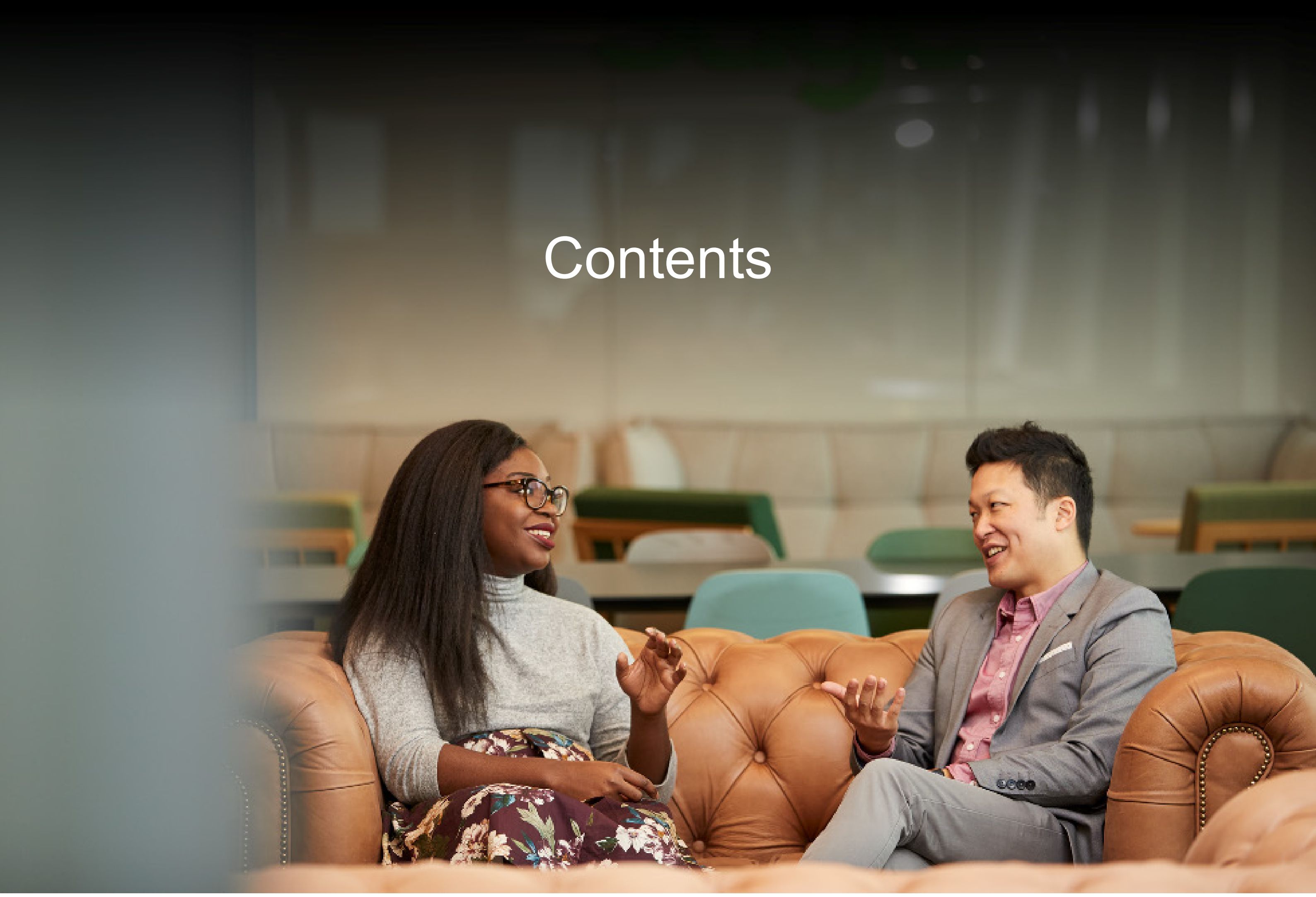
sage

Sage XRT Business Exchange

Version 12.2

Security Setup

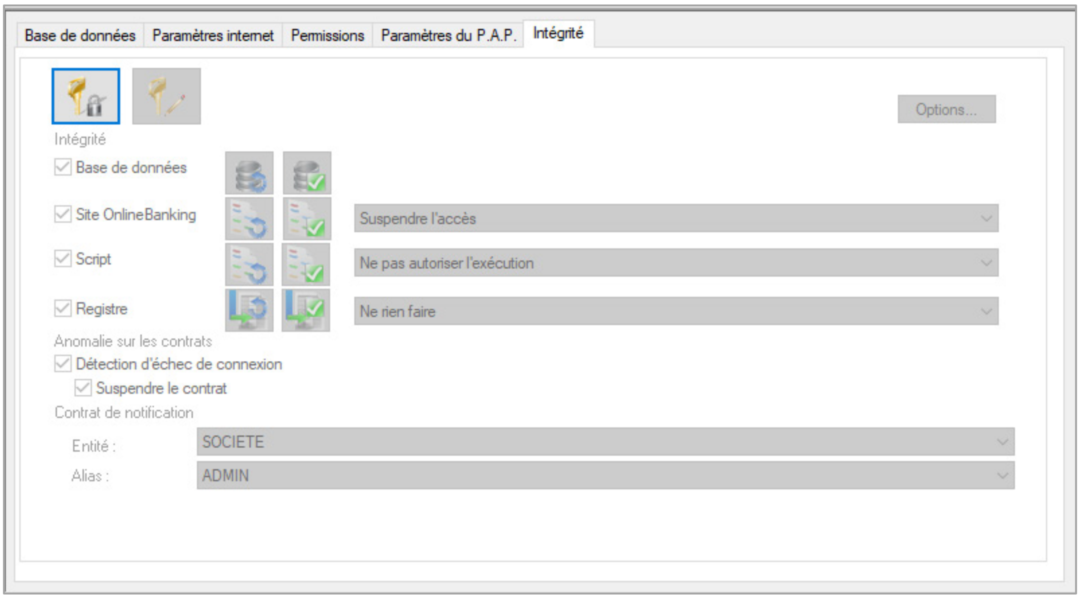


Contents

Description

To further strengthen the application security, the **Integrity** tab in of the system administration enables the setup of various options:

- Integrity which calculates a signature for the bank contract fields (Database Integrity), the SXBE registry keys (Registry Integrity) and the Online Banking files (Online Banking Site Integrity).
- Errors on Contracts show the detection of integrity breach because of an intrusion.
- Error on Bank Contract Connections show the detection of connection failures and the suspension of the bank contracts.
- Notification Contracts enable the definition of the notification entity and alias for all integrity errors, connection errors, SQL Injection, Cross Scripting and CSRF (Cross-Site Request Forgery) attack errors.



Intégrité

☑ Base de données

☑ Site OnlineBanking — Suspendre l'accès

☑ Script — Ne pas autoriser l'exécution

☑ Registre — Ne rien faire

Anomalie sur les contrats

☑ Détection d'échec de connexion

☑ Suspendre le contrat

Contrat de notification

Entité : SOCIETE

Alias : ADMIN

Important! In multisite mode, the derived sites inherit from the master site's setup. The **Integrity** tab is not available on the derived sites.

Integrity and Security

Setting up Master Site Integrity Tab

This setup enables the calculation and/or verification of the signature for:

- the database (requestor contracts)
- the **Online Banking** site
- scripts
- the registry (SXBE registry keys)

When activating integrities, watch agents check in real time:

- **Create**, **Change**, **Rename** and **Delete** actions on every file in the **Online Banking** directory.
- all interventions on the registry keys in SXBE

Watch agents log every non-authorized intrusion and notify administrators of it.

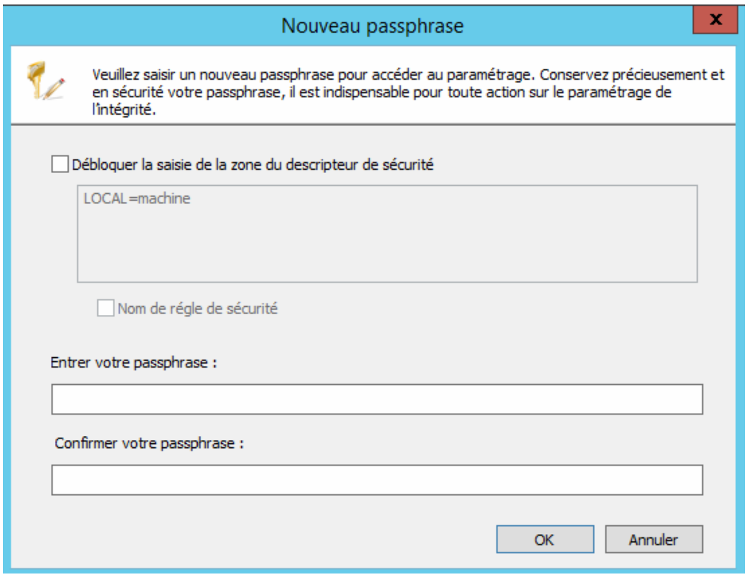
Integrity First Activation

All Sage XRT Business Exchange services must be stopped.

To enable the setup options, you need to specify a passphrase.

Important! Please keep this passphrase safe. You need it for each integrity modification. In case of loss, you must re-install the whole application.

Click the lock icon to open the passphrase creation window.



Nouveau passphrase

Veuillez 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

LOCAL=machine

□ Nom de régle de sécurité

Entrer votre passphrase :

Confirmer votre passphrase :

Enable the Security Descriptor field: This option secures the access to the passphrase key. The default setup is ***LOCAL=MACHINE***.

Note: To find out more on the syntax of Security Descriptors authorized for this field, refer to Microsoft documentation:
https://msdn.microsoft.com/en-us/library/cc230368.aspx
https://msdn.microsoft.com/en-us/library/windows/desktop/hh769091(v=vs.85).aspx
https://msdn.microsoft.com/en-us/library/windows/desktop/hh870248(v=vs.85).aspx

Please refer to the Appendices for setup examples.

Enter and confirm the passphrase in **Enter your Passphrase** and **Confirm your Passphrase**.

Important!

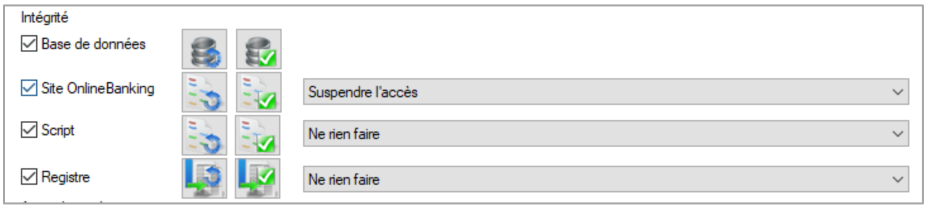
Protecting the safe with more than two *SID* will require to use an *AD* (*Active Directory*) with at least a 2012-compatible forest. To know the version you are using, type the following command in *PowerShell*:
[system.directoryservices.activedirectory.Forest]::GetCurrentForest().ForestMode

To activate the **Integrity** setup options for the database, **OnlineBanking** site and **Sage XRT Business Exchange** registry in *Windows* registry, the passphrase must be specified.

Defining Integrity Options

The integrity check can be activated for the following elements:

- **Database**
- **Online Banking Site**
- **Script**
- **Registry**



Intégrité

☑ Base de données

☑ Site OnlineBanking — Suspendre l'accès

☑ Script — Ne rien faire

☑ Registre — Ne rien faire

The calculation buttons (in the first icon column) enable the signature calculation.

The verification buttons are used to check the signature.

Note: The services must be stopped to enable the buttons and the options.

If you enable the option **Site OnlineBanking**, select from the corresponding dropdown menu, the action to carry out in case of an integrity problem:

- **Do nothing**

  When notifications have been set up, the administrator is informed of the corruption of one or several files by e-mail. The activity on **Online Banking** site goes on.

- **Suspend access**

  If a single file is corrupted in the application, **Online Banking** site is suspended and the following error message is displayed: "*The site integrity is no longer guaranteed. Please contact your administrator immediately*."
  When notifications have been set up, the administrator is informed of the corruption of one or several files by e-mail.

Important! If **OnlineBanking** site integrity is enabled and if the security descriptor is different from *LOCAL=MACHINE*, the identity of *IIS* application pool must be an AD account or a local account (and not a virtual one).

If you enable the **Script** option, select from the drop-down menu the action to be performed if an integrity issue is detected:

- **Do nothing**

  When notifications have been set up, the administrator is informed of the corruption of one or several files by email. The service goes on.

- **Do not authorize execution**

  The corrupted script is not executed.

Important! Scripts are signed and checked if they are stored in the folder for **Sage XRT Business Exchange** scripts.

You can change the folder through INSTALLSCRIPTS variable: // SCRIPTS LOCATION

Scripts are checked during the execution.

If you enable the **Registry** option, select from the drop-down menu the corresponding action to be performed if an integrity issue is detected.

- **Do nothing**

  When notifications have been set up, the administrator is informed of the corruption of one or several files by e-mail. The service goes on.

- **Stop service**

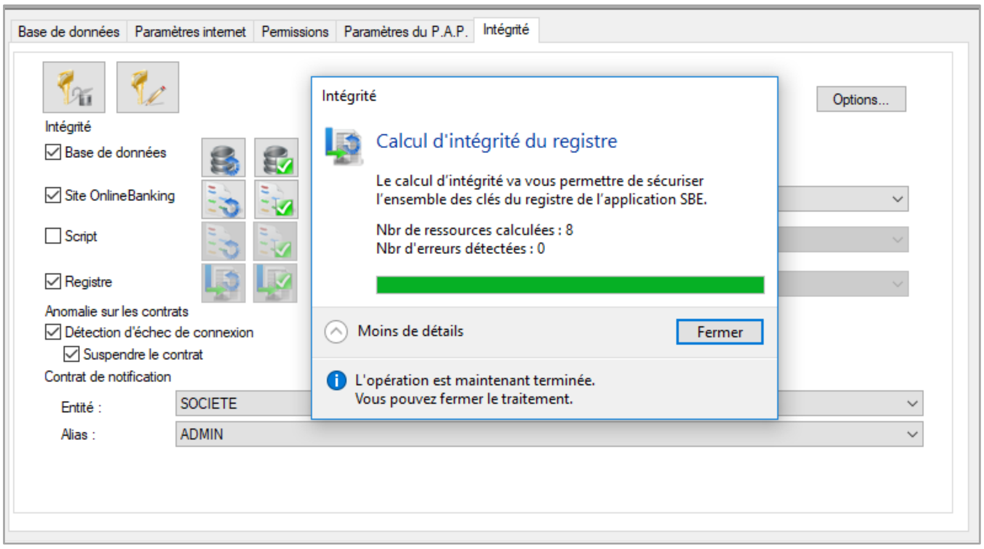
  The service is totally stopped. When notifications have been set up, the administrator is informed of the corruption of one or several files by e-mail.

- **Suspend access**

  The service is suspended. When notifications have been set up, the administrator is informed of the corruption by e-mail.

When you select one of the options **Database**, **OnlineBanking Site**, **Script** or **Registry**, the signature is automatically calculated.

Integrity and Security



Intégrité

☑ Base de données

☑ Site OnlineBanking

☐ Script

☑ Registre

Anomalie sur les contrats

☑ Détection d'échec de connexion

☑ Suspendre le contrat

Contrat de notification

Entité : SOCIETE

Alias : ADMIN

Intégrité

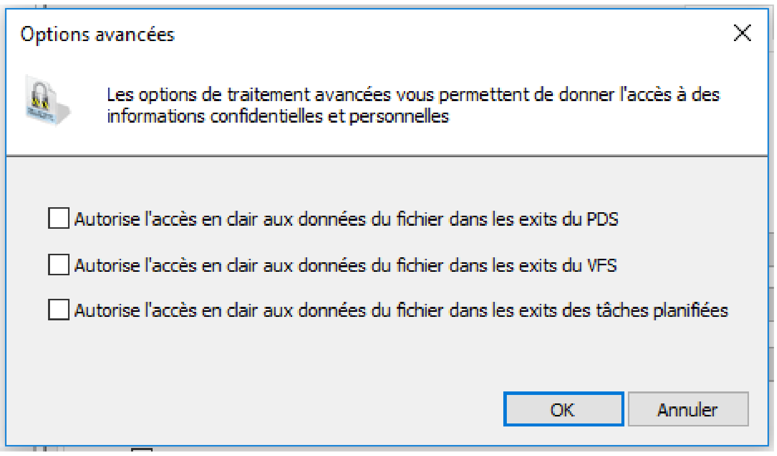
Calcul d'intégrité du registre

Le calcul d'intégrité va vous permettre de sécuriser l'ensemble des clés du registre de l'application SBE.

Nbr de ressources calculées : 8
Nbr d'erreurs détectées : 0

L'opération est maintenant terminée.
Vous pouvez fermer le traitement.

The advanced options enable you to grant access to personal and confidential data for further processing.



Options avancées

Les options de traitement avancées vous permettent de donner l'accès à des informations confidentielles et personnelles

☐ Autorise l'accès en clair aux données du fichier dans les exits du PDS

☐ Autorise l'accès en clair aux données du fichier dans les exits du VFS

☐ Autorise l'accès en clair aux données du fichier dans les exits des tâches planifiées

Modifying Integrity Options

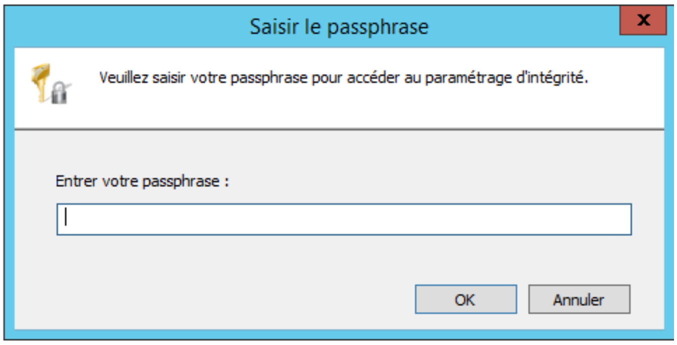
Important! All services must be stopped before modifying the setup.

Regarding the integrity check setup, you may modify the following elements:

- Disable signatures checks
- Recalculate signatures: **Calculation** (*/COMPUTE*)
- Check signature: **Verification** (*/CHECK*)

Integrity and Security

To modify the setup, click the lock icon and enter the passphrase in the new dialog box.



Saisir le passphrase

Veuillez saisir votre passphrase pour accéder au paramétrage d'intégrité.

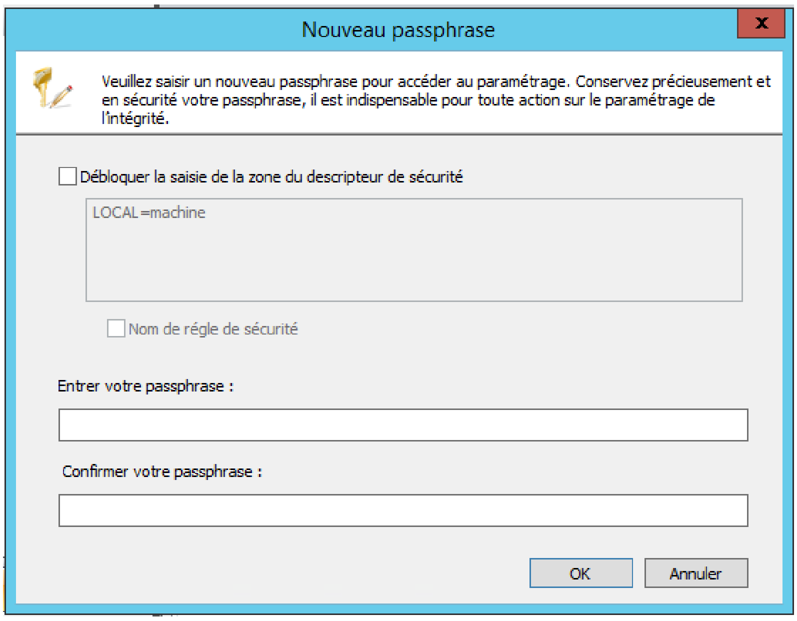
Entrer votre passphrase :

Note: No recalculation is performed when the **Integrity** option is disabled.

Modifying Passphrase

Important! All services must be stopped before modifying the passphrase.

Click **Modification** .



Nouveau passphrase

Veuillez 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

LOCAL =machine

□ Nom de régle de sécurité

Entrer votre passphrase :

Confirmer votre passphrase :

In the **New Passphrase** dialog box, enter the passphrase, confirm your entry, and click **OK**.

Note: If services are running,only the checking actions are available.

Calculating and Checking Tools for Signatures

Requestor Contracts Integrity for Database (P5SECDB)

P5SECDB is a tool that calculates and checks the consistency of the database for the requestor contracts.

This tool launches the **CHECK** command, if no other setup has been defined.

Usage: P5SECDB {/CHECK | /COMPUTE} [/P: /S: /C: /T: /LOG: /SERVER:]	
/CHECK	Signature check
/COMPUTE	Signature calculation
/LOG:	Log File name
/P:	Entity filter
/S:	Service filter
/C:	Client filter
/T:	Protocol filter
/SERVER:	Site name (enabling the recovery of resources associated with the site, eg.: DB)

Important! If any one of the requestor contract elements is incorrect, then you cannot use this contract.
Each attempt to use contract is logged in the audit.
The tool can be planned for the */CHECK* action. In case of integrity breach, the errors are compiled in an XML file sent through an email.

OnlineBanking Site and Scripts Integrity (P5SECFILE)

This P5SECFILE tool enables the calculation and verification of the signature for:

- Files from **OnlineBanking** website
- Scripts

All the files that constitute the site are controlled through an integrity check.

Usage: P5SECFILE {/CHECK | /COMPUTE} [/LOG:]	
/CHECKOLB	Control of the signature for OnlineBanking site files
/CHECKSCR	Control of the scripts signature
/CHECKBIN	Control of the signature for the Application binary files
/COMPUTEOLB	Calculation of the signature for OnlineBanking site files
/COMPUTESCR	Calculation of the scripts signature
/LOG:	Log File name

Important! The check is performed all over the **OnlineBanking** site before it is started. The start is aborted when corruption is detected.
The check can also be performed on the application binary files (*/CHECKBIN*).
The tool can be planned for the */CHECK* action. In case of integrity breach, the errors are compiled in an XML file sent through an email.

Registry Integrity (P5SECREG)

P5SECREG is a tool that calculates and checks the signature of the registry.

The signed and checked keys in the registry are the following:

- **SMP-P5** (and its multisite version)
- **AUTO**
- **COM**
- **ISAPI**
- **NTF**
- **PDS**
- **RCP**
- **WEB**

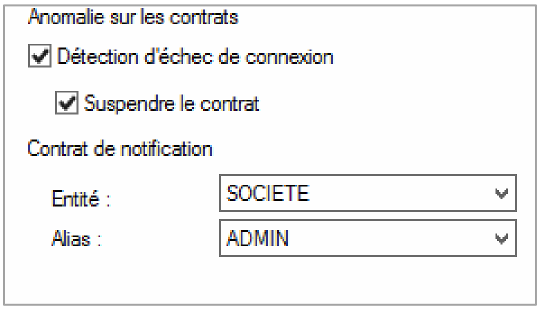
Usage: P5SECREG {/CHECK | /COMPUTE} [/LOG: /SERVER:]	
/CHECK	Signature check
/COMPUTE	Signature calculation
/COMPUTER :	Registry check on another station (Computer Name)
/LOG:	Log File name
/SERVER:	Site name

Important: The tool can be planned for the */CHECK* action. In case of integrity breach, the errors are compiled in an XML file sent through an email.

Connection Errors

In the **Error on Contracts** section, enable the **connection failure detection** option to log the logical or physical connection phases with errors on requestor bank contracts. These errors are notified.

When this option is selected, the **Suspend Contract** option becomes available.



Anomalie sur les contrats

☑ Détection d'échec de connexion

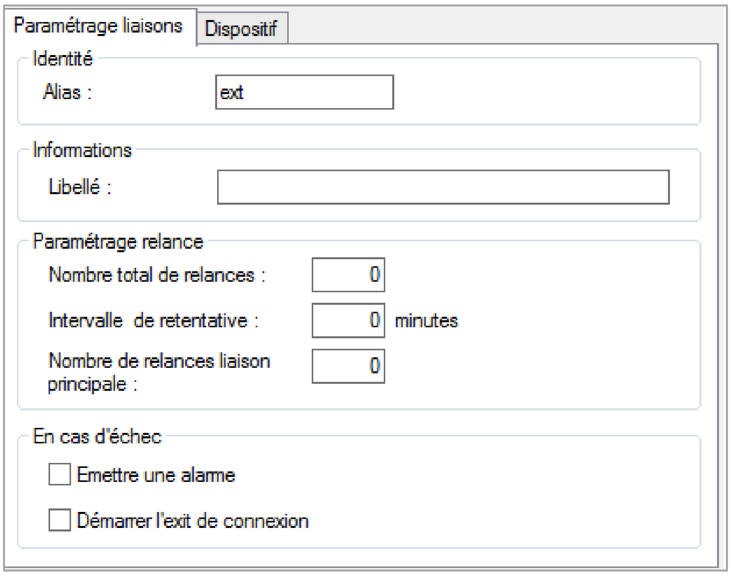
☑ Suspendre le contrat

Contrat de notification

Entité : SOCIETE

Alias : ADMIN

The bank contract is suspended when the total number of attempts specified in the setup for requestor contract link is reached.



Identité

Alias : ext

Informations

Libellé :

Paramétrage relance

Nombre total de relances : 0

Intervalle de retentative : 0 minutes

Nombre de relances liaison principale : 0

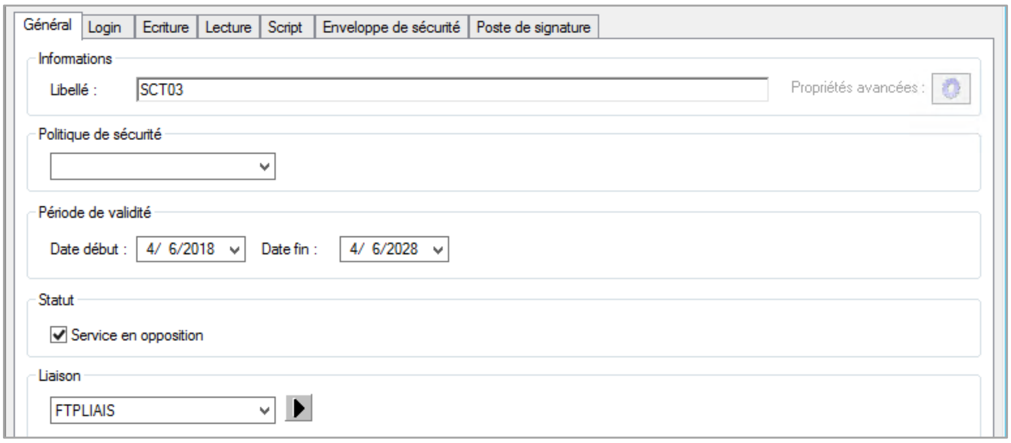
En cas d'échec

☐ Emettre une alarme

☐ Démarrer l'exit de connexion

After the contract suspension, no connection is possible without the administrator's intervention.

The option **Pause Access to Service** is enabled in the requestor contract.



Informations

Libellé : SCT03

Politique de sécurité

Période de validité

Date début : 4/ 6/2018 Date fin : 4/ 6/2028

Statut

☑ Service en opposition

Liaison

FTPLIAIS

If no new attempt has been specified, the contract is not suspended.

Consequences

Signed Data

All the data of the requestor contract are signed (including the Protocol link data and the **Network** setup from the **Device** tab) except for **Description** and **Advanced Properties**.

Affected Tables

Table	Description	Comment
HTTPMD	Http Contract	Adding column: HASHSIGNATURE varchar (255) NULL
OFTPMD	Odette FTP Contract	
SWIFTFTIMD	Swift Contract	
EXTMD	External Contract	
CPFMD	CopyFile Contract	
MOMMD	MsMQ Contract	
SMTPPOP3MD	Email Contract	
X400MD	X400 Contract	
AS2MD	AS2 Contract	
SOAPMD	Soap Contract	
PADEFMD	PaDeF Contract	
SFTPMD	Sftp Contract	
EB3MD	Etebac3 Contract	
PTDMD	PeSIT D Contract	
PTEMD	PeSIT E Contract	
FTPMD	Ftp Contract	
EBICSMD	EBICS Contract	
EBICSUSERS_DEM	EBICS ID setting	
LIEN_NTW	Link	
X25	Link / X25 Network Device	
TCPIP	Link / TCPIP Network Device	
ISDN	Link / ISDN Network Device	
PSN	Link / PSN Network Device	

Exporting/Importing Setup

If the **Database Integrity** option is enabled, the setup import performed from the graphical interface automatically calculates the signature hash.

The import through *IMPVIR* requires the passphrase entry.

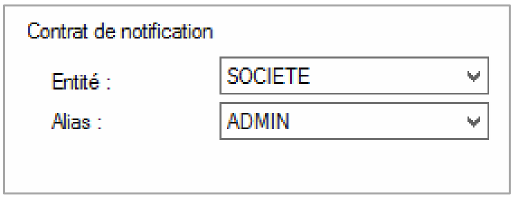
Conversely, it is not required for the setup export. The process is identical to *EXPVPS* one.

Important! The link info. or the identification setting data that are not linked to a bank contract are not signed (test data for example). They are included into the export.

Notifications

The notifications must be set up in the **Notification Contract** section in the **Integrity** tab of the Master site.

You must specify an **Entity** and an **Alias**.



Contrat de notification

Entité : SOCIETE

Alias : ADMIN

Alerts Description

Site Online Banking

- E-mail: *Online Banking Security Alert [Computer Name, Tenant (Site, Server)]*
- Contents: *OnlineBanking site is paused for intrusion detection. View log for more information...*

Script

- E-mail: *File Integrity Alert*
- Contents: *X/X invalid file(s). Check the details in the attached file.*

Bank Contract Data

- E-mail: *Database Integrity Alert*
- Contents: *X/X invalid record(s).*
  Check the details in the attached file.

Registry

- <u>E-mail</u>: *Registry Integrity Alert [Computer Name, Tenant (Site, Server)]*
- <u>Contents</u>: *An action has altered the integrity of the registry. Check the log file for more details...*

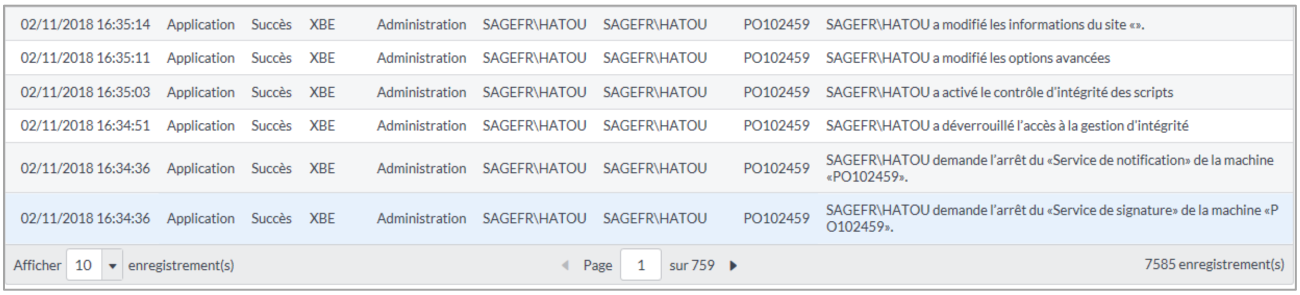
Connection failed

- <u>E-mail</u>: *Connection Failure Alert [Computer Name, Tenant (Site, Server)]*
- <u>Contents</u>: *Maximum connection attempts reached on Contract ENTITY, PROTOCOL, SERVICE, CLIENT. Contract suspended.*

Audits

Sage XRT Common Services User Audit

The **Security** tab setup is recapped in the **User Audit** of **Sage XRT Common Services**.



02/11/2018 16:35:14	Application	Succès	XBE	Administration	SAGEFR\HATOU	SAGEFR\HATOU	PO102459	SAGEFR\HATOU a modifié les informations du site «».
02/11/2018 16:35:11	Application	Succès	XBE	Administration	SAGEFR\HATOU	SAGEFR\HATOU	PO102459	SAGEFR\HATOU a modifié les options avancées
02/11/2018 16:35:03	Application	Succès	XBE	Administration	SAGEFR\HATOU	SAGEFR\HATOU	PO102459	SAGEFR\HATOU a activé le contrôle d'intégrité des scripts
02/11/2018 16:34:51	Application	Succès	XBE	Administration	SAGEFR\HATOU	SAGEFR\HATOU	PO102459	SAGEFR\HATOU a déverrouillé l'accès à la gestion d'intégrité
02/11/2018 16:34:36	Application	Succès	XBE	Administration	SAGEFR\HATOU	SAGEFR\HATOU	PO102459	SAGEFR\HATOU demande l'arrêt du «Service de notification» de la machine «PO102459».
02/11/2018 16:34:36	Application	Succès	XBE	Administration	SAGEFR\HATOU	SAGEFR\HATOU	PO102459	SAGEFR\HATOU demande l'arrêt du «Service de signature» de la machine «PO102459».

Data Integrity Audit

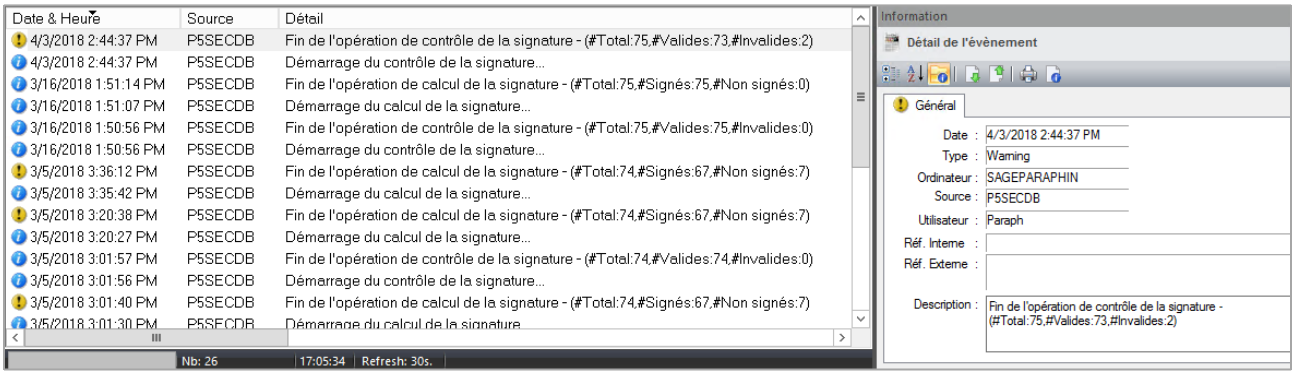
Calculation (*/COMPUTE*) and verification (*/CHECK*) for the tools signature are registered in the event log for the tools: *P5SECDB*, *P5SECFILE* and *P5SECREG*.

Calculation (*/COMPUTE*): Total number of signed records

Verification (*/CHECK*): Total number, OK number, NOK number

If any error is detected through the tools: *P5SECFILE*, *P5SECDB* and *P5SECREG*, an XML file is created and sent by e-mail.

This file is also available in the application Log.



Date & Heure	Source	Détail
! 4/3/2018 2:44:37 PM	P5SECDB	Fin de l'opération de contrôle de la signature - (#Total:75,#Valides:73,#Invalides:2)
i 4/3/2018 2:44:37 PM	P5SECDB	Démarrage du contrôle de la signature...
i 3/16/2018 1:51:14 PM	P5SECDB	Fin de l'opération de calcul de la signature - (#Total:75,#Signés:75,#Non signés:0)
i 3/16/2018 1:51:07 PM	P5SECDB	Démarrage du calcul de la signature...
i 3/16/2018 1:50:56 PM	P5SECDB	Fin de l'opération de contrôle de la signature - (#Total:75,#Valides:75,#Invalides:0)
i 3/16/2018 1:50:56 PM	P5SECDB	Démarrage du contrôle de la signature...
! 3/5/2018 3:36:12 PM	P5SECDB	Fin de l'opération de calcul de la signature - (#Total:74,#Signés:67,#Non signés:7)
i 3/5/2018 3:35:42 PM	P5SECDB	Démarrage du calcul de la signature...
! 3/5/2018 3:20:38 PM	P5SECDB	Fin de l'opération de calcul de la signature - (#Total:74,#Signés:67,#Non signés:7)
i 3/5/2018 3:20:27 PM	P5SECDB	Démarrage du calcul de la signature...
i 3/5/2018 3:01:57 PM	P5SECDB	Fin de l'opération de contrôle de la signature - (#Total:74,#Valides:74,#Invalides:0)
i 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)
i 3/5/2018 3:01:30 PM	P5SECDB	Démarrage du calcul de la signature

Nb: 26 | 17:05:34 | Refresh: 30s.

Information

Détail de l'évènement

! Général

Date : 4/3/2018 2:44:37 PM
Type : Warning
Ordinateur : SAGEPARAPHIN
Source : P5SECDB
Utilisateur : Paraph
Réf. Interne :
Réf. Externe :
Description : Fin de l'opération de contrôle de la signature - (#Total:75,#Valides:73,#Invalides:2)

The Watch agent notifies in real time the invalid signatures in the registry and **Online Banking** site.

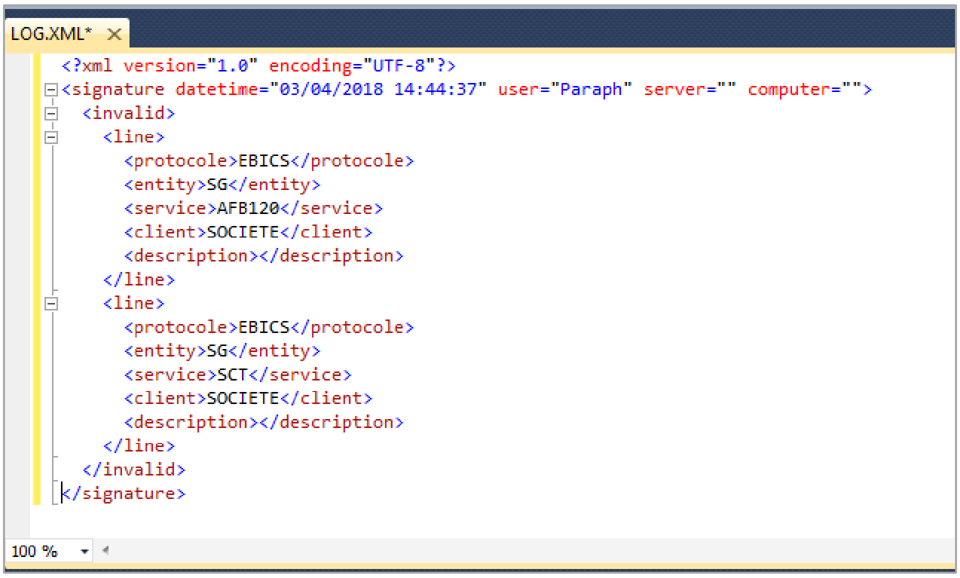
XML FILE STRUCTURE

Resources	Structure
Header	<?xml version="1.0" encoding="UTF-8"?> <signature datetime=" " user=" " computer="" server="">
P5SECFILE Binaries check	<binarypath> <invalid> <line><filename>apifmt.exe</filename></line> <line><filename>audit.exe</filename></line> </ invalid> </ binarypath>
P5SECFILE Check for OnlineBanking site and scripts	<onlinebankingpath> <invalid> <line><filename>apifmt.exe</filename></line> <line><filename>audit.exe</filename></line> </ invalid> </onlinebankingpath>

Integrity and Security

Resources	Structure
P5SECDB Requestor Contracts Check	<invalid> <line><protocole></protocole><entity></entity><service></service><client> </client><description> </description></line> <line><protocole>FTP</protocole><entity>SAGE</entity><service>AFB 160</service><client>SAG</client><description>Paiement</description></line> </ invalid>
P5SECREG Registry Check	<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 >
End	</signature>

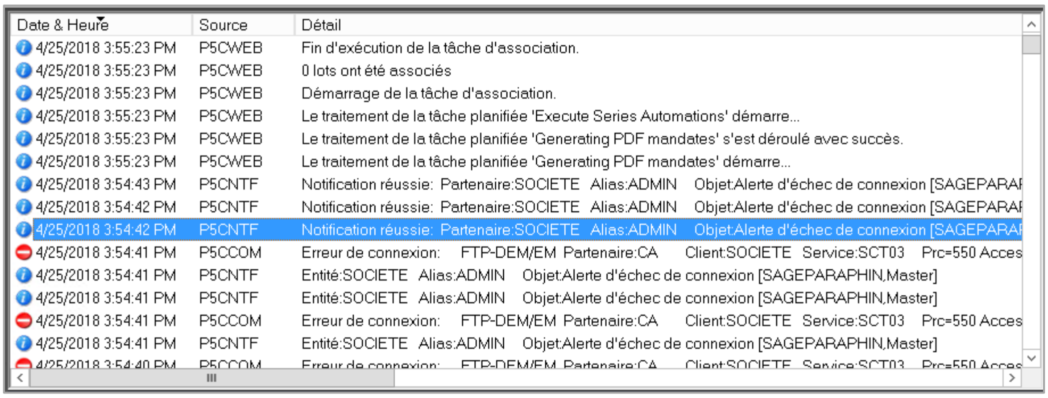
E.g.:



```
<?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>
```

Connection Errors Audit

Every connection error is registered in the event log.

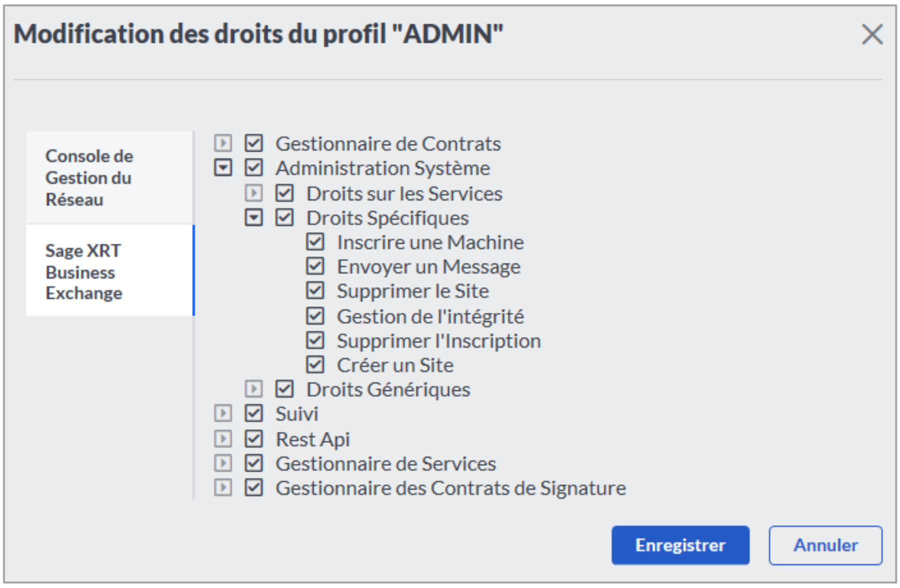


Date & Heure	Source	Détail
4/25/2018 3:55:23 PM	P5CWEB	Fin d'exécution de la tâche d'association.
4/25/2018 3:55:23 PM	P5CWEB	0 lots ont été associés
4/25/2018 3:55:23 PM	P5CWEB	Démarrage de la tâche d'association.
4/25/2018 3:55:23 PM	P5CWEB	Le traitement de la tâche planifiée 'Execute Series Automations' 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 [SAGEPARAI
4/25/2018 3:54:42 PM	P5CNTF	Notification réussie: Partenaire:SOCIETE Alias:ADMIN Objet:Alerte d'échec de connexion [SAGEPARAI
4/25/2018 3:54:42 PM	P5CNTF	Notification réussie: Partenaire:SOCIETE Alias:ADMIN Objet:Alerte d'échec de connexion [SAGEPARAI
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

Sage XRT Common Services Rights for Integrity Tab

The access right to the master site's **Integrity** tab must be set up in the profiles in **Sage XRT Common Services**.

In **Sage XRT Business Exchange** tab, expand the tree-view to **System Administration – Specific Rights – Integrity Management**.



Modification des droits du profil "ADMIN"

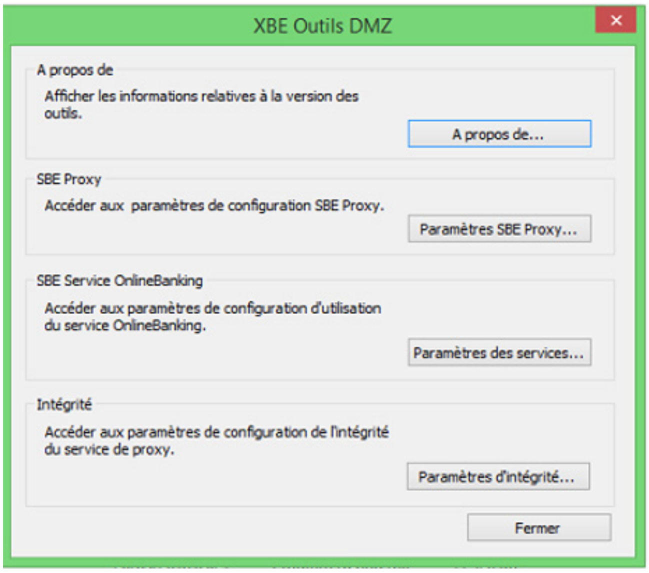
- ☑ Gestionnaire de Contrats
- ☑ Administration Système
  - ☑ Droits sur les Services
  - ☑ Droits Spécifiques
    - ☑ Inscrire une Machine
    - ☑ Envoyer un Message
    - ☑ Supprimer le Site
    - ☑ Gestion de l'intégrité
    - ☑ Supprimer l'Inscription
    - ☑ Créer un Site
  - ☑ Droits Génériques
- ☑ Suivi
- ☑ Rest Api
- ☑ Gestionnaire de Services
- ☑ Gestionnaire des Contrats de Signature

DMZ Tools Integrity

This check enables the calculation and/or verification of the signature for:

- **OnlineBanking** site
- **Registry**

The setups of **Online Banking** site and registry for DMZ tools can be accessed from the **dmztoolspanel.cpl** component interface.



XBE Outils DMZ

A propos de

Afficher les informations relatives à la version des outils.

SBE Proxy

Accéder aux paramètres de configuration SBE Proxy.

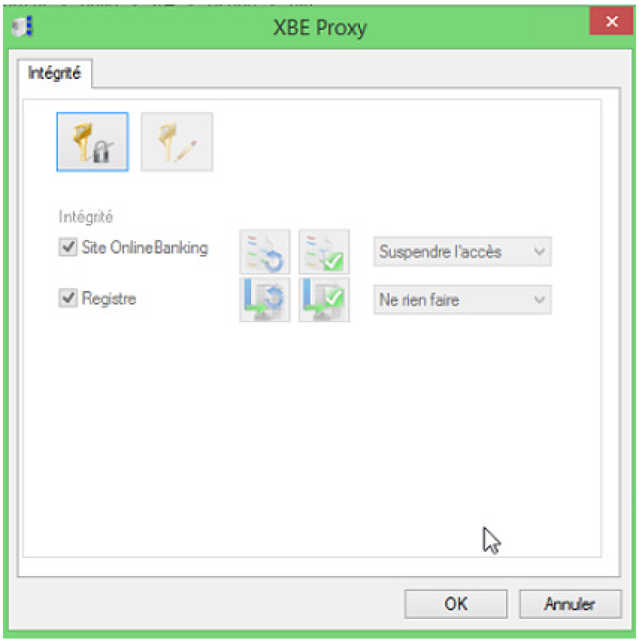
SBE Service OnlineBanking

Accéder aux paramètres de configuration d'utilisation du service OnlineBanking.

Intégrité

Accéder aux paramètres de configuration de l'intégrité du service de proxy.

1. In the **XBE DMZ Tools** dialog box, click **Integrity Parameters…** to open the **XBE Proxy** window.



XBE Proxy

Intégrité

Intégrité

☑ Site OnlineBanking — Suspendre l'accès

☑ Registre — Ne rien faire

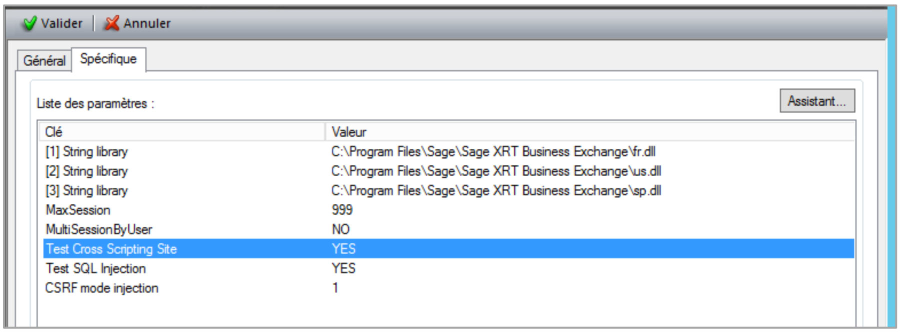
DMZ Tools Integrity

The data related to Integrity are logged in *Windows* Log (Event Observer).

2. Define a passphrase upon first connection.
3. In **Integrity**, enable the **Online Banking** option for the automatic calculation of the site signature, then select an action from the dropdown list:
   - **Suspend access**: if the integrity is compromised, the site is paused.
   - **Do nothing**: if the integrity is compromised, users may continue their activity. The event is logged in *Windows* log.
4. Activate the **Registry** options to launch the automatic calculation of Registry signature, then select one of the actions from the dropdown list:
   - **Suspend access**: if the Registry integrity is compromised, the site is paused.
   - **Do nothing**: if the Registry integrity is compromised, users may continue their activity. The event is logged in *Windows* log.
   - **Stop service**: if the Registry integrity is compromised, the Proxy service is paused. The event is logged in *Windows* log.

Attack Detection Notifications

Specific options help you detecting *SQL Injection* attacks through *Cross Scripting Site* and *CSRF* on the transaction service.



Liste des paramètres :

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

To implement the attack notification through e-mail, a notification contract must be set up in the **Integrity** tab of the master site.

This e-mail recaps the specified data:

- *SQL Injection* and *Cross Scripting*: Entity, User, Variable and content of the inserted data
- *CSRF*: Entity, User

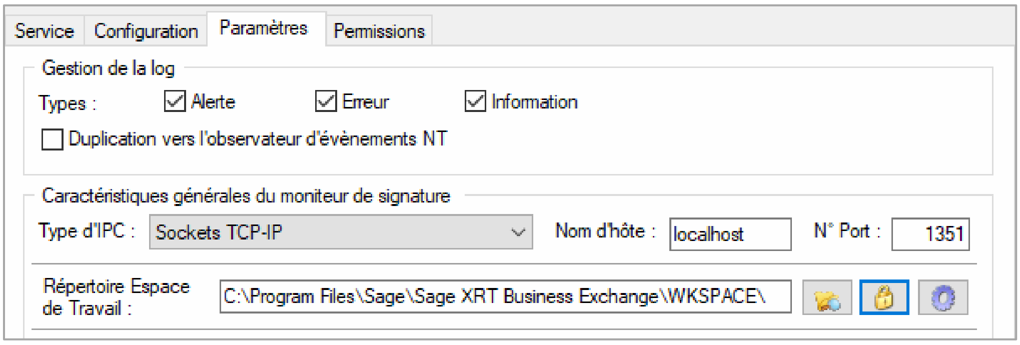
E-mail: *Integrity Alert [Computer Name, Tenant (Site, Server)]*

Contents: *Likely attack by **Attack Name** through **Form Name** form variable detected , **inserted data description** for the **Entity**, **User**, **Service** (Online Banking), **Function** (Online Banking) contract.*

Workspace

The data for **Workspace** directory are hashed with *SHA256* algorithm and encrypted in *AES 256*.

Access rights for this directory can be managed in the signature service.



Gestion de la log

Types : ☑ Alerte ☑ Erreur ☑ Information

□ Duplication vers l'observateur d'évènements NT

Caractéristiques générales du moniteur de signature

Type d'IPC : Sockets TCP-IP

Nom d'hôte : localhost

N° Port : 1351

Répertoire Espace de Travail : C:\Program Files\Sage\Sage XRT Business Exchange\WKSPACE\

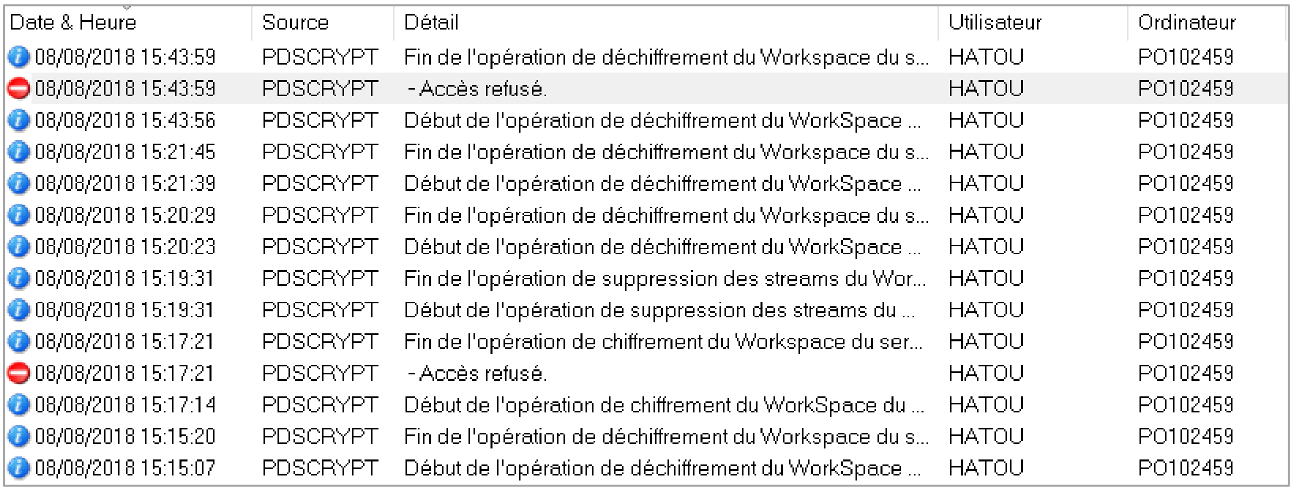
The *PDSCRYPT* command enables you to decrypt the data from the **Workspace** directory.

Usage: PDSCRYPT {/D | /C | /S} [/SERVER:]	
/D	Workspace Decryption
/C	Workspace Encryption
/S	Workspace Streams Deletion (files cache)
/SERVER	Site name

Important! A Passphrase must be specified in the **Integrity** tab in order to decrypt or encrypt the **Workspace** data.

Workspace

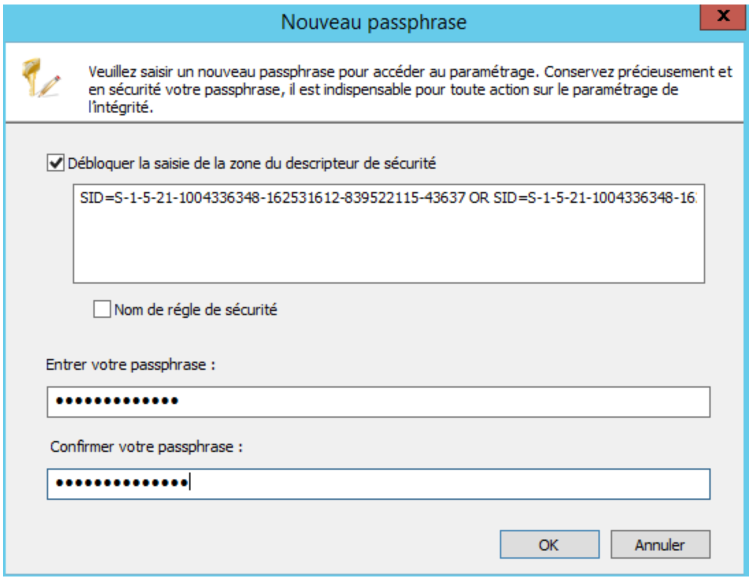
Every intervention is registered in the event log.



Date & Heure	Source	Détail	Utilisateur	Ordinateur
ⓘ 08/08/2018 15:43:59	PDSCRYPT	Fin de l'opération de déchiffrement du Workspace du s...	HATOU	PO102459
⛔ 08/08/2018 15:43:59	PDSCRYPT	- Accès refusé.	HATOU	PO102459
ⓘ 08/08/2018 15:43:56	PDSCRYPT	Début de l'opération de déchiffrement du WorkSpace ...	HATOU	PO102459
ⓘ 08/08/2018 15:21:45	PDSCRYPT	Fin de l'opération de déchiffrement du Workspace du s...	HATOU	PO102459
ⓘ 08/08/2018 15:21:39	PDSCRYPT	Début de l'opération de déchiffrement du WorkSpace ...	HATOU	PO102459
ⓘ 08/08/2018 15:20:29	PDSCRYPT	Fin de l'opération de déchiffrement du Workspace du s...	HATOU	PO102459
ⓘ 08/08/2018 15:20:23	PDSCRYPT	Début de l'opération de déchiffrement du WorkSpace ...	HATOU	PO102459
ⓘ 08/08/2018 15:19:31	PDSCRYPT	Fin de l'opération de suppression des streams du Wor...	HATOU	PO102459
ⓘ 08/08/2018 15:19:31	PDSCRYPT	Début de l'opération de suppression des streams du ...	HATOU	PO102459
ⓘ 08/08/2018 15:17:21	PDSCRYPT	Fin de l'opération de chiffrement du Workspace du ser...	HATOU	PO102459
⛔ 08/08/2018 15:17:21	PDSCRYPT	- Accès refusé.	HATOU	PO102459
ⓘ 08/08/2018 15:17:14	PDSCRYPT	Début de l'opération de chiffrement du WorkSpace du ...	HATOU	PO102459
ⓘ 08/08/2018 15:15:20	PDSCRYPT	Fin de l'opération de déchiffrement du Workspace du s...	HATOU	PO102459
ⓘ 08/08/2018 15:15:07	PDSCRYPT	Début de l'opération de déchiffrement du WorkSpace ...	HATOU	PO102459

Appendix

Example of security policy setup for the **Security Descriptor** field



Nouveau passphrase

Veuillez 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 régle de sécurité

Entrer votre passphrase : ••••••••••••••

Confirmer votre passphrase : •••••••••••••••

Security Policy	Examples

"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"	Grants access to this object for user 1 or user 2 **User 1** SID=S-1-5-21-1004336348-162531612-XXXXXXX-43637 **User 2** SID=S-1-5-21-1004336348-162531612-XXXXXXXX- Value: SID= SID=S-1-5-21-1004336348-162531612-XXXXXXX-43637 OR SID=S-1-5-21-1004336348-162531612-XXXXXXXX-

Appendix

Security Policy	Examples
"SDDL"	The security descriptor definition language (SDDL) protects a resource through a *Windows* security descriptor. **Policy: Allow Execute to Everyone if both of the following conditions are met:** Title = PM Division = Finance or Division = Sales Value: SDDL=D:(XA; ;FX;;;S-1-1-0; (@User.Title=="PM" && (@User.Division=="Finance" || @User.Division ==" Sales"))) **Policy: Allow execute if any of the user's projects intersect with the file's projects.** Value: 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.** Value: SDDL=D:(XA; ;FR;;;S-1-1-0; (Member_of {SID(Smartcard_SID), SID(BO)} && @Device.Bitlocker))

"CERTIFICATE"	CERTIFICATE=HashId:4DA11316E5943B27454001515BB0C8DC1BFDC347
	CERTIFICATE=HashId:%HexValue%
	or %HexValue% is hex-encoded SHA1 thumbprint of the certificate
	CERTIFICATE=CertBlob:%Base64String%
	or %Base64String% is base64-encoded certificate blob