



# Sage XRT Business Exchange

Version 12.3

## Paramétrage de la Sécurité



# Sommaire

<b>Description .....</b>	<b>4</b>
<b>Intégrité et sécurité .....</b>	<b>5</b>
Paramétrage de l'onglet Intégrité du site Master .....	5
Première activation de l'intégrité.....	5
Paramétrage des options de l'intégrité.....	7
Modification du paramétrage de l'intégrité.....	9
Modification du passphrase .....	10
Utilitaires de calcul et de vérification des signatures.....	11
Anomalies de connexion .....	14
Impacts .....	15
Données signées.....	15
Tables impactées .....	15
Export/Import du paramétrage.....	16
Notifications .....	16
Description des alertes .....	17
Audits.....	18
Audit Utilisateur Sage XRT Common Services .....	18

Audit de l'intégrité des données .....	18
Audit des anomalies de connexions .....	20
Droits Sage XRT Common Services sur l'onglet Intégrité .....	21
<b>Intégrité des outils DMZ .....</b>	<b>22</b>
<b>Notifications des détections d'attaques .....</b>	<b>24</b>
<b>Workspace .....</b>	<b>25</b>
<b>Annexe .....</b>	<b>26</b>
<b>Avertissement.....</b>	<b>28</b>

## Description

Pour renforcer la sécurité de l'application, l'onglet Intégrité de l'administration système vous permet de paramétrer différentes options :

- l'intégrité calcule une signature sur les champs des contrats bancaires (Intégrité BDD), les clés de registre (Intégrité Registre), sur les fichiers de l'application Online Banking (Intégrité Site Online Banking), sur les scripts (intégrité des scripts) et sur les fichiers du Vfs (intégrité du Vfs)
- l'anomalie sur les contrats vous permet de détecter les ruptures d'intégrité survenues par intrusion
- l'anomalie de connexions des contrats bancaires permet de détecter les échecs de connexions et de suspendre les contrats bancaires demandeurs
- le contrat de notification vous permet de définir l'entité et l'alias de notification pour toutes les anomalies d'intégrité, de connexions, d'attaques *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 **Intégrité** ne sera pas accessible sur les sites dérivés.

## Intégrité et sécurité

### Paramétrage de l'onglet Intégrité du site Master

Ce paramétrage permet de calculer et/ou 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* logue les intrusions non autorisées et notifie les administrateurs en cas de détection.

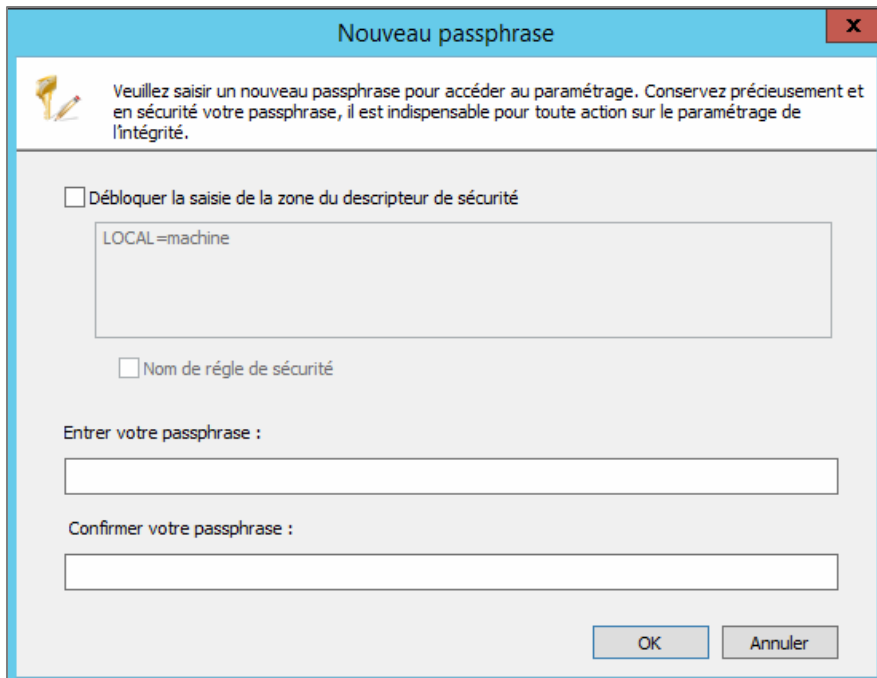
### Première activation de l'intégrité

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

Pour activer les options de paramétrage, il est nécessaire de 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. Par défaut le paramétrage est défini sur **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/hh769091(v=vs.85).aspx)  
[https://msdn.microsoft.com/fr-fr/library/windows/desktop/hh870248\(v=vs.85\).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 zones **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 égale à 2012.

Commande sous PowerShell pour obtenir la version :  
`[system.directoryservices.activedirectory.Forest]::GetCurrentForest().ForestMode`











**Important !** 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 de l'intégrité

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

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

Intégrité		
<input checked="" type="checkbox"/> Base de données		
<input checked="" type="checkbox"/> Site OnlineBanking		
<input checked="" type="checkbox"/> Vfs		
<input checked="" type="checkbox"/> Script		
<input checked="" type="checkbox"/> Registre		

Suspendre l'accès	▼
Ne pas démarrer le transfert	▼
Ne rien faire	▼
Ne rien faire	▼

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 renseigné, 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 est affiché : *"L'intégrité du site n'est plus assurée. Veuillez contacter d'urgence votre administrateur."*

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

**Important !** Si l'intégrité du site OnlineBanking est activé 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).

## Intégrité et sécurité

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 renseigné, 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 si ils sont stockés dans le répertoire \scripts de l'application SBE.

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 renseigné, 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 renseigné, 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 renseigné, l'administrateur est averti par E-mail de la corruption d'un ou plusieurs fichiers.

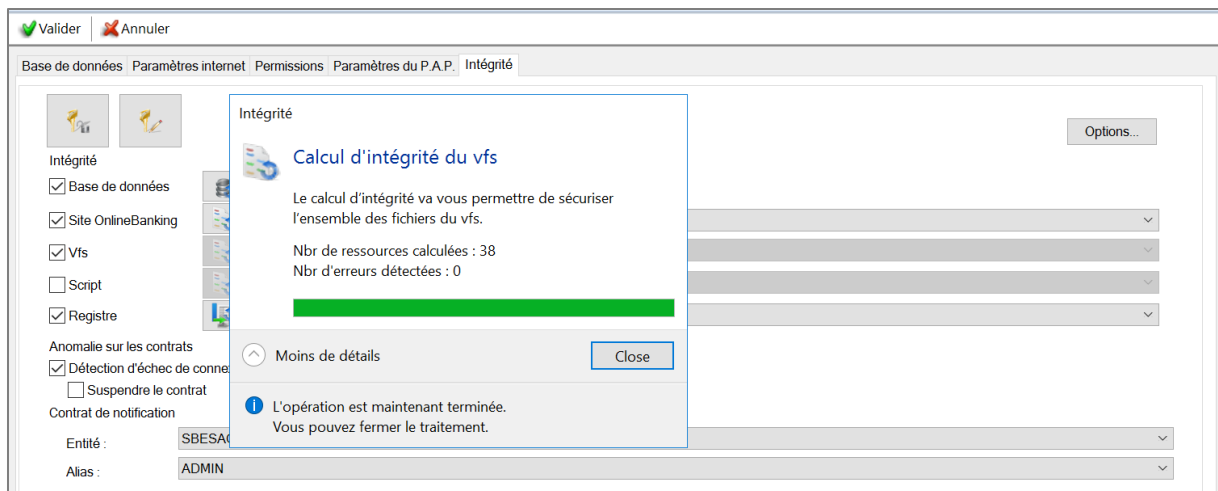
- **Suspendre l'accès**

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

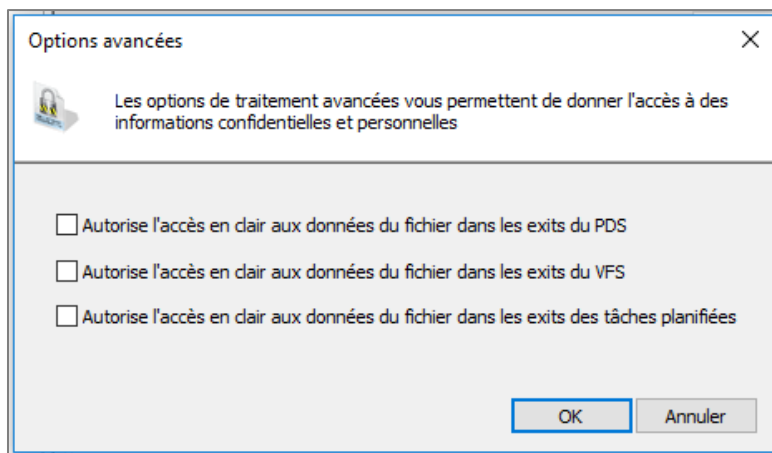
Dès que l'une des options **Base de données**, **Site onlineBanking**, **Script** ou **Registre** est sélectionnée, le calcul de la signature est automatiquement lancé.



## Intégrité et sécurité



Les options de traitements avancées vous permettent de donner les autorisations pour des traitements à des données confidentielles et personnelles.




## Modification du paramétrage de l'intégrité

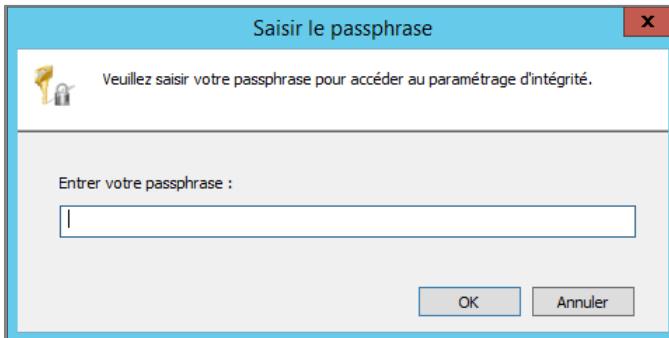
**Important !** Pour modifier le paramétrage, tous les services doivent être arrêtés.

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)

## Intégrité et sécurité

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

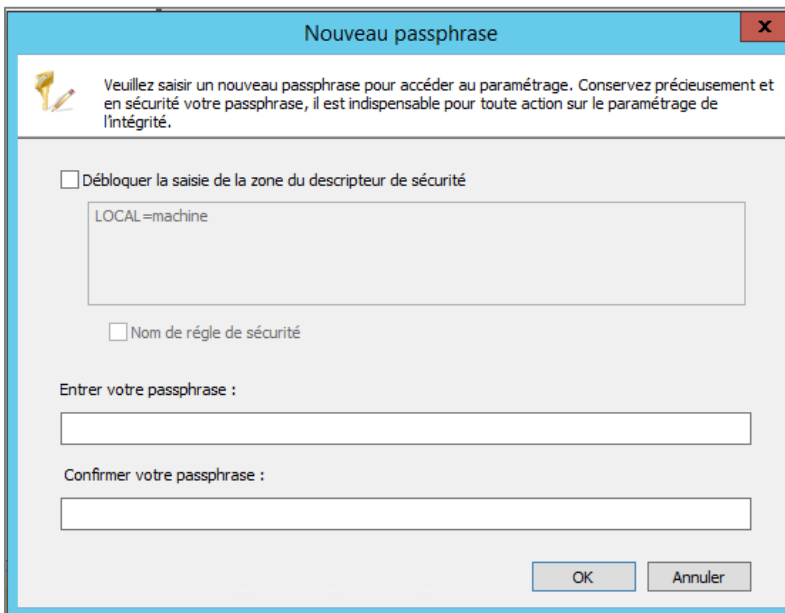


**Note :** Aucun recalcul n'est effectué lorsque l'option **Intégrité** est désactivée.

## 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 BDD des contrats demandeurs (P5SECDB)

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:]	
<i>/CHECK</i>	Vérification de la signature
<i>/COMPUTE</i>	Calcul de la signature
<i>/LOG</i>	Nom du fichier de rapport
<i>/P:</i>	Filtre entité
<i>/S:</i>	Filtre service
<i>/C :</i>	Filtre client
<i>/T:</i>	Filtre protocole
<i>/SERVER:</i>	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 (P5SECFILE)

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:]	
<i>/CHECKOLB</i>	Vérification de la signature des fichiers OnlineBanking
<i>/CHECKSCR</i>	Vérification de la signature des scripts
<i>/CHECKBIN</i>	Vérification de la signature des binaires de l'application
<i>/CHECKVFS</i>	Vérification de la signature des fichiers du Vfs
<i>/COMPUTEOLB</i>	Calcul de la signature des fichiers OnlineBanking
<i>/COMPUTESCR</i>	Calcul de la signature des scripts
<i>/COMPUTEVFS</i>	Calcul de la signature des fichiers du Vfs
<i>/LOG</i>	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 (P5SECREG)

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:]	
<i>/CHECK</i>	Vérification de la signature
<i>/COMPUTE</i>	Calcul de la signature
<i>/COMPUTER :</i>	Vérification du registre sur une autre machine (Nom Ordinateur)
<i>/LOG</i>	Nom du fichier de rapport
<i>/SERVER:</i>	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.

Lorsque cette option est sélectionnée, l'option **Suspendre le contrat** devient également accessible.

The screenshot shows a configuration window titled 'Anomalie sur les contrats'. It contains two checked checkboxes: 'Détection d'échec de connexion' and 'Suspendre le contrat'. Below these is a section 'Contrat de notification' with two dropdown menus: 'Entité' set to 'SOCIETE' and 'Alias' set to 'ADMIN'.

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

The screenshot shows a configuration window titled 'Paramétrage liaisons' with a 'Dispositif' tab selected. It contains several sections: 'Identité' with an 'Alias' field set to 'ext'; 'Informations' with a 'Libellé' field; 'Paramétrage relance' with three numeric input fields (all set to 0) for 'Nombre total de relances', 'Intervalle de retentative' (with 'minutes' unit), and 'Nombre de relances liaison principale'; and 'En cas d'échec' with two unchecked checkboxes for 'Emettre une alarme' and 'Démarrer l'exit de connexion'.

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.

The screenshot shows a configuration window titled 'Général' with tabs for 'Login', 'Ecriture', 'Lecture', 'Script', 'Enveloppe de sécurité', and 'Poste de signature'. The 'Général' tab is active. It contains several sections: 'Informations' with a 'Libellé' field set to 'SCT03' and a 'Propriétés avancées' button; 'Politique de sécurité' with a dropdown menu; 'Période de validité' with 'Date début' and 'Date fin' fields set to '4/ 6/2018' and '4/ 6/2028' respectively; 'Statut' with a checked checkbox for 'Service en opposition'; and 'Liaison' with a dropdown menu set to 'FTPLIAIS' and a play button.

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	
SMTPOP3MD	Contrat eMail	
X400MD	Contrat X400	
AS2MD	Contrat AS2	
SOAPMD	Contrat Soap	
PADEFMD	Contrat PaDeF	
SFTPMMD	Contrat Sftp	
EB3MD	Contrat Etebac3	
PTDMD	Contrat PeSIT D	
PTEMD	Contrat PeSIT E	
FTPMMD	Contrat Ftp	
EBICSMD	Contrat EBICS	
EBICSUSERS_DEM	Paramètre d'identification EBICS	
LIEN_NTW	Liaison	

## Intégrité et sécurité

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, le passphrase 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'identifications 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 devez renseigner une **Entité** et un **Alias**.

Contrat de notification	
Entité :	<input type="text" value="SOCIETE"/>
Alias :	<input type="text" value="ADMIN"/>

### 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.*

## Audits

### 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 événements des utilitaires *P5SECDB*, *P5SECFILE* et *P5SECREG*.

**Calcul** (*/COMPUTE*) : Nombre total d'enregistrement signé

**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.

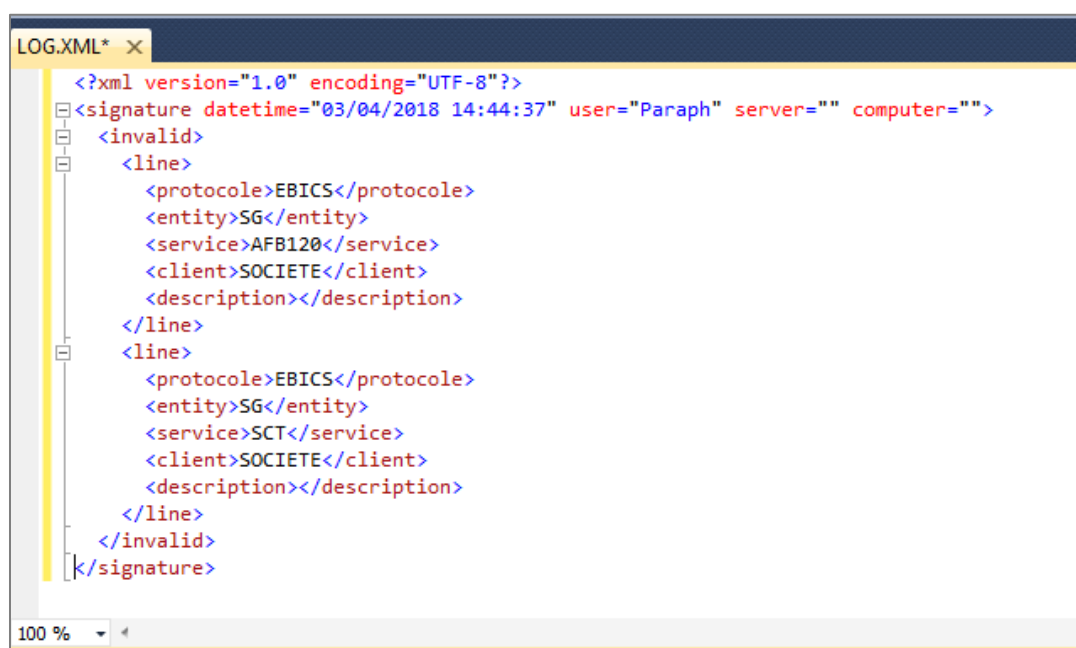
Date & Heure	Source	Détail	Information
4/3/2018 2:44:37 PM	P5SECDB	Fin de l'opération de contrôle de la signature - (#Total:75,#Valides:73,#Invalides:2)	Détail de l'évènement
4/3/2018 2:44:37 PM	P5SECDB	Démarrage du contrôle de la signature...	Général
3/16/2018 1:51:14 PM	P5SECDB	Fin de l'opération de calcul de la signature - (#Total:75,#Signés:75,#Non signés:0)	Date : 4/3/2018 2:44:37 PM
3/16/2018 1:51:07 PM	P5SECDB	Démarrage du calcul de la signature...	Type : Warning
3/16/2018 1:50:56 PM	P5SECDB	Fin de l'opération de contrôle de la signature - (#Total:75,#Valides:75,#Invalides:0)	Ordinateur : SAGEPARAPHIN
3/16/2018 1:50:56 PM	P5SECDB	Démarrage du contrôle de la signature...	Source : P5SECDB
3/5/2018 3:36:12 PM	P5SECDB	Fin de l'opération de calcul de la signature - (#Total:74,#Signés:67,#Non signés:7)	Utilisateur : Paraph
3/5/2018 3:35:42 PM	P5SECDB	Démarrage du calcul de la signature...	Réf. Interne :
3/5/2018 3:20:38 PM	P5SECDB	Fin de l'opération de calcul de la signature - (#Total:74,#Signés:67,#Non signés:7)	Réf. Externe :
3/5/2018 3:20:27 PM	P5SECDB	Démarrage du calcul de la signature...	Description : Fin de l'opération de contrôle de la signature - (#Total:75,#Valides:73,#Invalides:2)
3/5/2018 3:01:57 PM	P5SECDB	Fin de l'opération de contrôle de la signature - (#Total:74,#Valides:74,#Invalides:0)	
3/5/2018 3:01:56 PM	P5SECDB	Démarrage du contrôle de la signature...	
3/5/2018 3:01:40 PM	P5SECDB	Fin de l'opération de calcul de la signature - (#Total:74,#Signés:67,#Non signés:7)	
3/5/2018 3:01:30 PM	P5SECDB	Démarrage du calcul de la signature...	

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	<pre>&lt;?xml version="1.0" encoding="UTF-8"?&gt;  &lt;signature datetime=" " user=" " computer="" server=""&gt;</pre>
P5SECFILE Check des binaires	<pre>&lt;binarypath&gt;      &lt;invalid&gt;          &lt;line&gt;&lt;filename&gt;apifmt.exe&lt;/filename&gt;&lt;/line&gt;          &lt;line&gt;&lt;filename&gt;audit.exe&lt;/filename&gt;&lt;/line&gt;      &lt;/invalid&gt;  &lt;/binarypath&gt;</pre>
P5SECFILE Check du Site OnlineBanking et des scripts	<pre>&lt;onlinebankingpath&gt;      &lt;invalid&gt;          &lt;line&gt;&lt;filename&gt;apifmt.exe&lt;/filename&gt;&lt;/line&gt;          &lt;line&gt;&lt;filename&gt;audit.exe&lt;/filename&gt;&lt;/line&gt;      &lt;/invalid&gt;  &lt;/onlinebankingpath&gt;</pre>
P5SECDB Check des contrats demandeurs	<pre>&lt;invalid&gt;      &lt;line&gt;&lt;protocole&gt;&lt;/protocole&gt;&lt;entity&gt;&lt;/entity&gt;&lt;service&gt; &lt;/service&gt;&lt;client&gt; &lt;/client&gt;&lt;description&gt; &lt;/description&gt;&lt;/line&gt;      &lt;line&gt;&lt;protocole&gt;FTP&lt;/protocole&gt;&lt;entity&gt;SAGE&lt;/entity&gt;&lt;service&gt;AFB 160&lt;/service&gt;&lt;client&gt;SAG&lt;/client&gt;&lt;description&gt;Palement&lt;/description&gt;&lt;/line&gt;  &lt;/invalid&gt;</pre>
P5SECREG Check du registre	<pre>&lt;SMP_P5   COM   ISAPI   NTF  PDS  RCP  WEB &gt;      &lt;invalid&gt;          &lt;line&gt;&lt;keyname&gt;[Keyname]&lt;/keyname&gt;&lt;/line&gt;          &lt;line&gt;&lt;keyname&gt;[Keyname]&lt;/keyname&gt;&lt;/line&gt;      &lt;/invalid&gt;  &lt;/SMP_P5   COM   ISAPI   NTF  PDS  RCP  WEB &gt;</pre>
Fin	<pre>&lt;/signature&gt;</pre>

Exemple :



```
<?xml version="1.0" encoding="UTF-8"?>
<signature datetime="03/04/2018 14:44:37" user="Paraph" server="" computer="">
  <invalid>
    <line>
      <protocole>EBICS</protocole>
      <entity>SG</entity>
      <service>AFB120</service>
      <client>SOCIETE</client>
      <description></description>
    </line>
    <line>
      <protocole>EBICS</protocole>
      <entity>SG</entity>
      <service>SCT</service>
      <client>SOCIETE</client>
      <description></description>
    </line>
  </invalid>
</signature>
```

## Audit des anomalies de connexions

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

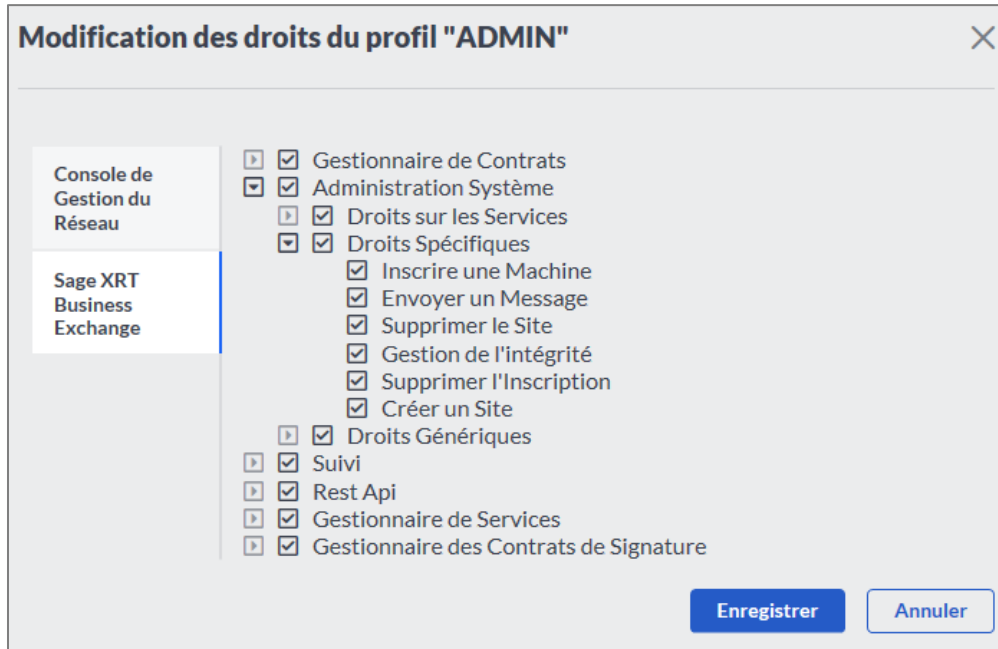
Date & Heure	Source	Détail
4/25/2018 3:55:23 PM	P5CWEB	Fin d'exécution de la tâche d'association.
4/25/2018 3:55:23 PM	P5CWEB	0 lots ont été associés
4/25/2018 3:55:23 PM	P5CWEB	Démarrage de la tâche d'association.
4/25/2018 3:55:23 PM	P5CWEB	Le traitement de la tâche planifiée 'Execute Series Automations' 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 **Intégrité** 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**.

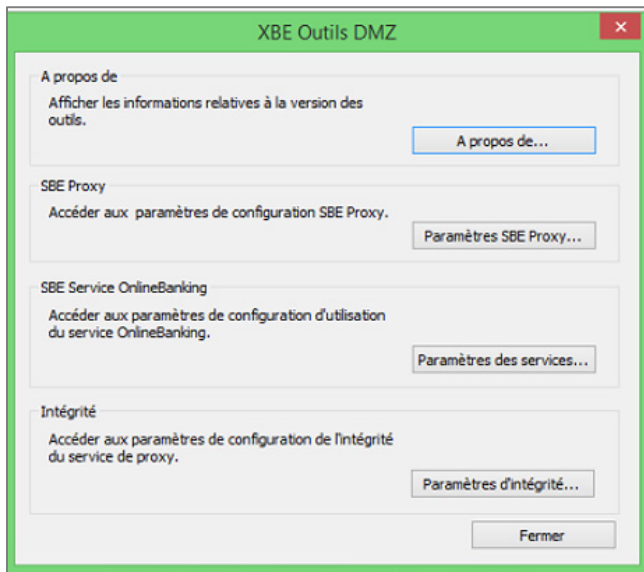


## Intégrité des outils DMZ

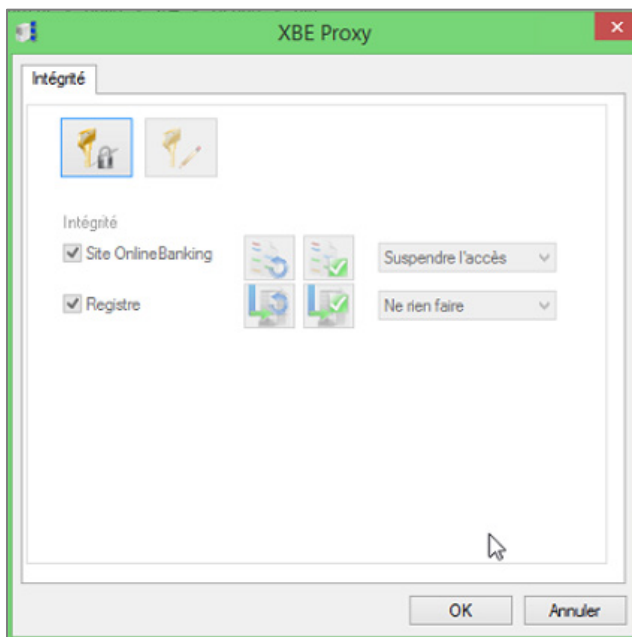
Le contrôle de l'intégrité permet de calculer et/ou de vérifier la signature :

- du site **OnlineBanking**
- 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**.



## Intégrité des outils DMZ

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'évènement 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'évènement est consigné dans la *Log* système de *Windows*.

# Notifications des détections 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.

The screenshot shows a configuration window titled 'Sage XRT Business Exchange' with two tabs: 'Général' and 'Spécifique'. The 'Spécifique' tab is active, displaying a table of parameters. The table has two columns: 'Clé' (Key) and 'Valeur' (Value). The parameters are as follows:

Clé	Valeur
[1] String library	C:\Program Files\Sage\Sage XRT Business Exchange\fr.dll
[2] String library	C:\Program Files\Sage\Sage XRT Business Exchange\us.dll
[3] String library	C:\Program Files\Sage\Sage XRT Business Exchange\sp.dll
MaxSession	999
MultiSessionByUser	NO
Test Cross Scripting Site	YES
Test SQL Injection	YES
CSRF mode injection	1

Buttons at the top include 'Valider' (green checkmark) and 'Annuler' (red X). An 'Assistant...' button is located in the top right corner of the parameter list area.

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).*

## Workspace

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

Des droits d'accès à ce répertoire sont paramétrables sur le service de signature.

The screenshot shows the 'Paramètres' (Parameters) tab of the Workspace configuration window. It includes sections for 'Gestion de la log' (Log Management) with checkboxes for 'Alerte', 'Erreur', and 'Information', and 'Caractéristiques générales du moniteur de signature' (General characteristics of the signature monitor) with fields for 'Type d'IPC' (set to 'Sockets TCP-IP'), 'Nom d'hôte' (set to 'localhost'), and 'N° Port' (set to '1351'). At the bottom, there is a field for 'Répertoire Espace de Travail' (Working Space Directory) set to 'C:\Program Files\Sage\Sage XRT Business Exchange\WKSPACE\'. There are also icons for help, save, and refresh.

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 événements.

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**

**Nouveau passphrase**

Veillez saisir un nouveau passphrase pour accéder au paramétrage. Conservez précieusement et en sécurité votre passphrase, il est indispensable pour toute action sur le paramétrage de l'intégrité.

☒ Débloquer la saisie de la zone du descripteur de sécurité

SID=S-1-5-21-1004336348-162531612-839522115-43637 OR SID=S-1-5-21-1004336348-16

☐ Nom de règle de sécurité

Entrer votre passphrase :

.....

Confirmer votre passphrase :

.....

OK Annuler

Politique de sécurité	Exemples
"LOCAL"	<p>LOCAL=logon</p> <p>LOCAL=user</p> <p>LOCAL=machine</p> <p><b>logon</b>: protects to the current logon session, user will not be able to unprotect after logoff or reboot ;</p> <p><b>user</b> : protects to the user on local machine, only this caller on the local machine will be able to unprotect;</p> <p><b>Machine</b> : protects to Local Machine, all users on the local machine will be able to unprotect;</p>
"SID"	<p>Autorise l'accès à l'objet pour l'utilisateur 1 ou l'utilisateur 2</p> <p><b>Utilisateur 1</b> SID=S-1-5-21-1004336348-162531612-XXXXXXX-43637</p> <p><b>Utilisateur 2</b> SID=S-1-5-21-1004336348-162531612-XXXXXXX-</p> <p>Valeur : SID= SID=S-1-5-21-1004336348-162531612-XXXXXXX-43637</p> <p>OR SID=S-1-5-21-1004336348-162531612-XXXXXXX-</p>



Politique de sécurité	Exemples
"SDDL"	<p>Le SDDL est un langage permettant de protéger une ressource par un descripteur de sécurité Windows.</p> <p><b>Policy: Allow Execute to Everyone if both of the following conditions are met:</b></p> <p>Title = PM</p> <p>Division = Finance or Division = Sales</p> <p>Valeur : SDDL=D:(XA; ;FX;;;S-1-1-0; (@User.Title=="PM" &amp;&amp; (@User.Division=="Finance"    @User.Division == " Sales")))</p> <p><b>Policy: Allow execute if any of the user's projects intersect with the file's projects.</b></p> <p>Valeur : SDDL=D:(XA; ;FX;;;S-1-1-0; (@User.Project Any_of @Resource.Project))</p> <p><b>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.</b></p> <p>Valeur : SDDL=D:(XA; ;FR;;;S-1-1-0; (Member_of {SID(Smartcard_SID), SID(BO)} &amp;&amp; @Device.Bitlocker))</p>
"CERTIFICATE"	<p>CERTIFICATE=HashId:4DA11316E5943B27454001515BB0C8DC1BFDC347</p> <p>CERTIFICATE=HashId:%HexValue%</p> <p>ou %HexValue% is hex-encoded SHA1 thumbprint of the certificate</p> <p>CERTIFICATE=CertBlob:%Base64String%</p> <p>ou %Base64String% is base64-encoded certificate blob</p>

## 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 réglementation 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.