



Sage Business Exchange

Version 12.3

Préconisations de Sécurité



Sommaire

Mesures de sécurité	4
Mesures générales	4
Utilisation de https	4
Mots de passe solides	4
Sécurisation des serveurs par droit d'accès	5
Protection des serveurs.....	5
Transparent Data Encryption TDE	6
Chiffrement des données en transit.....	6
Chiffrement des sauvegardes de la base de données.....	6
Sécurité du système de fichiers.....	6
Configuration SSL/TLS sécurisée sur un serveur windows	6
Mesures applicatives.....	7
Signature de l'application du site web et des fichiers.....	7
La solution prend en charge plusieurs modes d'authentification.....	7
Autorisations	8
Protection contre les attaques	8
XML EXternal Entity (XXE) Prevention.....	9
Support de la sécurisation SameSite sur le cookie de Session sur OnlineBanking	9

Mesures de sécurité

HTTP Strict-Transport-Security Header	9
Périodicité d'accès au site web	9
Pour aller plus loin.....	10

Mesures de sécurité

Afin de minimiser le risque de violation de données et de pénalité, certains principes élémentaires de sécurité sont recommandés.

Même si la sécurisation du système et du réseau reste sous votre responsabilité, la plateforme de la solution vous fournit quelques outils :

- Les navigateurs web standard et les protocoles *http* ou *https* sont utilisés. La technologie web assure une isolation de premier niveau entre le serveur web et le poste de travail.
- Les mots de passe ne sont pas transférés sur le réseau. Le système d'authentification est basé sur des normes. Il peut s'agir d'une connexion *Windows* contrôlée dans un annuaire *LDAP* ou d'une authentification par certificat. Par souci de simplicité, une solution basée sur les utilisateurs et les mots de passe cryptés stockés dans le serveur web de la solution est disponible. Vous pouvez ajouter une double authentification.
- La gestion des droits est effectuée au niveau des entités. Elle est basée sur les profils de fonctions associés à l'utilisateur. Il est également possible de gérer les permissions d'accès aux contrats au niveau des services pour chaque entité.

Mesures générales

Utilisation de https

La solution est une application web accessible via une connexion *http* ou *https*. Bien que *http* soit disponible, nous vous recommandons de toujours utiliser *https* pour les instances de production, en particulier si votre solution est accessible à partir de l'internet public.

Mots de passe solides

Si vous utilisez ce mode d'authentification, n'oubliez pas d'établir une politique de gestion des mots de passe, afin que les utilisateurs définissent un mot de passe fort.

Pour optimiser la sécurité, un mot de passe fort doit :

- Contenir 6 caractères minimum (plus il y a de caractères, plus le mot de passe est solide)
- Utiliser une combinaison de chiffres, de majuscules et minuscules et de symboles (tels que @ # \$ % ! ? &, etc.)
- Ne pas contenir un motif de clavier tel que *azerty*
- Ne pas contenir la date de naissance de l'utilisateur
- Ne pas être utilisé sur plusieurs applications

Sécurisation des serveurs par droit d'accès

Les serveurs hébergeant les composants de la solution contiennent des fichiers de configuration et d'autres données vulnérables aux menaces internes.

Les administrateurs doivent être les seules personnes autorisées à se connecter aux serveurs.

Veillez à octroyer à ces utilisateurs les droits destinés à l'administration de la solution sur les répertoires appropriés.

Important ! Les administrateurs de serveur doivent être différents des administrateurs de la solution.

Protection des serveurs

Les serveurs de solution doivent être construits en utilisant les normes de l'industrie.

Utilisation de pare-feux locaux

Utilisez des pare-feux locaux sur vos serveurs pour verrouiller tout port IP qui n'est pas nécessaire au fonctionnement de la solution ou à l'accès des utilisateurs.

Généralement, si tous les composants de la solution sont installés sur un même serveur, la solution n'a besoin que des ports *http* ou *https* pour fonctionner.

Pour les installations à plusieurs serveurs, vous devez ouvrir les ports (ou plages de ports) nécessaires à la communication entre les différents composants.

Sécurisation de l'architecture internet

L'architecture que vous implémentez est la clé de votre sécurité, tout particulièrement si votre système est accessible à partir de l'internet public.

Pour connecter vos systèmes et les rendre disponibles sur internet, vous devez décider :

- quels serveurs et ports doivent être vus du monde extérieur
- comment les requêtes extérieures sont interceptées, traduites et dirigées vers ces serveurs et ports, le cas échéant.

Cela implique des équipements tels que :

- un pare-feu, situé entre votre réseau interne et internet pour intercepter les requêtes entrantes et les transférer vers les serveurs appropriés de votre réseau
- une *DMZ* ou "zone démilitarisée", c'est-à-dire une zone de réseau physique ou logique qui isole votre réseau local d'internet.

Le pare-feu est le gardien des *points de contrôle* de votre *DMZ*.

Note : Ces recommandations ne s'appliquent que si votre solution est visible sur internet. Vous n'avez pas besoin de configurer de **DMZ** ni de pare-feu externe si vous utilisez votre propre réseau local.

Transparent Data Encryption TDE

Pour mieux sécuriser votre base de données, vous pouvez utiliser le chiffrement *TDE (Transparent Data Encryption)*.

Le chiffrement *TDE* vous permet de crypter la base de données.

Sage XRT Business Exchange 12.1 a été validé avec les environnements suivants :

- SQL Server 2016 TDE
- Oracle 12c TDE

Chiffrement des données en transit

La communication entre votre couche applicative et votre base de données peut se faire à travers la norme *TLS (Transparent Layer Security)*.

L'option **ForceEncryption** de **SQL Server** force le chiffrement du protocole et vous permet de préserver la confidentialité des informations en cryptant les données.

Chiffrement des sauvegardes de la base de données

Afin de protéger les données, il est recommandé de chiffrer les sauvegardes de la base de données.

Le chiffrement *TDE* protège de fait les sauvegardes car il est impossible de restaurer ou d'attacher des fichiers sans le certificat.

Important ! Il est fondamental de sauvegarder le certificat en lieu sûr, et de ne pas stocker au même endroit les sauvegardes des bases et celle du certificat. Pour *Oracle*, vous pouvez utiliser le cryptage du réseau natif.

Sécurité du système de fichiers

La sécurité du système de fichiers des différents serveurs doit être implémentée avec les outils appropriés (antivirus, sécurité d'accès au réseau, etc.).

Assurez-vous que ces outils n'entraînent aucun problème de performance.

Par exemple, évitez d'exécuter une analyse antivirus continue sur un serveur de base de données.

Configuration SSL/TLS sécurisée sur un serveur Windows

Vous pouvez configurer le serveur IIS pour limiter l'utilisation des protocoles non sécurisés.

Reportez-vous à la documentation Microsoft suivante :

<https://medium.com/@rootsecdev/configuring-secure-cipher-suites-in-windows-server-2019-iis-7d1ff1ffe5ea>

Mesures applicatives

Signature de l'application du site web et des fichiers

Le code de votre application est signé. Cette signature certifie que le programme est légitime et conforme au développement initial et que l'intégrité des fichiers binaires de votre application est assurée.

Pour assurer l'intégrité du site web **Online Banking**, des **scripts**, des **fichiers du VFS**, vous pouvez calculer une signature.

Un administrateur habilité gère le calcul et le contrôle de la signature sur le site *master* de **Sage XRT Business Exchange**.

Base de données Paramètres internet Permissions Paramètres du P.A.P. Intégrité

Options...

Intégrité

☒ Base de données

☒ Site OnlineBanking

☒ Vfs

☒ Script

☒ Registre

Suspendre l'accès

Ne pas démarrer le transfert

Ne rien faire

Ne rien faire

Anomalie sur les contrats

☒ Détection d'échec de connexion

☐ Suspendre le contrat

Contrat de notification

Entité : SBESAGE

Alias : ADMIN

Important ! Pour activer l'intégrité du site web, vous devez définir un passphrase. Ce passphrase doit être stocké en lieu sûr.

La solution prend en charge plusieurs modes d'authentification

- **Sécurité intégrée de Windows NT** : l'utilisateur est authentifié grâce à son compte NT. Ce niveau d'authentification est recommandé.
- **Nom d'utilisateur et un mot de passe** : l'utilisateur est authentifié grâce à un nom d'utilisateur et un mot de passe.
- **Authentification de l'utilisateur via un certificat X509** : pour le client web, l'authentification forte est un système d'authentification à deux phases :
 - Vérification du certificat sur le répertoire *Active Directory* de l'entreprise
 - Challenge/Réponse entre le client et le composant d'authentification, permettant de vérifier l'identité du client
- **Double authentification** : un deuxième facteur est utilisé pour l'authentification des utilisateurs afin de générer un mot de passe à usage unique.
- **SageID**

Autorisations

Un utilisateur a accès à une ou plusieurs entités. Il est associé à un profil qui détermine ses droits d'accès aux fonctions de l'application et ses privilèges : consultation de liste, saisie d'information, autorité de validation, autorité d'approbation, autorité d'administration et signataire.

Les privilèges sont déterminés par les packages d'import.

Il est possible sur chaque contrat bancaire de paramétrer des autorisations spécifiques pour les utilisateurs et les signataires (accès aux contrats, accès aux éditions, droits d'archivage et droits d'extraction).

Grâce à ces fonctionnalités, vous pouvez définir différemment l'accès aux données critiques sur chaque entité pour un utilisateur donné.

Important ! Assurez-vous de conserver ces règles au fil du temps. Simplifiez-les au maximum, sans compromettre votre politique de sécurité.

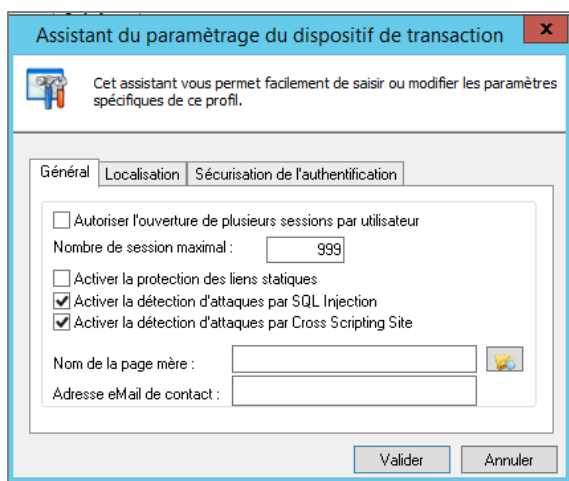
Protection contre les attaques

Certaines attaques peuvent compromettre la sécurité de vos données et de votre domaine.

Les requêtes *SQL injection* permettent d'injecter dans une requête SQL en cours un morceau de requête non prévu par le système et pouvant compromettre la sécurité du site web.

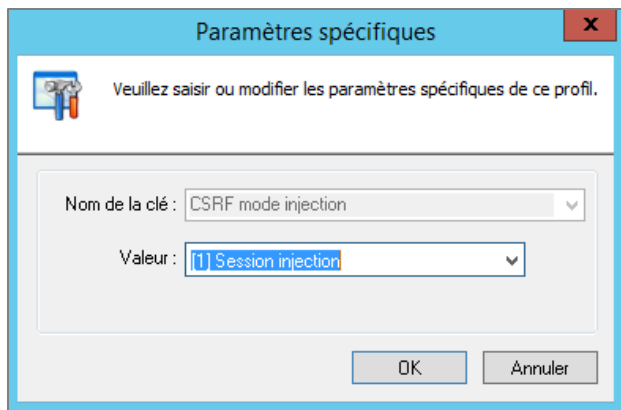
Le *Cross-Site Scripting* est un type de faille de sécurité des sites web qui injecte du contenu dans une page, permettant ainsi des actions sur les navigateurs web visitant la page.

Vous pouvez activer les options de détection d'attaque au niveau du service de transaction.



L'objectif d'une attaque *CSRF (Cross-Site Request Forgery)* est de transmettre à un utilisateur authentifié une requête *http* falsifiée qui pointe sur une action interne au site, afin qu'il l'exécute sans en avoir conscience et en utilisant ses propres droits.

Activez l'option dans les paramètres spécifiques du service.



Les attaques *DTD* sont des failles de sécurité sur les parseurs *XML*.

Ces failles ont déjà été utilisées pour réaliser des attaques par déni de service. Elles permettent également d'obtenir le contenu d'un fichier en intégrant une entité externe.

Le code de l'application utilise le compilateur *XSL.NET* de dernière génération.

XML EXternal Entity (XXE) Prevention

Les attaques XXE consistent à l'envoi d'un fichier malicieux à destination d'un analyseur syntaxique XML.

Support des XML EXternal Entity (XXE).

Support de la sécurisation SameSite sur le cookie de Session sur OnlineBanking

L'instruction SameSite permet de limiter les risques liés aux attaques de type CSRF (Cross-Site Request Forgery) et XSSI (Cross-Site Script Inclusion).

Support de l'instruction SameSite.

HTTP Strict-Transport-Security Header

HTTP Strict Transport Security (HSTS) est un dispositif de sécurité par lequel un site web peut déclarer aux navigateurs qu'ils doivent communiquer avec lui en utilisant exclusivement le protocole HTTPS, au lieu du HTTP.

HTTP Strict Transport Security (HSTS) est supporté sur le Header des requêtes du serveur.

Périodicité d'accès au site web

Vous pouvez définir une périodicité d'accès au site web, afin de contrôler la légitimité des connexions.

Un calendrier d'accès aux données peut être défini.

Exemple : Accès des utilisateurs au site web **Online Banking** non autorisé le week-end.

Pour aller plus loin

La mise en œuvre de ces mesures de sécurité complémentaires nécessite des compétences ainsi que des retours d'expérience que nos équipes de consulting sont en mesure de vous apporter.

Nous vous engageons à les contacter si vous souhaitez appliquer ces recommandations.