Sage XRT Business Exchange

Sécurité et mesures de protection

Version 14

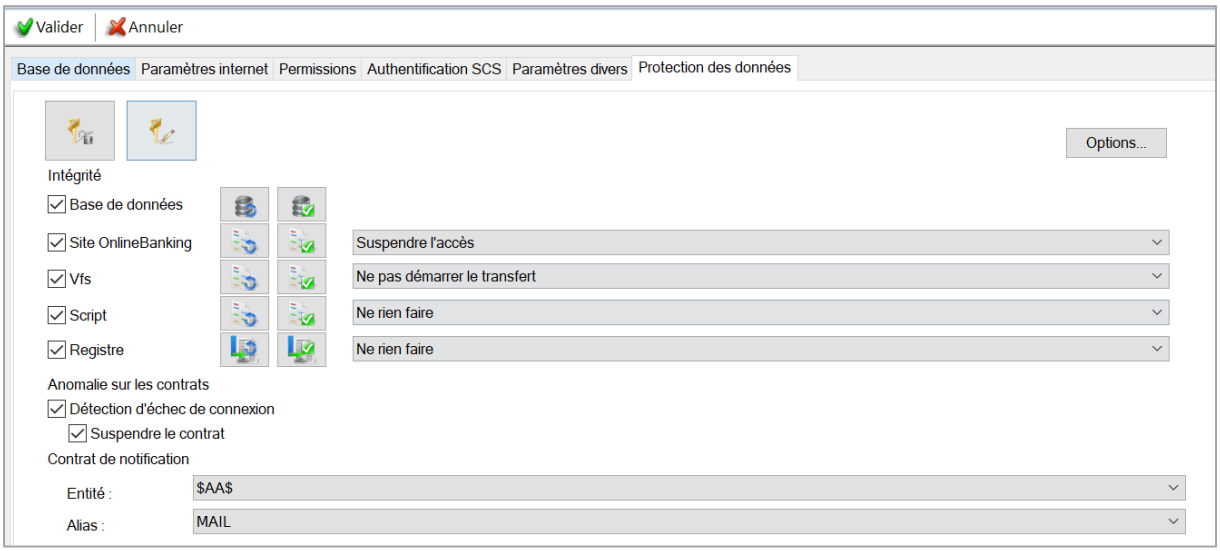
Sage

Sommaire

Description

Pour renforcer la sécurité de l'application, l'onglet **Protection des données** de l'**Administration système** vous permet de paramétrer différentes options :

- **Intégrité** calcule une signature sur les champs des contrats bancaires pour **Intégrité Base de données**, les clés de registre pour **Intégrité Registre**, sur les fichiers de l'application **Online Banking** pour **Intégrité Site Online Banking**, sur les scripts pour **Intégrité Script** et sur les fichiers du Vfs pour **Intégrité Vfs**.
- **Anomalie sur les contrats** vous permet de détecter les ruptures d'intégrité survenues par intrusion.
- **Détection d'échec de connexion** et **Suspendre le contrat** pour les contrats bancaires demandeurs
- **Contrat de notification** vous permet de définir l'entité et l'alias de notification pour toutes les anomalies d'intégrité, de connexion, d'attaque *SQL Injection*, *Cross Scripting* et *CSRF (cross-site request forgery)*.



Important ! En mode multisites, les sites dérivés héritent du paramétrage du site *master*. L'onglet **Protection des données** ne sera pas accessible sur les sites dérivés.

D'autres politiques de sécurisation sont également mises en place.

Protection des données

Paramétrage de l'intégrité

Ce paramétrage permet de calculer et de vérifier la signature :

- de la base de données (des contrats demandeurs)
- du site **Online Banking**
- du Vfs (des fichiers demandeurs/émetteurs)
- des scripts
- du registre

Lors de l'activation des intégrités, un agent *Watch* vérifie en temps réel :

- les actions **Créer**, **Modifier**, **Renommer** et **Détruire** sur tous les fichiers du répertoire de l'application **Online Banking**.
- toute intervention sur la base de registre

L'agent *Watch* répertorie les intrusions non autorisées et notifie les administrateurs en cas de détection.

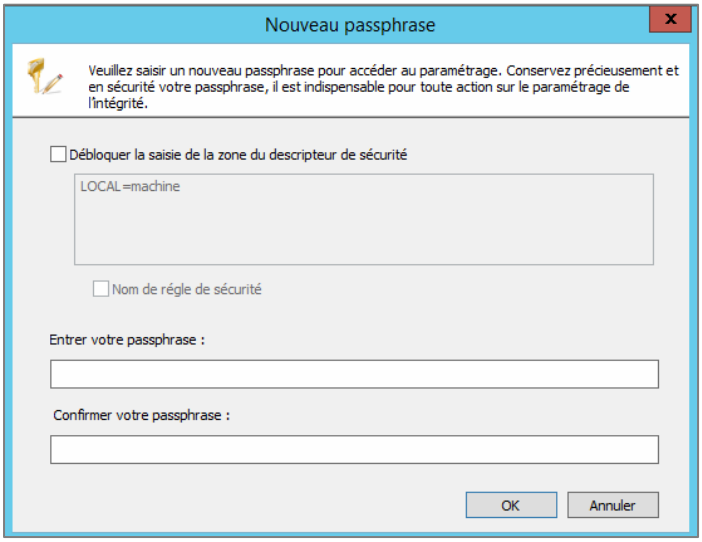
Première activation

Tous les services **Sage XRT Business Exchange** doivent être arrêtés.

Pour activer les options de paramétrage, vous devez renseigner un *passphrase*.

Important ! Conservez en sécurité ce *passphrase*. Il vous sera nécessaire pour chaque modification de l'intégrité. En cas de perte, vous serez dans l'obligation de procéder à la réinstallation complète de l'application.

Cliquez sur l'icône **Verrou**  pour ouvrir la fenêtre de création du *passphrase*.



Débloquer la saisie de la zone du descripteur de sécurité : cette zone permet de sécuriser l'accès à la clé du *passphrase*. Le paramétrage défini par défaut est **LOCAL=MACHINE**.

Note : Pour trouver des informations sur la syntaxe des descripteurs de sécurité autorisés pour ce champ, consultez la documentation **Microsoft** :

https://msdn.microsoft.com/en-us/library/cc230368.aspx
https://msdn.microsoft.com/fr-fr/library/windows/desktop/hh769091(v=vs.85).aspx
https://msdn.microsoft.com/fr-fr/library/windows/desktop/hh870248(v=vs.85).aspx

Quelques exemples de paramétrage sont disponibles en annexe de ce document.

Saisissez et confirmez le *passphrase* dans les champs **Entrer votre passphrase** et **Confirmer votre passphrase**.

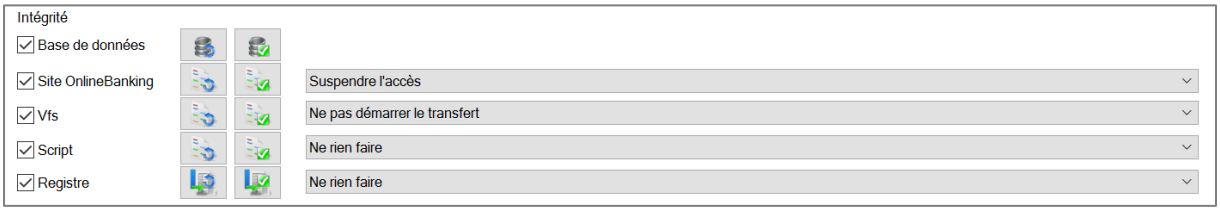
Important !La protection du coffre-fort avec plus de **deux SID** nécessite d'utiliser une AD avec un mode de compatibilité de la forêt au moins égal à 2012.
Commande **PowerShell** pour obtenir la version :
[system.directoryservices.activedirectory.Forest]::GetCurrentForest().ForestMode

Pour activer le paramétrage des options **Intégrité** de la base de données, du site **Online Banking** et du registre **SXBE** de la base de registre *Windows*, le *passphrase* doit être renseigné.

Paramétrage des options

Le contrôle de l'intégrité peut être activé sur les éléments suivants :

- Base de données
- Site **OnlineBanking**
- Vfs
- Script
- Registre



Les boutons de **Calcul** (première colonne d'icônes) permettent de lancer le calcul de la signature.

Les boutons de **Vérification** sont utilisés pour vérifier la signature.

Note : Les services doivent être arrêtés pour que les boutons soient actifs et les options accessibles.

Si vous activez l'option **Site OnlineBanking**, sélectionnez dans la liste déroulante correspondante l'action à effectuer en cas de détection d'un problème d'intégrité :

- **Ne rien faire**

Lorsque le paramétrage des notifications est spécifié, l'administrateur est averti par E-mail de la corruption d'un ou plusieurs fichiers. L'activité sur le site **Online Banking** se poursuit.

- **Suspendre l'accès**

Si un seul fichier de l'application est corrompu, le site **Online Banking** est suspendu et un message d'erreur s'affiche : **L'intégrité du site n'est plus assurée. Veuillez contacter d'urgence votre administrateur**.
Lorsque le paramétrage des notifications est spécifié, l'administrateur est averti par E-mail de la corruption d'un ou plusieurs fichiers.

Important ! Si l'intégrité du site **OnlineBanking** est activée et si le descripteur de sécurité est différent de **LOCAL=MACHINE**, l'identité du *pool* d'application d'*IIS* doit être un compte AD ou un compte local (un compte non virtuel).

Si vous activez l'option **Script**, sélectionnez dans la liste déroulante correspondante l'action à effectuer en cas de détection d'un problème d'intégrité :

- **Ne rien faire**

Lorsque le paramétrage des notifications est spécifié, l'administrateur est averti par E-mail de la corruption d'un ou plusieurs scripts. L'activité se poursuit.

- **Ne pas autoriser l'exécution**

Le script corrompu ne s'exécute pas.

Important ! Les scripts sont signés et vérifiés s'ils sont stockés dans le répertoire **\scripts** de **Sage XRT Business Exchange**.

Il est possible de modifier le répertoire via la variable **INSTALLSCRIPTS : // CHEMIN DE LOCALISATION DES SCRIPTS**.

La surveillance des scripts est effectuée au moment de l'exécution.

Si vous activez l'option **Vfs**, sélectionnez dans la liste déroulante correspondante l'action à effectuer en cas de détection d'un problème d'intégrité :

- **Ne rien faire**

Lorsque le paramétrage des notifications est spécifié, l'administrateur est averti par E-mail de la corruption du fichier demandeur émetteur lors de la transmission. L'activité se poursuit.

- **Ne pas démarrer le transfert**

Le fichier est bloqué, le transfert n'est pas effectué. L'administrateur est averti par E-mail de la corruption du fichier à transférer.

Si vous activez l'option **Registre**, sélectionnez dans la liste déroulante correspondante l'action à effectuer en cas de détection d'un problème d'intégrité :

- **Ne rien faire**

Lorsque le paramétrage des notifications est spécifié, l'administrateur est averti par E-mail de la corruption d'un ou plusieurs fichiers. L'activité se poursuit.

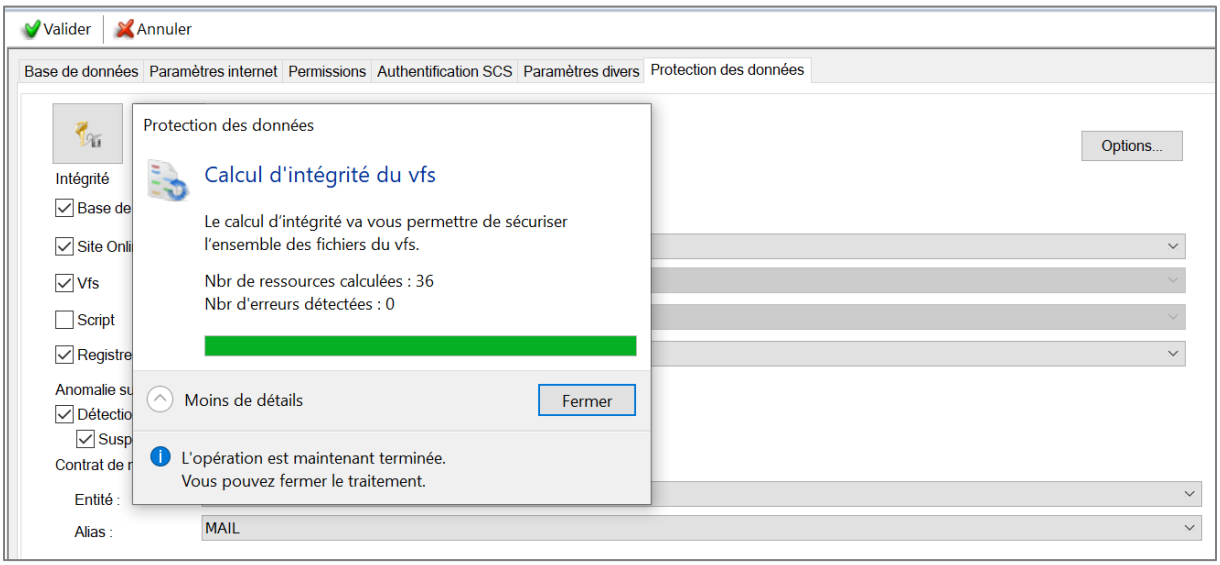
- **Arrêter le service**

L'activité est totalement interrompue. Si le paramétrage des notifications est spécifié, l'administrateur est averti par E-mail de la corruption d'un ou plusieurs fichiers.

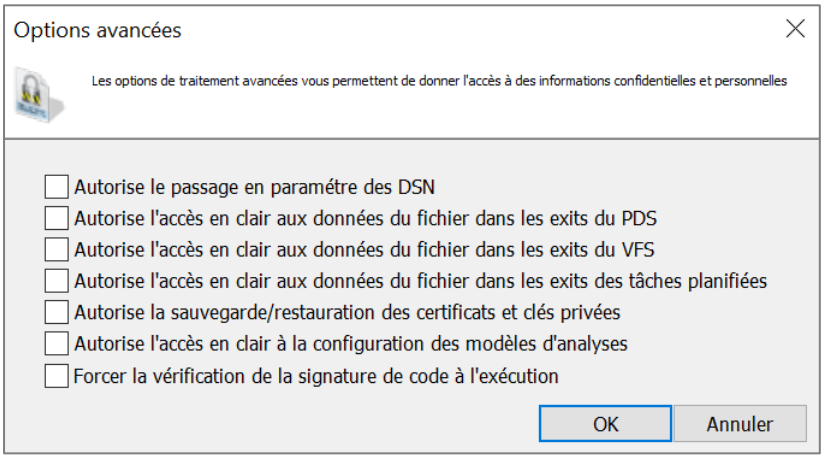
- **Suspendre l'accès**

L'activité du service est suspendue. Si le paramétrage des notifications est spécifié, l'administrateur est averti par E-mail de la corruption.

Dès que l'une des options **Base de données**, **Site onlineBanking**, **Script** ou **Registre** est sélectionnée, le calcul de la signature démarre automatiquement.



Les options de traitement avancées vous permettent d'autoriser l'accès à des données confidentielles et personnelles dans certains cas.



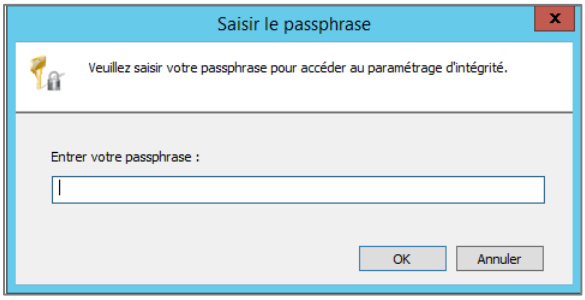
Modification du paramétrage

Important ! Pour modifier le paramétrage, tous les services doivent être arrêtés.

Vous pouvez effectuer les modifications suivantes sur le paramétrage du contrôle d'intégrité :

- Désactiver le contrôle des signatures
- Recalculer les signatures : **Calcul** (*/COMPUTE*)
- Contrôler la signature : **Vérification** (*/CHECK*)

Pour modifier le paramétrage, cliquez sur l'icône **Verrou**  et renseignez le *passphrase* dans la boîte de dialogue qui apparaît.

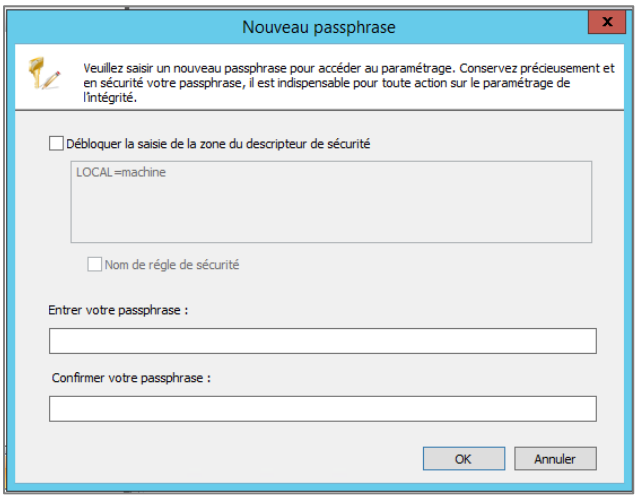


Note : Aucun recalcul n'est effectué lorsque l'option **Intégrité** est désactivée.

Modification du passphrase

Important ! Pour modifier le passphrase, tous les services doivent être arrêtés.

Cliquez sur le bouton **Modification**  .



Dans la boîte de dialogue **Nouveau passphrase**, saisissez le *passphrase*, confirmez votre saisie, puis cliquez sur le bouton **OK**.

Note : Si les services sont en cours d'exécution, seules les actions de **Vérification** sont disponibles.

Utilitaires de calcul et de vérification des signatures

Intégrité en base de données des contrats demandeurs

L'utilitaire **P5SECDB** permet de calculer et de vérifier l'état de cohérence de la base de données pour les contrats demandeurs.

Par défaut, l'utilitaire lance la commande **CHECK** si aucun autre paramétrage n'est renseigné.

Usage : P5SECDB {/CHECK | /COMPUTE} [/P: /S: /C: /T: /LOG: /SERVER:]	
/CHECK	Vérification de la signature
/COMPUTE	Calcul de la signature
/LOG	Nom du fichier de rapport
/P:	Filtre entité
/S:	Filtre service
/C :	Filtre client
/T:	Filtre protocole
/SERVER:	Nom de site permet de retrouver les ressources associées au site exemple : BDD

Important ! Si un seul des éléments du contrat demandeur est incorrect le contrat est inutilisable.
L'information est sérialisée dans l'audit à chaque tentative d'utilisation de contrat.
L'utilitaire peut être planifié pour l'action */CHECK*. En cas d'erreur d'intégrité, les erreurs sont compilées dans un fichier *XML* envoyé par E-mail.

Intégrité du site OnlineBanking et des scripts

L'utilitaire **P5SECFILE** permet de calculer et de vérifier la signature :

- des fichiers du site **Online Banking**
- des scripts
- des fichiers du Vfs

Un contrôle d'intégrité est effectué sur l'ensemble des fichiers constituant le site, les scripts et les fichiers demandeurs émetteurs du vfs.

Usage : P5SECFILE {/CHECK | /COMPUTE} [/LOG:]	
/CHECKOLB	Vérification de la signature des fichiers OnlineBanking
/CHECKSCR	Vérification de la signature des scripts
/CHECKBIN	Vérification de la signature des binaires de l'application
/CHECKVFS	Vérification de la signature des fichiers du Vfs
/COMPUTEOLB	Calcul de la signature des fichiers OnlineBanking
/COMPUTESCR	Calcul de la signature des scripts
/COMPUTEVFS	Calcul de la signature des fichiers du Vfs
/LOG	Nom du fichier de rapport

Important ! Le contrôle s'effectue sur l'ensemble du site **OnlineBanking** avant son démarrage. Le démarrage n'est pas assuré si une corruption est détectée.
Le contrôle peut être également effectué sur les binaires de l'application (*/CHECKBIN*).
L'utilitaire peut être planifié pour l'action */CHECK*. En cas d'erreur d'intégrité, les erreurs sont compilées dans un fichier *XML* envoyé par E-mail.

Intégrité du registre

L'utilitaire **P5SECREG** permet de calculer et de vérifier la signature de la base de registre.

Les clés signées et vérifiées dans le registre sont les suivantes :

- **SMP-P5** (et sa version multisite)
- **AUTO**
- **COM**
- **ISAPI**
- **NTF**
- **PDS**
- **RCP**
- **WEB**

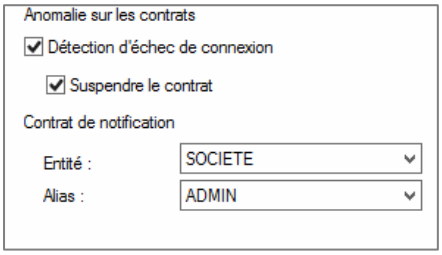
Usage : P5SECREG {/CHECK | /COMPUTE} [/LOG: /SERVER:]	
/CHECK	Vérification de la signature
/COMPUTE	Calcul de la signature
/COMPUTER :	Vérification du registre sur une autre machine (Nom Ordinateur)
/LOG	Nom du fichier de rapport
/SERVER:	Nom de site

Important ! L'utilitaire peut être planifié pour l'action */CHECK*. En cas d'erreur d'intégrité, les erreurs sont compilées dans un fichier *XML* envoyé par E-mail.

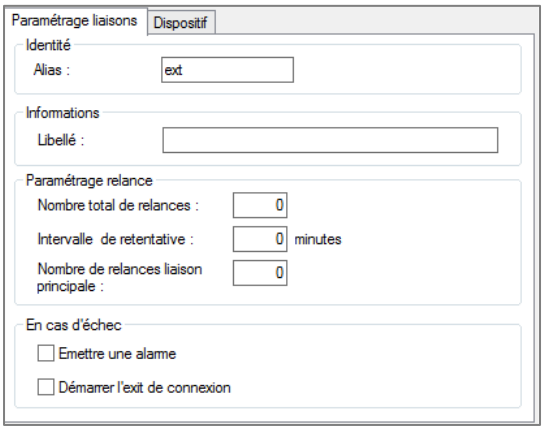
Anomalies de connexion

Dans la rubrique **Anomalie sur les contrats**, activez l'option **Détection d'échec de connexion** pour enregistrer en Log les phases de connexion logique ou physique en erreur sur les contrats bancaires demandeurs. Ces erreurs seront alors notifiées.

L'option **Suspendre le contrat** devient également accessible.

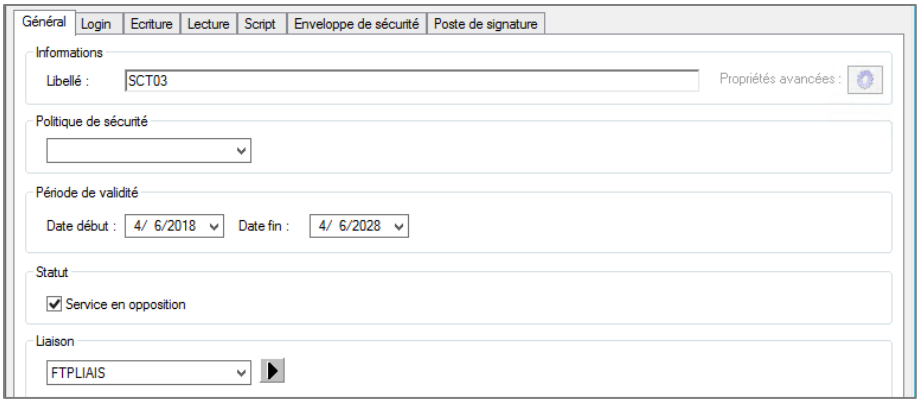


Le contrat bancaire est suspendu une fois que le nombre de tentatives indiqué dans le paramétrage de liaison du contrat demandeur est atteint.



Après suspension du contrat, aucune connexion n'est possible sans l'intervention de l'administrateur.

L'option **Accès au service suspendu** est activée au niveau du contrat demandeur.



Si aucune relance n'est indiquée, le contrat n'est pas suspendu.

Impacts

Données signées

Toutes les données du contrat demandeur sont signées (y compris les **Données de la liaison Protocole** et le paramétrage **Réseau** de l'onglet **Dispositif**), excepté **Libellé** et **Propriétés avancées**.

Tables impactées

Table	Description	Commentaire
HTTPMD	Contrat http	Ajout colonne HASHSIGNATURE varchar (255) NULL
OFTPMD	Contrat Odette FTP	
SWIFTFTIMD	Contrat Swift	
EXTMD	Contrat External	
CPFMD	Contrat CopyFile	
MOMMD	Contrat MsMQ	
SMTPPOP3MD	Contrat eMail	
X400MD	Contrat X400	
AS2MD	Contrat AS2	

SOAPMD	Contrat Soap	
PADEFMD	Contrat PaDeF	
SFTPMD	Contrat Sftp	
EB3MD	Contrat Etebac3	
PTDMD	Contrat PeSIT D	
PTEMD	Contrat PeSIT E	
FTPMD	Contrat Ftp	
EBICSMD	Contrat EBICS	
EBICSUSERS_DEM	Paramètre d'identification EBICS	
LIEN_NTW	Liaison	
X25	Liaison / dispositif réseau X25	
TCPIP	Liaison / dispositif réseau TCPIP	
RNIS	Liaison / dispositif réseau RNIS	
RTC	Liaison / dispositif réseau RTC	

Export/Import du paramétrage

Si l'option **Intégrité Base de données** est activée, l'import du paramétrage effectué depuis l'interface graphique calcule automatiquement le *hash* de signature.

L'import via **IMPVIR** nécessite la saisie du *passphrase*.

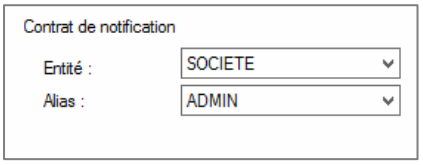
En revanche, il n'est pas demandé lors de l'export du paramétrage. Le traitement est identique à celui de l'utilitaire **EXPVPS**.

Important ! Les données de liaison ou de paramètres d'identification non liées à un contrat bancaire ne sont pas signées (données de tests, par exemple). Ces données seront intégrées à l'export.

Notifications

Le paramétrage des notifications doit être effectué dans la rubrique **Contrat de notification** de l'onglet **Intégrité** du site *Master*.

Vous devez renseigner une **Entité** et un **Alias**.



Description des alertes

- **Site Online Banking**

Objet E-mail : *Alerte de sécurité du site OnlineBanking [Nom Machine, tenant physique (site, serveur)]*

Contenu : *Le site Online Banking est suspendu à cause de la détection d'une intrusion. Veuillez consulter la log pour obtenir plus d'information.*

- **Script**

Objet E-mail : *Alerte de contrôle d'intégrité des fichiers*

Contenu : *X/X fichier(s) ne sont pas valide(s). Veuillez consulter le détail des fichiers incorrects disponible dans le fichier en pièce jointe.*

- **Données du contrat bancaire**

Objet E-mail : *Alerte de contrôle d'intégrité de la base de données*

Contenu : *X/X enregistrement(s) ne sont pas valide(s).Veuillez consulter le détail des enregistrements incorrectes disponible dans le fichier en pièce jointe.*

- **Registre**

Objet E-mail : *Alerte d'intégrité du registre [Nom Machine, tenant physique (site, serveur)]*

Contenu : *Le registre a subi une action qui a modifié son intégrité. Veuillez consulter la log pour obtenir plus d'information.*

- **Détection d'échec de connexion**

Objet E-mail : *Alerte d'échec de connexion [Nom Machine, tenant physique (site, serveur)]*

Contenu : *Le nombre de tentative de connexion sur le contrat ENTITE, PROTOCOLE, SERVICE, CLIENT a été atteint. Le contrat a été suspendu.*

Audit

Audit Utilisateur Sage XRT Common Services

Le paramétrage de l'onglet **Sécurité** est consigné dans l'**Audit utilisateur** de **Sage XRT Common Services**.

Date/Heure	Statut	Utilisateur	Compte utilisateur	Machine	Description
26/12/2018 16:17:54	Succès	SIG1	FR\ SIG1	PHILAE-W16	Création d'un utilisateur 'SIG2' (Administrateur de sécurité de niveau 1, Authentification standard)
26/12/2018 16:18:08	Succès	SIG1	FR\ SIG1	PHILAE-W16	Modification de l'utilisateur 'SIG2' (Administrateur de sécurité de niveau 1)
26/12/2018 16:18:08	Succès	SIG1	FR\ SIG1	PHILAE-W16	Ajouter l'utilisateur 'SIG2' au profil 'ADMINISTRATEURS'
27/12/2018 15:00:07	Succès	SIG1	FR\ SIG1	PHILAE-W16	Création d'un utilisateur 'SIG3' (Administrateur de sécurité de niveau 1, Authentification standard)

Audit de l'intégrité des données

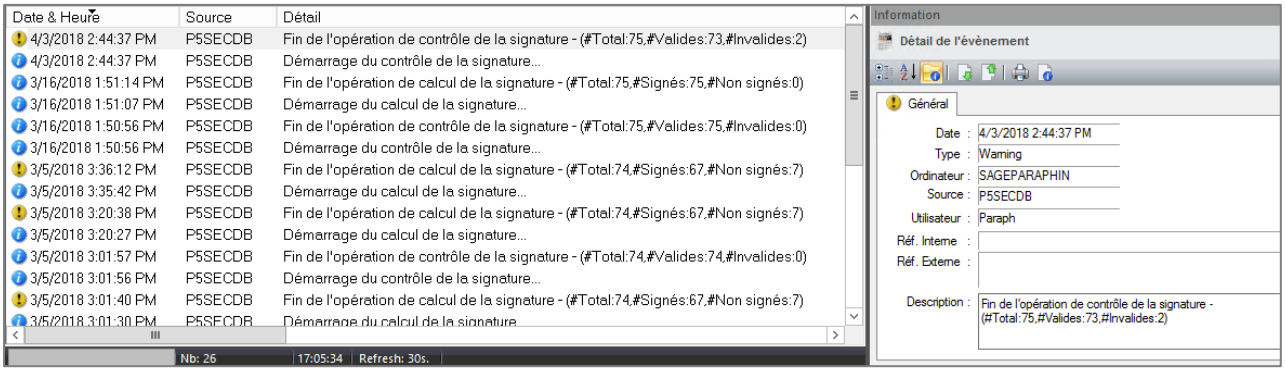
Le calcul (*/COMPUTE*) et la vérification (*/CHECK*) de la signature des utilitaires sont consignés dans le journal des évènements des utilitaires **P5SECDB**, **P5SECFILE** et **P5SECREG**.

Calcul (*/COMPUTE*) : Nombre total d'enregistrements signés

Vérification (*/CHECK*) : Nombre total, Nombre OK, Nombre NOK

Lorsqu'au moins une erreur a été détectée via les utilitaires **P5SECFILE**, **P5SECDB** et **P5SECREG**, un fichier *XML* est créé et envoyé par E-mail.

Ce fichier *XML* est également disponible dans la *Log* de l'application.

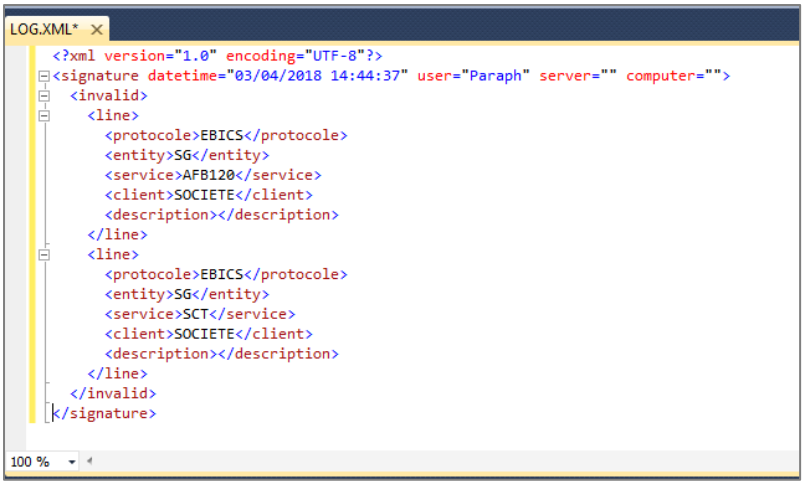


L'agent *Watch* notifie en temps réel les signatures incorrectes du registre et du site **Online Banking**.

Structure du fichier XML

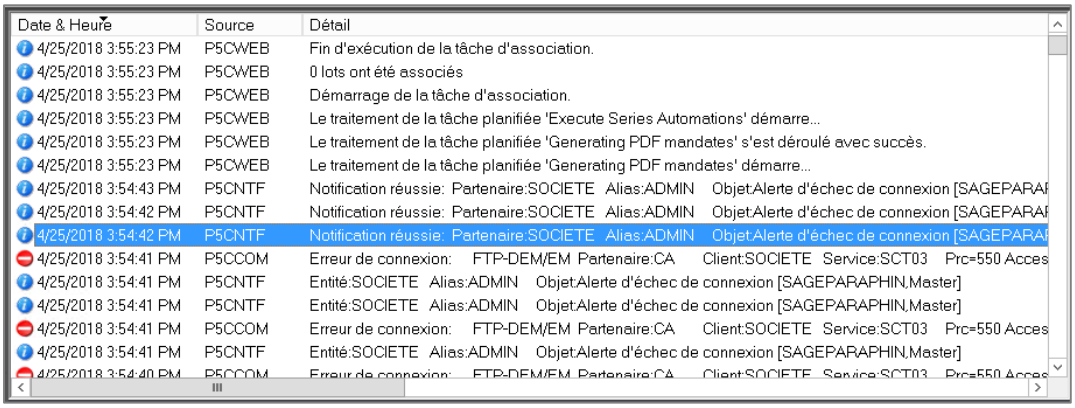
Ressources	Structure
En-tête	<?xml version="1.0" encoding="UTF-8"?> <signature datetime=" " user=" " computer="" server="">
P5SECFILE Check des binaires	<binarypath> <invalid> <line><filename>apifmt.exe</filename></line> <line><filename>audit.exe</filename></line> </invalid> </binarypath>
P5SECFILE Check du Site OnlineBanking et des scripts	<onlinebankingpath> <invalid> <line><filename>apifmt.exe</filename></line> <line><filename>audit.exe</filename></line> </invalid> </onlinebankingpath>
P5SECDB Check des contrats demandeurs	<invalid> <line><protocole></protocole><entity></entity><service></service><client> </client><description> </description></line> <line><protocole>FTP</protocole><entity>SAGE</entity><service>AFB160</service><client>SAG</client><description>Paiement</description></line> </invalid>
P5SECREG Check du registre	<SMP_P5 | COM | ISAPI | NTF| PDS| RCP| WEB > <invalid> <line><keyname>[Keyname]</keyname></line> <line><keyname>[Keyname]</keyname></line> </invalid> </SMP_P5 | COM | ISAPI | NTF| PDS| RCP| WEB >
Fin	</signature>

Exemple :



Audit des anomalies de connexion

Toutes les anomalies de connexion sont consignées dans le journal des évènements.



Date & Heure	Source	Détail
4/25/2018 3:55:23 PM	P5CWEB	Fin d'exécution de la tâche d'association.
4/25/2018 3:55:23 PM	P5CWEB	0 lots ont été associés
4/25/2018 3:55:23 PM	P5CWEB	Démarrage de la tâche d'association.
4/25/2018 3:55:23 PM	P5CWEB	Le traitement de la tâche planifiée 'Execute Series Automations' démarre...
4/25/2018 3:55:23 PM	P5CWEB	Le traitement de la tâche planifiée 'Generating PDF mandates' s'est déroulé avec succès.
4/25/2018 3:55:23 PM	P5CWEB	Le traitement de la tâche planifiée 'Generating PDF mandates' démarre...
4/25/2018 3:54:43 PM	P5CNTF	Notification réussie: Partenaire:SOCIETE Alias:ADMIN Objet:Alerte d'échec de connexion [SAGEPARAF
4/25/2018 3:54:42 PM	P5CNTF	Notification réussie: Partenaire:SOCIETE Alias:ADMIN Objet:Alerte d'échec de connexion [SAGEPARAF
4/25/2018 3:54:42 PM	P5CNTF	Notification réussie: Partenaire:SOCIETE Alias:ADMIN Objet:Alerte d'échec de connexion [SAGEPARAF
4/25/2018 3:54:41 PM	P5CCOM	Erreur de connexion: FTP-DEM/EM Partenaire:CA Client:SOCIETE Service:SCT03 Prc=550 Acces
4/25/2018 3:54:41 PM	P5CNTF	Entité:SOCIETE Alias:ADMIN Objet:Alerte d'échec de connexion [SAGEPARAPHIN,Master]
4/25/2018 3:54:41 PM	P5CNTF	Entité:SOCIETE Alias:ADMIN Objet:Alerte d'échec de connexion [SAGEPARAPHIN,Master]
4/25/2018 3:54:41 PM	P5CCOM	Erreur de connexion: FTP-DEM/EM Partenaire:CA Client:SOCIETE Service:SCT03 Prc=550 Acces
4/25/2018 3:54:41 PM	P5CNTF	Entité:SOCIETE Alias:ADMIN Objet:Alerte d'échec de connexion [SAGEPARAPHIN,Master]
4/25/2018 3:54:40 PM	P5CCOM	Erreur de connexion: FTP-DEM/EM Partenaire:CA Client:SOCIETE Service:SCT03 Prc=550 Acces

Droits Sage XRT Common Services sur l'onglet Intégrité

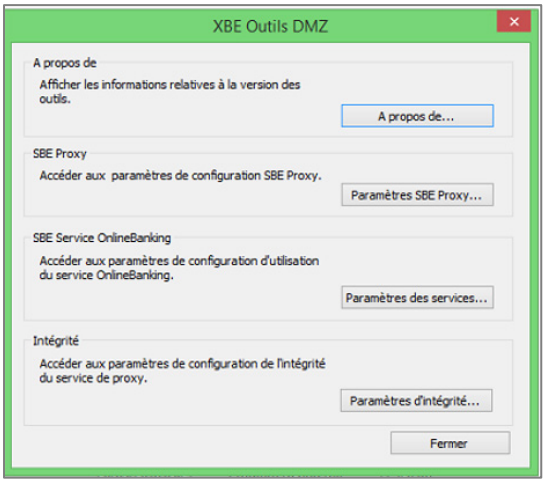
Le droit d'accès à l'onglet **Protection des données** du site *Master* est paramétrable dans **Sage XRT Common Services** au niveau des profils.

Dans l'onglet **Sage XRT Business Exchange**, développez l'arborescence jusqu'au niveau **Administration système – Droits spécifiques – Gestion de l'intégrité**.

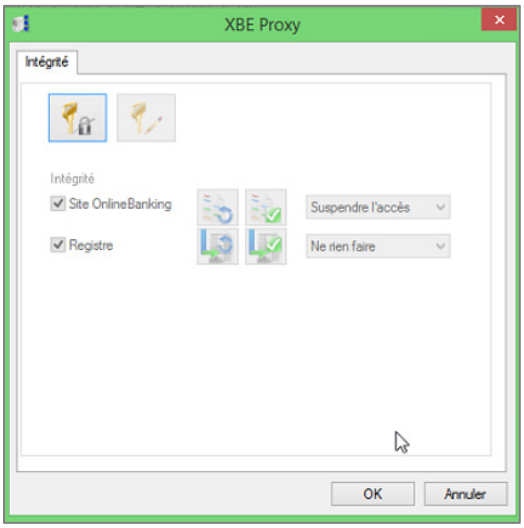
Intégrité des outils DMZ

Le contrôle de l'intégrité permet de calculer et de vérifier la signature du site **Online Banking** et du registre.

Le paramétrage du site **Online Banking** et du registre pour les outils *DMZ* est disponible dans l'interface du composant **dmztoolspanel.cpl**.



1. Dans la boîte de dialogue **XBE Outils DMZ**, cliquez sur **Paramètres d'intégrité...** pour ouvrir la boîte **XBE Proxy**.



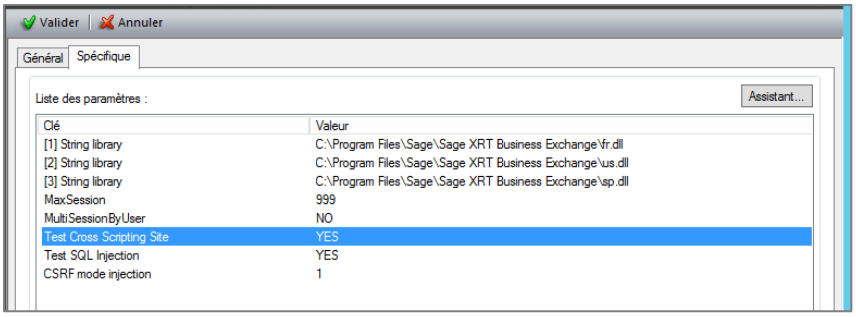
   Les informations relatives à l'intégrité sont consignées dans la *Log* système de **Windows** (observateur d'évènements).

2. Lors du premier accès, définissez un *passphrase*.

3. Dans la rubrique **Intégrité**, activez l'option **Site Online Banking** pour lancer automatiquement le calcul de la signature sur le site, puis sélectionnez une action dans la liste déroulante :
   - **Suspendre l'accès** : si l'intégrité n'est pas respectée, le site est suspendu.
   - **Ne rien faire** : si l'intégrité n'est pas respectée, les utilisateurs peuvent continuer leurs opérations. L'évènement est consigné dans la *Log* système de **Windows**.
4. Activez l'option **Registre** pour lancer automatiquement le calcul de la signature sur le registre, puis sélectionnez une action dans la liste déroulante :
   - **Suspendre l'accès** : si l'intégrité du registre n'est pas respectée, le site est suspendu.
   - **Ne rien faire** : si l'intégrité du registre n'est pas respectée, les utilisateurs peuvent continuer leurs opérations. L'événement est consigné dans la *Log* système de **Windows**.
   - **Arrêter le service** : si l'intégrité du registre n'est pas respectée, le service *Proxy* est arrêté. L'événement est consigné dans la *Log* système de **Windows**.

Notification de détection d'attaques

Des options sont disponibles pour activer les détections d'attaques *SQL Injection*, par *Cross Scripting Site* et *CSRF* sur le service de transaction.



Pour déclencher la notification par E-mail d'une attaque, un contrat de notification doit être renseigné au niveau de l'onglet **Intégrité** du site *Master*.

L'E-mail envoyé reprend les informations consignées :

- *SQL Injection et Cross Scripting* : Entité, Utilisateur, Variable et contenu des données insérées
- CSRF : Entité, Utilisateur

Objet E-mail : *Alerte de sécurité [Nom Machine, tenant physique (site, serveur)]*

Contenu : *Détection d'une probable attaque par [Nom de l'attaque] par la variable du formulaire [Nom du formulaire, description des données insérées] pour le contrat [Entité, Utilisateur, Service (Online Banking), Fonction (Online Banking)].*

Politique de sécurisation des headers http

Onlinebanking

Pour parer aux attaques possibles sur **OnlineBanking**, une politique de sécurisation a été mise en place dans le fichier **web.config** à la racine du site.

Retrait des informations identifiant le serveur IIS

<remove name="X-AspNet-Version" />

<remove name="X-Powered-By" />

<remove name="Server" />

Conservation des anciennes politiques pour compatibilité avec d'anciens navigateurs

Valeurs	Informations
<add name="X-XSS-Protection" value="1; mode=block" />	Cet en-tête protège votre page contre les attaques *XSS* réfléchi. Il a été remplacé par la directive *Content-Security-Policy* et n'est plus implémenté dans les versions modernes des navigateurs.
<add name="X-Frame-Options" value="SAMEORIGIN" />	Cet entête protège votre page contre son inclusion dans des *frames* ou *iframes*. Il a été remplacé par la directive *Content-Security-Policy* (équivalent à *frame-ancestors 'self'*) et n'est plus implémenté dans les versions modernes des navigateurs.
<add name="X-Content-Type-Options" value="nosniff" />	Cet entête protège contre la vulnérabilité de type *Mime Sniffing*.

Ajout des nouvelles politiques

Valeurs	Informations
<add name="Strict-Transport-Security" value="max-age=31536000; includeSubDomains; preload" />	Cet entête indique au navigateur que l'ensemble des ressources du domaine n'est accessible qu'en *https* et que toute tentative d'y accéder en *http* sera convertie en *https*. Pour plus d'informations sur cet entête, consultez la page : **https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security**
<add name="Content-Security-Policy" value="default-src 'none'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; connect-src 'self' https://127.0.0.1:48080; frame-src 'self'; font-src 'self' data:; img-src 'self' data:; object-src 'self'; frame-ancestors 'self'; base-uri 'self'; form-action 'self' https://id.sage.com" />	Cet entête permet de se protéger des attaques *XSS* (*Cross Scripting Site*) et de ses variantes. Il permet via les directives sources **-src* de : • spécifier le ou les domaines d'où peuvent provenir des ressources (script, style, etc.), • d'interdire ou non via la directive *frame-ancestors* l'intégration d'une page dans un autre site, d'autoriser la directive *base-uri* et sa localisation possible, • de contrôler via la directive *form-action* l'endroit où les données des formulaires peuvent être envoyées Suivant le déploiement nécessaire à votre client (utilisation d'une GED, Kibana, etc.), vous pouvez assouplir ces directives par défaut. Vous pouvez ajouter des exceptions aux directives ci-dessus, mais il est important de ne pas les supprimer. **default-src 'none'** : par défaut aucune ressource ne sera chargée. **script-src 'self' 'unsafe-eval' 'unsafe-inline'** : les scripts ne sont chargés que relativement à soi, autorise l'instruction *Eval*, autorise l'exécution de script *inline*. **style-src 'self' 'unsafe-inline' :** les styles ne sont chargés que relativement à soi, autorise la définition de style *inline* **connect-src 'self'** https://127.0.0.1:48080 : Connexion à des services REST ou autre relativement à soi, autorise la connexion à **SageEIDSign** (peut être retiré si le service de signature n'est pas déployé) **frame-src 'self'** : l'insertion dans des *frames/iframes* n'est autorisé que pour des pages relatives à soi **font-src 'self' data** : le téléchargement des polices n'est autorisé que relativement à soi et via une directive *data* (nécessaire pour **Carbon**)

Valeurs	Informations
	img-src 'self' data : le téléchargement des images n'est autorisé que relativement à soi et via une directive *data* (nécessaire pour **Carbon**) **object-src 'self'** : l'utilisation des inclusions *<OBJECT>/<EMBED>/<APPLET>* n'est autorisée que relativement à soi (nécessaire uniquement pour les *widgets* de **SCS**). **frame-ancestors 'self'** : indique les containers possibles des pages, seulement soi **base-uri 'self'** : l'instruction *<BASE>* ne peut pointer que sur soi. **form-action 'self'** https://id.sage.com**"** : les données des formulaires ne peuvent être envoyées qu'à soi, autorisation de redirection sur le site de production de **SageID** (peut être supprimé si **SageID** n'est pas utilisé). Pour plus d'informations sur cet entête, consultez la page : **https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP**
<add name="permissions-policy" value="accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()" />	Cet entête contrôle l'utilisation de dispositifs physiques permettant d'obtenir des informations diverses. Toute tentative d'utilisation de la caméra, de la géolocalisation, etc. est interdite sur le site **OnlineBanking**. Pour plus d'informations sur cet entête, consultez la page : **https://developer.mozilla.org/en-US/docs/Web/HTTP/Feature_Policy**
<add name="referrer-policy" value="strict-origin-when-cross-origin" />	Cet entête contrôle la quantité d'informations du référent qui sera incluse dans la requête. *strict-origin-when-cross-origin* : Envoie l'origine, le chemin et les paramètres de requête pour les requêtes de même origine. Pour plus d'informations sur cet entête, consultez la page : **https://developer.mozilla.org/fr/docs/Web/HTTP/Headers/Referrer-Policy**

Service REST de production

Pour parer aux attaques possibles sur le service **REST Rapi**, une politique de sécurisation a été mise en place dans la variable *HKEY_LOCAL_MACHINE\SOFTWARE\XRT\SMP_P5<.site>\RAPI\Spec\CustomHeaders*.

Valeurs	Informations
"Cache-Control no-cache,no-store,must-revalidate"	Cet entête indique au *proxy* de ne pas mettre en cache le résultat |*Content-Security-Policy default-src 'self' 'unsafe-inline'; object-src 'none'; frame-ancestors 'none'*
"Strict-Transport-Security max-age=31536000; includeSubDomains; preload"	Cet entête indique au navigateur que l'ensemble des ressources du domaine n'est accessible qu'en *https* et que toute tentative d'y accéder en *http* sera convertie en *https*. Pour plus d'information sur cet entête, consultez la page : **https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security**
"Content-Security-Policy default-src 'self' 'unsafe-inline'; object-src 'none'; frame-ancestors 'none'"	Cet entête permet de se protéger des attaques *XSS* (*Cross Scripting Site*) et de ses variantes. **default-src 'self' 'unsafe-inline'** : les ressources relatives à soi peuvent être chargées + les *inlines* (si la documentation *SWAGGER* n'est pas autorisée, la valeur peut être définie par *'none'*) **object-src 'none'** : l'utilisation des inclusions *<OBJECT>/<EMBED>/<APPLET>* n'est pas autorisée **frame-ancestors 'none'** : n'autorise pas l'inclusion dans des *containers* Pour plus d'informations sur cet entête, consultez la page : **https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP**
Politique *Cross-Origin Resource Sharing* (CORS)	Par défaut le service *REST* de **SXBE** autorise : • toutes les origines : il est possible de changer ce comportement en modifiant le contenu de la variable *"HKEY_LOCAL_MACHINE\SOFTWARE\XRT\SMP\P5<.site>\RAPI\Spec\corsAllowOrigins"* • tous les *headers* • les méthodes *GET*, *POST*, *OPTIONS* uniquement • le support des *credentials*

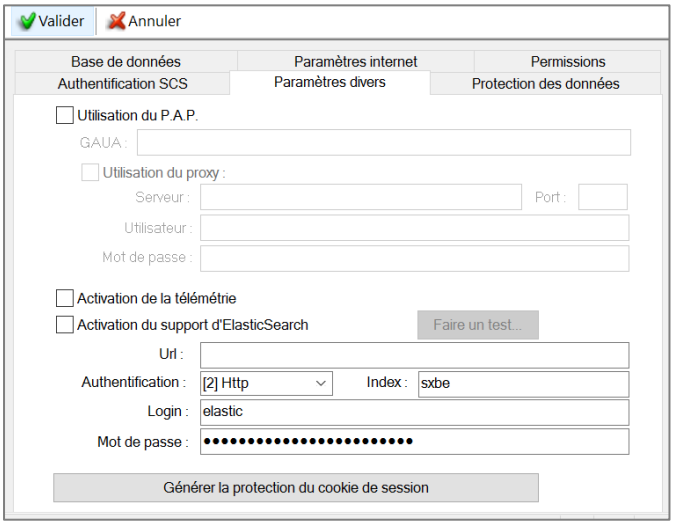
Autres politiques de sécurité

Support de la sécurisation SameSite

Sur **Online Banking**, le *cookie* de session est sécurisé grâce à l'instruction **SameSite**. Cet attribut permet de limiter les risques liés aux attaques de type *CSRF* (*Cross-Site Request Forgery*) et *XSSI* (*Cross-Site Script Inclusion*).

Protection du cookie de session

Activez le chiffrement *AES 256* du *cookie* de session en cliquant sur le bouton **Générer la protection du cookie de session** dans l'onglet **Paramètres divers** du site *Master*. Vous devez redémarrer le service de transaction et le site *IIS* pour finaliser cette activation.



XML EXternal Entity

Pour se protéger des attaques *XML EXternal Entity (XXE)*, consistant à l'envoi d'un fichier malveillant à destination d'un analyseur *XML*, la librairie **libxml2** a été mise à jour et les différentes *CVE (Common Vulnerabilities and Exposures)* référencées ont été amendées.

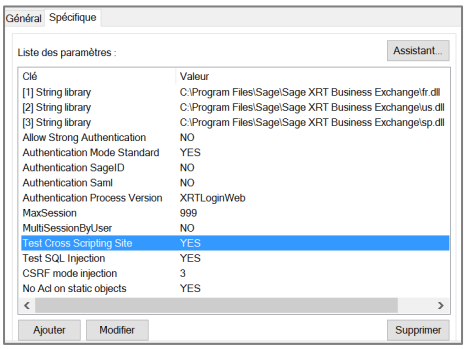
Protection contre les attaques

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 qui peut 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 pointant 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.

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 également être défini.

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

Périodicité d'accès des connexions

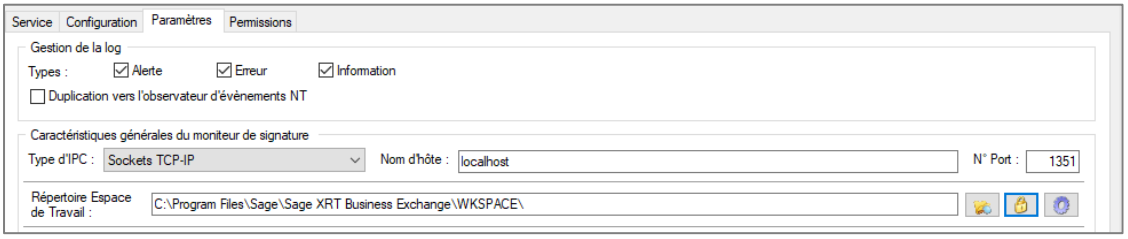
Vous pouvez définir une périodicité d'accès par protocole pour limiter les connexions des flux.

Un calendrier d'accès est disponible pour les protocoles.

Workspace

Les données du répertoire **Workspace** sont scellées avec l'algorithme *SHA256* et chiffrées en *AES 256*.

Des droits d'accès à ce répertoire peuvent être paramétré sur le service de **Signature**.



Il est possible de déchiffrer les données du répertoire **Workspace** à l'aide de la commande **PDSCRYPT**.

Usage : PDSCRYPT {/D | /C | /S} [/SERVER:]	
/D	Déchiffrement du Workspace
/C	Chiffrement du Workspace
/S	Suppression des streams du Workspace (cache des fichiers)
/SERVER	Nom du site

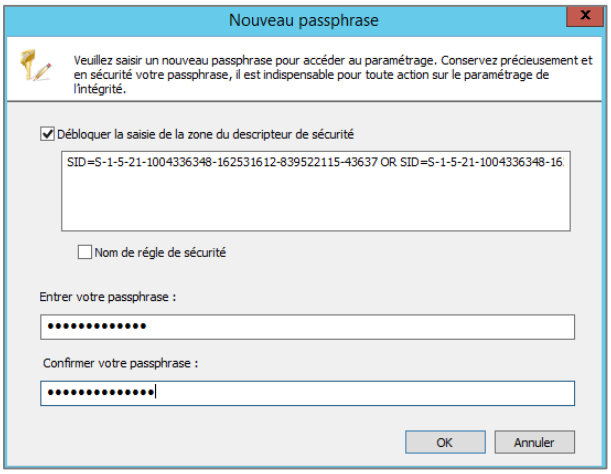
Important ! Vous devez avoir défini un *passphrase* dans l'onglet **Intégrité** pour déchiffrer ou chiffrer les données du répertoire **Workspace**.

Toutes les opérations sont consignées dans le journal des évènements.

Date & Heure	Source	Détail	Utilisateur	Ordinateur
08/08/2018 15:43:59	PDSCRYPT	Fin de l'opération de déchiffrement du Workspace du s...	HATOU	POXXXX
08/08/2018 15:43:59	PDSCRYPT	- Accès refusé.	HATOU	POXXXX
08/08/2018 15:43:56	PDSCRYPT	Début de l'opération de déchiffrement du WorkSpace ...	HATOU	POXXXX
08/08/2018 15:21:45	PDSCRYPT	Fin de l'opération de déchiffrement du Workspace du s...	HATOU	POXXXX
08/08/2018 15:21:39	PDSCRYPT	Début de l'opération de déchiffrement du WorkSpace ...	HATOU	POXXXX
08/08/2018 15:20:29	PDSCRYPT	Fin de l'opération de déchiffrement du Workspace du s...	HATOU	POXXXX
08/08/2018 15:20:23	PDSCRYPT	Début de l'opération de déchiffrement du WorkSpace ...	HATOU	POXXXX
08/08/2018 15:19:31	PDSCRYPT	Fin de l'opération de suppression des streams du Wor...	HATOU	POXXXX
08/08/2018 15:19:31	PDSCRYPT	Début de l'opération de suppression des streams du ...	HATOU	POXXXX
08/08/2018 15:17:21	PDSCRYPT	Fin de l'opération de chiffrement du Workspace du ser...	HATOU	POXXXX
08/08/2018 15:17:21	PDSCRYPT	- Accès refusé.	HATOU	POXXXX
08/08/2018 15:17:14	PDSCRYPT	Début de l'opération de chiffrement du WorkSpace du ...	HATOU	POXXXX
08/08/2018 15:15:20	PDSCRYPT	Fin de l'opération de déchiffrement du Workspace du s...	HATOU	POXXXX
08/08/2018 15:15:07	PDSCRYPT	Début de l'opération de déchiffrement du WorkSpace ...	HATOU	POXXXX

Annexe

Exemple de paramétrage d'une politique de sécurité pour le champ du **Descripteur de Sécurité**



Politique de sécurité	Exemples
"LOCAL"	*LOCAL=logon* *LOCAL=user* *LOCAL=machine* ***logon**: protects to the current logon session, user will not be able to unprotect after logoff or reboot ;* ***user** : protects to the user on local machine, only this caller on the local machine will be able to unprotect;* ***Machine** : protects to Local Machine, all users on the local machine will be able to unprotect;*
"SID"	Autorise l'accès à l'objet pour l'utilisateur 1 ou l'utilisateur 2 **Utilisateur 1** SID=S-1-5-21-1004336348-162531612-XXXXXXX-43637 **Utilisateur 2** SID=S-1-5-21-1004336348-162531612-XXXXXXXX- Valeur : SID= SID=S-1-5-21-1004336348-162531612-XXXXXXX-43637 OR SID=S-1-5-21-1004336348-162531612-XXXXXXXX-
"SDDL"	Le *SDDL* est un langage permettant de protéger une ressource par un descripteur de sécurité Windows. ***Policy: Allow Execute to Everyone if both of the following conditions are met:*** *Title = PM* *Division = Finance or Division = Sales* Valeur : SDDL=D:(XA; ;FX;;;S-1-1-0; (@User.Title=="PM" && (@User.Division=="Finance" || @User.Division ==" Sales")))

Politique de sécurité	Exemples
	Policy: Allow execute if any of the user's projects intersect with the file's projects. Valeur : SDDL=D:(XA; ;FX;;;S-1-1-0; (@User.Project Any_of @Resource.Project)) ***Policy: Allow read access if the user has logged in with a smart card, is a backup operator, and is connecting from a machine with Bitlocker enabled.*** Valeur : SDDL=D:(XA; ;FR;;;S-1-1-0; (Member_of {SID(Smartcard_SID), SID(BO)} && @Device.Bitlocker))
"CERTIFICATE"	CERTIFICATE=HashId:4DA11316E5943B27454001515BB0C8DC1BFDC347 CERTIFICATE=HashId:%HexValue% ou %HexValue% is hex-encoded SHA1 thumbprint of the certificate CERTIFICATE=CertBlob:%Base64String% ou %Base64String% is base64-encoded certificate blob

Avertissement

Les informations relatives au Règlement Général de Protection des Données (ci-après RGPD) fournies par Sage sont de nature générale et communiquées à titre informatif. Elles ne constituent pas un avis professionnel ou juridique. Sage ne saurait garantir qu'une information communiquée reproduise exactement une règlementation ou un texte législatif adopté officiellement. En cas de désaccord, le texte du journal officiel prévaut.

Bien que nous ayons fait notre possible pour nous assurer que les informations fournies soient exactes et à jour, les informations sont données telles quelles sans aucune garantie, explicite ou implicite. Sage n'assume aucune responsabilité pour toute erreur ou omission et n'est pas tenue responsable des dommages (y compris, entre autres, les dommages relatifs à la perte de clients ou de bénéfices) découlant de l'utilisation de ces informations ou de toute mesure ou décision prise en conséquence de l'utilisation de ces informations.

Nos produits intègrent des fonctions facilitatrices visant à accompagner l'utilisateur dans sa démarche de mise en conformité au RGPD. Toutefois, nous attirons l'attention des utilisateurs quant au fait que la seule utilisation des produits n'est pas de nature à garantir leur conformité au RGPD.

Nous rappelons que les informations communiquées ne dispensent pas l'utilisateur des produits Sage de consulter un conseil juridique afin d'obtenir toutes informations utiles relatives au RGPD et de s'y conformer.