglet des meilleures pratiques de sécurité apparaît, affichant un rapport sur les problèmes de sécurité détectés par l'analyse.

4. Cliquez sur chaque problème de sécurité. Une description complète du risque posé par le problème et une recommandation de ce que vous devriez faire au sujet de ce problème sont affichées.



14. Recevoir des infos en matière de sécurité

Le Centre des infos en matière de sécurité est votre espace personnel pour recevoir des messages importants de Trusteer sur la sécurité en ligne. Trusteer utilise votre Centre des infos en matière de sécurité pour vous envoyer des annonces et des conseils sur les nouvelles attaques dès qu'elles se produisent et la manière de les éviter. Protégé à 100 % contre l'hameçonnage et le courrier indésirable, le Centre des infos de sécurité ne reçoit jamais de messages non sollicités.

Les messages du Centre des infos de sécurité sont classés en différentes chaînes. Vous êtes automatiquement abonné à deux chaînes, toutes deux conçues pour fournir les données dont vous avez besoin pour être en ligne en toute sécurité :

- Trusteer. Conseils pour profiter au maximum de votre logiciel Trusteer Rapport pour améliorer la sécurité.
- Stay Safe. Des mises à jour sur les menaces émergentes de sécurité et des conseils pour vous aider à naviguer sur le Web en toute confiance.

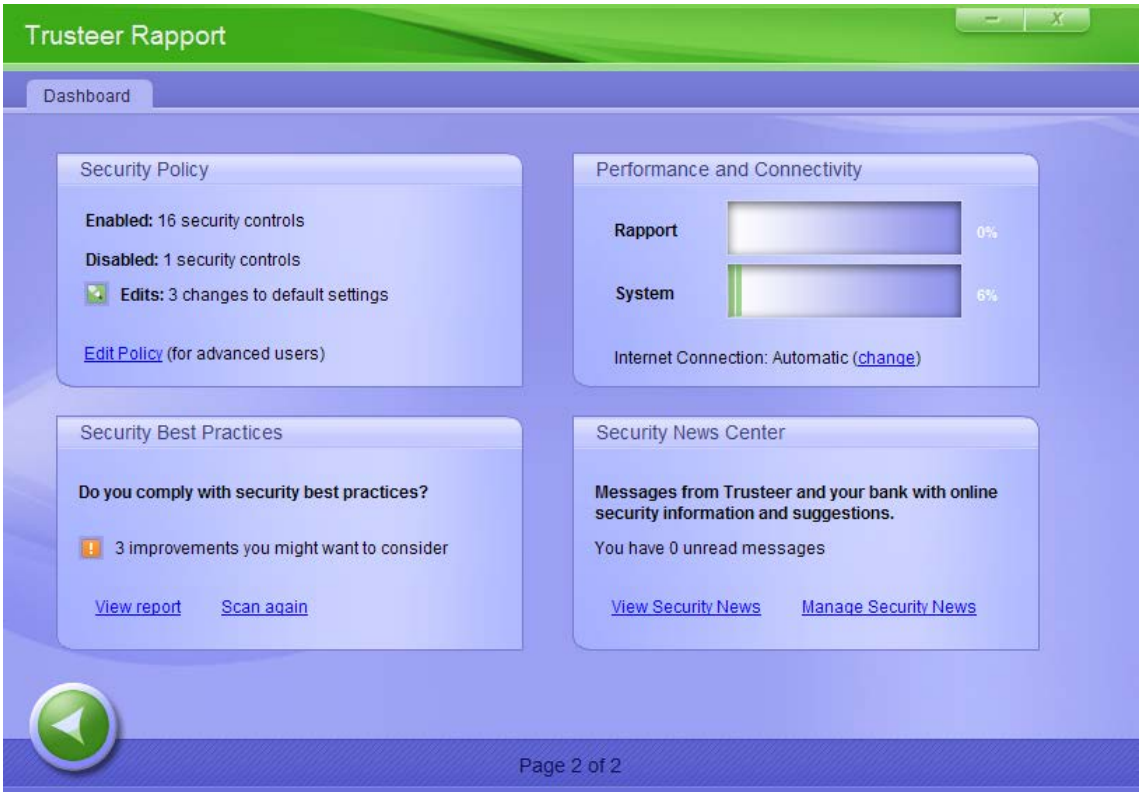
Afficher le Centre des infos de sécurité

Le Centre des infos de sécurité est accessible à partir de la console de Rapport.

➡ **Pour afficher le Centre des infos en matière de sécurité:**

1. Ouvrir la console Rapport (on page 72).

2. Dans le tableau de bord, cliquez sur . Le second écran du tableau de bord apparaît, affichant le Centre des infos de sécurité en bas à droite.



3. Cliquez sur Afficher les infos de sécurité. Le Centre des infos de sécurité apparaît.

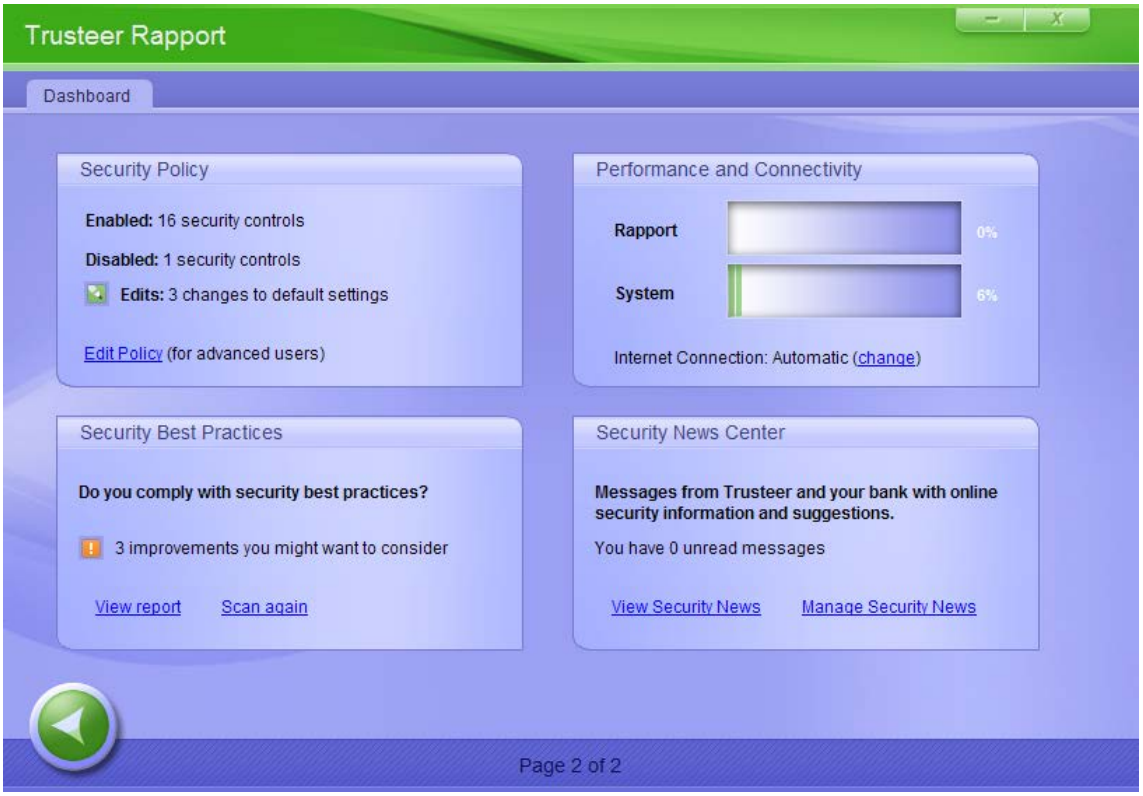
S'abonner aux chaînes d'infos de sécurité

Vous êtes automatiquement abonné à la chaîne de Trusteer et à la chaîne Stay Safe.

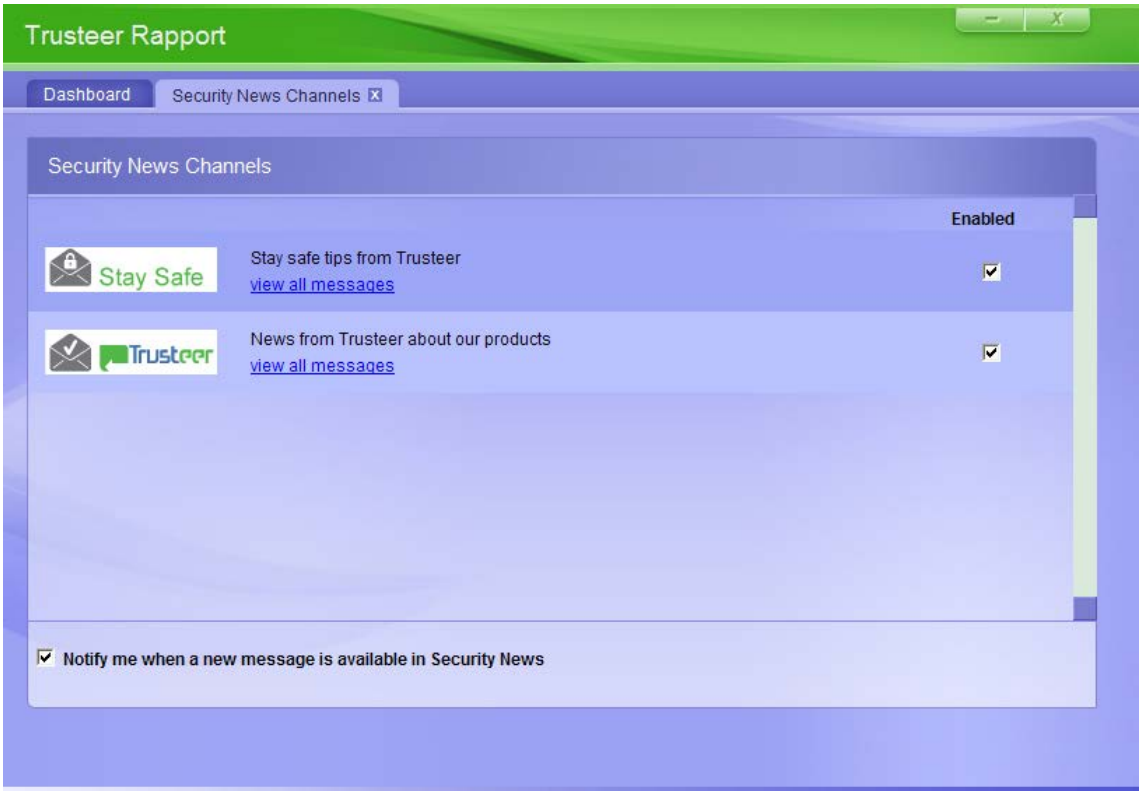
➡ **Pour vous abonner aux chaînes d'infos de sécurité:**

1. Ouvrir la console Rapport (on page 72).

2. Dans le tableau de bord, cliquez sur . Le second écran du tableau de bord apparait, affichant le résumé des infos de sécurité en bas à droite.



3. Cliquez sur Gérer les infos de sécurité. L'écran des chaînes d'infos de Sécurité apparaît, affichant les chaînes disponibles.



4. Sélectionnez Activée à côté de chaque chaîne à laquelle vous souhaitez vous abonner.

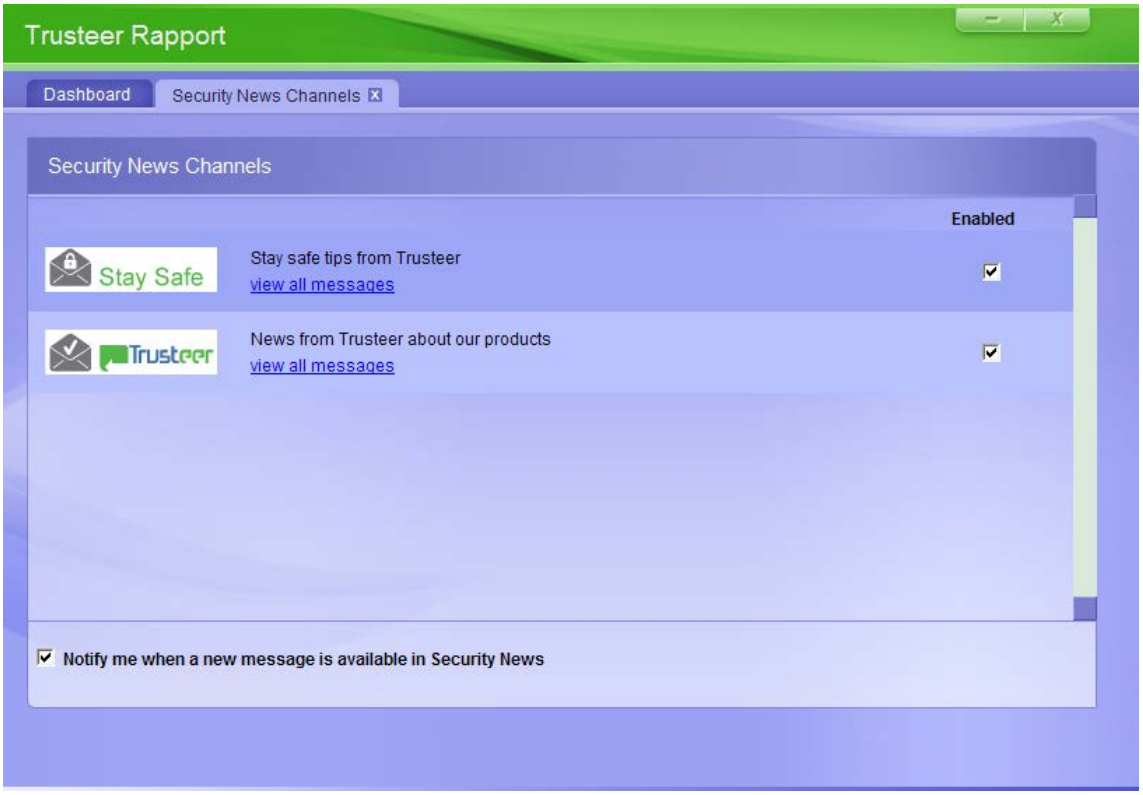
S'abonner aux notifications

Si vous vous abonnez aux notifications du Centre d'infos de sécurité, un message de notification apparaîtra sur votre écran chaque fois qu'un message d'infos de sécurité arrive.

➡ **Pour vous abonner aux notifications:**

1. Ouvrir la console Rapport (on page 72).
2. Dans le tableau de bord, cliquez sur . Le second écran du tableau de bord apparaît, affichant le Centre des infos en matière de sécurité en bas à droite.

3. Cliquez sur Gérer les infos de sécurité. L'onglet des chaînes d'info de sécurité apparaît.



4. Cochez la case Prévenez-moi lorsqu'un nouveau message est disponible dans les infos de sécurité.

15. Advanced

Gérer les sites protégés et les mots de passe

Trusteer Rapport fournit des informations sur les sites et les mots de passe qui sont protégés dans la console Rapport, et vous permet de supprimer des sites Web et des mots de passe.

Gérer des sites Web protégés

Il existe deux catégories de sites protégés:

- **Sites de partenaires de confiance**. Ce sont des sites appartenant à des partenaires de Trusteer. Ls partenaires de confiance travaillent directement avec Trusteer pour fournir la meilleure politique de sécurité pour leurs applications. Lorsque vous accédez au site d'un partenaire, vous êtes automatiquement protégé. Vous ne pouvez pas supprimer la protection de Trusteer Rapport de ces sites. Le nombre de sites protégés de partenaires ne constitue pas un fardeau pour votre système.
- **Les sites Web que vous avez ajoutés manuellement**. Ce sont des sites que vous avez ajoutés vous-même parce que vous avez souhaité bénéficier d'une protection de Trusteer Rapport lorsque vous vous connectez à ces sites. Vous pouvez supprimer la protection de Trusteer Rapport de ces sites en les supprimant de la liste.

Remarque: Dans certaines installations de Trusteer Rapport, la protection manuelle des sites est désactivée.

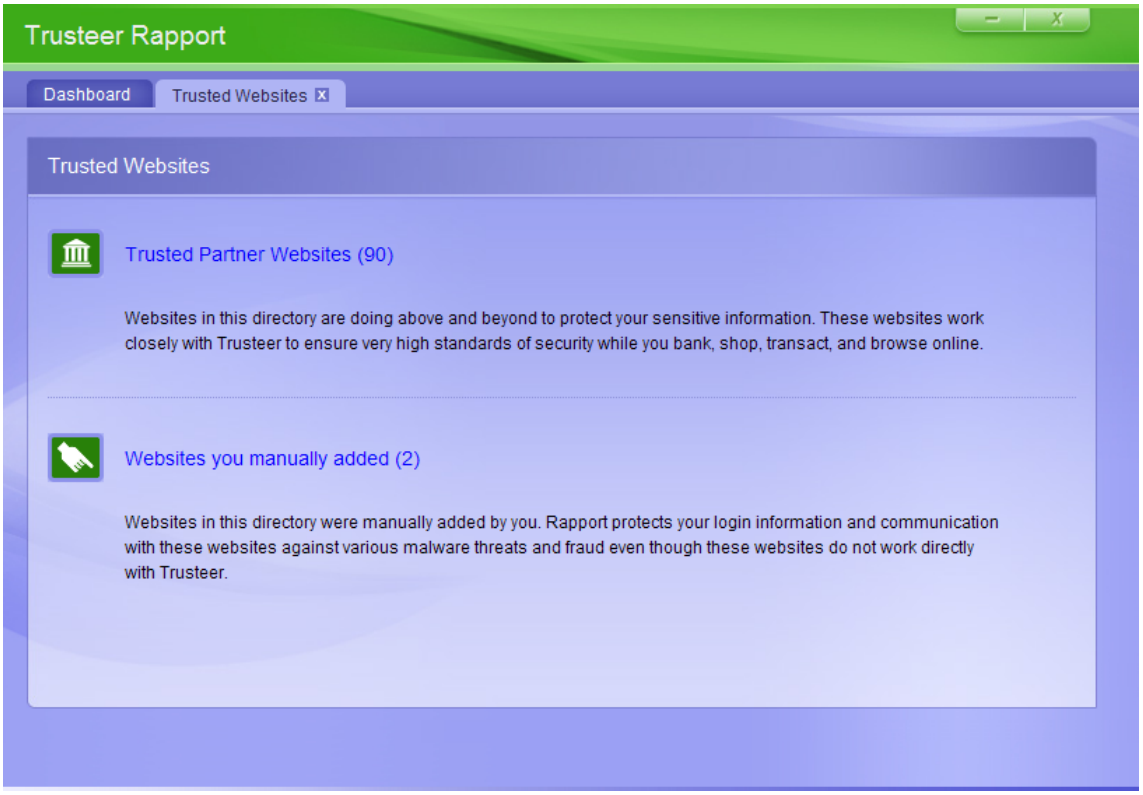
Remarque: Votre licence Trusteer Rapport vous permet d'ajouter de nombreux sites Web. Il n'est pas nécessaire de supprimer un site Web afin d'activer la protection de Trusteer Rapport sur un autre site Web. Si vous souhaitez protéger plus de sites que ne le permet votre licence, vous pouvez Répondre à une invite de mise à niveau de Trusteer Rapport (on page 138). La mise à niveau est gratuite.

La zone des sites Web de confiance de la console Rapport montre comment de nombreux sites dans chaque catégorie sont actuellement protégés. Vous pouvez voir une liste et une description des sites protégées de nos partenaires en cliquant sur Sites de partenaires de confiance. Vous pouvez voir une liste des sites Web que vous avez ajoutés manuellement en cliquant sur Sites ajoutés manuellement.

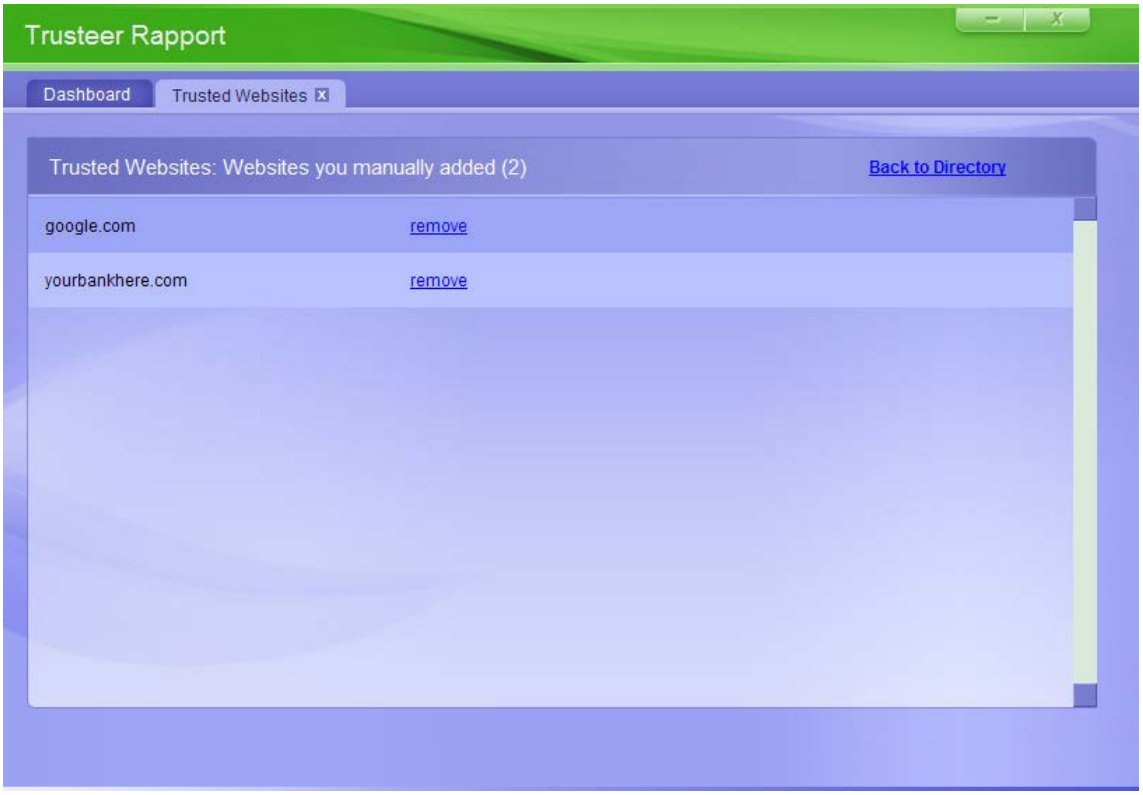
Pour supprimer des sites ajoutés manuellement:

1. Ouvrir la console Rapport (on page 72).

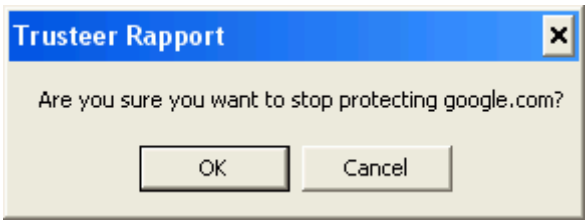
2. Dans la zone des sites Web de confiance, cliquez sur Parcourir les sites de confiance. Un onglet Sites Web de confiance s'affiche.



3. Cliquez sur Sites ajoutés manuellement. Une liste de tous les sites qui ont été ajoutés manuellement est affichée.



4. Cliquez sur le lien Supprimer à côté du site sur cette liste. Une boîte de confirmation apparaît.



5. Cliquez sur OK. Le site est supprimé de la liste. L'icône de Trusteer Rapport sera désormais grise lorsque vous naviguez sur le site Web que vous avez supprimé, indiquant qu'il n'est plus protégé.

Gérer les noms d'utilisateur et les mots de passe protégés

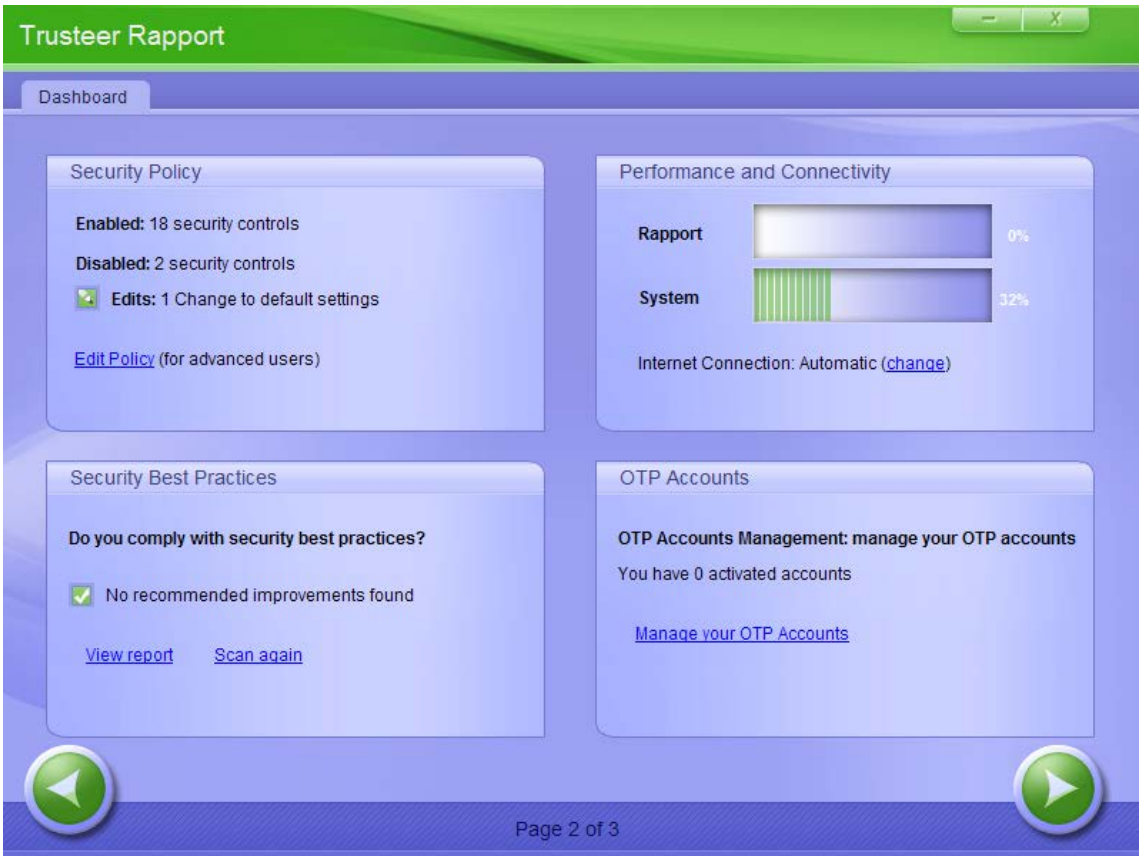
Après avoir accepté l'offre de Trusteer Rapport de protéger votre mot de passe sur un site protégé, Trusteer Rapport ne protège pas seulement ce mot de passe, mais aussi les mots de passe à venir que vous pourriez créer pour ce site. Trusteer Rapport se souvient de votre choix de protéger ou de ne pas protéger votre mot de passe sur chaque site, et ne vous offre plus de protéger votre mot de passe lorsque vous accédez à ce site, sauf si vous effacez le cache de la protection du mot de passe. La console de Rapport indique les sites dont la protection de Trusteer Rapport des mots de passe est actuellement activée. Vous pouvez désactiver la protection du mot de passe pour un site Web protégé si vous le souhaitez, et vous pouvez aussi effacer le cache de la protection des mots de passe, ce qui efface toutes les protections des mots de passe et les décisions de protection des mots de passe.

Remarque: Pour certains sites de partenaires de Trusteer, Trusteer Rapport protège les noms d'utilisateur ainsi que les mots de passe. La console de Rapport indique également la politique de protection des noms d'utilisateur par site.

➡ **Pour désactiver la protection des mots de passe sur un site protégé:**

1. Ouvrir la console Rapport (on page 72).

2. Dans le tableau de bord, cliquez sur . Le second écran du tableau de bord apparaît.



3. Dans la zone de la politique de sécurité, cliquez sur Modifier la politique. Un écran Approbation de l'utilisateur apparaît. L'écran vous montre une image contenant des caractères que vous devez saisir. Ceci a pour but d'empêcher les logiciels malveillants d'accéder à la console et de désactiver Trusteer Rapport de manière efficace.
4. Saisissez les caractères que vous voyez dans l'image.
5. Cliquez sur OK. L'écran de la politique de sécurité apparaît, affichant tous les contrôles de sécurité
6. Faites défiler la liste des contrôles de sécurité jusqu'à ce que vous trouvez le contrôle Avertir Lorsque les identifiants de connexion sont utilisés sur des sites Web inconnus.

7. Cliquez sur Avertir lorsque les identifiants de connexion sont utilisés sur des sites Web inconnus. La politique de protection des noms d'utilisateurs et des mots de passe sur chaque site est affichée.

8. Cochez la case Avertir si le mot de passe est utilisé ailleurs pour le site pour lequel vous souhaitez activer la protection des mots de passe. Trusteer Rapport ne protégera plus votre mot de passe pour ce site.

Remarque: Cliquer sur Effacer le cache efface tous les mots de passe et réinitialise toutes les politiques de protection des mots de passe, incitant Trusteer Rapport à afficher à nouveau une offre de protection des mots de passe la prochaine fois que vous visitez chaque site.

9. Cliquez sur Enregistrer. Vos modifications sont enregistrées.

Modifier la stratégie de sécurité de Trusteer Rapport

Remarque: Cette section s'adresse aux utilisateurs expérimentés.

Les fonctions de Trusteer Rapport ne nécessitent aucune configuration, mais vous pouvez en modifier un certain nombre pour les adapter à vos besoins.

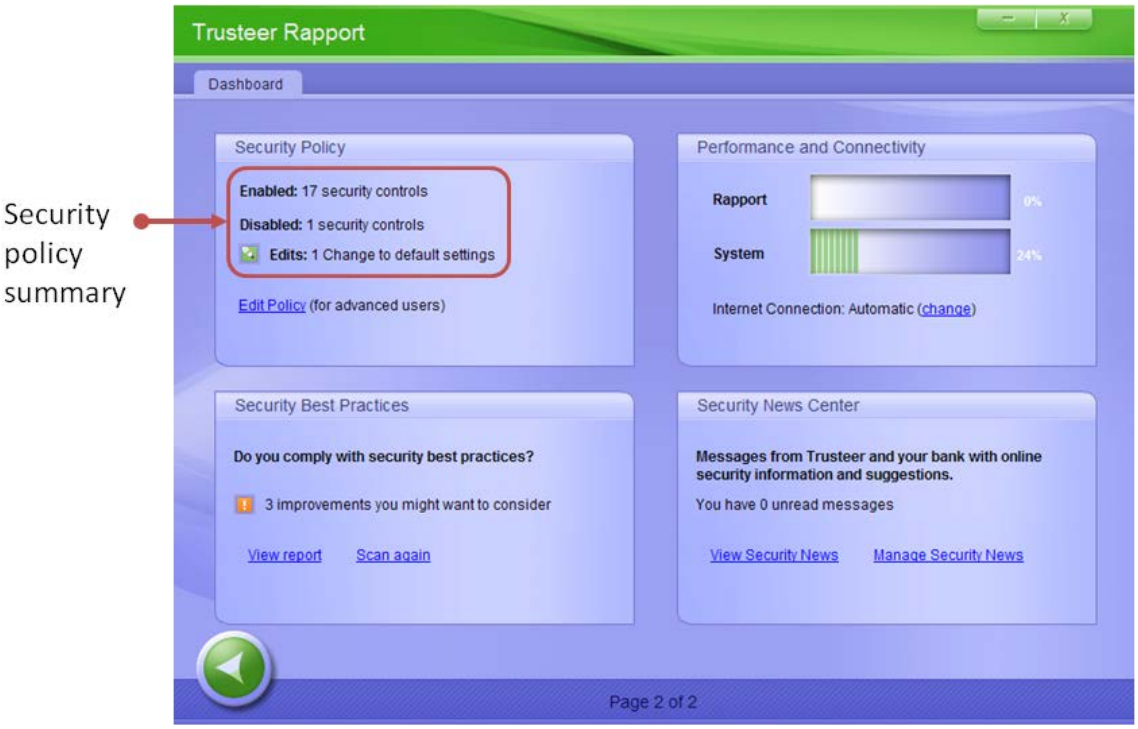
Afficher le résumé des règles de sécurité

La console Rapport affiche un résumé de vos règles de sécurité vous permettant de voir celles qui sont activées et celles qui sont désactivées.

➡ **Pour afficher le résumé des règles de sécurité :**

1. Ouvrir la console Rapport (on page 72).

2. Dans le tableau de bord, cliquez sur . Un second écran apparaît et affiche un résumé de la stratégie de sécurité dans la zone Security Policy (Stratégie de Sécurité).



Ce résumé contient les informations suivantes:

Zone d'affichage	Description
Activé	Nombre de règles de sécurité actuellement actives.
Désactivé	Nombre de règles de sécurité actuellement inactives.
Modifications	Nombre de modifications apportées aux paramètres par défaut.

Modifier les règles de sécurité

Les règles de sécurité de Trusteer Rapport offrent une sécurité optimale tout en réduisant les conflits éventuels avec les programmes légitimes. Par exemple, le blocage de la capture d'écran est activé par défaut pour ne protéger que les sites partenaires. Il existe en effet de nombreux produits légitimes de capture d'écran et Trusteer préfère n'intervenir que lorsque ces interférences sont cruciales pour la sécurité de votre banque en ligne ou de votre entreprise.

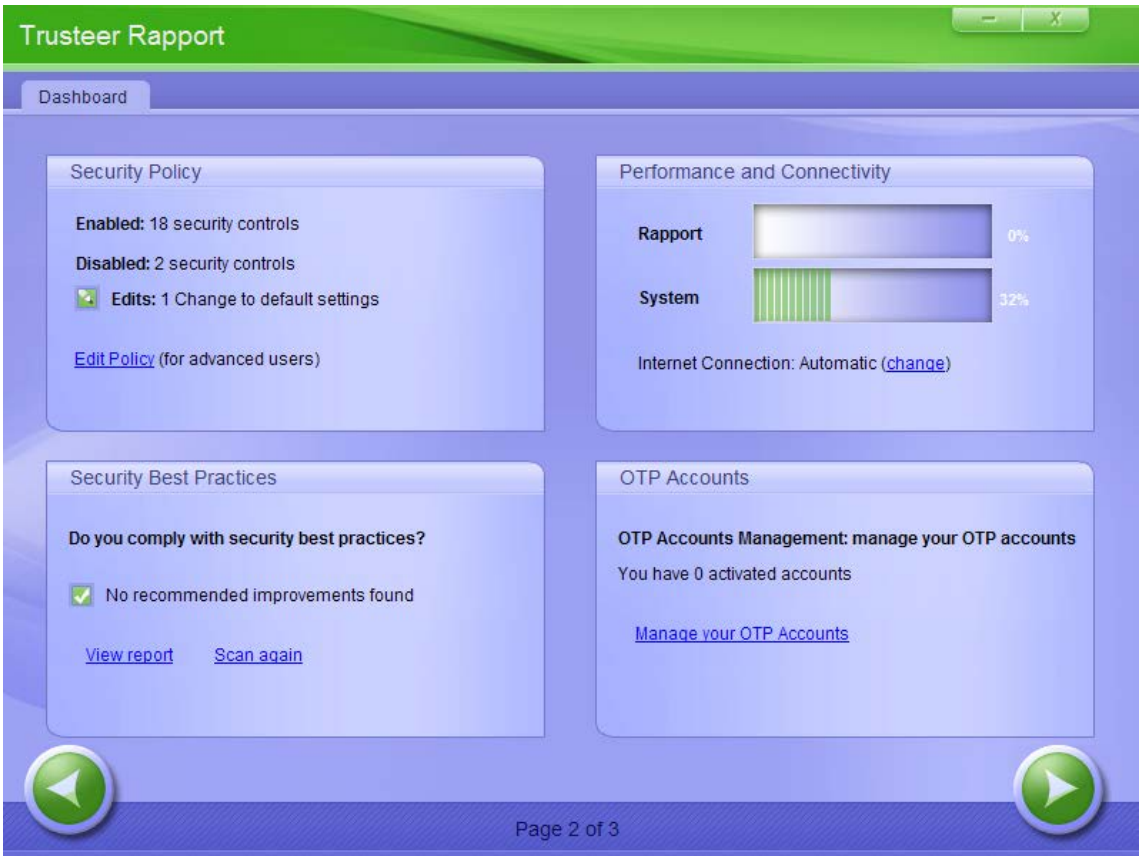
Trusteer Rapport vous permet de modifier les règles de sécurité en intervenant sur chaque paramètre. En modifiant ces paramètres, vous avez la possibilité d'activer une tâche légitime normalement bloquée par les règles de sécurité par défaut ou de résoudre un problème de compatibilité avec une autre application de sécurité. Toute modification apportée aux paramètres par défaut abaisse généralement le niveau de protection offert par Trusteer Rapport. Assurez-vous donc de bien comprendre les risques encourus avant de procéder à ces modifications.

Remarque: Si Trusteer Rapport a été installé à partir d'un compte administrateur Windows, vous ne pourrez procéder à certains paramétrages que si vous êtes connecté en tant qu'administrateur.

Pour modifier les règles de sécurité:

1. Ouvrir la console Rapport (on page 72).

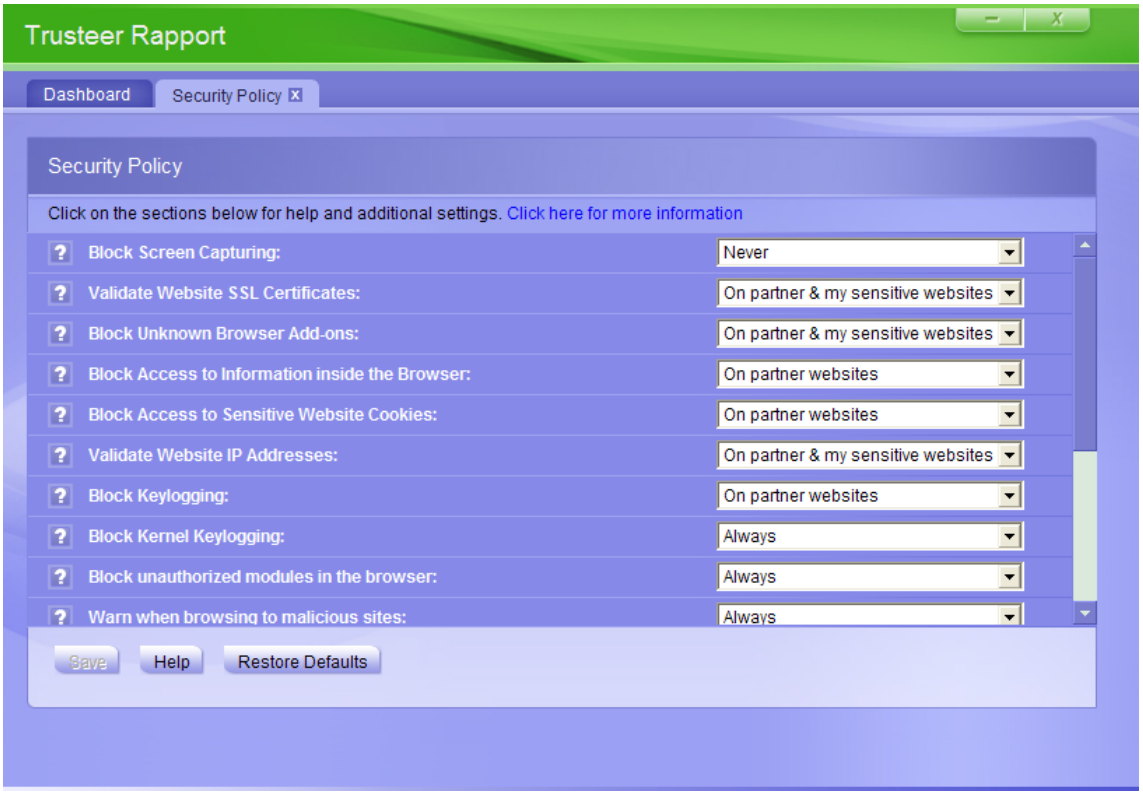
2. Dans le tableau de bord, cliquez sur . Le second écran du tableau de bord apparaît.



3. Dans la zone de la politique de sécurité, cliquez sur Modifier la politique. Un écran Approbation de l'utilisateur apparaît. L'écran vous montre l'image d'un mot pour que vous le saisissiez. Ceci est destiné à empêcher les logiciels malveillants d'accéder à la console et de désactiver Trusteer Rapport de manière efficace.

4. Saisissez le mot que vous voyez dans l'image.

5. Cliquez sur OK. L'écran Politique de sécurité apparaît, affichant tous les contrôles de sécurité.

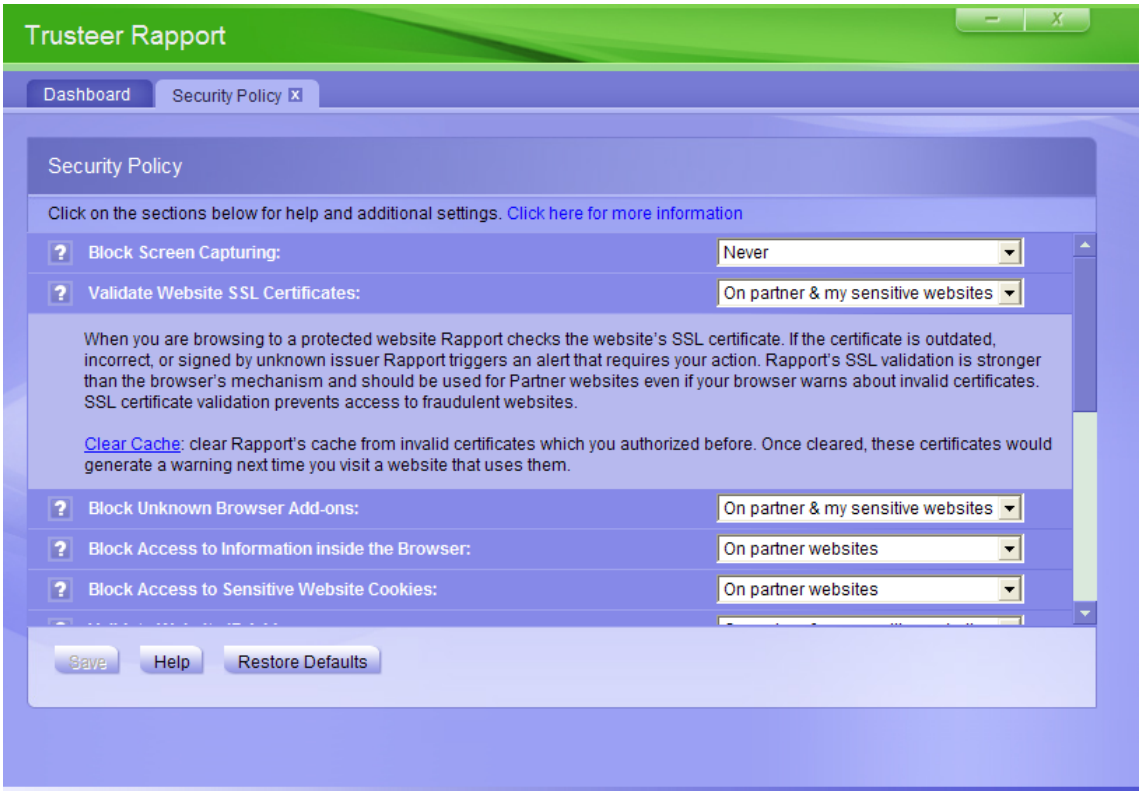


6. Dans le menu déroulant situé à droite de la règle que vous voulez modifier, sélectionnez le paramètre de votre choix. Avant toute modification, veillez à bien comprendre l'incidence sur le niveau de protection fourni par Trusteer Rapport. Reportez-vous à la section Comprendre les règles de sécurité (on page 182) pour les détails concernant ces règles, les options disponibles et les informations complémentaires s'y rapportant. Voici les paramètres que vous pouvez visualiser:

   - **Toujours** : la règle est toujours activée quel que soit le site.
   - **Jamais** : la règle est toujours désactivée.
   - **Sur les sites partenaires** : la règle est disponible pour les sites partenaires en fonction des paramètres de sécurité définis par le propriétaire du site. Les sites partenaires collaborent directement avec Trusteer pour fournir la politique de sécurité la plus adaptée.

- **Sur les sites partenaires et mes sites sensibles** : la règle protège les sites partenaires et les sites supplémentaires que vous Protecting Additional Websites (on page 70).

Cliquez sur le nom d'une règle pour afficher une description et les fonctions spécifiques associées à la règle:

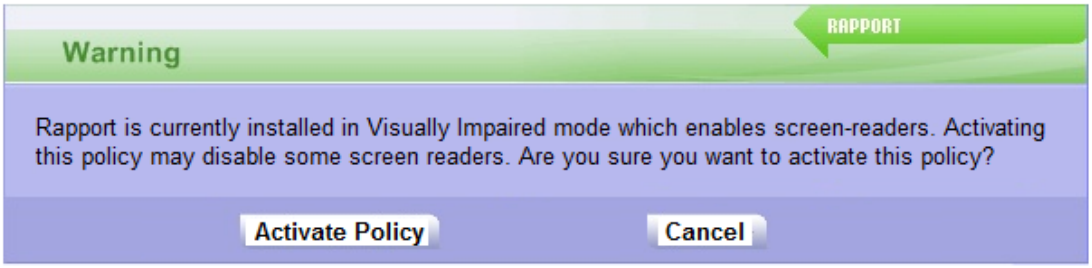


Si vous souhaitez revenir aux paramètres par défaut pour toutes les règles, cliquez sur Restore Defaults.

Remarque: Si Trusteer Rapport a été installé en mode Malvoyant, le paramètre par défaut pour la règle **Bloc Screen Capturing** (Bloquer la capture d'écran) et **Block Acess to Information inside the Browser** (Bloquer l'accès aux informations contenues dans le navigateur) est **Jamais**.

7. Cliquez sur **Save** (Enregistrer). Vos changements de règles sont enregistrés. Certaines modifications exigent de redémarrer le navigateur ou l'ordinateur pour être appliquées

Remarque: Si Trusteer Rapport a été installé en mode Compatibilité de lecteur d'écran et que vous activez la règle **Bloc Screen Capturing** ou **Block Acess to Information inside the Browser**, le message suivant apparaît :



Si vous souhaitez poursuivre et activer la règle, cliquez sur **Activate Policy** (Activer la règle). Dans le cas contraire (cette action va désactiver les lecteurs d'écran), cliquez sur **Cancel** (Annuler).

Comprendre les règles de sécurité

Avant de modifier les règles de sécurité, assurez-vous de bien comprendre les changements que vous apportez à la protection fournie par Rapport. Le tableau suivant décrit la stratégie de sécurité, les options de règles disponibles et les informations complémentaires s'y rapportant.

Règle	Description	Options des règles	Informations complémentaires
Bloquer la capture d'écran	Désactive toute tentative de capture d'écran lors de l'affichage d'un site protégé. Les programmes de votre ordinateur tentant d'effectuer une impression d'écran génèrent une image noire. Le but est d'empêcher un malware de capturer l'écran pour collecter des informations sensibles.	• **Jamais**. Permet la capture d'écran à tout moment. (Certaines opérations, telles que l'arrêt de Trusteer Rapport, appellent des messages de confirmation de sécurité qui ne peuvent capture être capturés même si cette règle est sur « Jamais »). • **Sur les sites partenaires** (défaut). Bloque toute capture d'écran sur l'ordinateur uniquement quand un site partenaire est ouvert dans le navigateur. • **Sur les sites partenaires et mes sites sensibles**. Bloque toute capture d'écran sur l'ordinateur uniquement quand un site protégé (partenaire ou ajouté manuellement) est ouvert dans le navigateur.	La touche Impression d'écran est actionnée différemment par d'autres mécanismes de capture d'écran. Si la touche de commande Impression d'écran est pressée, Trusteer Rapport affiche une Répondre à une alerte de détection d'une tentative d'impression écran (on page 125) demandant à l'utilisateur de choisir entre bloquer et activer la Même si vous avez besoin d'effectuer des impressions d'écran, ne désactivez pas cette fonction. Le blocage de capture d'écran de Rapport n'empêche pas les mécanismes de capture de fonctionner à tout moment lorsque des sites protégés ne sont pas affichés. Cette fonction de blocage par défaut ne s'applique qu'aux sites partenaires protégés. Même lorsque la capture est bloquée, vous pouvez utiliser cette fonction à l'aide de la touche Impression d'écran de votre clavier. Dans ce cas, une boîte de dialogue de Rapport apparaît et vous demande de confirmer que vous souhaitez bloquer ou activer la capture. Cliquez simplement sur Allow (Autoriser) pour procéder. Ainsi, vous ne désactivez le blocage que si vous avez besoin de capturer des écrans affichés sur des sites partenaires utilisant un mécanisme autre que la touche de votre clavier. Une fois vos impressions d'écran effectuées, vous pouvez réactiver le blocage de capture d'écran pour restaurer la protection fournie par cette fonction. Si Rapport vous bloque quand vous tentez de capturer un élément d'un site non protégé, réduisez toutes les fenêtres ouvertes du navigateur ou fermez les fenêtres ou onglets contenant des pages protégées. Vous pourrez ainsi capturer votre écran sans être bloqué.

Règle	Description	Options des règles	Informations complémentaires
Valider les certificats SSL des sites	Lorsque vous parcourez un site protégé, Trusteer Rapport vérifie son certificat SSL. Si le certificat est obsolète, incorrect ou signé par un émetteur inconnu, Rapport déclenche une alerte (page 125) demandant votre intervention. Le mécanisme de validation des certificats SSL de Rapport est plus strict que celui des navigateurs et doit être utilisé pour les sites partenaires même si votre navigateur affiche des messages d'alerte en cas de certificat non valide. Le but est d'empêcher la visite de sites frauduleux.	• **Jamais**. Ne vérifie pas les certificats SSL du site. • **Sur les sites** partenaires (défaut). Vérifie les certificats SSL utilisés par les sites partenaires quand vous les visitez. • **Sur** les sites partenaires et mes sites sensibles. Vérifie les certificats SSL utilisés par les sites partenaires et ceux ajoutés manuellement quand vous les visitez.	Pour vous informer sur la manière de répondre à une alerte de certificat non valide, consultez Répondre à une alerte de Certificat non valide (on page 134). Vous pouvez supprimer les certificats non valides que vous avez autorisés dans le cache de Trusteer Rapport. Après quoi, les certificats supprimés du cache génèreront une alerte si vous visitez un site qui les utilise. Pour supprimer les certificats non valides du cache, **cliquez sur** Clear Cache (Nettoyer le cache) sous la liste déroulante Validate Website SSL Certificates.
Bloquer les extensions inconnues du navigateur	Bloque les extensions non reconnues. Ces modules (barres d'outils ou BHO) sont des petits composants logiciels (généralement tiers) présents dans votre navigateur, pouvant contrôler vos communications. Si la plupart sont légitimes (tels que la barre Google), certains sont malveillants. Le but est d'empêcher des extensions malveillantes de voler vos identifiants ou de falsifier vos communications.	• **Jamais**. Autorise toutes les extensions sur **tous les sites.** • **Sur les sites partenaires**. Bloque les extensions non reconnues lors de l'accès à **des sites partenaires.** • **Sur les sites partenaires et mes sites sensibles** (défaut). Bloque les extensions non reconnues lors de l'accès à un site partenaire ou protégé manuellement.	La console affiche une liste d'extensions inconnues détectées par Trusteer Rapport et les bloque quand vous êtes connecté à un site protégé. Vous pouvez débloquer manuellement des modules spécifiques que vous savez être sûrs en cochant la case « Allow » pour chaque extension.

Règle	Description	Options des règles	Informations complémentaires
Bloquer l'accès aux données du navigateur	Bloque les processus de votre ordinateur qui accèdent aux sites via une interface de programmation DOM (API). Ceux-ci peuvent lire les données sensibles ou falsifier vos transactions. Rapport bloque ces processus qu'ils soient légitimes ou malveillants. Le but est d'empêcher des processus malveillants de lire illégalement des informations sensibles ou de falsifier vos transactions	• **Jamais**. Ne bloque • pas l'accès des processus aux sites. • **Sur les sites partenaires** (défaut). Bloque les processus lors de l'accès aux sites parte**naires.** • **Sur les sites partenaires et mes sites sensibles**. Bloque les processus lors de l'accès aux sites partenaires et protégés manuellement.	Un exemple courant est le gestionnaire de mots de passe qui retient vos mots de passe et les entre automatiquement lors de la connexion. Rapport empêche d'accéder à ces informations car il s'agit de données sensibles ; le logiciel peut avoir été trompé par un malware qui cherche à récupérer vos identifiants de connexion. Nous recommandons de ne pas utiliser de telles fonctions sur vos sites de transactions en ligne. Certains programmes légitimes ayant accès à ces données sont bloqués par Rapport sur les sites partenaires.
Bloquer l'accès aux cookies sensibles	Bloque l'accès des cookies applicatifs tels que les cookies de session qu'un propriétaire de site partenaire définit comme cookies sensibles. Le but est d'empêcher des cookies de session de contrôler votre session sur le site.	• **Jamai**s. Ne bloque pas l'accès des applications aux cookies sensibles. • **Sur les sites partenaires** (défaut). Bloque l'accès aux cookies sensibles lors de l'accès à un site partenaire.	Trusteer doit pouvoir reconnaître les cookies d'un site avant de configurer Rapport pour le protéger, sinon des conflits avec le site peuvent survenir. C'est pourquoi ce type de protection n'est disponible que pour les sites partenaires.

Règle	Description	Options des règles	Informations complémentaires
Valider les adresses IP du site	Valide les adresses IP du site par rapport aux tables de conversion d'adresses IP de confiance. Lors de l'accès à un site protégé, Rapport vérifie son adresse IP par rapport à une liste d'adresses sûres connues pour ce site. Si l'adresse IP est introuvable dans la liste, Rapport la remplace par une autre adresse sûre pour ce site. Le but est de vous empêcher d'accéder à un site frauduleux en raison d'une attaque de pharming[4].	• **Jamais**. Ne vérifie pas les adresses IP du site par rapport aux tables d'adresses IP de confiance. • **Sur les sites partenaires**. Vérifie les adresses IP du site par rapport aux tables d'adresses IP de confiance lors de l'accès aux sites partenaires. • **Sur les sites partenaires et mes sites sensibles** (défaut). Vérifie les adresses IP du site par rapport aux tables d'adresses de confiance lors de l'accès aux sites partenaires et protégés manuellement.	La fonction de nettoyage du cache pour cette règle n'est pour le moment pas prise en charge.
Bloquer les keyloggers	Chiffre toutes les saisies clavier sur le trajet vers le navigateur et les masque des programmes-espions enregistreurs de frappe. Le but est d'empêcher ces logiciels malveillants de lire vos saisies et de s'emparer de données sensibles telles que les mots de passe.	• **Jamais**. Ne bloque pas les keyloggers. • **Sur les sites partenaires.** Bloque les keyloggers lors de l'accès aux sites partenaires. • **Sur les sites partenaires et mes sites sensibles** (défaut). Bloque les keyloggeurs lors de l'accès aux sites partenaires et protégés manuellement.	Cette fonction peut entrer en conflit avec d'autres anti-keyloggers et provoquer des erreurs de frappe. Donc, si vous avez un autre antikeylogger activé (p. ex. intégré à votre antivirus), il se peut que vous deviez désactiver cette fonction. Vous pouvez le cas échéant désactiver cette protection dans votre antivirus existant. Si vous découvrez que cette règle est désactivée alors que vous ne l'avez pas désactivée vous-même, cela signifie que Trusteer Rapport a détecté un conflit entre votre configuration matérielle ou logicielle et Rapport. Rapport a désactivé ce mécanisme pour éviter le conflit.
M'alerter quand je navigue sur des sites potentiel-lement infectés	Vous alerte si vous tentez d'accéder à un site susceptible d'infecter votre navigateur avec un malware.	• **Jamais**. Pas d'alerte. • **Toujours** (défaut). Vous alerte lors de l'accès à des sites potentiellement infectés	

[4] Les attaques de pharming sont des tentatives pour rediriger le trafic de votre site vers des sites fictifs.

Règle	Description	Options des règles	Informations complémentaires
Bloquer les keyloggers logiciels	Chiffre toutes les frappes sur leur trajet vers le navigateur et les masque des composants logiciels malicieux intégrés au système d'exploitation (appelés « kernel keyloggers » ou keyloggers logiciels). Il s'agit d'une version renforcée du blocage de keylogging. Une fois cette fonction activée, Rapport chiffre les frappes au niveau du noyau système et bloque les keyloggers où qu'ils se trouvent sur le chemin d'accès au navigateur. Si Block Keylogging est désactivée, Block kernel keylogging est aussi désactivée, même si la règle est définie sur Toujours. Block kernel keylogging complète et renforce Block keylogging, mais ne fonctionne pas seule. Le but est d'empêcher des composants malveillants de lire vos frappes et de s'emparer de données sensibles comme les numéros de carte de paiement.	• Jamais • Toujours (défaut)	Si Trusteer Rapport a été installé depuis un compte administrateur Windows, vous ne pouvez modifier ce paramètre que si vous êtes connecté en tant qu'administrateur.
Bloquer les modules du navigateur non-autorisés	Surveille les fichiers DLL chargés dans les navigateurs et bloque le chargement de fichiers malveillants.	• Jamais • Toujours (défaut)	Cette opération s'activant au démarrage du navigateur, tous les sites sont protégés, sites partenaires comme sites ajoutés manuellement.
Alerter à la visite d'un site malveillant	Vous alerte si vous tentez d'accéder à un site connu comme frauduleux.	• Jamais • Toujours (défaut)	

Règle	Description	Options des règles	Informations complémentaires
		•	Vous pouvez voir les règles de protection du mot de passe et du nom d'utilisateur pour chaque site en cliquant sur **Warn When Login Information is Used in Unknown Websites** (Alerter quand les informations de connexion sont utilisées sur des sites inconnus). Si vous souhaitez désactiver la protection du mot de passe ou du nom d'utilisateur pour un site spécifique, décochez cette case ; Rapport ne vous alertera plus si vous entrez ce mot de inconnus. Vous pouvez vider le cache des PII protégées. Après avoir vidé le cache, Rapport ne protège plus aucun mot de passe. Ceci réinitialise également tous vos choix de protection pour les sites protégés individuellement. Lors du premier accès à chaque site protégé après avoir vidé le cache, Rapport vous propose à nouveau de protéger votre mot de passe. Pour vider le cache, cliquez sur **Warn When Login Information is Used in Unknown Websites** puis sur **Clear Cache**.
Bloquer les modifications des processus navigateur	Bloque les tentatives de modification des processus du navigateur. Appelée également patching de fonctions, cette technique permet de prendre le contrôle du navigateur et d'accéder à vos données sensibles. Utilisée par les malwares et par certains logiciels légitimes. Trusteer Rapport analyse chaque tentative de modification et bloque les processus suspects.	• **Jamais** • **Toujours** (défaut)	Du fait que cette protection opère au démarrage du navigateur, elle protège tous les sites et ne fait pas de différence entre sites partenaires et sites ajoutés manuellement.

Règle	Description	Options des règles	Informations complémentaires
Protéger Rapport des suppressions non-autorisées	Protège Trusteer Rapport lui-même contre une suppression et falsification non-autorisées. Rapport empêche ses processus d'être arrêtés et protège ses fichiers et ses clés de registre contre les suppressions ou falsifications. L'exécution d'opérations simples telles que Terminer le processus ou Supprimer les fichiers est dès lors impossible. Rapport empêche ainsi les malwares de le supprimer de l'ordinateur.	• **Jamais** • **Toujours** (défaut)	Si Trusteer Rapport a été installé depuis un compte administrateur Windows, vous ne pouvez modifier ce paramètre que si vous êtes connecté en tant qu'administrateur. Trusteer Rapport ne peut et ne doit être supprimé qu'à partir du panneau de configuration, comme décrit dans Désinstaller Trusteer Rapport (on page 233).
Protection anticipée du navigateur	Commence à protéger le navigateur dès la phase démarrage la plus précoce.	• **Jamais** • **Toujours** (défaut)	Du fait que cette protection opère au démarrage du navigateur, elle protège tous les sites et ne fait pas de différence entre sites partenaires et sites ajoutés manuellement. Si Trusteer Rapport a été installé depuis un compte administrateur Windows, vous ne pouvez modifier ce paramètre que si vous êtes connecté en tant qu'administrateur.

Règle	Description	Options des règles	Informations complémentaires
Envoyer les événements et erreurs de sécurité pour analyse	Chaque fois que Rapport détecte une application ou activité suspecte, un événement de sécurité est généré et envoyé au service central de Trusteer Rapport pour analyse. Des tests complets sont effectués pour déterminer si l'activité est frauduleuse. Dans ce cas, le service central demande à Trusteer Rapport de renforcer le blocage de la menace. Outre les événements de sécurité, Rapport envoie de temps en temps des informations sur les erreurs logicielles internes. Ces données aident Trusteer à identifier et réparer ces erreurs. Toutes les informations envoyées depuis votre ordinateur au service central de Trusteer Rapport sont des données techniques, anonymes et exemptes de tout caractère privé. La désactivation de cette fonction peut gravement compromettre votre sécurité. Dans le cas d'une menace réelle sur votre sécurité en ligne, cette fonction permet au propriétaire du site attaqué tel que votre banque ou entreprise d'être alerté et de prendre des mesures préventives afin de sécuriser vos avoirs et/ou vos fonds.	• **Événements critiques uniquement** • **Toujours** (défaut)	Si Trusteer Rapport a été installé depuis un compte administrateur Windows, vous ne pouvez modifier ce paramètre que si vous êtes connecté en tant qu'administrateur. Pour vous informer sur la politique de confidentialité et les pratiques de Trusteer relatives à l'information de l'utilisateur, consultez http://www.trusteer.com/support/privacy-policy et http://www.trusteer.com/support/end-user-license-agreement.

Règle	Description	Options des règles	Informations complémentaires
Supprimer les malwares	Trusteer Rapport supprime certains types de malwares de votre ordinateur. Ceci fournit une couche supplémentaire de sécurité importante qui complète la capacité de Rapport à bloquer l'accès des malwares à vos informations sensibles.	• **Jamais** • **Toujours** (défaut)	Si Trusteer Rapport a été installé depuis un compte administrateur Windows, vous ne pouvez modifier ce paramètre que si vous êtes connecté en tant qu'administrateur. **Remarque:** sur certaines installations de Rapport, ce paramètre ne peut pas être désactivé.
Protéger du vol les numéros de cartes de paiement	Vous alerte lorsque vous envoyez des informations de paiement par carte à des sites locaux non sécurisés. L'alerte apparaît dans une boîte de dialogue vous permettant de stopper l'envoi. Active l'antikeylogging lorsque vous entrez un numéro de carte de paiement sur un site protégé par Rapport ou un site sécurisé (HTTPS) contenant un terme associé au paiement par carte tel que Visa, Mastercard ou Amex. Ceci empêche un keyloggeur de capturer vos détails de carte de paiement. Le but est de vous protéger du vol de carte de paiement en vous évitant d'envoyer un numéro de carte à un site de phishing ou à un site légitime non sécurisé, et en empêchant des malwares de s'emparer de vos informations de carte.	• **Jamais** • **Toujours** (défaut)	Cette protection n'est disponible que pour les cartes émises par des marques partenaires. Les sites dans la liste « You chose to trust the following sites : » (Vous avez choisi de faire confiance aux sites suivants) sont les sites auxquels vous avez décidé de faire confiance en cliquant **Ignore, I trust this website** (Ignorer, j'ai confiance en ce site) dans la boîte de dialogue Répondre à une alerte de détection d'envoi de carte de paiement (on page 123). Pour supprimer un site de la liste des sites de confiance, cliquez sur **Clear this site** à côté du site que vous voulez supprimer. Pour supprimer tous les sites, cliquez sur **Clear all** sites. Si vous ne souhaitez pas être alerté quand Rapport active l'antikeylogging, décochez **Notify me when Trusteer activates payment card protections** (M'alerter quand Trusteer active la protection des cartes de paiement) (activé par défaut). Si vous ne souhaitez pas être alerté quand vous envoyez des informations de paiement par carte à des sites locaux et non sécurisés, décochez **Alert me when Rapport detects high risk payment card submission** (M'alerter quand Rapport détecte un envoi de paiement par carte à haut risque) (activé par défaut).

Règle	Description	Options des règles	Informations complémentaires
M'alerter quand j'envoie des données sensibles à des sites non sécurisés	Vous alerte quand vous venez d'entrer un mot de passe sur un site sur lequel l'envoi de données n'est pas sécurisé. Le but est de vous empêcher d'envoyer des données sensibles à des sites à haut risque qui pourraient être facilement interceptées par des criminels, y compris des sites légitimes.	• **Jamais** • **Toujours** (défaut)	Si Trusteer Rapport a été installé depuis un compte administrateur Windows, vous ne pouvez modifier ce paramètre que si vous êtes connecté en tant qu'administrateur. Les sites dans la liste « You chose to trust the following sites: » (Vous avez choisi de faire confiance aux sites suivants) sont les sites auxquels vous avez décidé de faire confiance en cliquant sur **I trust this site, don't alert me again** (J'ai confiance en ce site, ne plus m'alerter) dans la boîte de dialogue Répondre à une alerte de soumission non sécurisée (on page 114) ou sur **Trust this site** (Faire confiance à ce siteResponding to a Protected Information Warningoi protégé. Pour supprimer un site spécifique de la liste des sites de confiance, cliquez sur Clear this site à côté du site que vous voulez supprimer. Pour supprimer tous les sites, cliquez sur **Clear all sites**.

Règle	Description	Options des règles	Informations complémentaires
Proposer l'utilisation du navigateur virtualisé de Trusteer Rapport sur les sites pris en charge	Vous alerte quand vous visitez un site prenant en charge le navigateur virtualisé de Trusteer Rapport et propose d'ouvrir le site dans le navigateur virtualisé si celui-ci est installé sur votre ordinateur. Si le navigateur virtualisé n'a pas été encore installé sur votre ordinateur, le message vous propose de le télécharger.	• **Jamais** • **Toujours** (défaut)	Cette règle est définie sur **Jamais** si vous avez cliqué sur **Do not show this alert again** (Ne plus afficher) quand un site a présenté une Répondre à une alerte facultative de téléchargement du navigateur virtualisé (on page 93) ou une Répondre à une alerte facultative du navigateur virtualisé (on page 99). Si vous rétablissez la règle sur **Always** dans le menu déroulant, un message apparaîtra à votre prochaine visite d'un site compatible avec le navigateur virtualisé. Les sites dans la liste « You chose not to see the Virtualized Browser alerts for the following sites: » (Vous avez choisi de ne pas afficher les alertes de navigateur virtualisé pour les sites suivants) sont les sites pour lesquels vous avez cliqué sur **Do not ask again for this site** (Ne plus me demander pour ce site) quand le site a présenté une Répondre à une alerte facultative de téléchargement du navigateur virtualisé (on page 93) ou une Répondre à une alerte facultative du navigateur virtualisé (on page 99). Les sites dans la liste « You chose to open the following sites using the Virtualized Browser » (Vous avez choisi d'ouvrir les sites suivants à l'aide du navigateur virtualisé) sont les sites pour lesquels vous avez coché **Remember my decision for this website** (Se souvenir de ma décision pour ce site) avant de cliquer sur Yes quand le site a affiché une Répondre à une alerte facultative du navigateur virtualisé (on page 99). Pour supprimer un site spécifique d'une liste, cli**quez sur Re**move site à côté du site que vous voulez supprimer. Pour supprime**r tous les sites, cliquez sur Remove all sites**.

16. Dépannage

Vous rencontrez un problème avec Trusteer Rapport ? Consultez notre FAQ ici: http://www.trusteer.com/support/faq.

Vous trouGetting Support (on page 196) 187) comment obtenir de l'aide. Les sections ci-dessous expliquent certaines procédures à suivre pour vous aider à résoudre les problèmes.

Vous pouvez toujours Arrêter Trusteer Rapport (on page 194) sans le supprimer de votre ordinateur. Ceci vous permet de vérifier si un problème est lié à Trusteer Rapport. Évitez de supprimer Trusteer Rapport pendant la résolution d'un problème. Arrêter Trusteer Rapport (on page 194) produit le même effet et permet à Trusteer de résoudre rapidement et efficacement le problème quand vous contactez l'assistance.

Arrêter Trusteer Rapport

L'arrêt de Rapport stoppe les fonctionnalités de Truster Rapport rapidement et simplement sans désinstallation. Arrêtez Rapport pour déterminer si Trusteer Rapport est la cause du problème que vous rencontrez. Pour relancer le programme, vous pouvez Démarrer Trusteer Rapport (on page 195) Rapport sans avoir à le réinstaller.

Si vous pensez que Trusteer Rapport est la cause du problème rencontré, commencez par arrêter Rapport. Si le problème persiste après l'arrêt de Rapport, celui-ci n'en est probablement pas la cause. Si le problème disparaît après l'arrêt de Rapport, celui-ci en est probablement la cause au moins en partie.

Trusteer recommande de ne pas désinstaller Trusteer Rapport. Si vous envisagez de le désinstaller, Getting Support (on page 196) pour vous faire aider.

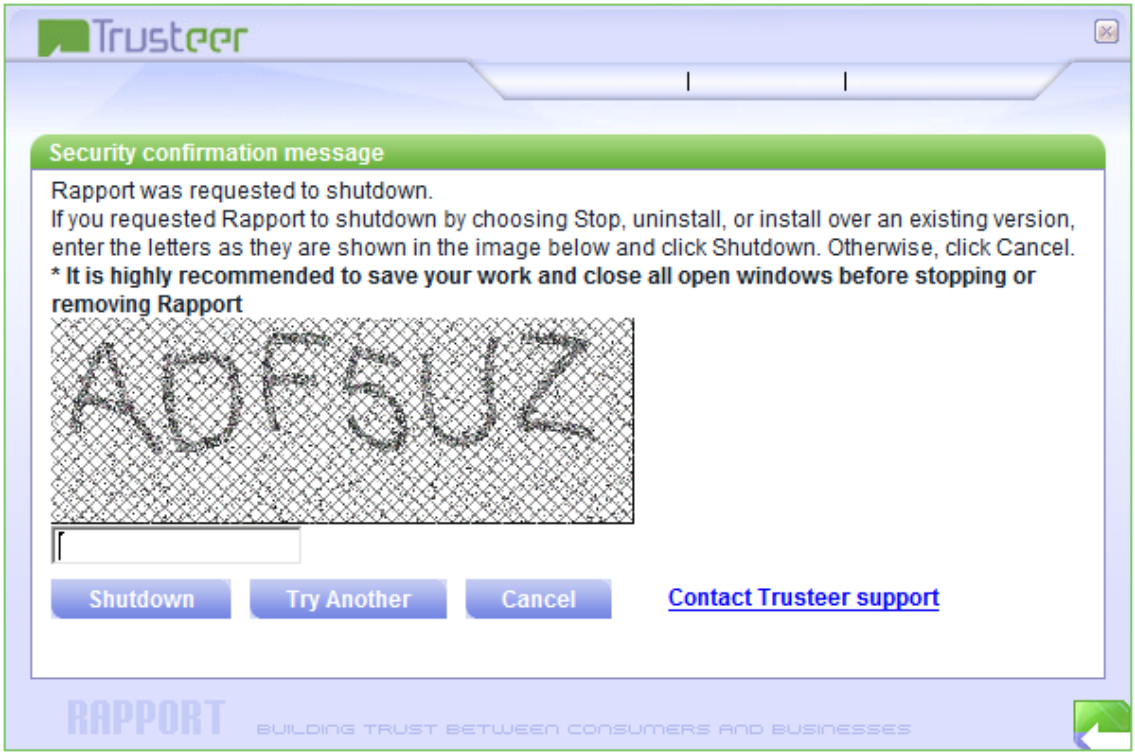
Remarque : Si Trusteer Rapport a été installé depuis un compte administrateur Windows, vous ne pouvez l'arrêter que si vous êtes connecté en tant qu'administrateur

➡ **Pour arrêter Trusteer Rapport:**

1. Enregistrez votre travail et fermez toutes les fenêtres ouvertes.

Remarque:	n'arrêtez pas Trusteer Rapport lorsque le navigateur est ouvert afin d'éviter tout risque de plantage.

2. Dans le menu Démarrer de Windows, sélectionnez **Tous les programmes > Trusteer Rapport > Stop Rapport**. Un message de confirmation apparaît et affiche une image représentant des caractères à saisir. Ceci a pour but d'empêcher des malwares de parvenir à désactiver Trusteer Rapport.



3. Entrez les caractères affichés dans l'image.

4. Cliquez sur **Shutdown**. Le message suivant apparaît pendant que Trusteer Rapport arrête le programme : « Veuillez patienter pendant le processus d'arrêt de Rapport. » Quand le message disparaît, Trusteer Rapport n'est plus en exécution. Pour le vérifier, ouvrez votre navigateur ; l'icône de Rapport n'apparaît plus à droite de la barre d'adresse.

Démarrer Trusteer Rapport

Le démarrage de Rapport relance le programme lorsqu'il a été précédemment arrêté.

Remarque:	Si Trusteer Rapport a été installé depuis un compte administrateur Windows, vous ne pouvez le démarrer que si vous êtes connecté en tant qu'administrateur.

➡ **Pour démarrer Trusteer Rapport:**

Dans le menu Démarrer, sélectionnez **Tous les programmes > Trusteer Trusteer Rapport > Start**. Le message « Please wait while Rapport shuts down. » (Veuillez patienter pendant que Rapport démarre) apparaît. Lorsque le message disparaît, Trusteer Rapport a redémarré. Ceci est confirmé par la présence de l'icône de Rapport dans la barre d'état système ().

Obtenir de l'aide

Le support Trusteer est disponible 24h/24 et 7j/7 et propose plusieurs formules d'assistance:

- Si Trusteer Rapport est installé sur votre ordinateur et que vous n'avez pas de souci de connexion, vous pouvez signaler votre problème depuis la console Rapport. Consultez Envoyer le signalement d'un problème d'utilisation (on page 220). Quand vous signalez un problème depuis la console Rapport, Trusteer Rapport envoie une demande d'assistance à Trusteer accompagnée de votre rapport et des fichiers journaux importants qui permettront à Trusteer de le résoudre.
- Si Trusteer Rapport n'est pas installé ou que vous ne parvenez pas à envoyer une demande d'assistance depuis la console, utilisez le formulaire sur la page http://www.trusteer.com/support/submit-ticket. Veuillez fournir le plus de renseignements possible sur le problème et votre ordinateur (votre système d'exploitation, votre navigateur, le comportement que vous avez constaté, etc.).
- Si vous rencontrez des problèmes de performances, de connexion, de stabilité ou de navigateur, cliquez sur le lien « Live Support » (Assistance en direct) sur la page http://www.trusteer.com/support pour démarrer une discussion en ligne avec un conseiller.

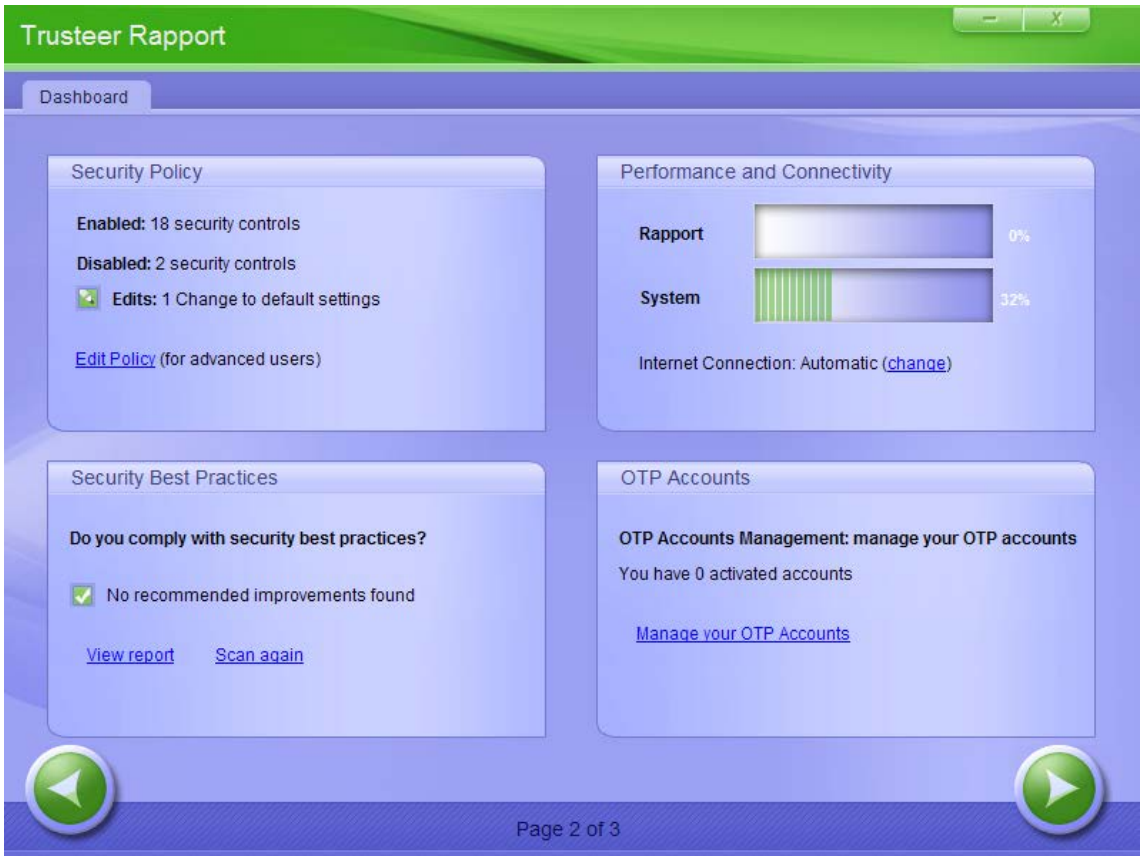
Remarque: En cas de question à propos de Trusteer Rapport non liée à un problème particulier, reportez-vous à ce manuel d'utilisation ou utilisez notre service nanoRep sur la page http://www.trusteer.com/support/faq.

Débloquer des extensions de navigateur légitimes

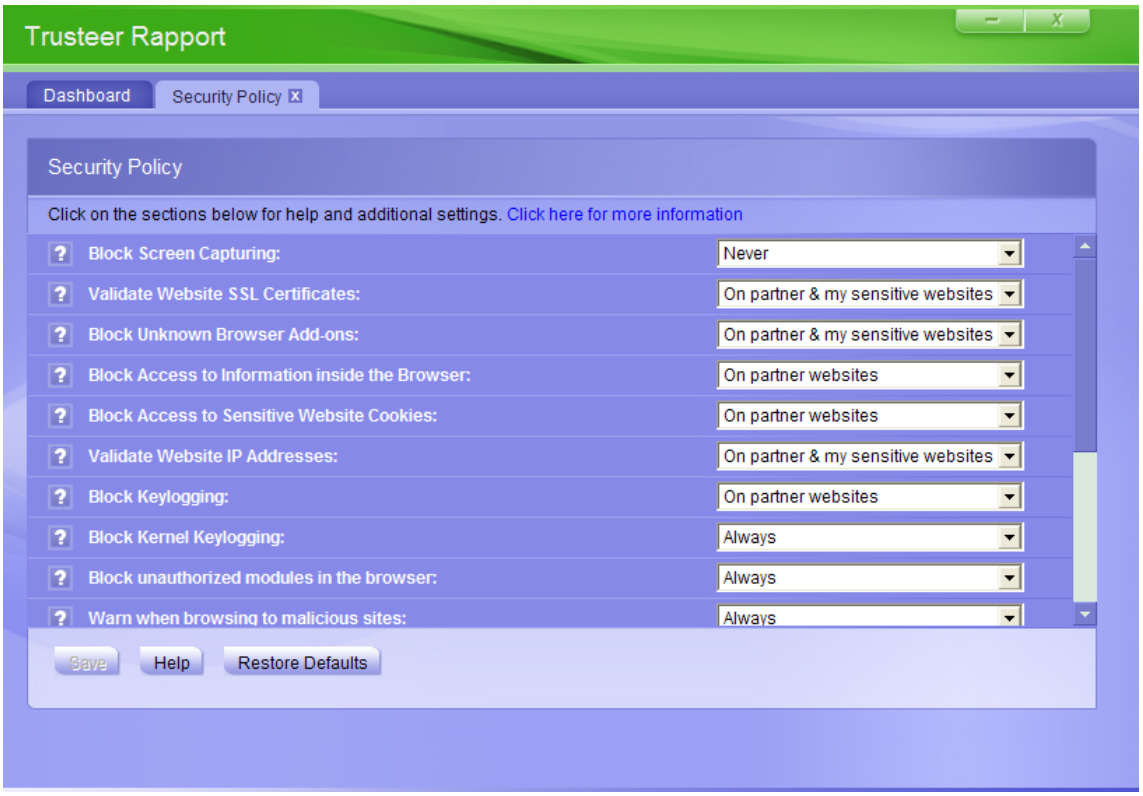
Si vous rencontrez un problème d'affichage de certaines pages Web dans votre navigateur causé selon vous par le blocage d'une extension légitime, vérifiez si Trusteer Rapport est la source du blocage.

➡ **Pour débloquer une extension légitime du navigateur:**

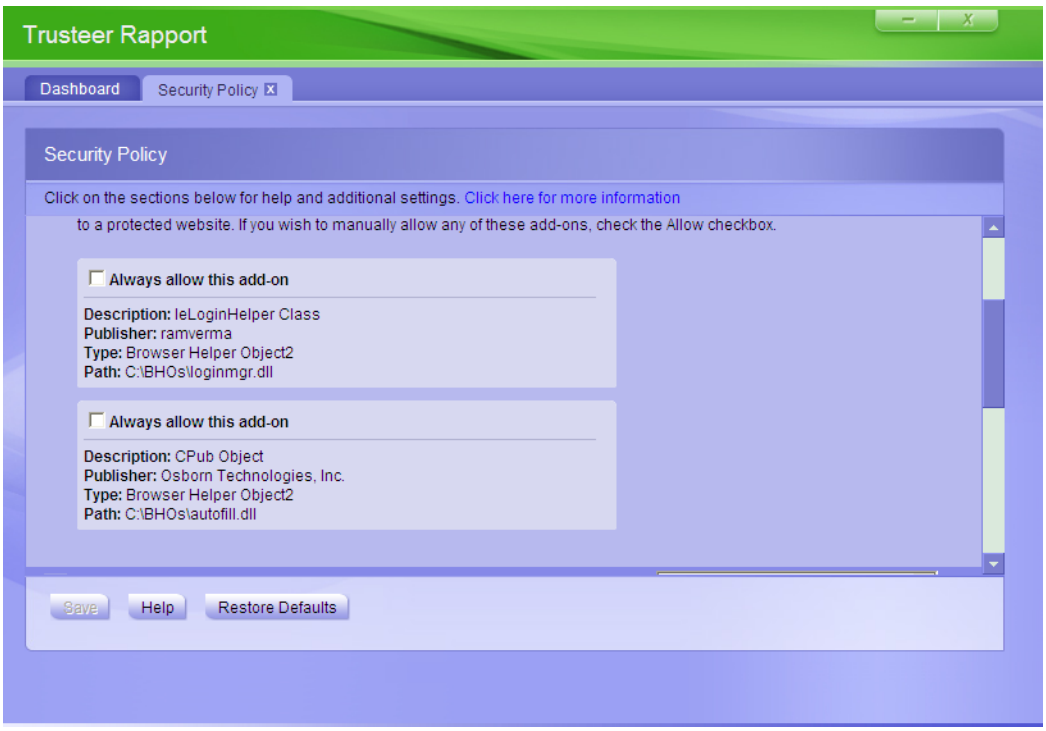
1. Ouvrir la console Rapport (on page 72).
2. Dans le tableau de bord, cliquez sur . Le second écran du tableau de bord apparaît.



3. Dans la zone de la politique de sécurité, cliquez sur Modifier la politique. Un écran Approbation de l'utilisateur apparaît. L'écran vous montre l'image d'un mot pour que vous le saisissiez. Ceci est destiné à empêcher les logiciels malveillants d'accéder à la console et de désactiver Trusteer Rapport de manière efficace.
4. Saisissez le mot que vous voyez dans l'image.
5. Cliquez sur OK. L'écran Politique de sécurité apparaît, affichant tous les contrôles de sécurité.



6. Cliquez sur **Block Unknown Browser Add-ons** (Bloquer les extensions de navigateur inconnues). Une liste des extensions bloquées s'affiche. Chaque extension bloquée comporte une case à cocher intitulée **Always Allow this add-on** (Toujours autoriser cette extension).



7. Cochez la case **Always allow this add-on** correspondant à l'extension que vous souhaitez autoriser.

8. Cliquez sur **Save**. L'extension est maintenant débloquée.

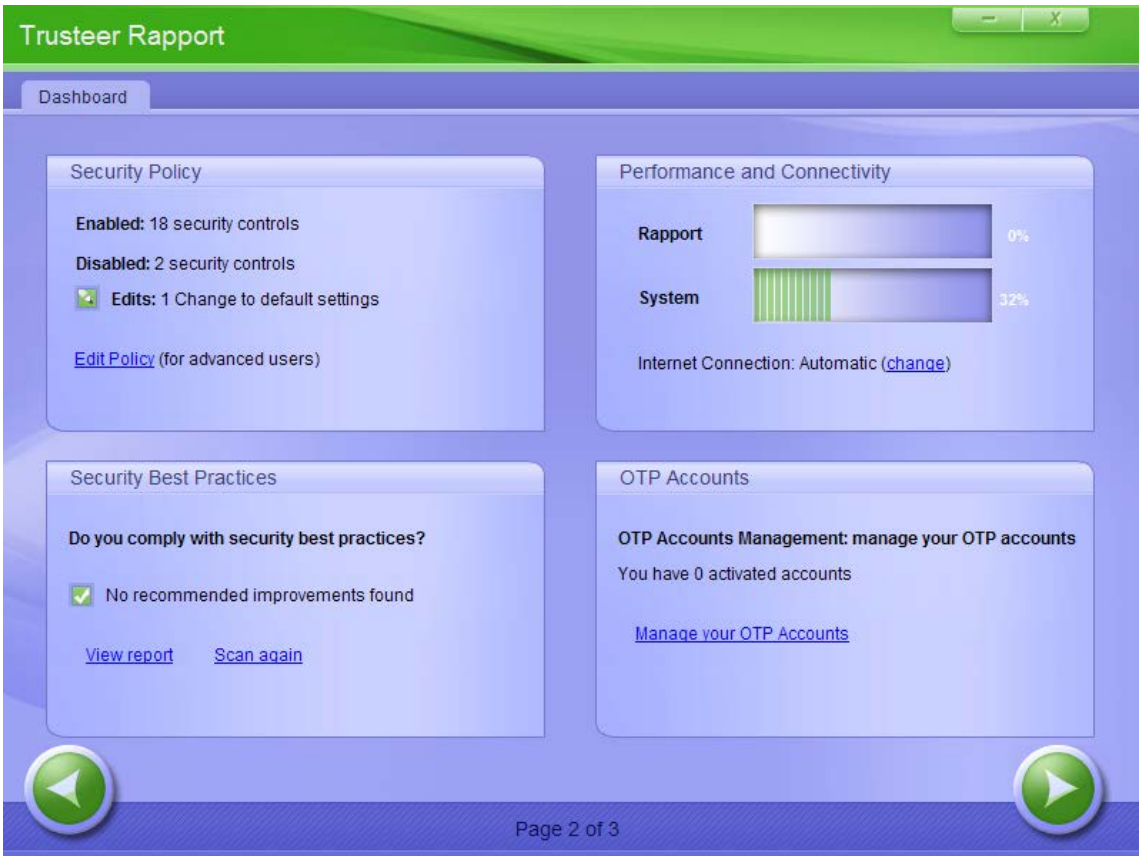
Désactiver le blocage des enregistreurs de frappe

La fonction de blocage des enregistreurs de frappe peut entrer en conflit avec d'autres antikeyloggers. Par conséquent, si vous disposez d'un autre antikeylogger en exécution (par exemple intégré à votre antivirus), il se peut que vous deviez désactiver cette fonction. Vous pouvez également, le cas échant, désactiver la protection contre le keylogging dans votre antivirus existant.

➡ **Pour désactiver le blocage des enregistreurs de frappe:**

1. Ouvrir la console Rapport (on page 72).

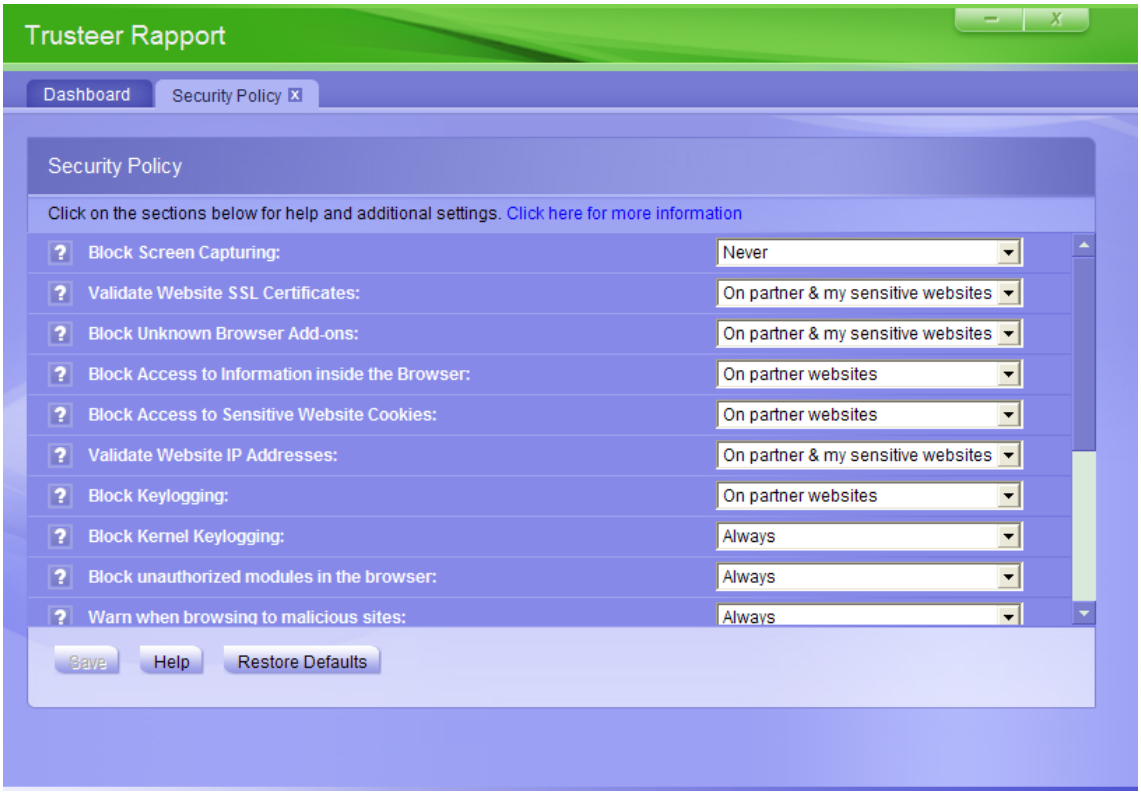
2. Dans le tableau de bord, cliquez sur . Le second écran du tableau de bord apparaît.



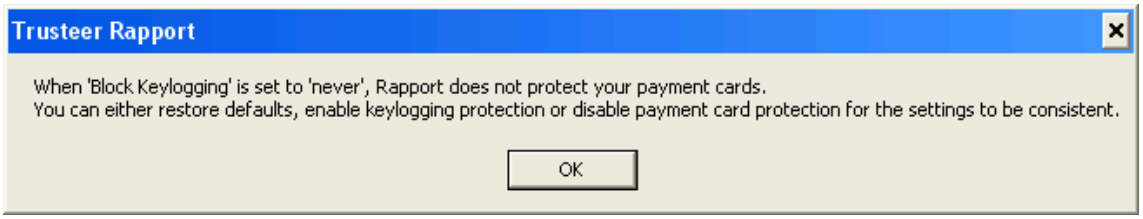
3. Dans la zone de la politique de sécurité, cliquez sur Modifier la politique. Un écran Approbation de l'utilisateur apparaît. L'écran vous montre l'image d'un mot pour que vous le saisissiez. Ceci est destiné à empêcher les logiciels malveillants d'accéder à la console et de désactiver Trusteer Rapport de manière efficace.

4. Saisissez le mot que vous voyez dans l'image.

5. Cliquez sur OK. L'écran Politique de sécurité apparaît, affichant tous les contrôles de sécurité.



6. Dans la liste déroulante face à **Block Keylogging** (Bloquer les enregistreurs de frappe), sélectionnez Never. Ce message apparaît alors :



7. Cliquez sur **OK**.
8. Dans la liste déroulante face à **Block Kernel Keylogging** (Bloquer les enregistreurs de frappe logiciels), sélectionnez **Never**.
9. Cliquez sur **Save**. Un message apparaît vous informant que vos changements prendront effet au redémarrage de votre ordinateur.
10. Cliquez sur **OK**.

11. Redémarrez l'ordinateur. Le blocage des enregistreurs de frappe par Trusteer Rapport est maintenant désactivé.

Annuler des autorisations accidentelles

Certains avertissements de Trusteer Rapport vous permettent d'autoriser des sites ou certificats que Rapport ne reconnaît pas comme légitimes. Après autorisation d'un site ou d'un certificat, vous n'êtes plus alerté pour ce site ou certificat puisque l'autorisation est conservée dans le cache. Si vous avez autorisé un site ou un certificat par mégarde, vous pouvez effacer le cache de sorte que ce site ou ce certificat génère un avertissement lors d'une prochaine connexion.

Effacer des certificats SSL invalides autorisés

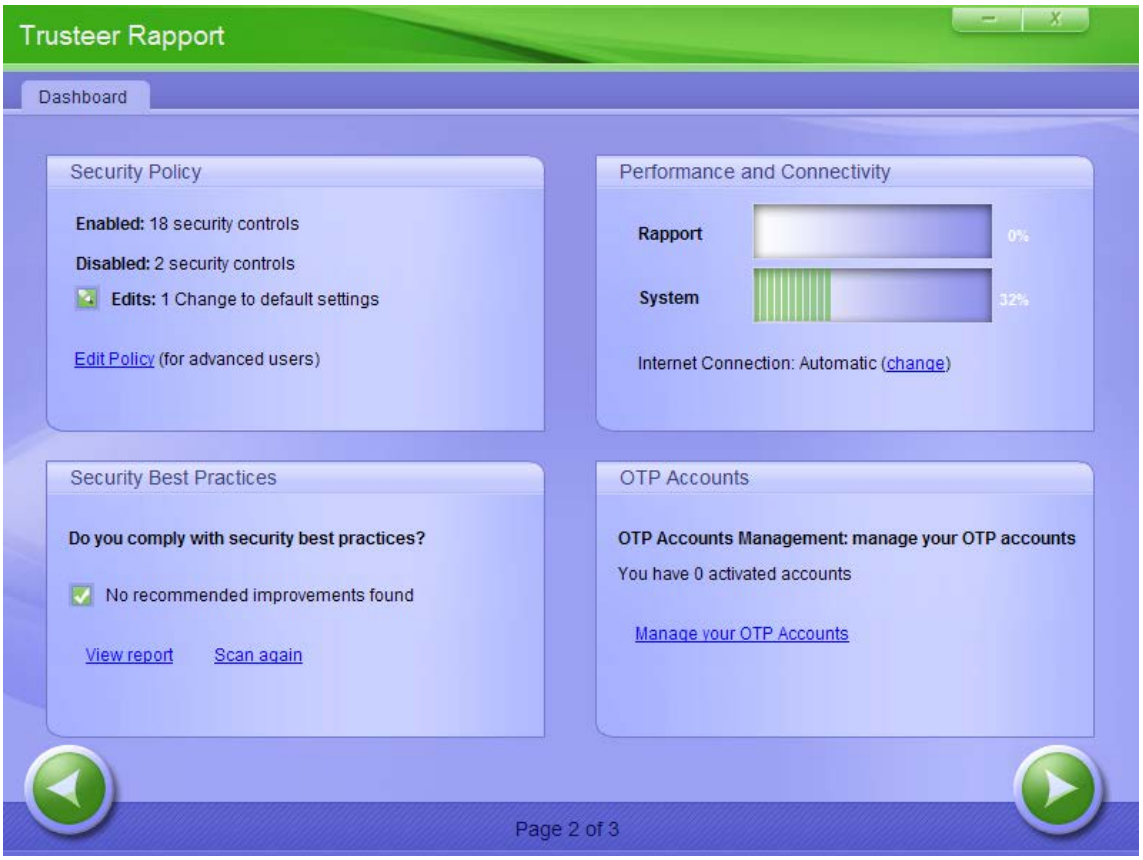
Lorsque Trusteer Rapport détecte que le certificat[5] d'un site est invalide, Trusteer Rapport affiche un Répondre à une alerte de Certificat non valide (on page 134) pour vous empêcher d'envoyer des informations à un site frauduleux. Si vous cochez **Do not warn me about this website again** (Ne plus m'alerter pour ce site) dans la boîte de dialogue de l'avertissement de certificat invalide, le certificat du site auquel vous vous connectez est ajouté au cache des certificats invalides autorisés. Le nettoyage de ce cache supprime les autorisations que vous avez accordées aux certificats présents dans le cache et Trusteer Rapport vous alertera à nouveau si vous revisitez ces mêmes sites.

➡ **Pour effacer des certificats SSL invalides autorisés:**

1. Ouvrir la console Rapport (on page 72).

[5] Un certificat SSL est un certificat numérique chiffré qui valide l'identité d'un site Web t crée une connexion chiffrée pour envoyer des donnés privées sur le site. Lorsque vous voyez le cadenas dans la barre d'adresse ou en bas du navigateur, cela signifie qu'une connexion sécurisée a été établie, utilisant le protocole SSL. Cependant, ceci n vous indique pas que l certificat est valide.

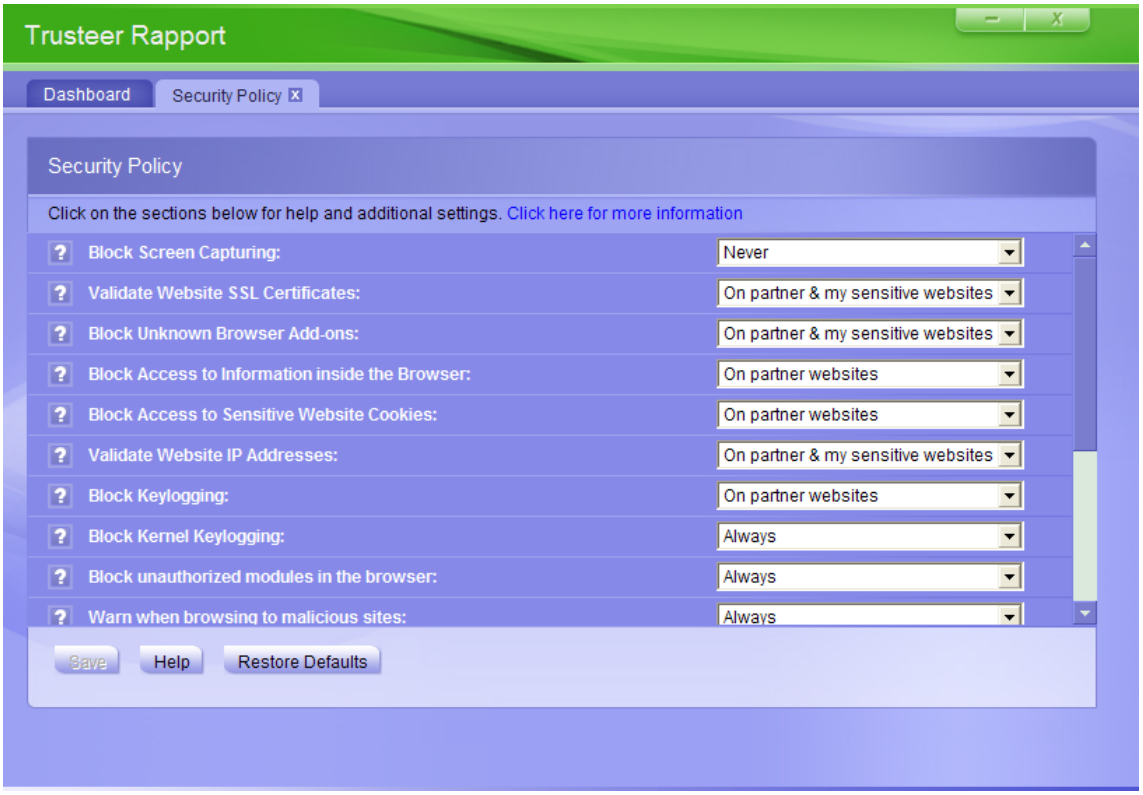
2. Dans le tableau de bord, cliquez sur . Le second écran du tableau de bord apparaît.



3. Dans la zone de la politique de sécurité, cliquez sur Modifier la politique. Un écran Approbation de l'utilisateur apparaît. L'écran vous montre l'image d'un mot pour que vous le saisissiez. Ceci est destiné à empêcher les logiciels malveillants d'accéder à la console et de désactiver Trusteer Rapport de manière efficace.

4. Saisissez le mot que vous voyez dans l'image.

5. Cliquez sur OK. L'écran Politique de sécurité apparaît, affichant tous les contrôles de sécurité.



6. Cliquez sur **Validate Website SSL Certificates** (Valider les certificats SSL du site). Des informations concernant cette règle s'affichent au-dessous ainsi qu'un bouton **Clear cache.**
7. Cliquez sur **Clear Cache** dans le bloc d'informations développé. Une boîte de confirmation apparaît.
8. Cliquez sur **OK**. Le cache est vidé.

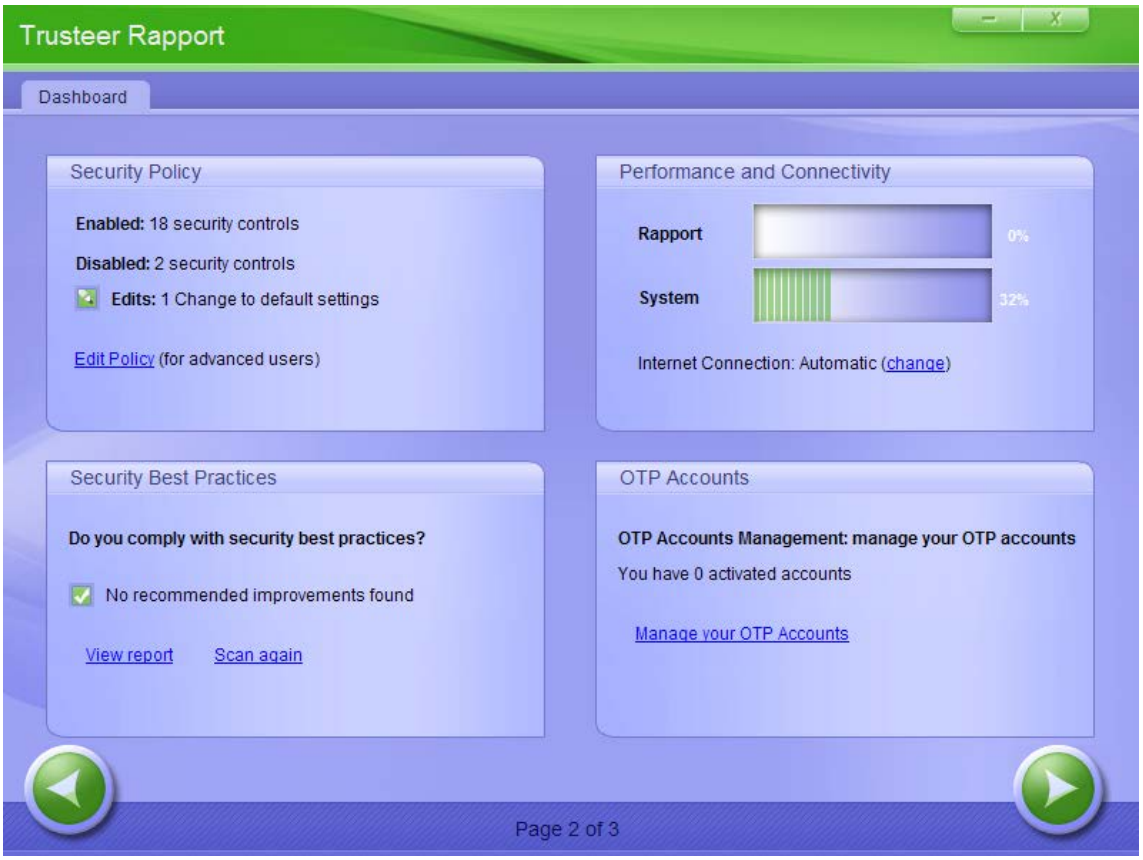
Supprimer les sites de confiance pour l'envoi d'informations de carte de paiement

Lorsque Trusteer Rapport détecte que vous avez saisi un numéro de carte de paiement protégé sur une page Web hébergée localement ou un site non sécurisé, Rapport affiche un Répondre à une alerte de détection d'envoi de carte de paiement (on page 123). Le but de cette boîte de message est de vous éviter d'envoyer votre numéro de carte de paiement à un site de phishing ou un site légitime mais non sécurisé. Si vous cliquez sur **Ignore, I trust this website** (Ignorer, je fais confiance à ce site) dans la boîte de dialogue de l'avertissement de détection d'envoi d'informations de carte de paiement, le site est ajouté à une liste de sites auxquels vous avez choisi de faire confiance, et vous n'êtes plus alerté si vous entrez votre numéro de carte de paiement sur ce site. Vous pouvez supprimer un site de cette liste.

➡ **Pour supprimer des sites de confiance pour l'envoi d'informations de carte de paiement:**

1. Ouvrir la console Rapport (on page 72).

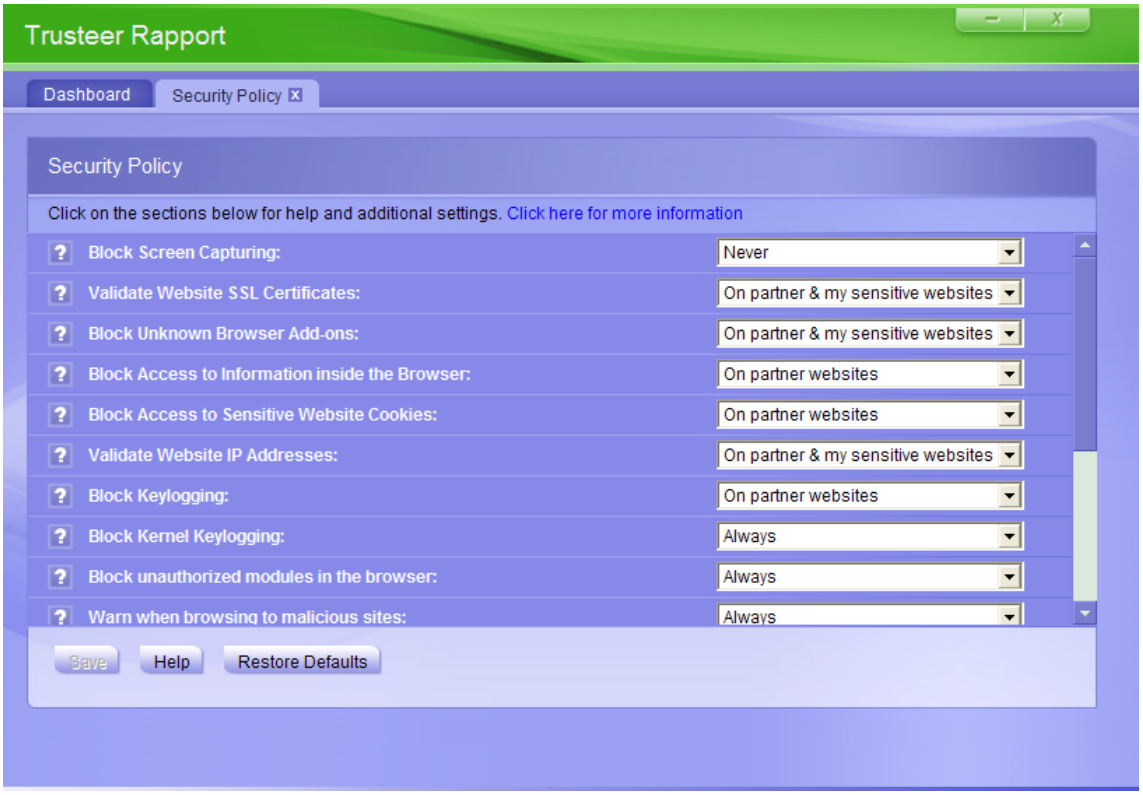
2. Dans le tableau de bord, cliquez sur . Le second écran du tableau de bord apparaît.



3. Dans la zone de la politique de sécurité, cliquez sur Modifier la politique. Un écran Approbation de l'utilisateur apparaît. L'écran vous montre l'image d'un mot pour que vous le saisissiez. Ceci est destiné à empêcher les logiciels malveillants d'accéder à la console et de désactiver Trusteer Rapport de manière efficace.

4. Saisissez le mot que vous voyez dans l'image.

5. Cliquez sur OK. L'écran Politique de sécurité apparaît, affichant tous les contrôles de sécurité.



6. Cliquez sur la règle Protect Payment Card Numbers from Theft (Protéger du vol les numéros de carte de paiement.
7. Vos sites de confiance sont répertoriés dans l'espace développé. Il s'agit des sites auxquels vous avez choisi de faire confiance en cliquant sur **Ignore, I trust this website** (Ignorer, je fais confiance à ce site) dans la boîte de dialogue de l'avertissement de détection d'envoi d'informations de carte de paiement.
8. Cliquez sur **Clear this site** pour chaque site que vous voulez retirer de la liste, ou sur **Clear all sites** pour supprimer tous les sites. Une boîte de confirmation apparaît.
9. Cliquez sur **OK**.

Supprimer les sites de confiance pour les envois non sécurisés

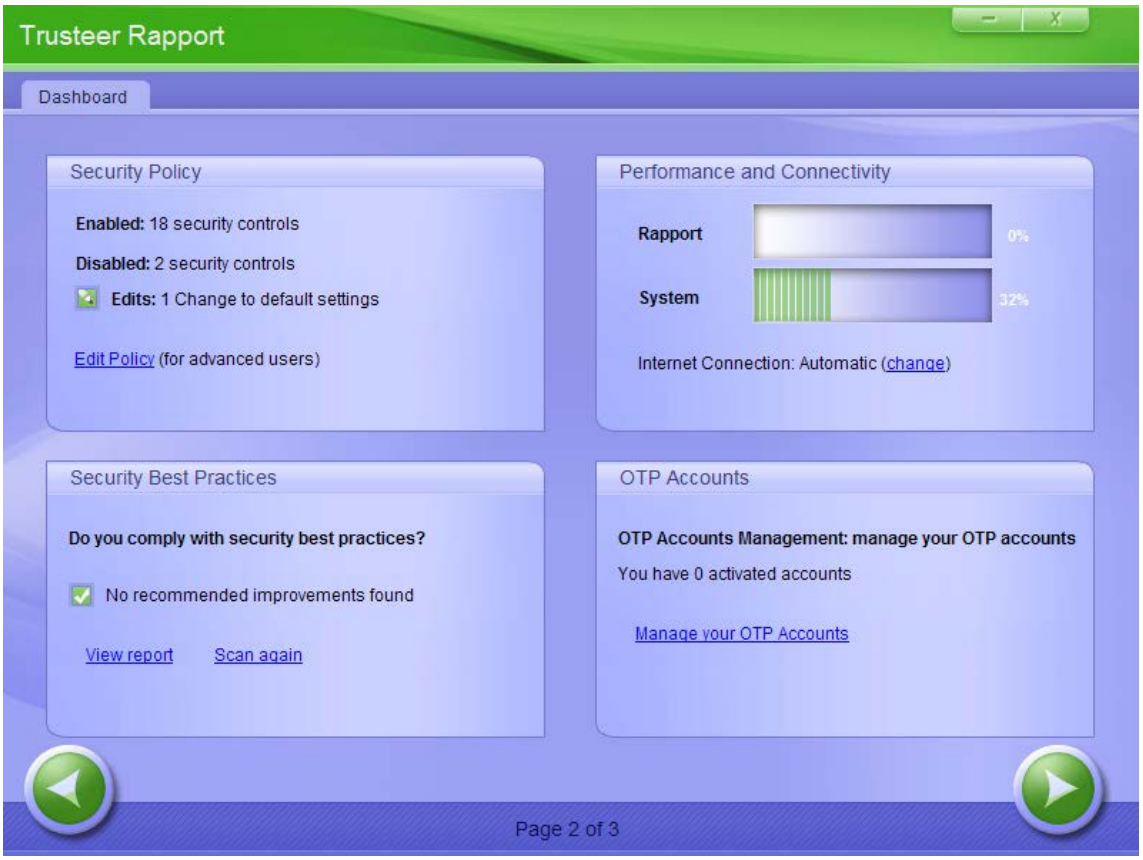
Lorsque Trusteer Rapport détecte que vous avez saisi un mot de passe sur un site qui ne sécurise pas l'envoi de données, Rapport affiche un Répondre à une alerte de soumission non sécurisée (on page 114). Le but de cet avertissement est de vous empêcher d'envoyer des données sensibles à des sites à haut risque qui pourraient facilement être interceptées par des criminels, y compris sur des sites légitimes.

Si vous cliquez sur I trust this site, don't alert me again (Je fais confiance à ce site, ne plus m'alerter) dans la boîte de dialogue de Répondre à une alerte de soumission non sécurisée (on page 114)), le site est ajouté à une liste de sites auxquels vous avez choisi de faire confiance et vous n'êtes plus alerté si vous entrez votre numéro de carte de paiement sur ce site. Vous pouvez retirer un site de cette liste.

➡ **Pour supprimer des sites non sécurisés de vos sites de confiance:**

1. Ouvrir la console Rapport (on page 72).

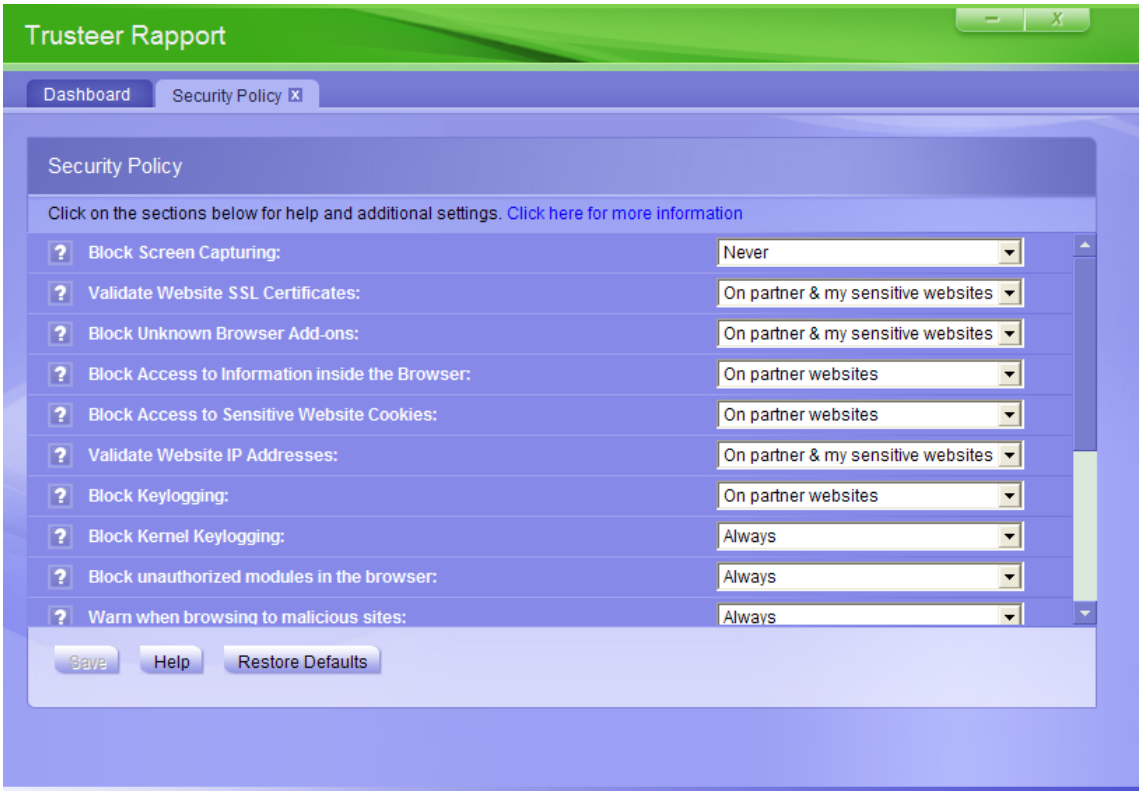
2. Dans le tableau de bord, cliquez sur . Le second écran du tableau de bord apparaît.



3. Dans la zone de la politique de sécurité, cliquez sur Modifier la politique. Un écran Approbation de l'utilisateur apparaît. L'écran vous montre l'image d'un mot pour que vous le saisissiez. Ceci est destiné à empêcher les logiciels malveillants d'accéder à la console et de désactiver Trusteer Rapport de manière efficace.

4. Saisissez le mot que vous voyez dans l'image.

5. Cliquez sur OK. L'écran Politique de sécurité apparaît, affichant tous les contrôles de sécurité.



6. Cliquez sur la règle **Warn me when I submit security data to insecure sites** (M'alerter quand j'envoie des données de sécurité à des sites non sécurisés). Vos sites de confiance sont répertoriés dans l'espace développé. Ce sont les sites auxquels vous avez choisi de faire confiance en cliquant sur **I trust this site, don't alert me again** (Je fais confiance à ce site, ne plus m'alerter) dans la boîte de dialogue de Répondre à une alerte de soumission non sécurisée (on page 114) ou en cliquant sur Trust this site (Faire confiance à ce site) dans la boîte de dialogue Avertissement d'informations protégées.
7. Cliquez sur **Clear this site** pour chaque site que vous voulez retirer de la liste, ou sur **Clear all sites** pour supprimer tous les sites. Une boîte de confirmation apparaît.
8. Cliquez sur **OK**.

Supprimer les sites pour lesquels vous avez autorisé l'envoi d'informations de connexion

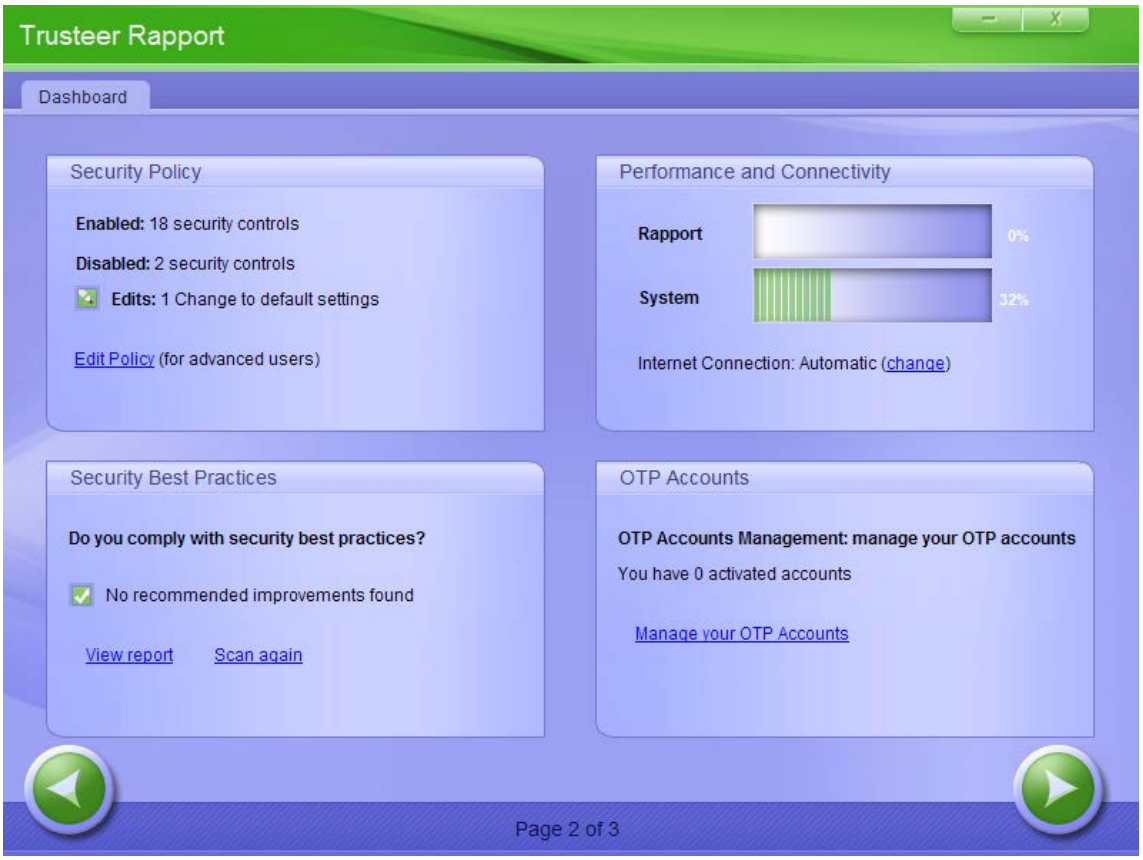
Lorsque vous entrez des caractères correspondant à un mot de passe protégé sur un site inconnu, Trusteer Rapport affiche un Répondre à une alerte d'informations protégées (on page 112). Si vous choisissez d'ignorer l'avertissement, le site devient un site autorisé et Trusteer Rapport ne vous alerte plus si vous entrez un mot de passe protégé sur ce site. Les sites que vous autorisez de cette manière sont conservés dans un cache. Le nettoyage du cache supprime ces autorisations.

Si vous avez cliqué par mégarde sur Ignore this warning (Ignorer cet avertissement) dans une boîte de dialogue d'avertissement d'information protégée, vous pouvez vider le cache des sites pour lesquels vous avez autorisé l'envoi d'informations de connexion. Ceci n'annule pas les envois de mot de passe effectués auparavant mais rétablit le statut inconnu des sites que vous avez autorisés par accident.

➡ **Pour vider le cache des sites autorisés pour lesquels vous avez autorisé l'envoi d'informations de connexion :**

1. Ouvrir la console Rapport (on page 72).

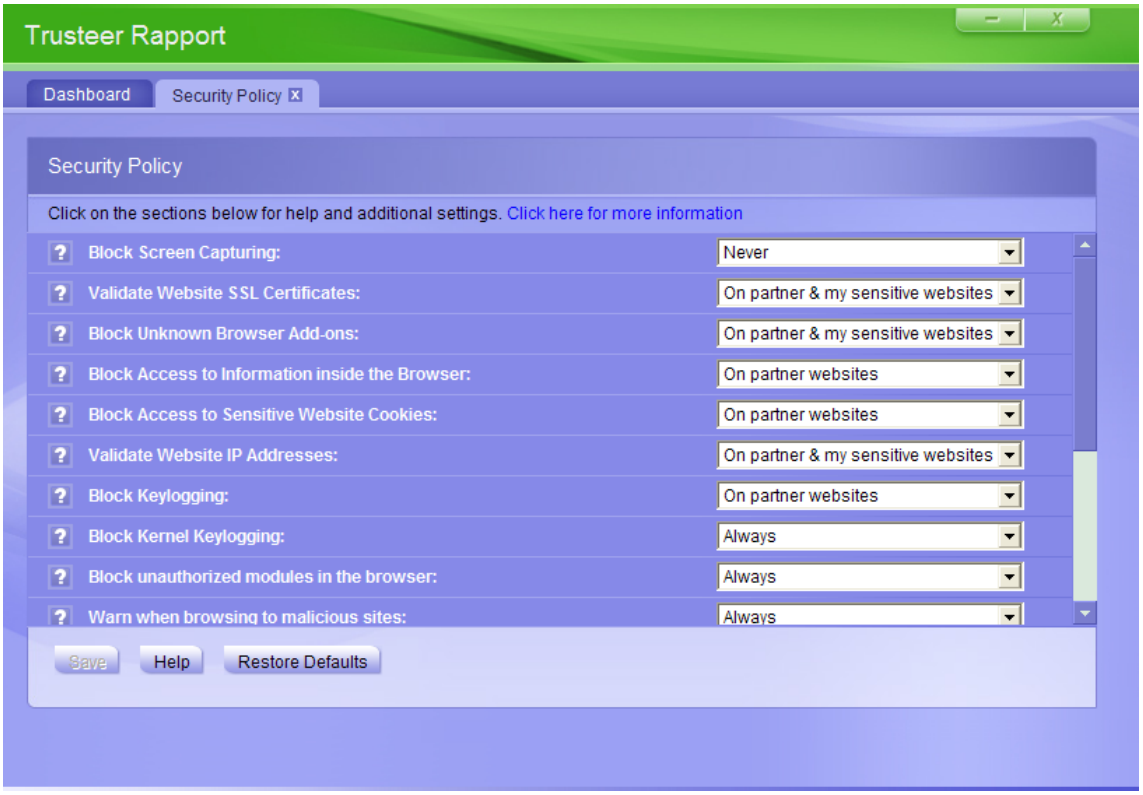
2. Dans le tableau de bord, cliquez sur . Le second écran du tableau de bord apparaît.



3. Dans la zone de la politique de sécurité, cliquez sur Modifier la politique. Un écran Approbation de l'utilisateur apparaît. L'écran vous montre l'image d'un mot pour que vous le saisissiez. Ceci est destiné à empêcher les logiciels malveillants d'accéder à la console et de désactiver Trusteer Rapport de manière efficace.

4. Saisissez le mot que vous voyez dans l'image.

5. Cliquez sur OK. L'écran Politique de sécurité apparaît, affichant tous les contrôles de sécurité.



6. Faites défiler jusqu'à **Warn When Login Information is Used in Unknown Websites** (M'alerter quand des informations de connexion sont utilisées sur des sites inconnus) et cliquez sur le nom de la règle. Des informations sur cette règle s'affichent ainsi qu'un bouton **clear cache**.
7. Cliquez sur **Clear Cache** dans le bloc d'informations développé. Une boîte de confirmation apparaît.
8. Cliquez sur **OK**. Le cache est vidé.

Gestion des erreurs

Si vous avez constaté une erreur de Trusteer Rapport, consultez cette section.

Gérer une erreur de page Web postérieure à l'installation

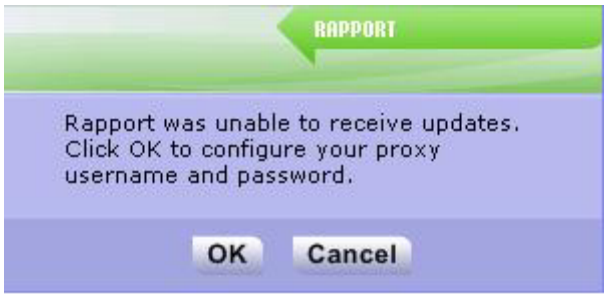
Voici un exemple d'erreur de page Web postérieure à l'installation:

Cette erreur apparaît après une installation de Trusteer Rapport si le programme ne parvient pas à lancer votre navigateur par défaut pour exécuter un court test de compatibilité.

Si vous voyez cette alerte, vérifiez que vous pouvez aller en ligne avec votre navigateur internet. Suivez ensuite les instructions fournies dans la boîte de dialogue

Gérer une erreur de mise à jour

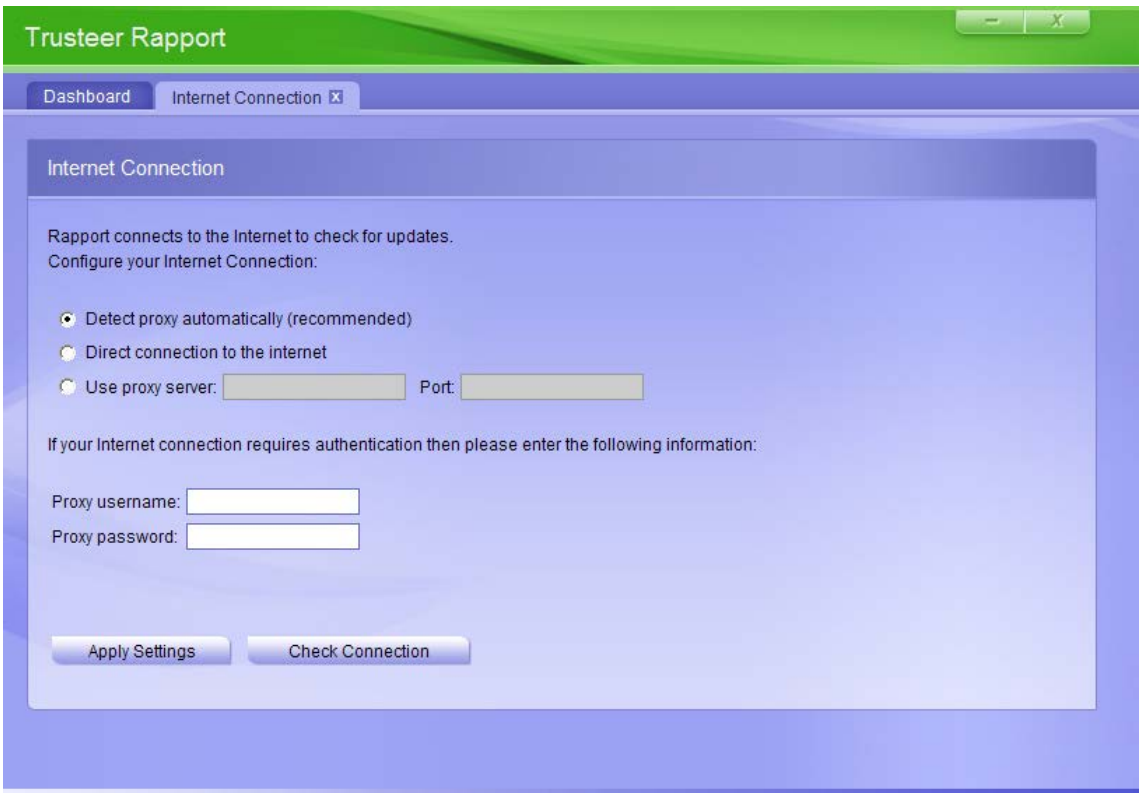
Voici un exemple d'erreur de mise à jour de Trusteer Rapport:



Cette erreur apparaît si Trusteer Rapport n'est pas parvenu à se connecter à internet pour vérifier les mises à jour car vous vous connectez à internet via un proxy. Trusteer Rapport n'ayant pas pu détecter les informations de proxy automatiquement, la boîte de dialogue vous permet de configurer votre serveur proxy pour permettre à Rapport de se connecter à internet et d'obtenir les mises à jour.

➡ **Si vous recevez cette erreur:**

1. Cliquez sur **OK**. La console Rapport s'ouvre et affiche l'onglet de la connexion internet.

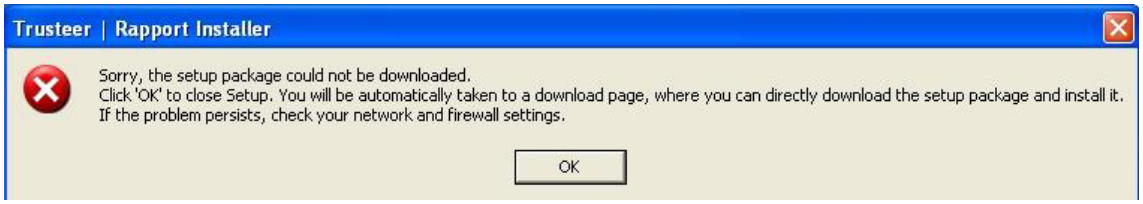


2. Sélectionnez **Use proxy server** (Utiliser le serveur proxy). Entrez le nom ou l'adresse IP du serveur proxy dans le champ fourni.
3. Dans le champ **Port**, entrez le port TCP utilisé pour vous connecter au serveur proxy.
4. Si votre serveur proxy requiert une authentification, entrez le nom d'utilisateur dans le champ **Proxy username** et le mot de passe dans le champ **Proxy password**.

5. Cliquez sur Apply Settings (Appliquer les paramètres).
6. Cliquez sur **Check Connection** (Vérifier la connexion) pour vérifier que Trusteer Rapport parvient à se connecter à internet maintenant que vous avez configuré un serveur proxy.

Gérer des erreurs de l'assistant d'installation de Rapport

Voici un exemple d'erreur de l'assistant d'installation de Trusteer Rapport:



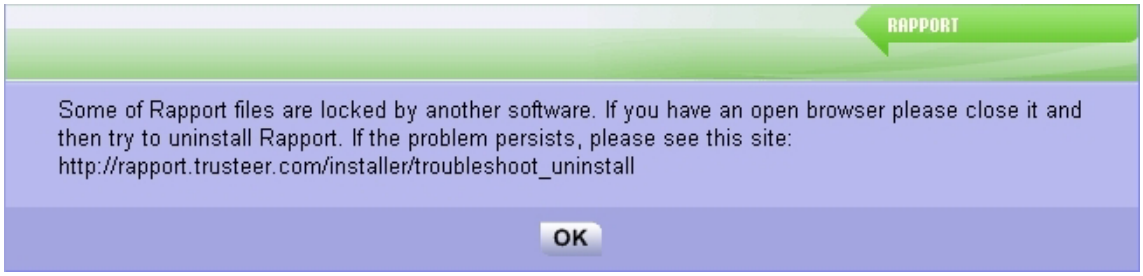
Cette erreur apparaît au cours de l'installation de Trusteer Rapport si l'assistant ne parvient pas à télécharger le pack d'installation complet.

Si vous voyez cette erreur, cliquez sur **OK**. Le site de Truster s'ouvre. Téléchargez le pack d'installation complet directement depuis le site de Trusteer.

Remarque: Si vous rencontrez des difficultés avec les instructions fournies sur le site, contactez le support Trusteer sur http://www.trusteer.com/support/submit-ticket.

Gérer des erreurs de désinstallation

Voici un exemple d'erreur pouvant survenir pendant le processus de désinstallation :



Cette boîte de dialogue apparaît si un fichier de Trusteer Rapport est bloqué par un autre programme lors de la désinstallation de Rapport.

Si vous rencontrez cette erreur, suivez les instructions de la boîte de dialogue. Le site mentionné vous permet de télécharger notre utilitaire de désinstallation spécifique avec lequel vous pourrez désinstaller correctement le programme.

Remarque: Si vous rencontrez des difficultés avec les instructions fournies sur le site, déposez une demande d'assistance auprès du support Trusteer sur http://www.trusteer.com/support/submit-ticket.

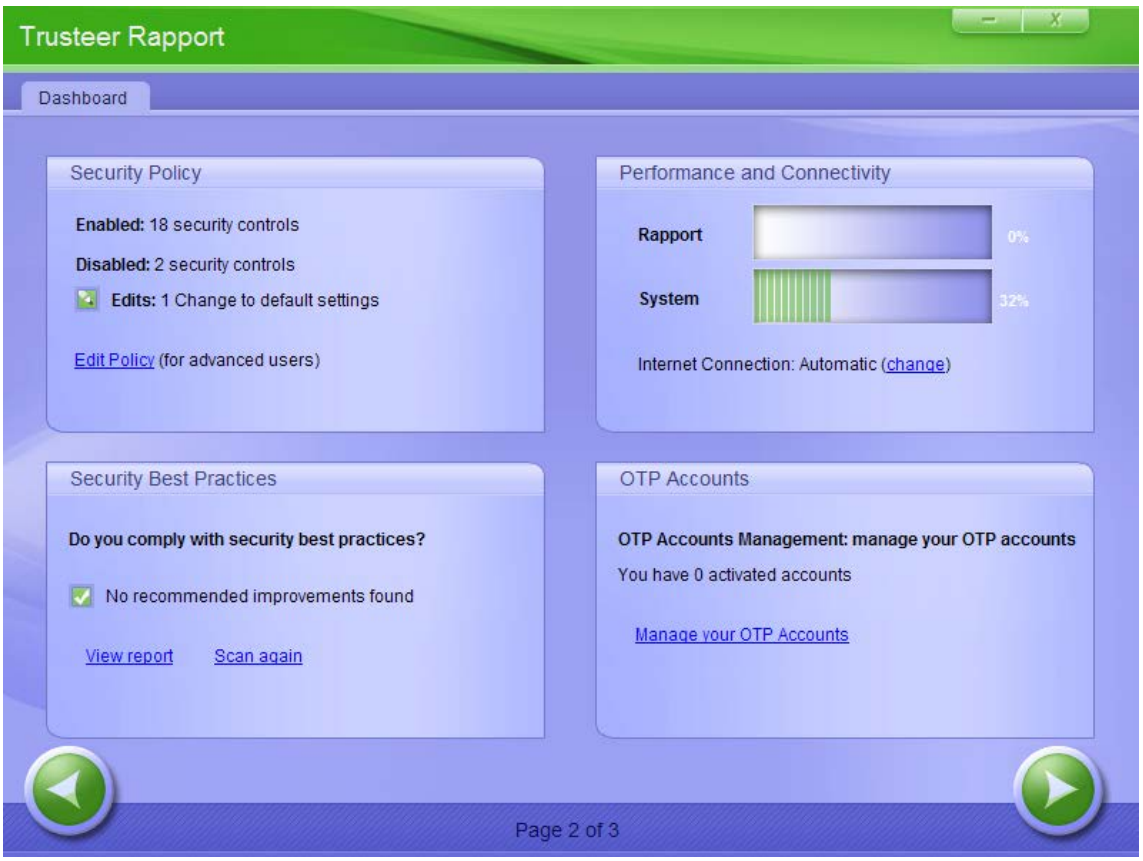
Configurer un serveur proxy pour les mises à jour automatiques

Trusteer Rapport se connecte automatiquement à internet pour vérifier les mises à jour et télécharger les stratégies de sécurité. La plupart des configurations proxy sont automatiquement détectées par Trusteer Rapport. Si toutefois Rapport ne parvient pas à détecter automatiquement votre proxy, vous devez le configurer vous-même.

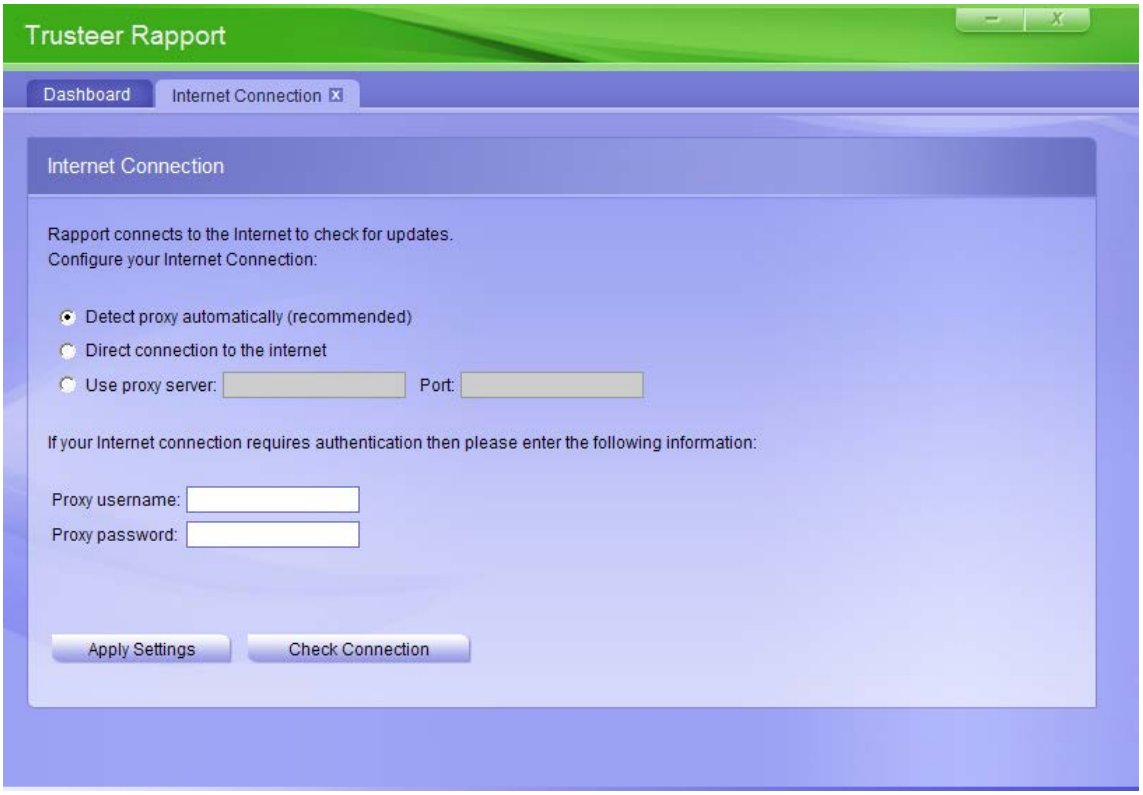
➡ **Pour configurer un serveur proxy:**

1. Ouvrir la console Rapport (on page 72).

2. Dans le tableau de bord, cliquez sur . Un deuxième écran apparaît.



3. Dans la zone Performance and Connectivity à côté du champ Internet Connection, cliquez sur Change. L'onglet de la connexion internet apparaît.



4. Sélectionnez **Use proxy server** (Utiliser le serveur proxy). Entrez le nom ou l'adresse IP du serveur proxy dans le champ fourni.
5. Dans le champ **Port**, entrez le port TCP utilisé pour vous connecter au serveur proxy.
6. Si votre serveur proxy requiert une authentification, entrez le nom d'utilisateur dans le champ **Proxy username** et le mot de passe dans le champ **Proxy password**.
7. Cliquez sur **Apply Settings** (Appliquer les paramètres).
8. Cliquez sur Check Connection (Vérifier la connexion) pour vérifier que Trusteer Rapport parvient à se connecter à internet maintenant que vous avez configuré un serveur proxy

Envoyer le signalement d'un problème d'utilisation

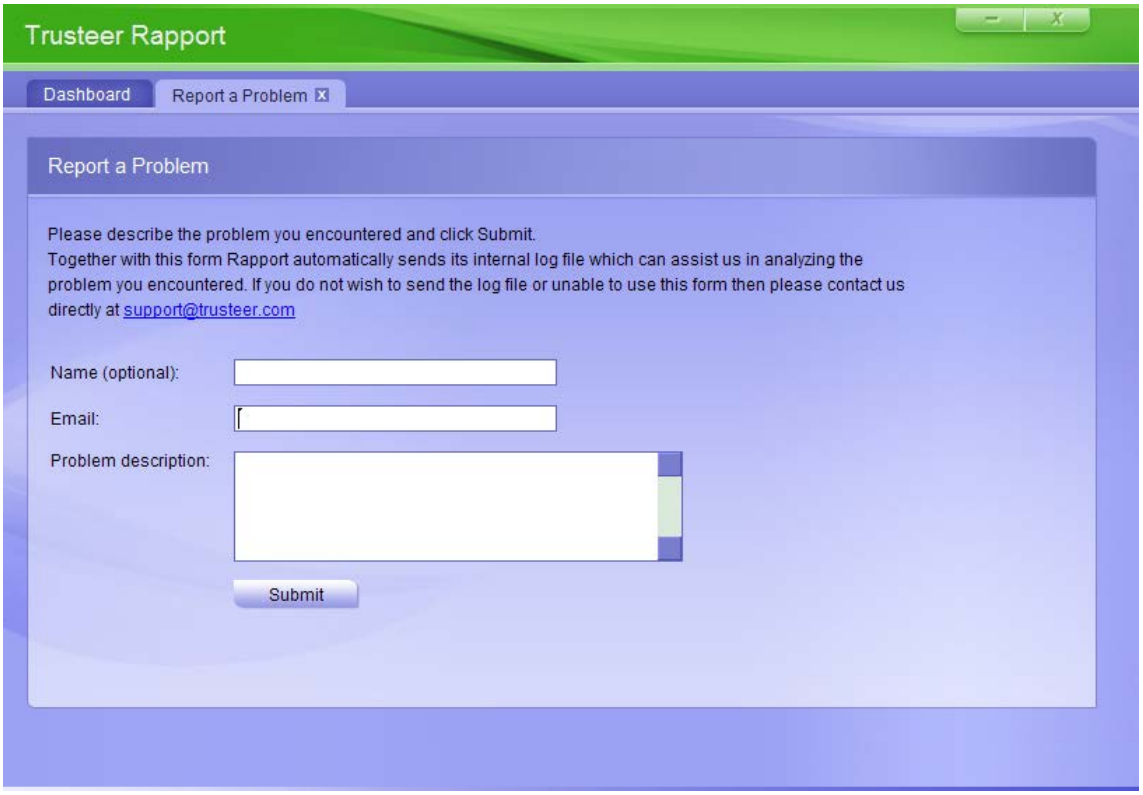
Lorsque vous utilisez la fonction de signalement d'un problème de Trusteer Rapport, un rapport technique contenant des fichiers journaux internes importants de Trusteer Rapport est envoyé, accompagné de votre description du problème. Ce rapport technique aide Trusteer à identifier le problème et à le résoudre. C'est la meilleure façon de signaler un problème car Trusteer dispose ainsi des informations les plus complètes lui permettant de fournir une assistance optimale.

Remarque : Les fichiers journaux ne contiennent que des informations techniques et sont exempts de données sensibles ou d'informations personnelles vous concernant.

Pour signaler un problème :

1. Ouvrir la console Rapport (on page 72). Le tableau de bord apparaît.

2. Dans la zone Help and Support, cliquez sur **Report a problem** (Signaler un problème). L'onglet Report a problem s'ouvre.

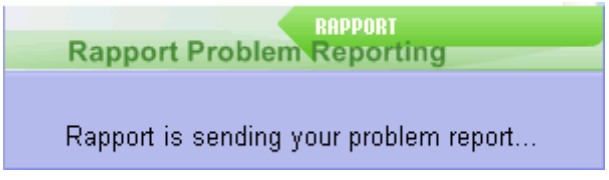


3. Dans le champ **Name**, entrez votre nom (facultatif).

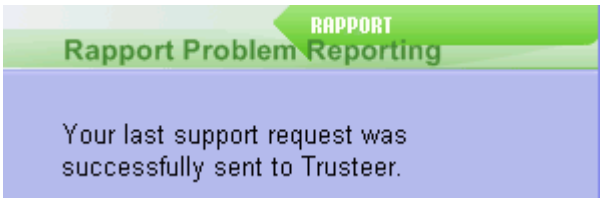
4. Dans le champ **Email**, entrez votre adresse e-mail. Trusteer utilisera cette adresse pour vous communiquer la solution à votre problème.

5. Dans le champ **Problem description**, entrez une description détaillée du problème en précisant autant de détails que possible.

6. Cliquez sur **Submit**. Le message suivant apparaît en bas à droite de l'écran pendant que Trusteer Rapport envoie votre signalement du problème.



Après l'envoi du signalement, un message s'affiche confirmant cet envoi.



Un conseiller Trusteer vous contactera par e-mail pour vous aider à résoudre le problème.

Envoyer les fichiers journaux de Trusteer Rapport à Trusteer

Si le support Trusteer vous demande de localiser les fichiers journaux de Rapport sur votre ordinateur et de les envoyer à Trusteer pour les aider à résoudre votre problème, suivez cette procédure.

- Obtenir les journaux sur Windows 7 (on page 222)
- Obtenir les journaux sur Windows XP (on page 224)

Obtenir les journaux sur Windows 7

➡ **To gather Rapport log files on a Windows 7 computer:**

1. Dans le menu **Démarrer** de Windows, cliquez sur **Exécuter**. La fenêtre d'invite de commande **Exécuter** s'ouvre.
2. Dans la fenêtre d'invite de commande **Exécuter**, insérez **%appdata%\trusteer\rapport\user\logs**
3. Cliquez sur **OK**. Un dossier s'ouvre affichant une liste de fichiers logs associés à Trusteer Rapport.
4. Dans le menu **Organiser**, cliquez sur **Sélectionner tout**. Tous les fichiers contenus dans le dossier sont alors sélectionnés.
5. Ouvrez le menu contextuel d'un clic droit et cliquez sur **Copier**.
6. Créez un dossier pour les fichiers journaux, par exemple:

a. Faites un clic droit sur le bureau, cliquez sur Nouveau puis sélectionnez **Dossier**.

b. Nommez le dossier Journaux.

7. Ouvrez le dossier créé pour les fichiers journaux par double-clic sur l'icône du dossier.
8. Faites un clic droit à l'intérieur du dossier Journaux ouvert et sélectionnez **Coller** dans le menu contextuel. Tous les fichiers journaux sélectionnés sont collés dans le dossier.
9. Dans le menu **Démarrer** de Windows, cliquez à nouveau sur **Exécuter** pour rouvrir la fenêtre d'invite de commande **Exécuter**.
10. Dans la fenêtre d'invite de commande **Exécuter**, insérez **%programdata%\Trusteer\Rapport\user\logs**
11. Cliquez sur **OK**. Un dossier s'ouvre affichant une autre liste de fichiers journaux associés à Trusteer Rapport.
12. Dans le menu **Organiser**, cliquez sur **Sélectionner tout**. Tous les fichiers dans le dossier sont sélectionnés.
13. Ouvrez le menu contextuel d'un clic droit et cliquez sur **Copier**.
14. Revenez au dossier de fichiers journaux que vous avez créé.
15. Cliquez à l'intérieur du dossier et vérifiez que tous les fichiers que vous avez collés précédemment ne sont pas sélectionnés.
16. Faites un clic droit à l'intérieur du dossier de fichiers journaux ouvert et cliquez sur **Coller** dans le menu contextuel. La deuxième série de fichiers journaux que vous avez copiés est collée dans le dossier.
17. Fermez le dossier de fichiers journaux.

18. Faites un clic droit sur le dossier de fichiers journaux (sur votre bureau ou à l'emplacement où vous avez créé le dossier), cliquez sur **Envoyer vers** puis sélectionnez **Dossier compressé**. Une version compressée du dossier de fichiers journaux apparaît.
19. . Envoyez le dossier compressé par e-mail à **support@trusteer.com**.

Obtenir les journaux sur Windows XP

➡ **Pour récupérer les fichiers journaux de Rapport sur Windows XP:**

1. Dans le menu **Démarrer** de Windows, cliquez sur Exécuter. La fenêtre d'invite de commande **Exécuter** s'ouvre.
2. Dans la fenêtre d'invite de commande **Exécuter**, insérez %appdata%\trusteer\rapport\user\logs
3. Cliquez sur **OK**. Un dossier s'ouvre affichant une liste de fichiers journaux associés à Trusteer Rapport.
4. Dans le menu **Édition**, cliquez sur **Sélectionner** tout. Tous les fichiers dans le dossier sont alors sélectionnés.
5. Ouvrez le menu contextuel d'un clic droit et sélectionnez **Copier**.
6. Créez un dossier pour les fichiers journaux, par exemple :
   a. Faites un clic droit sur votre bureau, cliquez sur **Nouveau** et sélectionnez **Dossier**.
   b. Nommez le dossier **Journaux**.
7. Ouvrez le dossier que vous avez créé pour les fichiers journaux par double clic sur l'icône du dossier.
8. Faites un clic droit à l'intérieur du dossier de fichiers journaux ouvert et sélectionnez **Coller** dans le menu contextuel. Tous les fichiers journaux que vous avez copiés sont collés dans le dossier.

9. Dans le menu Démarrer de Windows, cliquez à nouveau sur **Exécuter** pour rouvrir la fenêtre d'invite de commande Exécuter.
10. Dans la fenêtre d'invite de commande Exécuter, insérez **%allusersprofile%\application data\trusteer\rapport\logs**
11. Cliquez sur **OK**. Un dossier s'ouvre affichant une autre liste de fichiers journaux associés à Trusteer Rapport.
12. Dans le menu **Édition**, cliquez sur **Sélectionner** tout. Tous les fichiers dans le dossier sont alors sélectionnés.
13. Ouvrez le menu contextuel d'un clic droit et sélectionnez **Copier**.
14. Revenez au dossier de fichiers journaux que vous avez créé.
15. Faites un clic droit à l'intérieur du dossier de fichiers journaux et vérifiez que tous les fichiers que vous avez collés précédemment ne sont pas sélectionnés.
16. Faites un clic droit à l'intérieur du dossier de fichiers journaux ouvert et sélectionnez **Coller** dans le menu textuel. La deuxième série de fichiers journaux que vous avez copiés est collée dans le dossier.
17. Fermez le dossier de fichiers journaux.
18. Faites un clic droit sur le dossier de fichiers journaux (sur votre bureau ou à l'emplacement où vous avez créé le dossier), cliquez sur Envoyer vers puis sélectionnez Dossier compressé. Une version compressée du dossier de fichiers journaux apparaît.
19. Envoyez le dossier compressé par e-mail à support@trusteer.com.

17. Maintenir Trusteer Rapport à jour

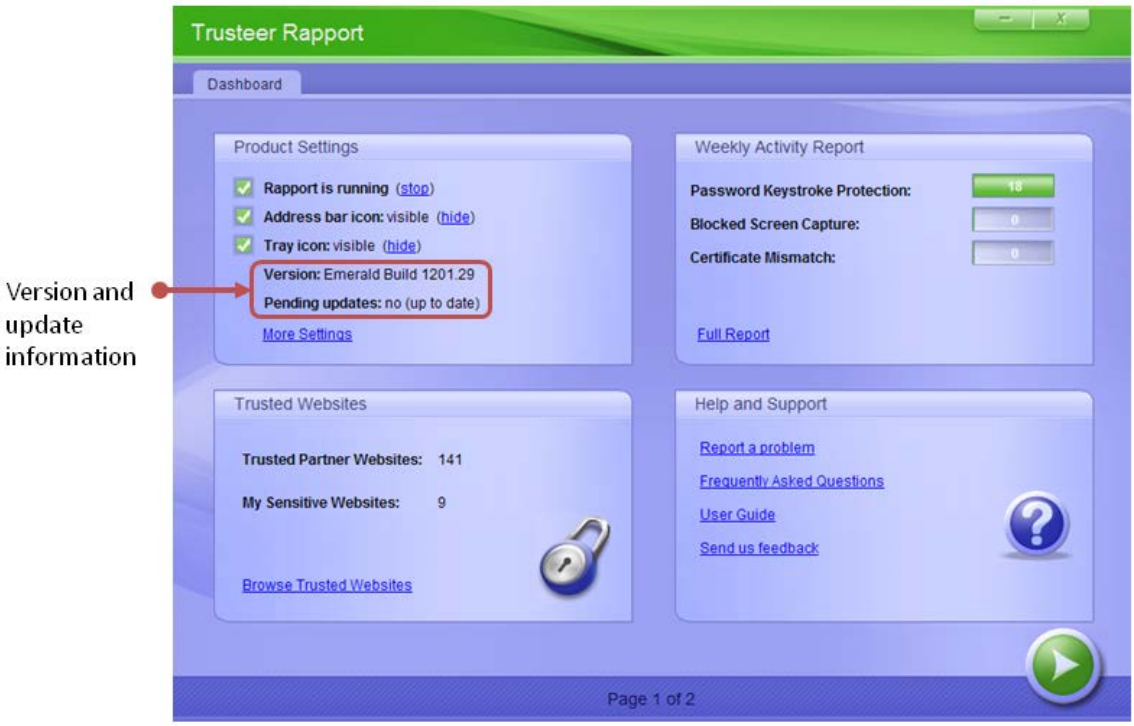
Des mises à jour régulières sont essentielles à l'efficacité de Trusteer Rapport. C'est pourquoi le programme se met à jour automatiquement. Les mises à jour s'effectuent de manière indépendante et silencieuse. Il est toutefois possible de mettre à jour Trusteer Rapport manuellement à tout moment, comme de désactiver les mises à jour automatiques si vous le souhaitez.

Vérifier l'état des mises à jour de Trusteer Rapport

Des informations concernant l'état des mises à jour de Trusteer Rapport sont affichées dans la zone Product Settings (Paramètres produit) de la console Rapport.

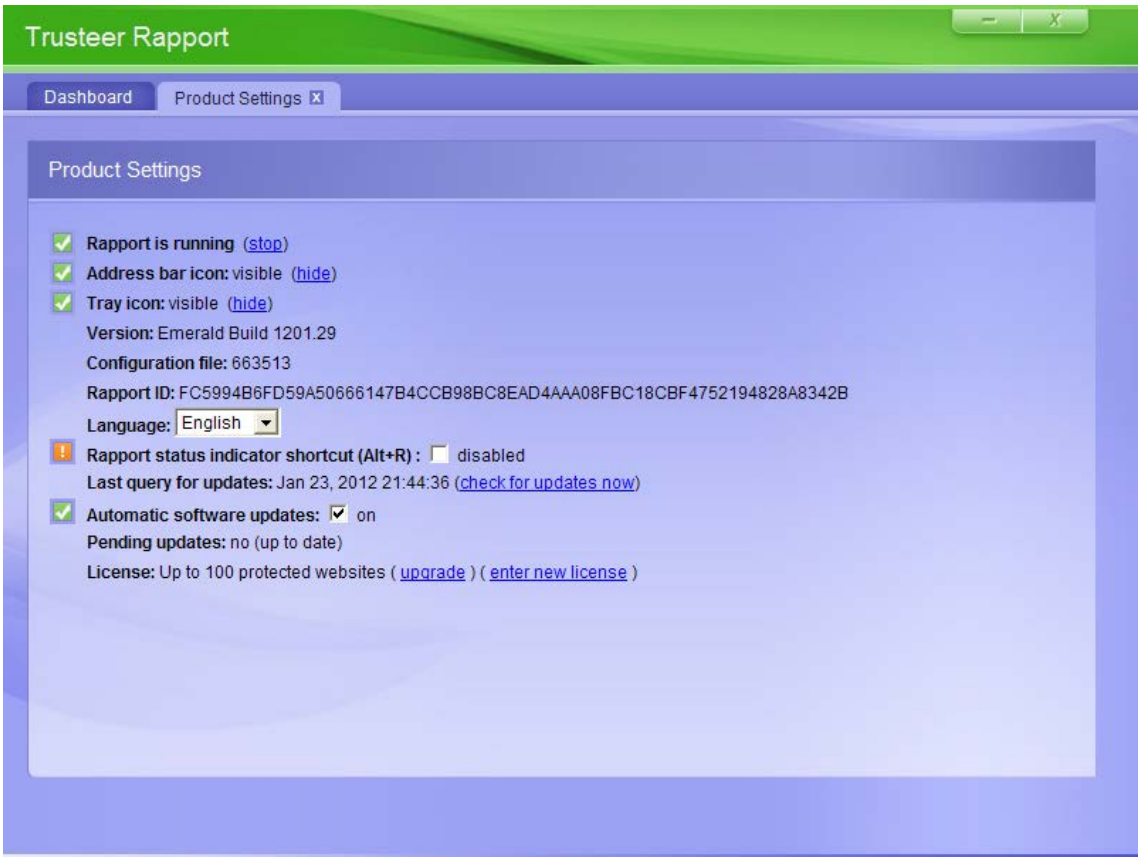
➡ **Pour vérifier l'état des mises à jour de Trusteer Rapport:**

1. Ouvrir la console Rapport (on page 72). La zone Product Settings (Paramètres produit) s'affiche en haut à gauche du tableau de bord.



La zone d'affichage des **Mises à jour en attente** indique si des mises à jour sont en attente et, par conséquent, si Trusteer Rapport est à jour. Un yes apparaît si la dernière mise à jour téléchargée nécessite un redémarrage système avant de prendre effet.

2. Cliquez maintenant sur **More Settings** (Plus de paramètres). L'onglet Product Settings apparaît affichant davantage d'informations.



Les zones d'affichage suivantes donnent des indications sur les mises à jour:

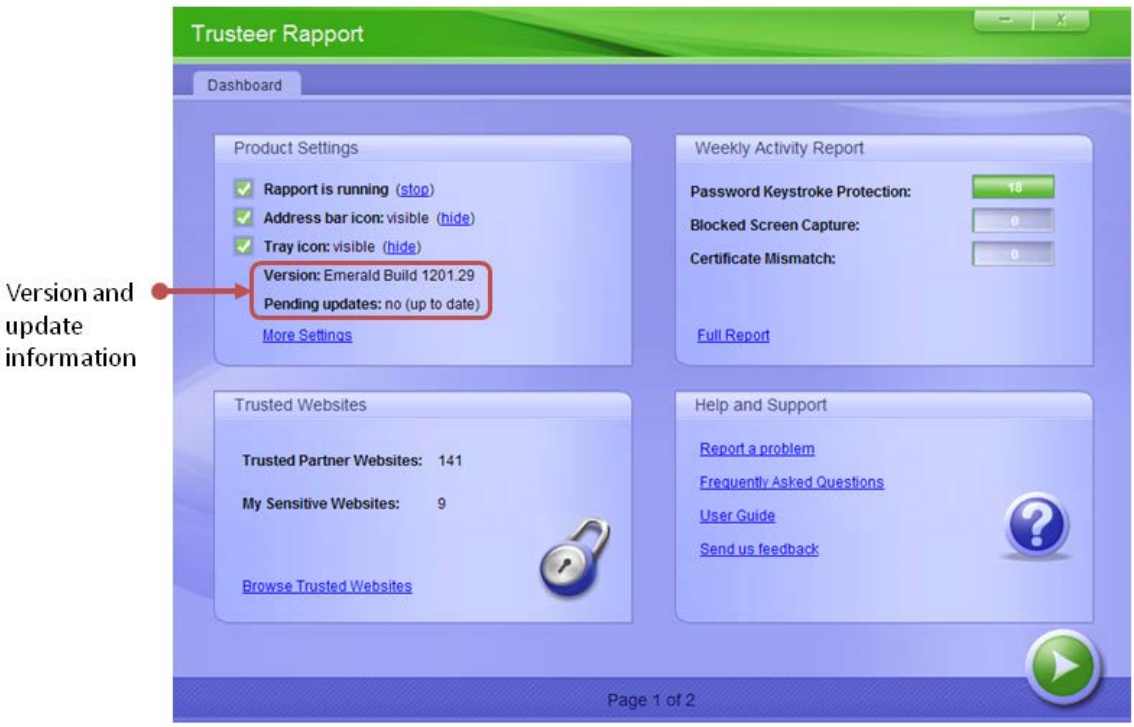
- Last query for updates (Dernière requête de mises à jour). Date et heure auxquelles Rapport a envoyé une requête pour rechercher de nouvelles mises à jour.
- Automatic software updates (Mises à jour automatiques du logiciel). S'effectuent même si la fonction de mise à jour automatique est désactivée. Cette fonction est activée par défaut. Trusteer recommande de conserver le paramètre par défaut activé pour assurer la réception de toutes les mises à jour.

Mettre à jour Rapport manuellement

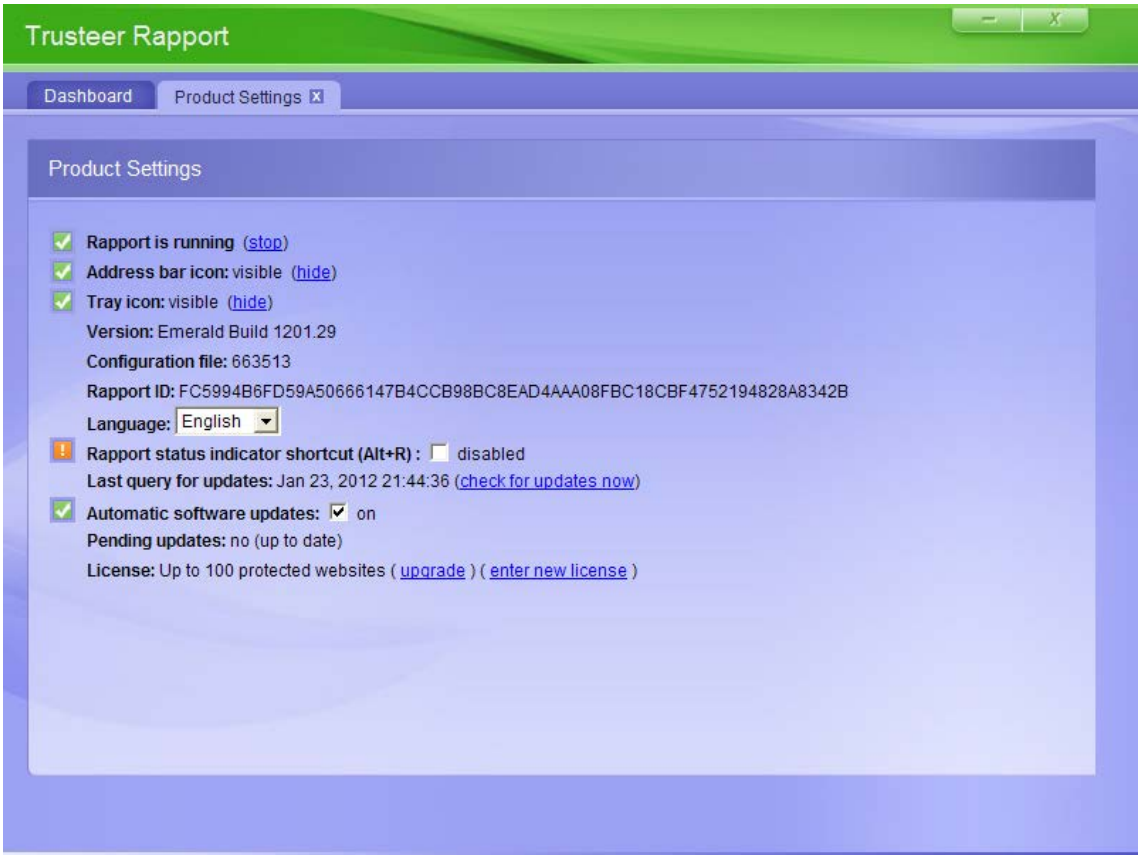
Trusteer Rapport est mis à jour automatiquement par défaut. Vous pouvez également mettre à jour le programme manuellement.

➡ **Pour mettre à jour Trusteer Rapport manuellement :**

1. Ouvrir la console Rapport (on page 72). La zone Product Settings (Paramètres produit) s'affiche en haut à gauche du tableau de bord.



2. Cliquez sur **More Settings** (Plus de paramètres). L'onglet Product Settings apparaît.



3. Cliquez sur **check for updates now** (vérifier les mises à jour maintenant). Trusteer Rapport vérifie les mises à jour. Pendant le processus, la progression est indiquée par un texte sous les zones d'affichage contenant l'une ou l'autre des informations suivantes :

   - Trusteer Rapport ne détecte aucune mise à jour en attente. Le message suivant apparaît : « You are already running the latest Trusteer Rapport configuration. » (Vous disposez déjà de la dernière configuration de Trusteer Rapport)

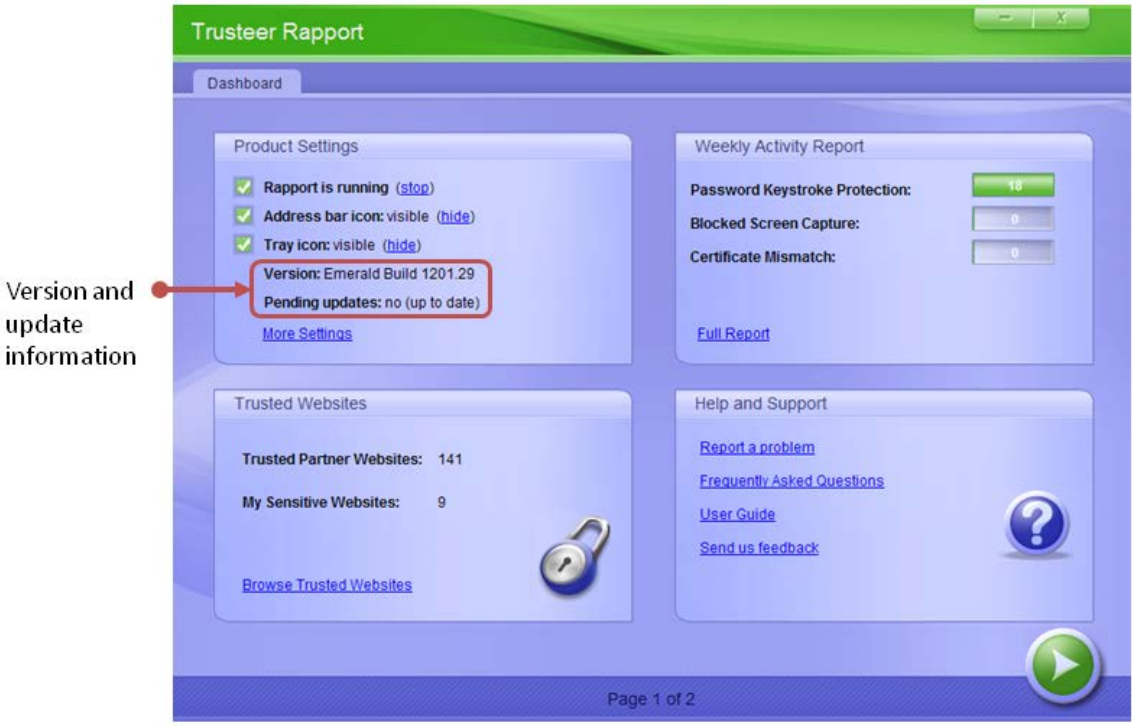
- Trusteer Rapport détecte, télécharge et applique une mise à jour. Le message suivant apparaît : « Configuration updated. You are now running with the latest Rapport configuration. » (Configuration mise à jour. Vous disposez maintenant de la dernière configuration de Rapport.) Le nombre dans la zone d'affichage **Configuration file** (fichier de configuration) a légèrement augmenté.
- Trusteer Rapport détecte et télécharge une mise à jour à appliquer au redémarrage de l'ordinateur. Le message suivant apparaît : « A software update is ready. The configuration is up to date. » (Une mise à jour du logiciel est prête. La configuration est à jour.) La zone d'affichage **Pending updates** (Mises à jour en attente) affiche alors « yes (restart PC to apply) » (oui – redémarrer le PC pour appliquer la MàJ).
- Trusteer Rapport détecte et télécharge plus d'une mise à jour. Certaines mises à jour sont appliquées immédiatement et d'autres le sont au redémarrage de l'ordinateur. Le message suivant apparaît : « A software update is ready. The configuration was updated. » (Une mise à jour du logiciel est prête. La configuration a été mise à jour.) Le nombre dans la zone d'affichage **Configuration file** (fichier de configuration) a légèrement augmenté. La zone d'affichage **Pending updates** affiche alors « yes (restart PC to apply) ».

Désactiver les mises à jour automatiques

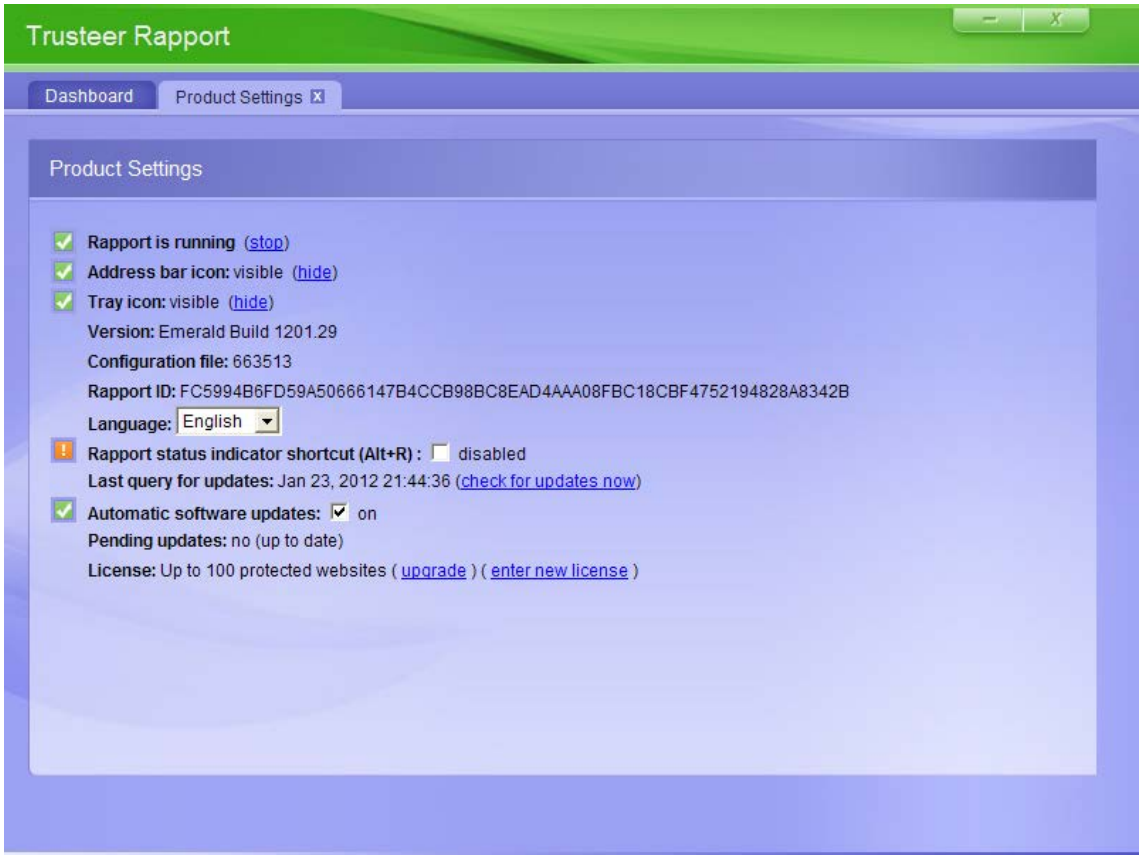
Trusteer Rapport se met à jour automatiquement. Les mises à jour s'effectuent de manière indépendante et silencieuse. Des mises à jour régulières sont essentielles à l'efficacité de Trusteer Rapport. Trusteer recommande de ne pas désactiver les mises à jour automatiques.

➡ **Pour désactiver les mises à jour automatiques:**

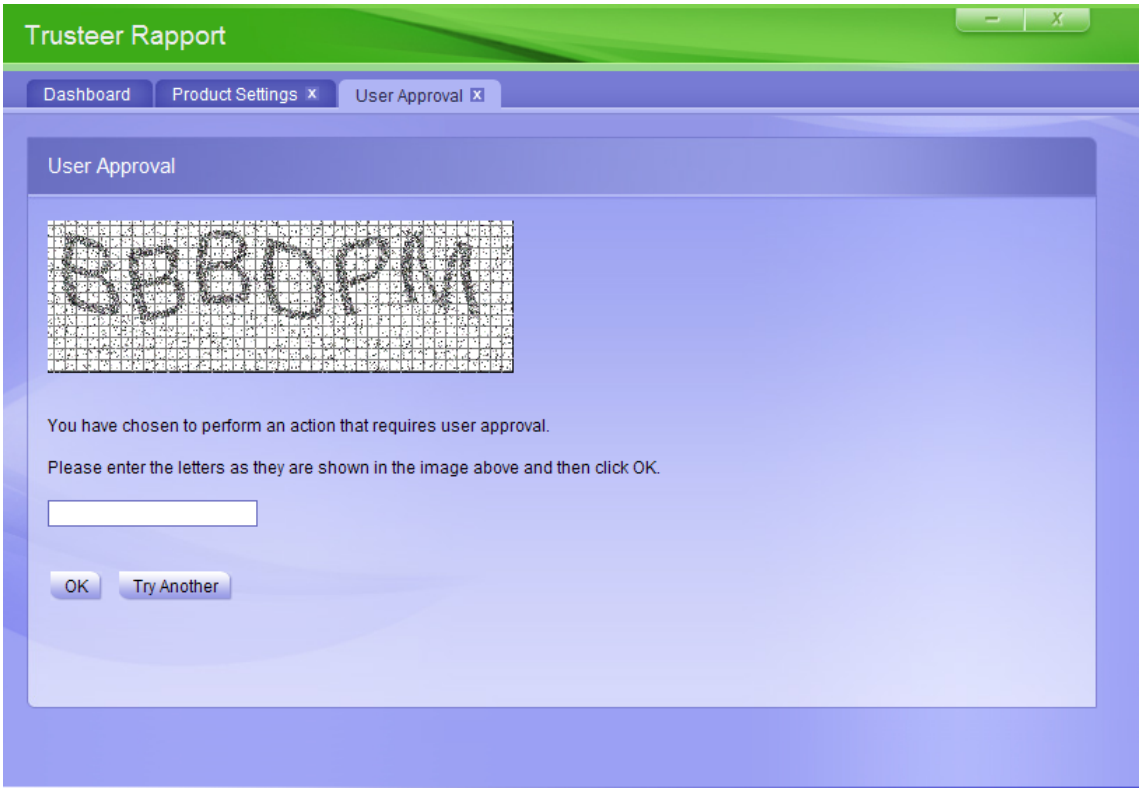
1. Ouvrir la console Rapport (on page 72). La zone Product Settings (Paramètres produit) s'affiche en haut à gauche du tableau de bord.



2. Cliquez sur **More Settings** (Plus de paramètres). L'onglet Product Settings apparaît.



3. Décochez **Automatic software updates** (Mises à jour automatiques du logiciel). L'onglet de validation apparaît. L'écran affiche une image contenant des caractères à saisir. Le but est d'empêcher des malwares d'accéder à la console et de parvenir à désactiver Trusteer Rapport.



4. Entrez les caractères affichés dans l'image.
5. Cliquez sur OK. Les mises à jour automatiques sont maintenant désactivées. Avec ce paramètre, Trusteer Rapport n'est pas mis à jour à moins que vous procédiez à une Mettre à jour Rapport manuellement (on page 228).

Désinstaller Trusteer Rapport

Nous vous recommandons fortement de ne pas désinstaller Trusteer Rapport. Si vous rencontrez des difficultés avec le programme, déposez une demande d'assistance sur http://www.trusteer.com/support/submit-ticket. Pendant l'examen de votre demande, vous pouvez Arrêter Trusteer Rapport (on page 194) sans le désinstaller.

Trusteer Rapport n'accepte qu'une seule méthode de désinstallation, ceci pour protéger le programme contre une désinstallation non autorisée.

Remarque: Si Trusteer Rapport a été installé depuis un compte administrateur Windows, vous ne pouvez désinstaller Rapport que si vous êtes connecté en tant qu'administrateur.

Uninstalling Trusteer Rapport (Windows 7)

Pour désinstaller Trusteer Rapport :

1. Ouvrez le Panneau de configuration.
2. Sous Programmes, cliquez sur Désinstaller un programme.
3. Trouvez Trusteer Rapport dans la liste des programmes, puis double-cliquez sur Rapport. Un message de confirmation apparaît.
4. Cliquez sur Oui. Une boîte de dialogue de Trusteer Rapport s'affiche, vous montrant les événements récents que Trusteer Rapport a réussi à bloquer.
5. Cliquez sur Continuer. Une autre boîte de dialogue de Trusteer Rapport apparaît, vous offrant une assistance aux problèmes techniques que vous avez pu avoir avec Trusteer Rapport. Avant de poursuivre la désinstallation, fermez tous les fichiers et les applications qui pourraient être ouverts.
6. Cliquez sur Non Merci, Désinstaller maintenant. Trusteer Rapport termine la désinstallation comme demandé. Une fois la désinstallation terminée, une nouvelle fenêtre de navigateur s'ouvre et vous demande vos commentaires à propos de Trusteer Rapport et vous pose quelques questions de base

Uninstalling Trusteer Rapport (Windows XP)

Pour désinstaller Trusteer Rapport :

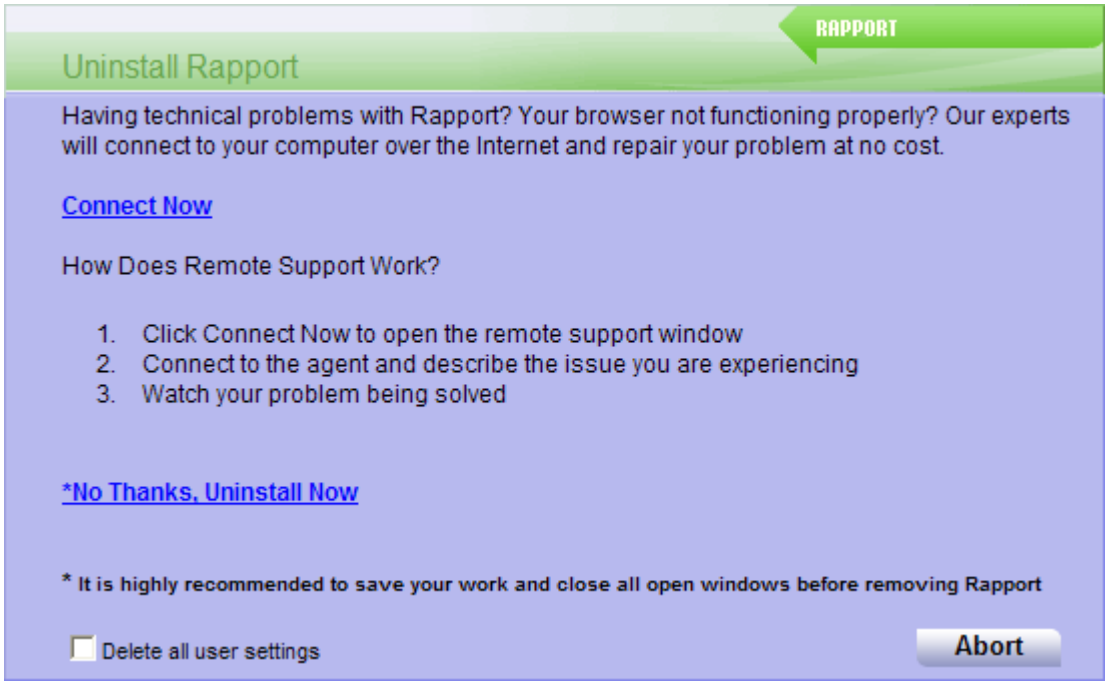
1. Ouvrez le Panneau de configuration.
2. Cliquez sur Ajouter/Supprimer des programmes.
3. Trouvez Trusteer Rapport dans la liste des programmes, puis cliquez sur le bouton Modifier/Supprimer pour Trusteer Rapport. Un message de confirmation apparaît.

4. Cliquez sur Oui. Une boîte de dialogue de Trusteer Rapport s'affiche, vous montrant les événements récents que Trusteer Rapport a réussi à empêcher.
5. Cliquez sur Continuer. Une autre boîte de dialogue de Trusteer Rapport apparaît, vous offrant une assistance aux problèmes techniques que vous avez pu rencontrer avec Trusteer Rapport. Avant de poursuivre la désinstallation, fermez tous les fichiers et les applications qui pourraient être ouverts.
6. Cliquez sur Non Merci, Désinstaller maintenant. Trusteer Rapport termine la désinstallation comme demandé. Une fois la désinstallation terminée, une nouvelle fenêtre de navigateur s'ouvre et vous demande vos commentaires à propos de Trusteer Rapport et vous pose quelques questions de base.

Remarque: En cas de difficulté pour désinstaller Trusteer Rapport, consultez la page http://www.trusteer.com/book/uninstalling-rapport-using-safeuninstall-utility pour des indications sur la désinstallation de Trusteer Rapport à l'aide de l'utilitaire spécifique de désinstallation.

Que signifie « Delete all user setting » à cocher sur l'écran de désinstallation?

La mention **Delete all user settings** (Supprimer tous les paramètres utilisateur) qui apparaît sur l'écran ci-dessous supprime toutes les modifications que vous avez apportées à Trusteer Rapport, y compris les sites que vous avez ajoutés et les mots de passe que vous avez choisis de protéger. Si vous cochez cette case puis installez Trusteer Rapport à nouveau dans le futur, Trusteer Rapport ne conservera aucune de vos modifications.



Uninstalling Trusteer Rapport (Windows 7)

➡ **To uninstall Trusteer Rapport:**

1. Open the Control Panel.
2. Under **Programs**, click **Uninstall a program**.
3. Find Trusteer Rapport in the list of programs, and double-click **Rapport**. A confirmation message appears.
4. Click **Yes**. A Trusteer Rapport dialog box appears, showing you recent events Trusteer Rapport successfully prevented.

5. Click **Continue**. Another Trusteer Rapport dialog box appears, offering you assistance with technical problems you may have had with Trusteer Rapport. Before continuing with the uninstall, close any files and applications you may have open.
6. Click **No Thanks, Uninstall Now**. Trusteer Rapport completes the uninstall as requested. Once the uninstall is complete, a new browser window opens, asking for your feedback about Trusteer Rapport and a few basic questions.

Uninstalling Trusteer Rapport (Windows XP)

➡ **To uninstall Trusteer Rapport:**

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

18. Mettre à niveau Trusteer Rapport

Pour mettre à niveau Trusteer Rapport avec une nouvelle version, installez simplement la nouvelle version sans supprimer l'ancienne version au préalable. Le processus d'installation est identique à celui de l'installation normale à l'exception de quelques étapes supplémentaires.

Pour mettre à niveau Rapport avec la nouvelle version, installez-la exactement comme d'ordinaire. Pour les instructions d'installation, reportez-vous à Installer Trusteer Rapport (on page 27). Au cours du processus d'installation, l'écran suivant apparaît:

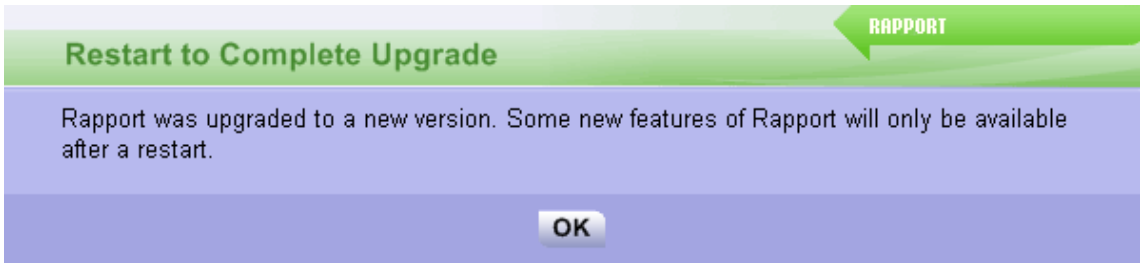
Cet écran s'affiche car vous installez une nouvelle version par-dessus une version existante. Lorsque cet écran apparaît, sélectionnez **It works - I just want to update it** (Cela fonctionne – Je veux juste mettre à jour). Cliquez ensuite sur **Next** et poursuivez l'installation normalement.

Remarque: Si Trusteer Rapport a été installé depuis un compte administrateur Windows, vous ne pouvez installer Rapport sur une version existante que si vous êtes connecté en tant qu'administrateur.

L'écran suivant apparaît également au cours du processus d'installation:

Cet écran apparaît car l'assistant d'installation doit fermer la version existante de Trusteer Rapport afin de pouvoir installer la nouvelle version. La fermeture requiert la confirmation de l'utilisateur. C'est grâce à cela que les malwares ne peuvent pas désactiver Trusteer Rapport. Lorsque vous voyez cet écran, entrez les caractères affichés dans l'image et cliquez sur **Shutdown**. L'installation se poursuit alors normalement.

Cet écran peut apparaître à la fin de l'installation:



Votre ordinateur est en sécurité, même si ce message apparaît. Il est toutefois préférable de redémarrer votre ordinateur dès que possible.