



STR-iCT
Documentation utilisateur
Sonde AUDJRN
Version 1.0A



GAYTE.IT SAS – Siège : 46, le Villeret – 48170 St Jean la Fouillouse – RCS Mende 910 254 754 - Agence sud :
32 chemin Notre Dame – 34160 BEAULIEU

E-mail : commercial@gayte.it – <https://i.gayte.it> - Tél. 06 30 17 02 55



Notices

© I.GAYTE.IT 2022, 2023

Publié par :

Gayte.it SAS

46, le Villeret – 48170 St Jean la Fouillouse – France

Tél : +33 (0) 6 30 17 02 55

E-mail support : support@gayte.it

E-mail service commercial : commercial@gayte.it

Site Web : <https://i.gayte.it>

Titre : STR-ICT for EIM - Documentation utilisateur – Version 1.0A

Publication : Août 2023

Comité d'écriture et de lecture : Dominique GAYTE

Copyright :

STR-ICT for EIM, est une marque déposée de GAYTE.IT SAS.

I.GAYTE.IT est une marque déposée de GAYTE.IT SAS.

IBM i est une marque déposée d'IBM Corp.

Aucune partie de ce document ne peut être reproduite ou copiée, sous quelque forme que ce soit et quel qu'en soit le moyen, sans l'autorisation explicite de GAYTE.IT SAS.

Les informations contenues dans ce document sont conformes à l'état du produit au moment de sa publication. Cependant, GAYTE.IT SAS ne donne aucune garantie, explicite ou implicite, sur l'exactitude de ces informations et se réserve le droit de réviser ce document ou d'apporter des modifications aux produits décrits dans le présent document à tout moment sans préavis et sans obligation. GAYTE.IT SAS n'est pas responsable de toute perte de données ou de connexion, dommage aux bases de données ou autres logiciels, ou toute autre perte résultant de l'utilisation de ce manuel.



Table des matières

Notices.....	2
Table des matières	3
Introduction.....	5
Version IBM i	5
Bibliothèque	5
CCSID	5
Lexique	5
Concepts.....	6
Architecture de STR-ICT.....	6
SONDES.....	7
EXIT POINT(Optional)	7
Metrics ou Données Système.....	7
Interfaces.....	8
Les programmes IBM i.....	8
L'Interface Graphique.....	9
Se connecter.....	9
Mise en place des licences	10
Premier démarrage	17
Paramétrage des sondes AUDJRN	22
Paramétrage des points d'Exit.....	30







Introduction

STR-ICT, prononcer strict, est un progiciel qui permet une analyse poussée des données de sécurité, système et métiers d'un IBM i tout en restituant synthétiquement les informations une fois correctement interprétées.

L'IBMi est source de la donnée et communique les informations collectées vers un serveur Cible Windows ou Linux intégrant une Base de Données PostGre ou autre ainsi qu'une interface graphique GRAFANA.

Les échanges se font de manière sécurisée par SSL (Authentification par certificats privés).

Il se compose de modules principaux et optionnels :

1. **STR-ICT Base** : il s'agit d'un ensemble de sondes qui permettent une gestion aisée et automatisée des informations contenues dans le journal d'Audit d'un IBMi ainsi que les Metrics.
2. **STR-ICT xx** : pour des données complémentaires issues des Exit Point permettant de tracer les informations relatives aux actions SQL, FTP et accès IFS.

Le présent document décrit l'installation de l'interface 5250 de ce produit.

Avant de pouvoir utiliser **STR-ICT**, Il faut installer **STR-ICT** comme indiqué dans le document « Document d'installation de STR-ICT ».

Version IBM i

La version minimale du système d'exploitation requise est V7R3M0 avec le niveau de *Technology Refresh* le plus récent.

Bibliothèque

Tous les objets sont placés, par défaut, dans la bibliothèque **ZSTRICK** et géré par l'utilisateur ZSTRICK.

CCSID

Le progiciel s'affranchit de l'encodage en forçant, si besoin, le **CCSID** du travail en cours à la valeur **297**

Lexique

IBM i : Nom de l'OS anciennement appelé OS/400 puis i5/OS fonctionnant sur les anciens AS/400, iSeries et POWER System.

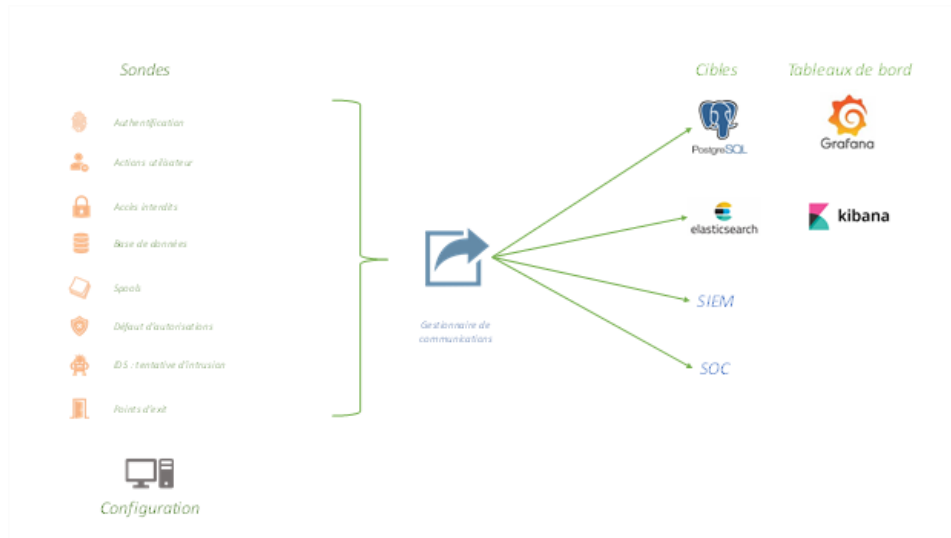


Concepts

Architecture de STR-ICT

STR-ICT est un progiciel complet qui extrait les données de Sécurité sur IBM i, qui les met en forme et les envoie vers un logiciel cible afin qu'elles soient exploitées.

Voici son organisation :



Les sondes s'exécutent sur l'IBM i. La partie cliente du gestionnaire de communications est sur l'IBM i, la partie serveur dépend de la cible mais réside généralement sur le serveur qui héberge la cible.

La configuration de STR-ICT est réalisée par une application autonome à installer sur un poste Windows. Il a été choisi, pour des questions de Sécurité, de ne pas mettre cette application à disposition sur un serveur Web qui pourrait être facilement accessible.



SONDES

On entend par sonde la capacité d'un IBM i à tracer une multitude de données au travers de journaux d'Audit et d'en permettre l'accès.

Exemple : Il sera ainsi possible d'interpréter les données d'audit relatives aux Objets supprimés ou Mot de passe modifiés.

Les types AUDJRN :

Initiales	Intitulé en français	Intitulé en Anglais
OM	Gestion Objets	Objects Managment Changes
AD	Modification Attribut Audit	Auditing Changes
CP	Modification Profil Utilisateur	User Profile Changes
IM	Tentative d'Intrusion	Intrusion Monitor
AF	Accès Refusé droits insuffisants	Authority Failure
DO	Suppression Objet	Delete Operation
PW	Mot De Passe	Password
DS	Modification Profil SST	Service Tools User ID Reset
NA	Modification TCP_IP	Attribute Change
OR	Objets Restaurés	Objects Restore
PA	Autorité Du Propriétaire	Program Adopt
PF	Actions PTF	PTF Operations
ST	Actions SST	SST Operations
SV	Actions Valeurs Systeme	Action to System Value
VP	Erreur mot de Passe Reseau	Network Password Error
X0	Authentification Reseau	Network Authentication

EXIT POINT(Optional)

L'IBM i permet l'interception et la validation par un programme interne des actions utilisateurs type accès STRSQL ou FTP.

Métrics ou Données Système (Optional)

On parle ici de l'ensemble des données système d'un IBM i restitué graphiquement :

- Mémoire
- ASP
- Espace Disque
- Travaux Actifs et autres

Interfaces

Les fonctions principales de STR-ICT sont fournies sous forme d'objets (programmes IBM i) et accessibles par une interface Graphique détaillée plus bas.

Les programmes IBM i

STR-ICT tourne dans le sous-système ZSTRICK démarré à partir du programme QSTRUP lui-même automatiquement déclenché post IPL (valeur système QSTRUPPGM)

- La configuration du sous-système ZSTRICK est paramétrée avec des travaux à démarrage automatique.
- Les sondes activées et les programmes associés s'exécutent via le travail **AUDJRN** en fonction du timing que vous déciderait (par défaut 600 secondes).
- Le User sur IBM i ZSTRICK est propriétaire de l'ensemble des fonctionnalités du produit par le biais des programmes et des tables.
- La description de Travail ZSTRICK est également l'environnement par défaut du produit
- Les travaux dans la file d'attente de travaux NOMAX de la bibliothèque ZSTRICK.
- Vous trouverez les logs des sondes activées sur l'IFS de l'IBM i : /STR-ICT/en fonction du serveur.
- Un ménage de ces logs sera proposé à intervalle régulier via WRKJOBSCDE : STR-ICT-ME.

```

Indiquez vos options et appuyez sur ENTREE.
 2=Modifier      3=Suspendre  4=Arrêter   5=Gérer   6=Libérer
 7=Afficher message 8=Gérer fichiers spoule 13=Déconnecter ...
  
```

Opt	S-syst/trav	Util en cours	Type	% UC	Fonction	Etat
—	ZSTRICK	QSYS	SBS	0,0		DEQW
—	ADM_CAPA	ZSTRICK	BCH	0,0	DLY-60	DLYW
—	AUDJRN	ZSTRICK	BCH	0,0	DLY-600	DLYW
—	EXIT_FTP	ZSTRICK	BCH	0,0	DLY-200	DLYW
—	EXIT_IFS	ZSTRICK	BCH	0,0	DLY-600	DLYW
—	EXIT_SQL	ZSTRICK	BCH	0,0	DLY-600	DLYW
—	EXIT_SQLD	ZSTRICK	BCH	0,0	DLY-300	DLYW

Fin

Paramètres ou commande
 ==>

F3=Exit F5=Réafficher F10=Relancer F11=Données intervalle écoulé
 F12=Annuler F23=Autres options F24=Autres touches



L'Interface Graphique

STR-ICT propose une interface graphique qui permet :

- La gestion des licences – *Présent document*
- Le paramétrage des sondes que vous souhaitez mettre en place – *Présent document*
- Et le paramétrage des cibles, abordé au travers des licences– *Présent document*

La version 1 de STR-ICT propose une version française et anglaise. Les copies d'écran ci-dessous sont présentées en français.

Se connecter

Pour pouvoir utiliser STR-ICT, l'utilisateur doit se connecter avec son login et mot de passe IBM i, en ciblant l'adresse IP de l'IBM i. Une fois les informations de connexion fournies, cliquez sur **connexion**.

Après s'être connecté, le logiciel vérifie la **validité des licences** (date d'expiration).

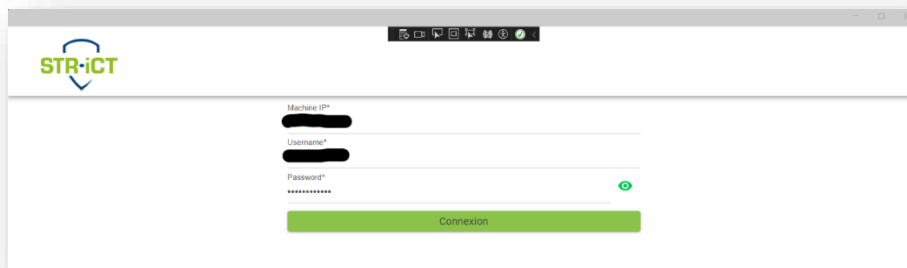


Figure 1 : Connexion

Une fois la vérification des licences effectuée, vous êtes dirigés vers la page d'accueil (Figure 2). Le logo I.GAYTE.IT est rappelé et le tableau des licences utilisées est proposé.

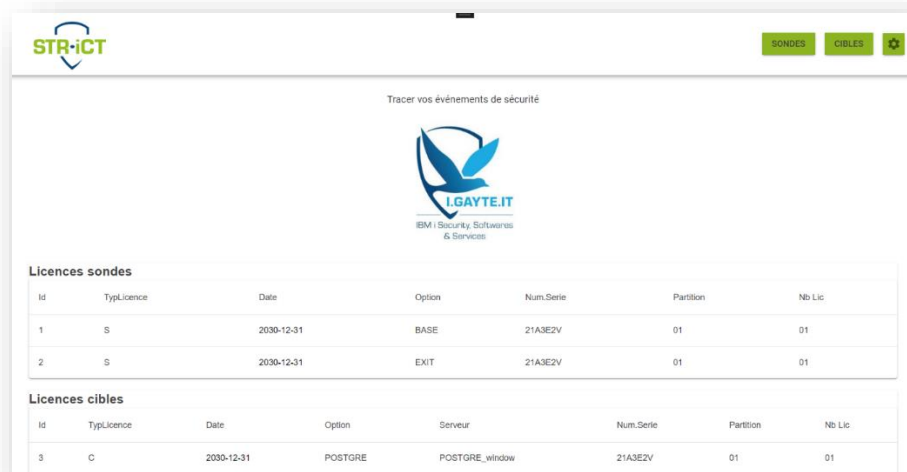


Figure 2 : Page d'accueil - tableau des licences utilisées



Mise en place des licences

STR-ICT fonctionne au minimum avec deux licences :

- Une licence SONDE de type BASE, comprenant 17 sondes AUDJRN
- Une licence CIBLE

A ce package de base, vous pouvez ajouter une licence de type EXIT pour le suivi des Exit POINT (FTP, SQL et IFS) et/ou une licence de type METRICS.

Vous avez également la possibilité d'ajouter une cible supplémentaire. Les cibles correspondent aux logiciels présentant les événements de sécurité (paramétrés depuis l'interface STR-ICT), sous la forme de tableaux de bord (dashboard).

Au démarrage

Se référer au paragraphe *Premier démarrage* de ce présent document.

Gestion des licences

■ Afficher le listing des licences

La liste des licences apparaît au démarrage (§. **Premier démarrage** en suivant). Vous pouvez également retrouver la liste au niveau de la **configuration** (roue crantée), menu **Gérer les licences** (cf. Figure 3).

Configuration des licences		
Licences sondes		
004TCnXwR71Ze5YYBQb/5P17hgFBvIk8jYsG0e	S	BASE
004TA3zW71Ze5YYBQb/5P17hgFBvIk8jYsG0ec	S	EXIT

Licences cibles			
Licence	Type Licence	Option	Serveur
004TMc5wR71Ze5YYBQb/5P17hgFBvIk8jYsG0e	C	POSTGRE	POSTGRE_window

Figure 3 : Formulaire de gestion des licences

Ce formulaire présente deux tableaux, le premier concerne la liste des licences sonde de type BASE, EXIT ou METRICS. Le second concerne la liste des licences dédiées aux cibles.

La **liste des licences dédiées aux cibles n'est pas modifiable depuis ce formulaire**, il faudra pour cela se reporter au menu **CIBLES**. Ce point est détaillé dans le paragraphe *Ajouter/supprimer/mettre à jour une licence*, en suivant.

■ Ajouter/ supprimer/ mettre à jour une licence **Cible**

Pour ajouter, supprimer ou modifier (mettre à jour) une licence cible, vous devez vous rendre dans le menu dédié aux cibles. Le menu CIBLES est disponible en haut, à droite (Figure 4).



Figure 4 : Accès au menu dédié aux cibles

➤ Ajouter une licence cible

Pour ajouter une licence Cible, il faut ajouter une cible. Pour cela, cliquez sur le menu **Ajouter une cible**.

Le formulaire d'ajout d'une cible s'ouvre alors (Figure 5).

The screenshot shows the 'Ajouter une cible' form in the STR-ICT application. The form is titled 'Ajouter une cible' and contains several input fields: 'Type' (a dropdown menu with the instruction 'Choisir un type de serveur existant'), 'Active' (a single character input), 'Mot de passe' (a password input), 'Trace' (a single character input), 'Serveur*' (a 20-character input), 'Nom utilisateur' (a 256-character input), 'URL' (a 256-character input), and 'Licence*' (a 150-character input). At the bottom right of the form are two buttons: 'VALIDER' and 'RETOUR'.


Figure 5 : Formulaire Ajout Cible

Saisissez les informations sur la cible et cliquez sur le bouton **VALIDER**. STR-ICT se charge de vérifier la validité de la licence et si toutes les informations indispensables sur la cible sont renseignées, l'ajout de la nouvelle cible est validé.

➤ Supprimer une licence cible

Attention, si vous supprimez toutes les cibles, STR-ICT ne peut plus fonctionner et lors de la prochaine ouverture du logiciel, il vous sera demandé de saisir une cible (avec une licence).

Pour supprimer une cible, vous devez vous rendre sur le sous menu **Liste des cibles** du menu **CIBLES**.

Le formulaire *Liste des cibles* s'ouvre alors (Figure 10). Cliquez ensuite sur le bouton  , situé à la fin de chaque cible.

➤ Mettre à jour une licence cible

Référez-vous au paragraphe **Pour une licence dédiée à une Cible** p.13

▪ Ajouter/ supprimer/ mettre à jour une licence Sonde BASE, EXIT, METRIQUES

➤ Ajouter une licence sonde de type BASE, EXIT, METRIQUES

Pour ajouter une licence sonde, vous devez vous rendre dans la **configuration** (roue crantée), menu **Gérer les licences**. Le formulaire de gestion des licences s'ouvre (Figure 3), pour ajouter une licence cliquez sur le bouton **Ajouter une licence**.

Le formulaire d'ajout d'une licence Sonde est présenté sur la figure ci-dessous.




Figure 6 : Formulaire Ajout d'une licence Sonde

Collez le numéro de licence, que vous avez reçu et cliquez sur le bouton **Valider**.

Si la licence est valide, les informations liées à la licence sont fournies (Figure 7), il s'agit de la date d'expiration, de l'option (BASE, EXIT, METRICS), du numéro de la machine, de la partition, et d'un numéro d'ordre. Ces informations ne sont pas modifiables.



Figure 7 : Ajout licence Sonde réussi



- Supprimer une licence SONDES de type BASE, EXIT ou METRICS.


Attention, si vous supprimez la licence SONDE de type BASE, STR-ICT ne peut plus fonctionner et lors de la prochaine ouverture du logiciel, il vous sera demandé de saisir une licence SONDE de type BASE.

Pour supprimer une licence, vous devez consulter le formulaire dédié aux licences ([Roue crantée/Gérer les licences](#)). Les formulaire *Gestion des licences* s'ouvre alors.

Licence	Type Licence	Option
004TCnXwR71Ze5YYBQb/5P17hgFBvIk8jYsG0e	S	BASE
004TA3zWR71Ze5YYBQb/5P17hgFBvIk8jYsG0e	S	EXIT

Licence	Type Licence	Option	Serveur
004TMc5wR71Ze5YYBQb/5P17hgFBvIk8j	C	POSTGRE	POSTGRE_window

Figure 8 : Formulaire Gestion des licences

Le premier tableau liste les licences dédiées aux sondes. Cliquer sur le bouton  pour supprimer une licence.

STR-ICT vous informe de la réussite ou de l'échec à l'aide d'un message informatif.

- Mettre à jour une licence SONDE

Référez-vous au paragraphe [Pour une licence dédiée aux Sondes \(Métriques, ou Exit Point\)](#) p.15

Expiration des licences : Renouvellement de licence

Pour mettre à jour une licence expirée, il existe deux manières de faire en fonction du type de licence, cependant dans les deux cas, il s'agit de remplacer la licence expirée par la nouvelle licence valide.

- **Pour une licence dédiée à une Cible**

La mise à jour d'une licence de type Cible expirée est à réaliser à partir du menu Cibles/Liste des cibles. Cf. Figure 9



Figure 9 : Renouvellement d'une licence Cible – Accès au formulaire Liste des Cibles

Le formulaire dédié aux cibles s'ouvre (Figure 10), double cliquez sur la ligne correspond à la cible dont la licence est expirée.

 The screenshot shows the 'Liste des cibles' table. The table has the following columns: Serveur, Licence, Type, Active, Trace, Nom utilisateur, Mot de passe, and URL. There is one data row for a PostgreSQL server.

Serveur	Licence	Type	Active	Trace	Nom utilisateur	Mot de passe	URL
POSTGRE_window	004Tmc5/wR71Ze5YBQb/5Pi7hgFBv/k8jY:	POSTGRE	Y	Y	postgres	*****	http://192.168.48.103:5001


Figure 10 : Formulaire Liste des cibles

La ligne devient alors éditable (Figure 11).

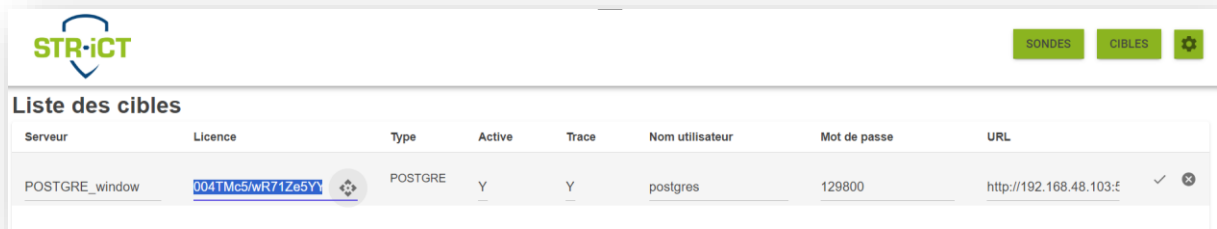
 The screenshot shows the 'Liste des cibles' table in an editable state. The 'Licence' cell for the first row is highlighted with a blue border and contains a small icon (a square with a cross) indicating it is clickable. The 'Mot de passe' field now shows the value '129800'. At the end of the row, there are checkmark and delete icons.

Serveur	Licence	Type	Active	Trace	Nom utilisateur	Mot de passe	URL
POSTGRE_window	004Tmc5/wR71Ze5Yy	POSTGRE	Y	Y	postgres	129800	http://192.168.48.103:f

Figure 11 : Liste des cible - ligne éditable

Dans le champ consacré à la licence, le symbole  apparaît (Figure 11), il permet de sélectionner l'entièreté de la licence (codée sur 150 caractères), cliquez dessus. La licence est sélectionnée (Figure 12).

Copiez la nouvelle licence et collez-la à la place de la licence expirée. Puis validez la saisie en cliquant sur la coche ✓ en fin de ligne.



Serveur	Licence	Type	Active	Trace	Nom utilisateur	Mot de passe	URL
POSTGRE_window	004TMc5wR71Ze5Yn	POSTGRE	Y	Y	postgres	129800	http://192.168.48.103:5432

Figure 12 : Liste des cibles : Sélection licence

Le logiciel va alors s'assurer de la validité de la licence, de sa mise à jour pour la cible et communiquera à l'aide de messages informatifs (Figure 13).

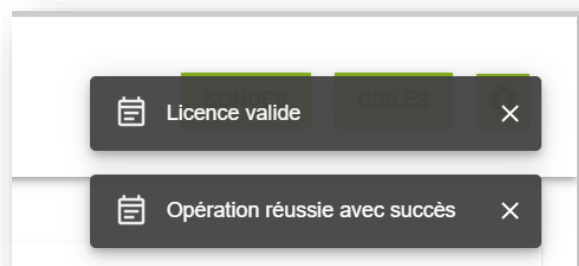


Figure 13 : Liste des cibles : Validation de la licence

- Pour une licence dédiée aux **Sondes** (Métriques, ou Exit Point)

La mise à jour des licences sondes est réalisée à partir du Menu Configuration (Roue crantée) / Gérer les licences (Figure 14).

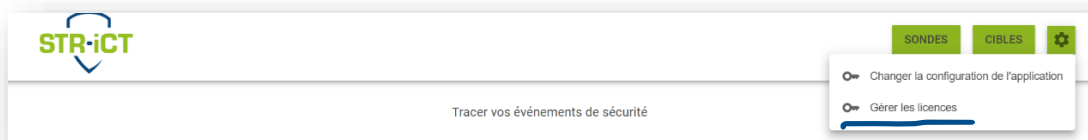
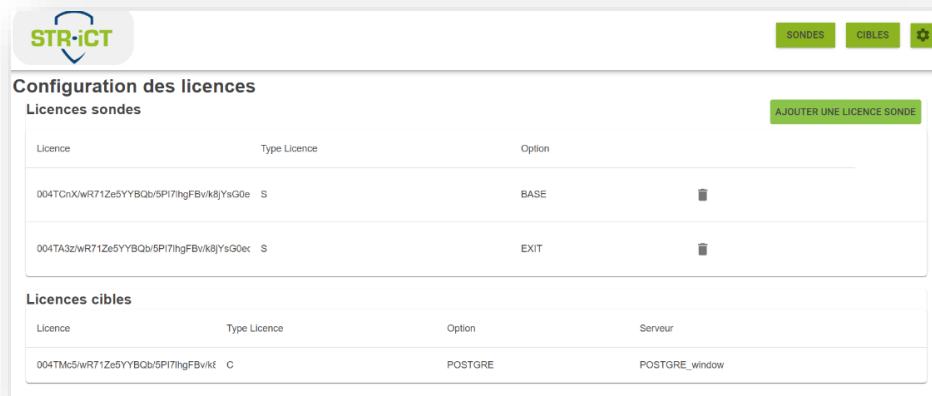


Figure 14 : Renouvellement d'une licence Sonde – Accès au formulaire Gestion des licences

Le formulaire de gestion des licences permet de consulter toutes les licences (Figure 15), mais seules les **licences dédiées aux sondes sont modifiables**.



Licence	Type Licence	Option
004TcnXwR71Ze5YYBQb/5P17hgFBvIk8jYsG0e	S	BASE
004TA3zW71Ze5YYBQb/5P17hgFBvIk8jYsG0e	S	EXIT

Licence	Type Licence	Option	Serveur
004Tmc5wR71Ze5YYBQb/5P17hgFBvIk8jYsG0e	C	POSTGRE	POSTGRE_window

Figure 15 : Formulaire de gestion des licences

Double-cliquez sur l'enregistrement correspondant à la licence sonde à mettre à jour, un formulaire s'ouvre alors. Il s'agit du formulaire dédié aux informations relatives aux licences sondes.

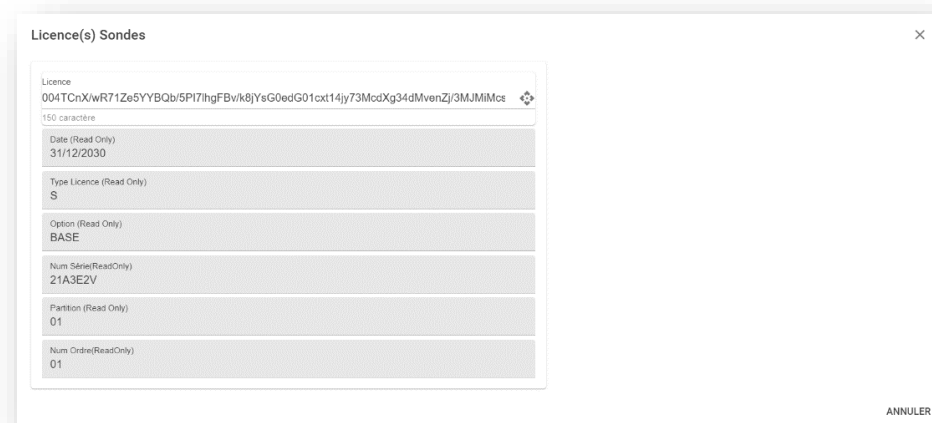



Figure 16 : Formulaire licence sonde

Seul le champ licence est modifiable. Sélectionnez l'entièreté de la licence à l'aide du symbole  et collez la nouvelle licence puis appuyer sur le bouton **Entrée**. STR-ICT se charge de vérifier la validité de la licence, si la licence est valide et appropriée (renouvellement du même type de licence : remplacement d'une licence sonde de type BASE par une licence sonde de type BASE). Dans le cas d'un succès, le message informatif présenté figure 17 apparaît. Sinon, le message d'échec apparaît (Figure 18).

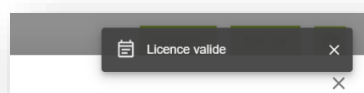


Figure 17 : Message de succès de renouvellement de licence sonde



Licence(s) Sondes

Erreur : Les caractéristiques de la licence ne correspondent à la licence à modifier (Option ou Num de série ou Partition ou Produit)

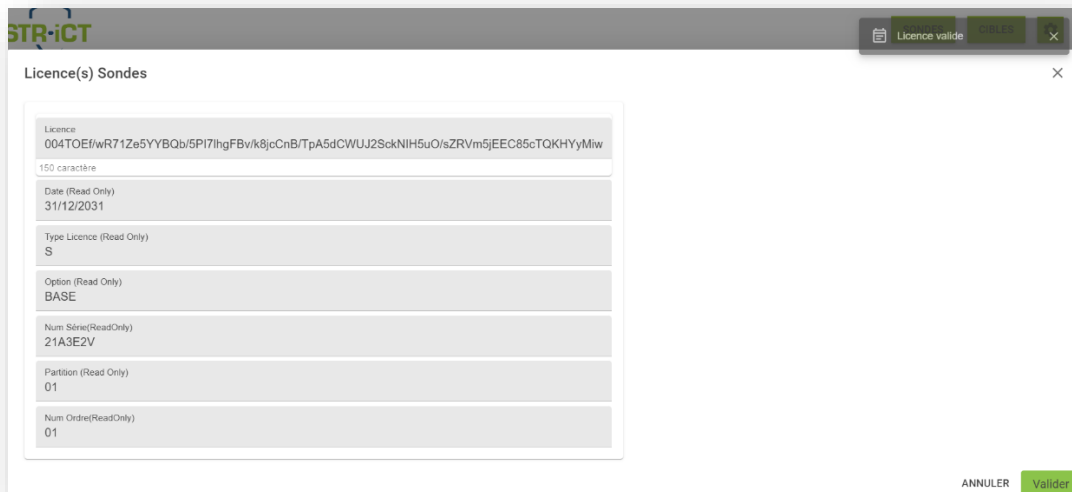
Erreur

004TA3z/wR71Ze5YYBQb/5PI7lhgFBv/k8jYsG0edG01cxt14jy73Mda61JGbEkBSVukhc3

150 caractère

Figure 18 : Message d'échec de renouvellement d'une licence sonde

Si STR-ICT valide la licence, le bouton **Valider** apparaît (Figure 19). Cliquez sur ce bouton, vous retournez sur le formulaire de Gestion des licences.



Licence(s) Sondes

Licence
004TOE/wR71Ze5YYBQb/5PI7lhgFBv/k8jYsG0edG01cxt14jy73Mda61JGbEkBSVukhc3

150 caractère

Date (Read Only)
31/12/2031

Type Licence (Read Only)
S

Option (Read Only)
BASE

Num Série(ReadOnly)
21A3E2V

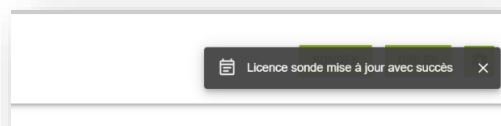
Partition (Read Only)
01

Num Ordre(ReadOnly)
01

ANNULER Valider

Figure 19 : Formulaire licence sonde : Licence valide

Un message informatif vous indique la mise à jour correcte de la licence sonde.



Licence sonde mise à jour avec succès

Figure 20 : Renouvellement licence sonde réalisé avec succès

Premier démarrage

Lors du premier démarrage, vous devez :

- Saisir deux licences, une licence SONDE de type BASE et une licence CIBLE.
- Paramétrer l'interface graphique (Bibliothèque de travail, langues)



Installation des licences

Lors du premier démarrage, vous devez saisir vos identifiants puis cliquer sur **Connexion**.

Figure 21 : Ouverture 1er démarrage

STR-ICT détecte l'absence d'une licence SONDES de type BASE et vous propose de saisir cette licence (Figure 22). Cliquez sur le bouton **SAISIE D'UNE LICENCE SONDE DE TYPE BASE**.

Figure 22: Détection absence de licence SONDE de type BASE

Cette action conduit à l'ouverture de formulaire de saisie d'une licence SONDE (Figure 23). Copiez/collez la licence cryptée puis cliquez sur **VALIDER**.

Figure 23 : Saisie d'une licence SONDE de type BASE

Vous devez alors paramétrer une CIBLE et saisir une licence de type CIBLE. Cliquez sur **VALIDER**.

Figure 24 : Saisie d'une licence CIBLE

Vous êtes ensuite dirigés vers le formulaire de listing des cibles. Cf. Figure 25.

Serveur	Licence	Type	Active
POSTGRE_window	004Tmc5wR71Ze5YYBQb/5PI7hgFBvk8jYsG0edG01cxt14jy73MdepCijFSTxti+b6wyeU0W0oeVB1ZLdEuELGUTWOITNDRzC5NGoStaVnKw4a5U8tmw==	POSTGRE	Y

Figure 25 : Liste des cibles

Vous pouvez, dès lors, utiliser l'application STR-ICT.

Configuration de l'interface graphique

Au premier démarrage, il convient également de paramétrer la configuration de l'interface STR-ICT. Elle permet de paramétrer :

- La langue
- Les bibliothèques
- Et une durée d'expiration de la session
- Un nom d'utilisateur par défaut
- Ainsi qu'une adresse IP

La configuration est à réaliser à partir de la roue crantée située en haut à droite (Figure 26) du logiciel, choisir **Changer la configuration de l'application**.



Figure 26 : Roue crantée : accès au menu configuration de l'application

L'application s'ouvre alors sur le panneau présenté sur la figure ci-dessous.

Figure 27 : Panneau de configuration

Configuration de langue

Cliquez sur la liste déroulante dédiée à la zone de texte **Choisir le langage de l'application** et sélectionnez la langue de votre choix.

Expiration de la session

L'expiration de la session est un paramétrage de sécurité.

L'utilisateur devra se reconnecter au bout d'un certain temps, exprimé en minutes. La valeur par défaut est 10 minutes.

Durée à paramétrer dans le champ **Durée d'expiration de la session**.

Dans le cas d'une session expirée, STR-iCT vous informe de l'expiration via un message d'erreur qui s'affichera sur le formulaire demandé. Sur la figure ci-dessous, l'expiration de la session est observée au moment de la consultation de la liste des cibles.

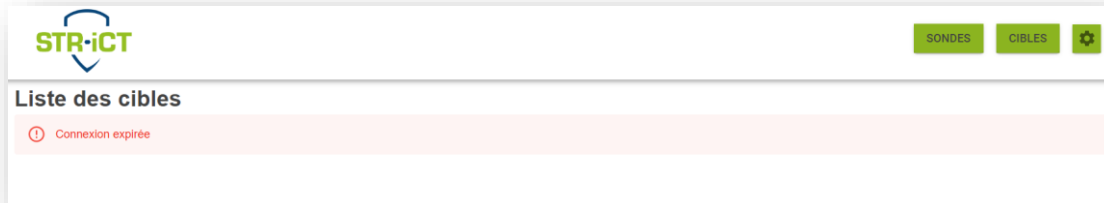


Figure 28 : Expiration de la session

Cliquez sur le **logo STR-iCT** en haut à gauche de l'application cela vous redirigera vers le formulaire de connexion. Puis cliquez sur **Connexion**, une fois vos identifiants saisis.

Figure 29 : Formulaire de connexion

Configuration IP

Dans le champ **IP** (cf. Figure 27), renseignez l'IP de l'IBM i. Ce champ est renseigné par défaut par l'IP fourni dans le formulaire de connexion.

Configuration Utilisateur

Dans le champ **Utilisateur** (cf. Figure 27), renseignez le login de votre compte IBM i. Ce champ est renseigné par défaut par l'utilisateur fourni dans le formulaire de connexion.

Configuration des bibliothèques

Dans le champ **Nom de la bibliothèque principale**, renseignez le nom de la bibliothèque principale (ZSTRICKT par défaut).

Dans le champ **Nom de la bibliothèque temporaire**, renseignez le nom de la bibliothèque temporaire (ZSTRICKTMP par défaut).

Configuration de la bibliothèque des récepteurs de journaux

Dans le champ **bibliothèque des récepteurs**, renseignez le nom de la bibliothèque où se situent les récepteurs de journaux (LOGS par défaut). Cette valeur mettra à jour la Bibliothèque réceptrice des sondes quand aucune autre valeur n'est renseignée, vous pouvez aussi appuyer sur la case à cocher à droite du champ afin d'écraser toutes les valeurs bibliothèques du formulaire (Sondes QAUDJRN).



Les paramétrages de la langue, de l'utilisateur, de l'ip, de la durée d'expiration et des bibliothèques sont pris en compte directement, il n'est donc pas nécessaire de valider vos choix. Le bouton **Valider** vous permet de revenir à la page d'accueil (listing des licences).

Paramétrage des sondes AUDJRN

Le paramétrage des sondes AUDJRN consiste :

- A **activer** les sondes que vous souhaitez suivre dans le cadre de votre gestion de la sécurité.
- A valider la présence des **prérequis** nécessaires au bon fonctionnement de chacune des sondes.
- A définir, le cas échéant, les **exceptions** pour chaque sonde. Les exceptions correspondent aux enregistrements à ignorer.
- A définir certaines informations quant à la durée d'**archivage** des événements enregistrés, à celle de l'archivage des événements sur la cible, exprimés en jours.
- A paramétrer le **journal récepteur** (RCV) pour chacune des sondes, avec leurs caractéristiques (Bibliothèque : BIBRCV, Prochaine Séquence).

Généralités sur le paramétrage des sondes

Le paramétrage des sondes AUDJRN est accessible via le **sous menu Sondes QAUDJRN** du **menu SONDES** disponible en haut à droite du logiciel. Cf. *Figure ci-dessous*.

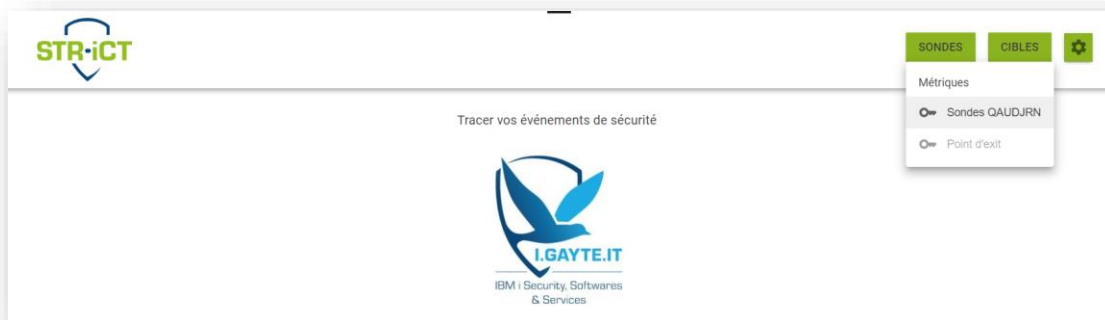



Figure 30 : Menu Sondes

La fenêtre dédiée au paramétrage des sondes s'ouvre alors (Figure 31). Elle présente la liste des 17 sondes paramétrables proposées dans la licence « BASE ». L'activation d'une sonde entraîne le calcul des prérequis nécessaires à sa mise en œuvre (cf. § Activation des sondes – Validation des prérequis en suivant). En utilisation de routine, dès que vous consultez le formulaire des sondes, le calcul des prérequis est effectué pour les sondes actives, avant l'ouverture du formulaire (Figure 32).



SONDES CIBLES ⚙️

Affichage des Sondes QAUDJRN

Active	Type	Libellé	Prochaine Séquence	RCV	BIBRCV	Durée de rétention cible (j)	Durée archivage (j)	Prérequis	Risque/Sévérité
<input checked="" type="checkbox"/>	PW	Invalid password	245563	AUDRCV0158	LOGS	90	190	✓ Prérequis Ok	
<input checked="" type="checkbox"/>	DO	Delete object	245588	AUDRCV0158	LOGS	90	190	✓ Prérequis Ok	
<input checked="" type="checkbox"/>	AD	Auditing changes	2102	AUDRCV0158	LOGS	90	190	Pas de prérequis	
<input checked="" type="checkbox"/>	CP	User profile changed, created, or restored	100643	AUDRCV0158	LOGS	90	190	✓ Prérequis Ok	
<input checked="" type="checkbox"/>	DS	DST security password reset	56921	AUDRCV0135	LOGS	90	190	✓ Prérequis Ok	

Rows per page: 10 1-10 of 17

Figure 31 : Liste des sondes



SONDES CIBLES ⚙️

Affichage des Sondes QAUDJRN

Calcul des pré requis en cours ...

Figure 32 : Formulaire QAUDJRN (Sondes) - calcul des prérequis

Pour **pouvoir modifier une sonde**, vous devez double cliquer sur la ligne correspondant à la sonde afin de la **rendre éditable** (Figure 33). Effectuer les modifications (activation de la sonde, paramétrages du journal récepteur, ...) puis cliquez au bout de la ligne sur la **coche** ✓ pour valider ou sur la **croix** ✕ pour annuler.

Notez qu'une seule ligne est modifiable à la fois. Ainsi, l'utilisateur s'assurera d'avoir correctement valider ou invalider les caractéristiques d'une sonde précédemment en mode éditable avant de pouvoir modifier une autre sonde.



Affichage des Sondes QAUDJRN

Active	Type	Libellé	Prochaine Séquence	RCV	BIBRCV	Durée de rétention cible (j)	Durée archivage (j)	Prérequis	Risque/Sévérité
<input checked="" type="checkbox"/>	PW	Invalid password	245563	AUDRCV0158	LOGS	90	190		✓ ✕

Figure 33 : Mode éditable d'une sonde

Activation des sondes – Validation des prérequis

L'**activation d'une sonde** est réalisée à l'aide de la case **Active** cochée. Elle permet de désigner le type d'événements de sécurité que vous souhaitez tracer (sur la Figure 34, la sonde IM). La ligne doit être en mode éditable pour pouvoir cocher la case Active. Pensez à valider votre choix à l'aide de la coche.

Affichage des Sondes QAUDJRN

Active	Type	Libellé	Prochaine Séquence	RCV	BIBRCV	Durée de rétention cible (j)	Durée archivage (j)	Prérequis
<input checked="" type="checkbox"/>	AF	Authority failure	129586 129586	AUDRCV0158 AUDRCV0...	LOGS	90	190	    Valider

Figure 34 : Activation d'une sonde

La **validation des prérequis** se déclenche à l'activation de la sonde (case **Active** cochée). Cette fonctionnalité concerne la validation de la présence de **valeurs systèmes** spécifiques à chacune des sondes.




<input checked="" type="checkbox"/>	PW	Invalid password	245563	AUDRCV0158	LOGS	90	190	  Prérequis Ok 
-------------------------------------	----	------------------	--------	------------	------	----	-----	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Figure 35 : Validation des prérequis à l'activation de la sonde

La validation des prérequis est mise en œuvre pour chacune des sondes à l'exception de la sonde AD (Auditing – Change) qui ne nécessite pas de prérequis pour son fonctionnement. Cf. Figure 36



<input checked="" type="checkbox"/>	AD	Auditing changes	2028	AUDRCV0158	LOGS	90	190	 Pas de prérequis 
-------------------------------------	----	------------------	------	------------	------	----	-----	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Figure 36 : Sonde AD - aucun prérequis

La sonde IM (Intrusion Monitoring) est particulière dans le sens où les prérequis concernent, en plus des valeurs systèmes, la configuration de la fonction IDS (Système de détection des intrusions) qui est à la charge de l'utilisateur. Cf. Figure 37




<input checked="" type="checkbox"/>	IM	Intrusion monitor	243872	AUDRCV0158	LOGS	90	190	  Prérequis Ok La fonction de la configuration IDS est à votre charge 
-------------------------------------	----	-------------------	--------	------------	------	----	-----	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Figure 37 : Prérequis Sonde IM



Les valeurs systèmes ne sont pas paramétrables par l'utilisateur depuis l'interface graphique. Il est de la responsabilité de l'utilisateur de STR-ICT de mettre à jour les valeurs système.

Si les prérequis ne sont pas validés (Mention en orange Pré requis non validés - *Figure ci-dessous*), STR-ICT vous en informe. **Dans ce cas, la sonde ne pourra pas enregistrer les événements et aucun enregistrement ne sera fourni.** De plus, le bouton **Exceptions** est désactivé.

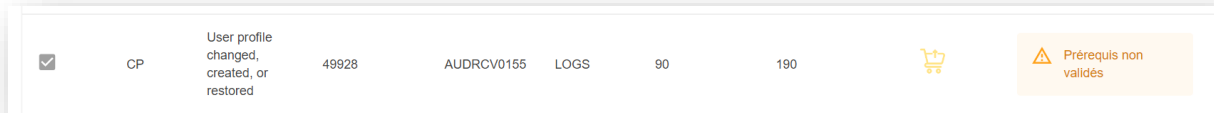


Figure 38 : Prérequis non validés

Gestion des exceptions

Pour chaque sonde, il est possible de définir des **valeurs à exclure**.

Par exemple, pour la sonde Intrusion Monitoring (surveillance des intrusions), vous pouvez exclure tous les enregistrements provenant de l'adresse IP de l'administrateur système et réseau. Ainsi seront tracées toutes les intrusions dont l'adresse IP est différente de celle de l'administrateur.

Le paramétrage des exceptions n'est pas définitif, vous pouvez décider de rajouter ou de supprimer des exceptions existantes, tout au long de votre utilisation du logiciel STR-ICT. Vous avez également la possibilité de créer des exceptions « manuellement ».

Afin de gérer les exceptions, vous devez renseigner quelques paramètres concernant le journal récepteur.

Le bouton dédié aux Exceptions (chariot orange) est actif que si la sonde est activée et que le prérequis sont validés.

Le **paramétrage des règles d'exception** est accessible en cliquant sur le chariot orange (Gérer les exceptions). Cf. *Figure ci-dessous*

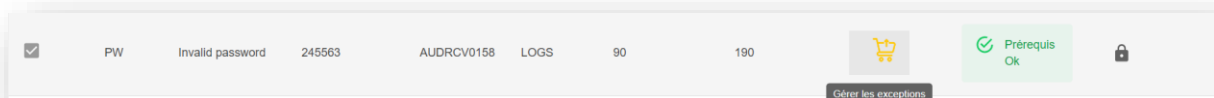


Figure 39 : Gérer les exceptions – Click chariot orange

Un clic sur le chariot orange entraîne l'ouverture de la fenêtre de la gestion des exceptions, fenêtre vide lors du premier démarrage de l'interface graphique.

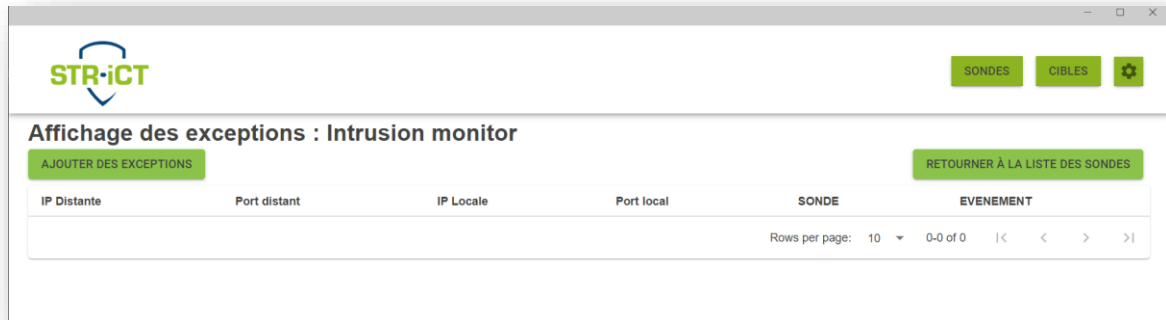


Figure 40 : Fenêtre affichage des exceptions pour la sonde Intrusion Monitoring : vide au premier démarrage

Le **paramétrage des exceptions** est réalisé à partir de la liste des événements enregistrés par la sonde. Pour obtenir la liste des événements, cliquez sur le bouton en haut à gauche **AJOUTER DES EXCEPTIONS** - Figure 40.

Une boîte de dialogue s'ouvre alors permettant de renseigner les paramètres du journal récepteur, sélectionner l'un des deux récepteurs **CURRENT** ou **CURCHAIN**. Figure 41

Si vous faites un autre choix que CURRENT ou CURCHAIN, vous devez alors préciser le journal récepteur (Figure 42).

Choisissez le récepteur que vous souhaitez, puis cliquez sur **Afficher les enregistrements**.

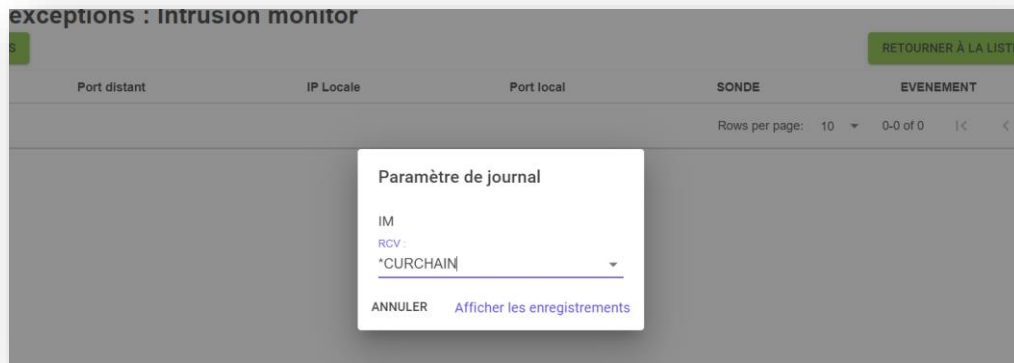


Figure 41 : Gestion des exceptions (Sonde IM) – Paramètres du journal CURCHAIN

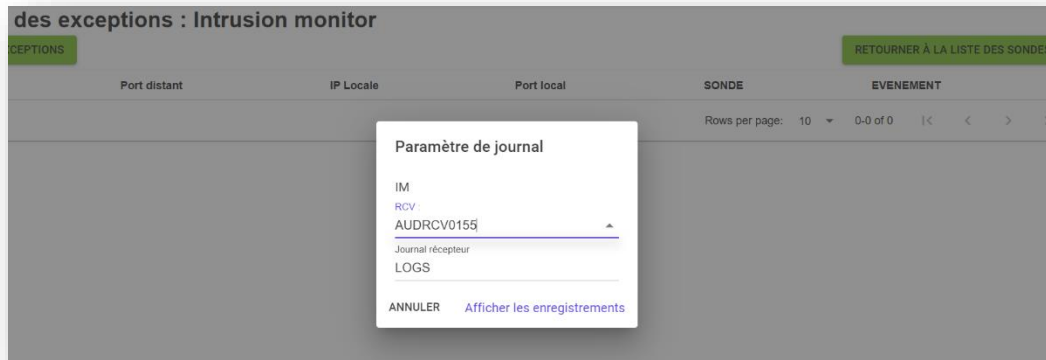


Figure 42 : Gestion des exceptions (Sonde IM) – Paramètres du journal

A noter que si le nombre d'enregistrements obtenus permettant de réaliser les règles d'exception est supérieur à 10000 lignes, un message d'information s'affichera, vous offrant la possibilité de continuer ou de revenir sur votre choix ou d'annuler (Figure 43).

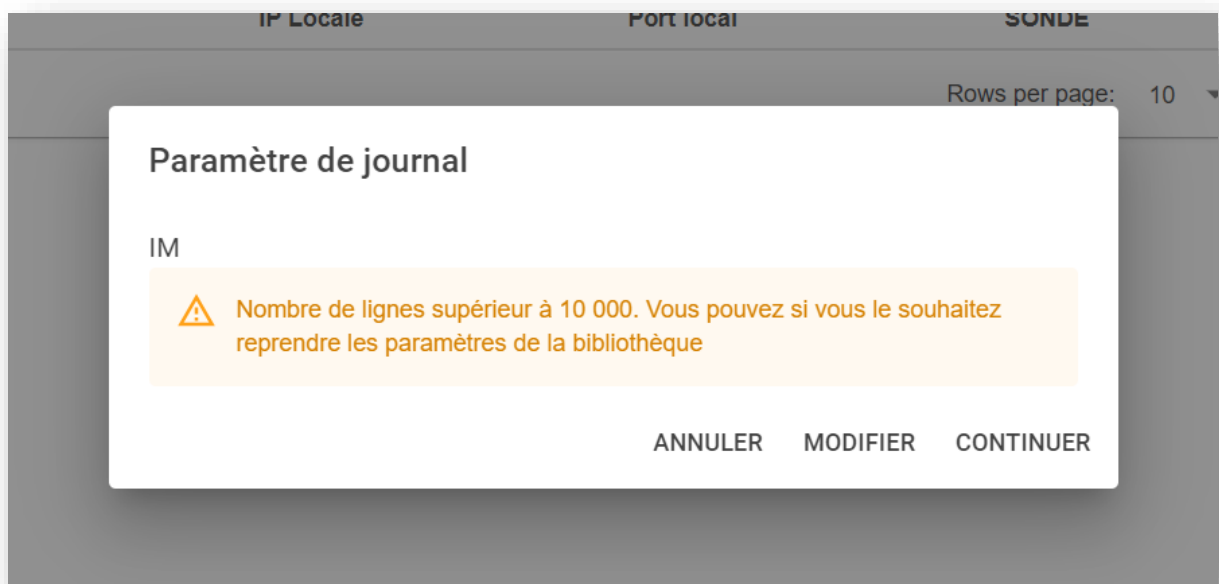
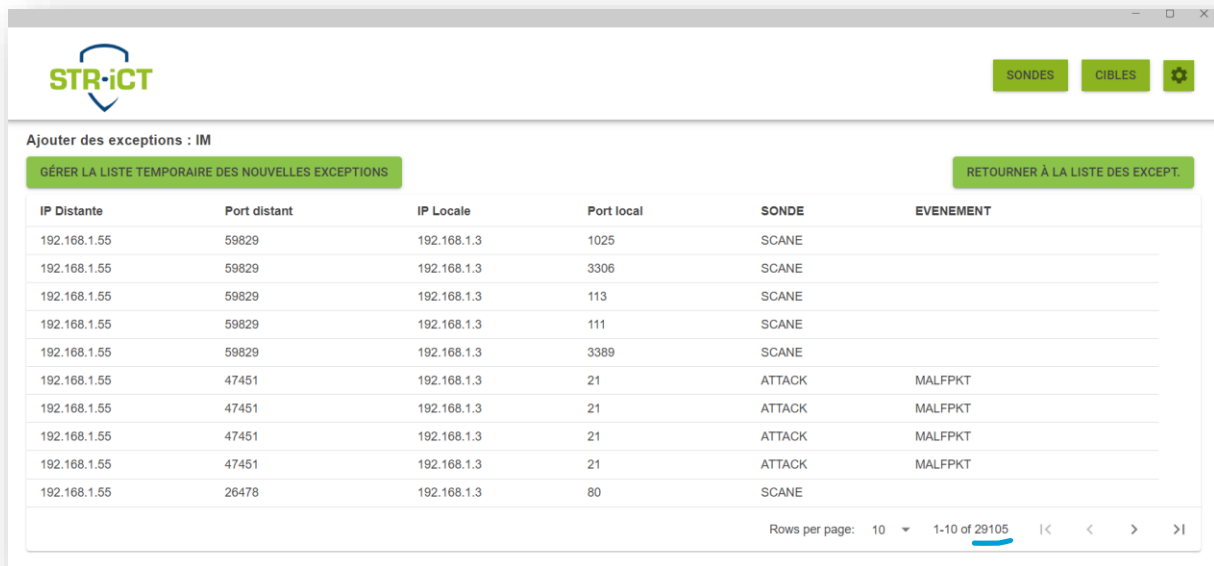


Figure 43 : Gestion des exceptions : Message informatif concernant un nombre d'enregistrements supérieur à 10000

Cliquez sur **CONTINUER**, la liste (Figure 44) des enregistrements du journal récepteur choisi sur la fenêtre précédente vous est alors présentée.

C'est à partir de cette liste que vous allez sélectionner les exceptions.

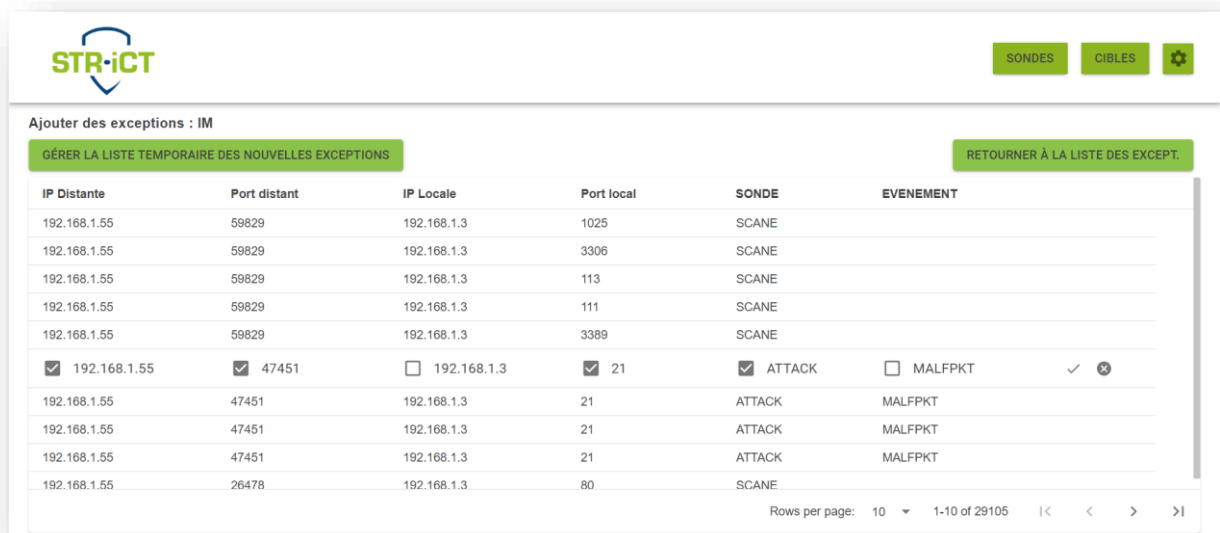


IP Distant	Port distant	IP Locale	Port local	SONDE	EVENEMENT
192.168.1.55	59829	192.168.1.3	1025	SCANE	
192.168.1.55	59829	192.168.1.3	3306	SCANE	
192.168.1.55	59829	192.168.1.3	113	SCANE	
192.168.1.55	59829	192.168.1.3	111	SCANE	
192.168.1.55	59829	192.168.1.3	3389	SCANE	
192.168.1.55	47451	192.168.1.3	21	ATTACK	MALFPKT
192.168.1.55	47451	192.168.1.3	21	ATTACK	MALFPKT
192.168.1.55	47451	192.168.1.3	21	ATTACK	MALFPKT
192.168.1.55	47451	192.168.1.3	21	ATTACK	MALFPKT
192.168.1.55	26478	192.168.1.3	80	SCANE	

Figure 44 : Liste des enregistrements du récepteur de journal (CURCHAIN pour la sonde IM)

Pour **rajouter des exceptions** il vous suffit de **cliquer sur la ligne** comprenant l'enregistrement des valeurs à exclure dans la liste de données générées par la sonde.

Une fois la ligne cliquée, vous avez la possibilité de cocher ou décocher les paramètres qui vous intéressent afin de garder seulement les valeurs à exclure – Figure 45.



IP Distant	Port distant	IP Locale	Port local	SONDE	EVENEMENT
192.168.1.55	59829	192.168.1.3	1025	SCANE	
192.168.1.55	59829	192.168.1.3	3306	SCANE	
192.168.1.55	59829	192.168.1.3	113	SCANE	
192.168.1.55	59829	192.168.1.3	111	SCANE	
192.168.1.55	59829	192.168.1.3	3389	SCANE	
<input checked="" type="checkbox"/> 192.168.1.55	<input checked="" type="checkbox"/> 47451	<input type="checkbox"/> 192.168.1.3	<input checked="" type="checkbox"/> 21	<input checked="" type="checkbox"/> ATTACK	<input type="checkbox"/> MALFPKT
192.168.1.55	47451	192.168.1.3	21	ATTACK	MALFPKT
192.168.1.55	47451	192.168.1.3	21	ATTACK	MALFPKT
192.168.1.55	47451	192.168.1.3	21	ATTACK	MALFPKT
192.168.1.55	26478	192.168.1.3	80	SCANE	

Figure 45 : Cocher ou décocher les valeurs d'une exception

Puis cliquez au bout de la ligne sur la **coche** ✓ pour valider votre choix et rajouter l'exception dans la **liste temporaire des nouvelles exceptions** ou sur la **croix** ✕ pour annuler votre sélection. Renouvelez l'opération pour une autre exception si nécessaire.


A noter qu'il est impossible de rajouter une exception sans valeur cochée.

Une fois votre sélection faite, **cliquez** sur **GERER LA LISTE TEMPORAIRE DES NOUVELLES EXCEPTIONS** (en haut à gauche de l'écran), la fenêtre des exceptions rajoutées temporairement dans la liste depuis le journal récepteur vous est alors présentée (Figure 46).

IP Distant	Port distant	IP Locale	Port local	SONDE	EVENEMENT
192.168.1.55	47451		21	ATTACK	

Figure 46 : Fenêtre de gestion de la liste temporaire des nouvelles exceptions

À partir de cet écran vous retrouvez vos exceptions rajoutées depuis la fenêtre précédente (**les valeurs décochées n'apparaissent pas**).

Vous avez la possibilité de retirer de la liste temporaire des exceptions en appuyant sur la poubelle  à droite pour chacune des lignes du tableau.

Il vous est aussi offert la possibilité de rajouter une exception manuellement en appuyant sur le bouton vert **AJOUTER UNE EXCEPTION MANUELLEMENT**, qui vous conduit sur le formulaire d'ajout manuel, présenté sur la ci-dessous.

IP Distant	Port distant	IP Locale	Port local	SONDE	EVENEMENT
192.168.1.55	47451		21	ATTACK	

Figure 47 : Fenêtre d'ajout manuel possible d'une exception



Depuis cette fenêtre vous pouvez renseigner **manuellement** les informations à exclure selon votre machine et votre système d'information.

Ce formulaire d'ajout **est propre à chaque sonde** (Figure 47– IM).

Une fois les informations transmises vous pouvez appuyer sur **ENVOYER** et votre exception manuelle sera **rajoutée dans la liste temporaire**.

Lorsque vous avez ajouté toutes les exceptions que vous vouliez rajouter dans la liste temporaire, vous pouvez appuyer sur le bouton vert **VALIDER LES NOUVELLES EXCEPTIONS**, qui en plus de rajouter vos exceptions vous renverra sur l'écran d'affichage des exceptions de la sonde (Figure 40 et Figure 48).

IP Distant	Port distant	IP Locale	Port local	SONDE	EVENEMENT
192.168.1.55	47451		21	ATTACK	

Figure 48 : Affichage des exceptions retenues pour la sonde IM

A noter que le parcours des exclusions et ses différentes étapes **est le même pour chaque sonde AUDJRN**.

Durée d'archivage

La durée d'archivage correspond au nombre de jours durant lesquels les données de la sonde sont archivées dans l'IBM i. Elle est modifiable sur l'écran de la figure 31 en passant en mode « édition de sonde » (figure 33), une fois en édition il vous suffit de rentrer le nombre de jours de votre choix.

Il vous est aussi donné la possibilité de paramétrer la **durée de rétention cible** sur le même écran (durée d'archivage des sondes pour les cibles). Afin d'effectuer une modification cliquez au bout de la ligne sur la **coche** ✓ pour valider ou sur la **croix** ✕ pour annuler.

Journal Récepteur

Afin de modifier le journal récepteur (RCV) et la prochaine séquence il faut se positionner sur l'écran de l'affichage des sondes (**figure 31**) en passant en mode « **édition de sonde** » (cf. \$. Généralités sur le paramétrage des sondes), puis vous avez la possibilité de choisir dans le RCV les valeurs **CURCHAIN**, **CURRENT**, ou celle de **votre choix**. Ainsi que dans la prochaine séquence les valeurs **FIRST** ou le nombre de **votre choix**.

Afin d'effectuer une modification cliquez au bout de la ligne sur la **coche** ✓ pour valider ou sur la **croix** ✕ pour annuler.



Sévérité & Risque

Nous définissons la **sévérité** comme le niveau d'impact d'un événement sur une organisation, en l'occurrence sur le fonctionnement de l'application sur IBM i, on pourrait aussi parler de gravité.

Le **risque** quant à lui est la possibilité qu'un événement entraîne directement ou indirectement, de manière volontaire ou involontaire, une altération du fonctionnement d'un système, en l'occurrence un IBM i. Il a pour mission d'informer sur la dangerosité potentielle d'un événement qui s'est déroulé et qui peut paraître anodin mais qui peut être une étape d'un processus dangereux.

L'interface graphique vous offre la possibilité de modifier ces 2 valeurs pour chaque type de violation et pour chaque cible


Pour commencer il vous suffit de vous rendre sur la Figure 31 puis d'appuyer sur l'icône  sur la ligne de la sonde de votre choix (Cf. Figure 49) afin d'arriver sur la Figure 50.



Figure 49 : Affichage des Sondes : Sévérité & Risque

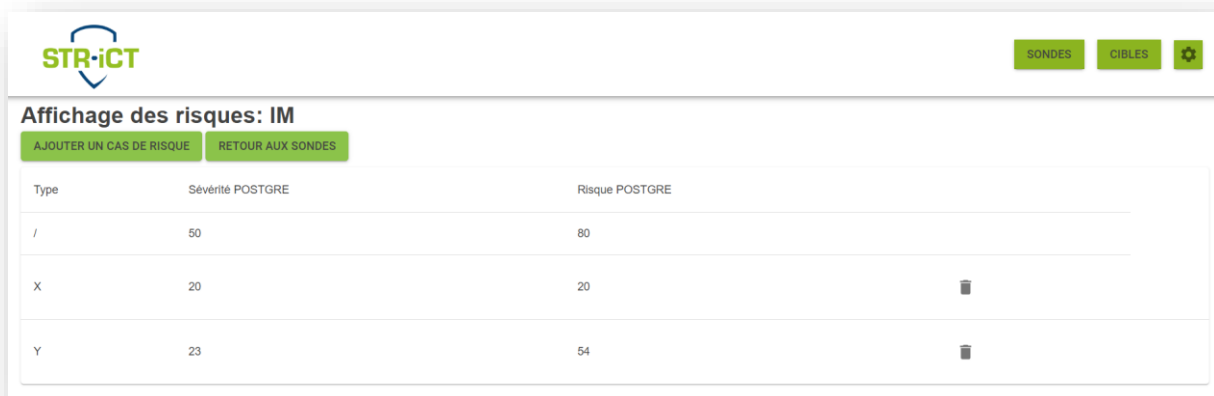
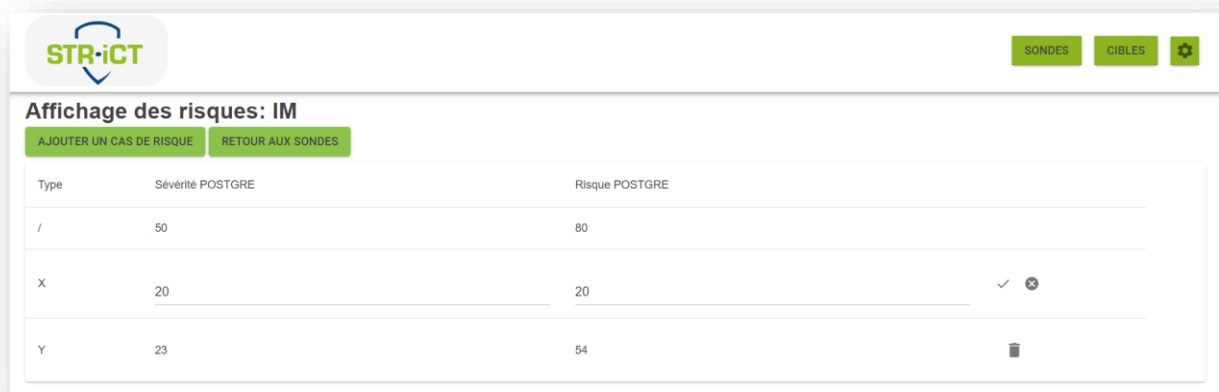


Figure 50 : Affichage des risques IM

Depuis cette fenêtre vous avez plusieurs actions possibles sur les valeurs des risques par Cibles, vous pouvez **modifier** ces valeurs en passant en mode édition de ligne (le même procédé vu précédemment dans cette documentation)



Type	Sévérité POSTGRE	Risque POSTGRE	
/	50	80	
X	20	20	✓ ✕
Y	23	54	🗑️

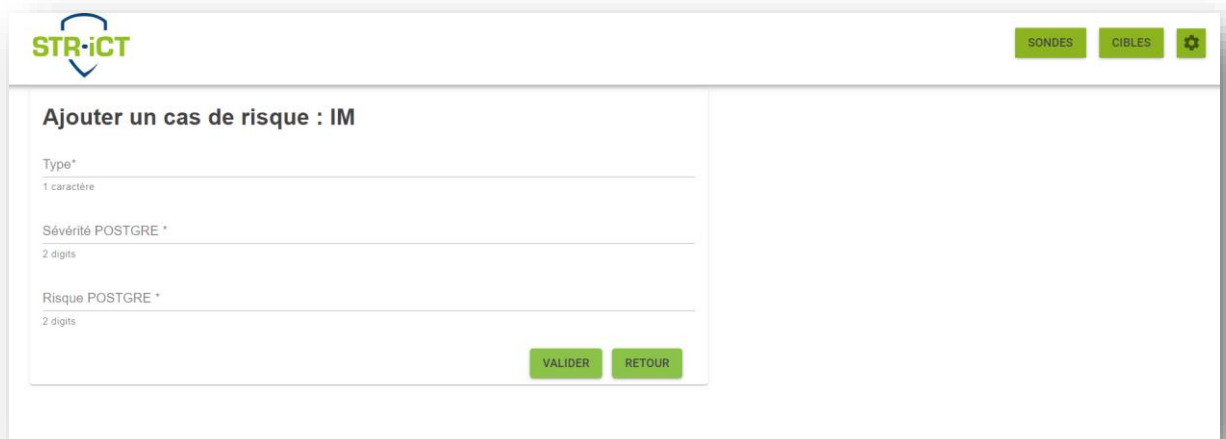
Figure 51 : Edition de risque pour la sonde IM

Puis pour valider vos modifications vous devez cliquer au bout de la ligne sur la **coche** ✓ pour valider ou sur la **croix** ✕ pour annuler.

Vous avez la possibilité de **retirer** des cas de risque en appuyant sur la poubelle 🗑️ situé à droite de chaque ligne du tableau pour chaque sonde indépendamment

Vous avez à votre disposition 2 boutons :

- **AJOUTER UN CAS DE RISQUE** : Renvoie sur un formulaire **d'ajout de cas de risque** manuellement (Cf. Figure 52)



Ajouter un cas de risque : IM

Type*
1 caractère

Sévérité POSTGRE *
2 digits

Risque POSTGRE *
2 digits

VALIDER RETOUR

Figure 52 : Ajout de risque manuellement IM

A noter que les valeurs de sévérité et risque ne peuvent dépasser 99 donc elles ne peuvent comprendre que 2 digits. Une fois vos valeurs saisies vous pouvez appuyer sur **VALIDER** afin de revenir sur l'affichage des cas de risques (Figure 50) et d'ajouter cas de risques dans la liste des risques.

- **RETOUR AUX SONDES** : Permet de naviguer dans l'application, renvoie à la Figure 31



Paramétrage des points d'Exit

Installation de la licence Exit point (optionnel)

Afin d'accéder aux sondes Exit points vous devez être en possession d'une licence de type EXIT, vous devriez pouvoir ensuite procéder comme vu précédemment dans le chapitre « **Mise en place des licences** » de cette documentation.

Activation des Exit Points

L'**activation d'un Exit point** est réalisée à l'aide de la case **Active** cochée. Elle permet de désigner l'exit points que vous souhaitez tracer (sur la Figure [...], l'exit point [...]). La ligne doit être en mode éditable pour pouvoir cocher la case Active. Pensez à valider votre choix à l'aide de la coche.

Gestion des inclusions

Pour chaque Exit point, il est possible de définir des **valeurs à inclure**.

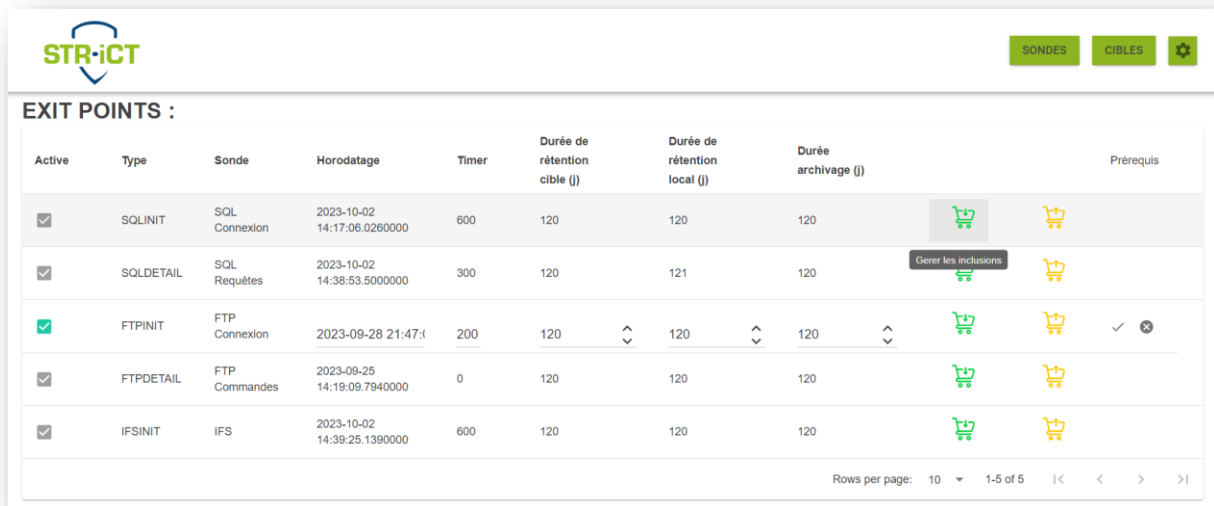
Par exemple, pour les connexions FTP(FTPINIT), vous avez la possibilité de rajouter des mots dit : d'inclusions. Ces mots serviront à filtrer les résultats des enregistrements, en effet les enregistrements qui contiennent les mots rentrer dans la table d'inclusions et seulement eux seront ainsi tracées et renvoyés dans votre génération d'enregistrements.

Vous pouvez à tout moment rajouter ou supprimer des mots, tout au long de votre utilisation du logiciel STR-ICT et cela indépendamment pour chaque Exit points.

A noter que les valeurs inclusions ne sont présentes que pour les exit point et non les sondes

Afin de gérer les valeurs incluses, vous devez vous rendre dans la page d'affichage des Exit points et cliquer sur le chariot vert, ce bouton n'est actif que si l'exit point en question est activé et que ses prérequis sont validés.

Le **paramétrage des règles d'inclusions** est accessible en cliquant sur le chariot vert (Figure 53)














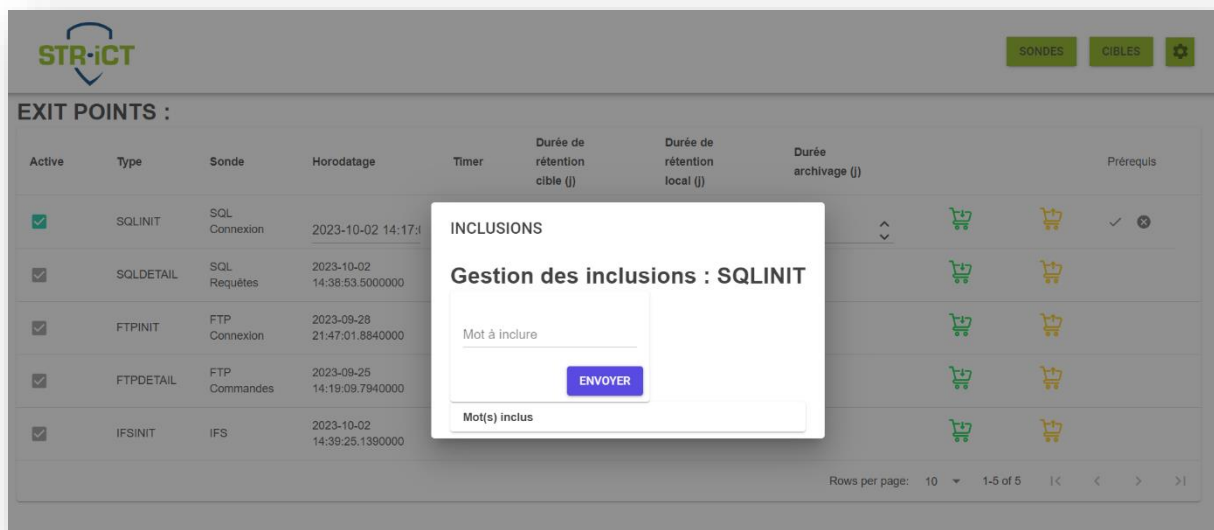
Active	Type	Sonde	Horodatage	Timer	Durée de rétention cible (j)	Durée de rétention local (j)	Durée archivage (j)	Prérequis
<input checked="" type="checkbox"/>	SQLINIT	SQL Connexion	2023-10-02 14:17:06.0260000	600	120	120	120	 
<input checked="" type="checkbox"/>	SQLDETAIL	SQL Requêtes	2023-10-02 14:38:53.5000000	300	120	121	120	 
<input checked="" type="checkbox"/>	FTPINIT	FTP Connexion	2023-09-28 21:47:01.8840000	200	120	120	120	  
<input checked="" type="checkbox"/>	FTPDETAIL	FTP Commandes	2023-09-25 14:19:09.7940000	0	120	120	120	 
<input checked="" type="checkbox"/>	IFSINIT	IFS	2023-10-02 14:39:25.1390000	600	120	120	120	 

Figure 53 : Affichage des Exit points















Active	Type	Sonde	Horodatage	Timer	Durée de rétention cible (j)	Durée de rétention local (j)	Durée archivage (j)	Prérequis
<input checked="" type="checkbox"/>	SQLINIT	SQL Connexion	2023-10-02 14:17:06.0260000	600	120	120	120	  
<input checked="" type="checkbox"/>	SQLDETAIL	SQL Requêtes	2023-10-02 14:38:53.5000000	300	120	121	120	 
<input checked="" type="checkbox"/>	FTPINIT	FTP Connexion	2023-09-28 21:47:01.8840000	200	120	120	120	  
<input checked="" type="checkbox"/>	FTPDETAIL	FTP Commandes	2023-09-25 14:19:09.7940000	0	120	120	120	 
<input checked="" type="checkbox"/>	IFSINIT	IFS	2023-10-02 14:39:25.1390000	600	120	120	120	 

Figure 54 : Fenêtre de gestion des inclusions

Une fois cela fait, vous devez vous trouver sur l'écran de la Figure 54. C'est sûr cet écran que vous pouvez configurer vos valeurs à inclure, il vous suffit alors de rentrer dans le champ « Mot à inclure » le mot de votre choix qui servira de filtre dans votre prochaine génération d'enregistrements, puis d'appuyer sur le bouton bleu **ENVOYER**.

A noter que les mots composés de lettres que vous rentrerez dans le champ seront **changer en majuscule** pour des raisons de cohérence avec les requêtes SQL/FTP/IFS.

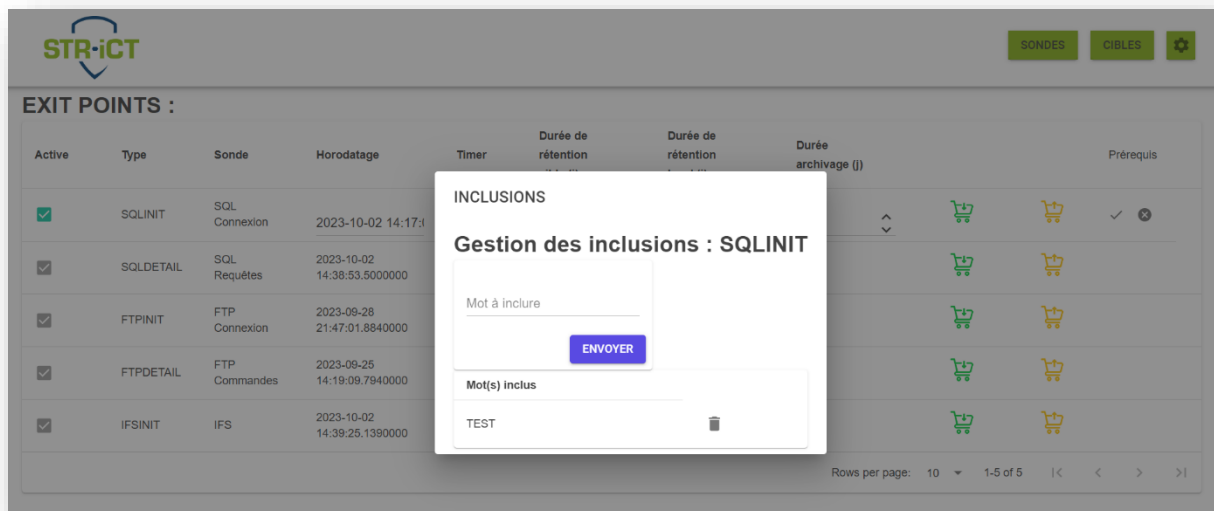



Figure 55 : Exemple d'inclusion

Comme précédemment dit, une fois votre mot envoyé vous pouvez facilement le **supprimer** en **appuyant** sur l'icône , vous avez la possibilité de répéter le processus d'ajout de valeurs incluent autant de fois que vous le désirez

Pour **quitter cette fenêtre** vous pouvez simplement cliquer en dehors de celle-ci

A noter que si le mot n'est pas envoyé il ne sera pas sauvegardé dans la table

Le parcours des inclusions **est le même** pour chaque Exit points vous pouvez donc définir des valeurs incluent pour chacun d'entre eux **indépendamment**

Gestion des exceptions

Pour chaque Exit point, il est possible de définir des **valeurs à exclure**.

Par exemple, pour les connexions SQL(SQLINIT), vous pouvez exclure tous les enregistrements qui contiennent des mots clés ou des profils d'utilisateurs. Ainsi seront tracées toutes les requêtes SQL qui ne contiennent pas valeurs exclues. (L'inverse est aussi possible par les valeurs dites : d'inclusions)

Le paramétrage des exceptions n'est pas définitif, vous pouvez décider de rajouter ou de supprimer des exceptions existantes, tout au long de votre utilisation du logiciel STR-iCT. Vous avez également la possibilité de créer des exceptions « manuellement ».

Afin de gérer les exceptions, vous devez renseigner une valeur horodatage qui s'occupera de filtrer les résultats pour presque tous les Exit points excepté SQLDETAIL (qui contient les requêtes SQL).

Le bouton dédié aux Exceptions (chariot orange) est actif que si l'exit point est activé et que ses prérequis sont validés.



Le **paramétrage des règles d'exception** est accessible en cliquant sur le chariot orange (Gérer les exceptions). Cf. Figure ci-dessus

Active	Type	Sonde	Horodatage	Timer	Durée de rétention cible (j)	Durée de rétention local (j)	Durée archivage (j)	Prérequis	
<input checked="" type="checkbox"/>	SQLINIT	SQL Connexion	2023-10-02 14:17:06.0260000	600	120	120	120		
<input checked="" type="checkbox"/>	SQLDETAIL	SQL Requêtes	2023-10-02 14:38:53.5000000	300	120	121	120		Gérer les exceptions
<input checked="" type="checkbox"/>	FTPINIT	FTP Connexion	2023-09-28 21:47:01.8840000	200	120	120	120		
<input checked="" type="checkbox"/>	FTPDETAIL	FTP Commandes	2023-09-25 14:19:09.7940000	0	120	120	120		
<input checked="" type="checkbox"/>	IFSINIT	IFS	2023-10-02 14:39:25.1390000	600	120	120	120		

Rows per page: 10 1-5 of 5

Figure 56 : Cliquez chariot orange EP

Un clic sur le chariot orange entraîne l'ouverture de la fenêtre de la gestion des exceptions, fenêtre vide lors du premier démarrage de l'interface graphique.

Profil	Nom Metier	Nom Utilisateur	IP

Rows per page: 10 0-0 of 0

Figure 57 : Fenêtre affichage des exceptions pour SQLINIT : vide au premier démarrage

Il y a sur cet écran 3 boutons qui ont tous trois des fonctions différentes, en voici une courte explication :

- **AJOUTER DES EXCEPTIONS** permet le paramétrage des exceptions qu'on reparlera plus en détail
- **TOUT EXCLURE** est une option seulement disponible sur les Exit points qui auras pour utilité de supprimer toutes vos règles d'exceptions et de laisser place à une ligne unique dans la table qui excluras toutes les valeurs. Si vous cliquez sur le bouton une fenêtre vous mettras en alerte que vous allez supprimer le contenu de la table (Figure 58)

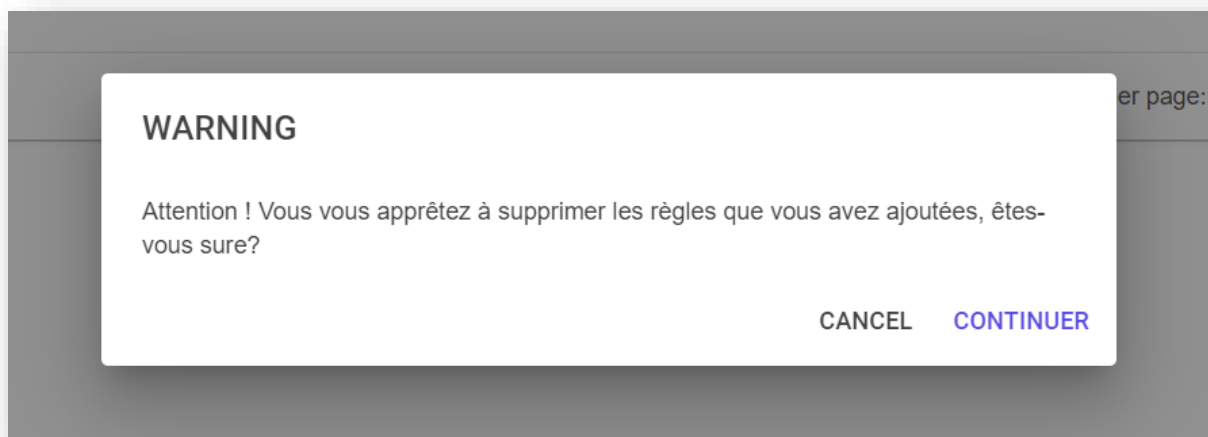


Figure 58: Tout exclure warning

- **RETOUR AUX EXIT POINTS** vous permet simplement de naviguer dans l'application et de revenir sur vos pas.

Le **paramétrage des exceptions** est réalisé à partir de la liste des événements enregistrés par la sonde. Pour obtenir la liste des événements, cliquez sur le bouton en haut à gauche **AJOUTER DES EXCEPTIONS** - Figure 57

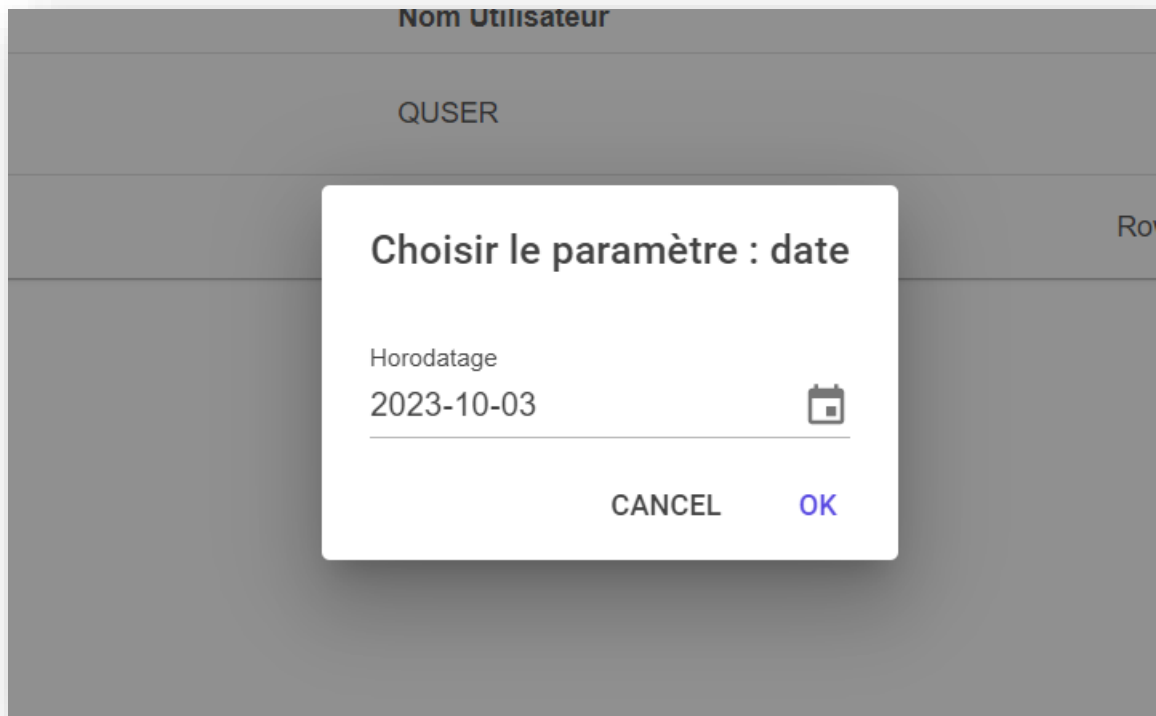


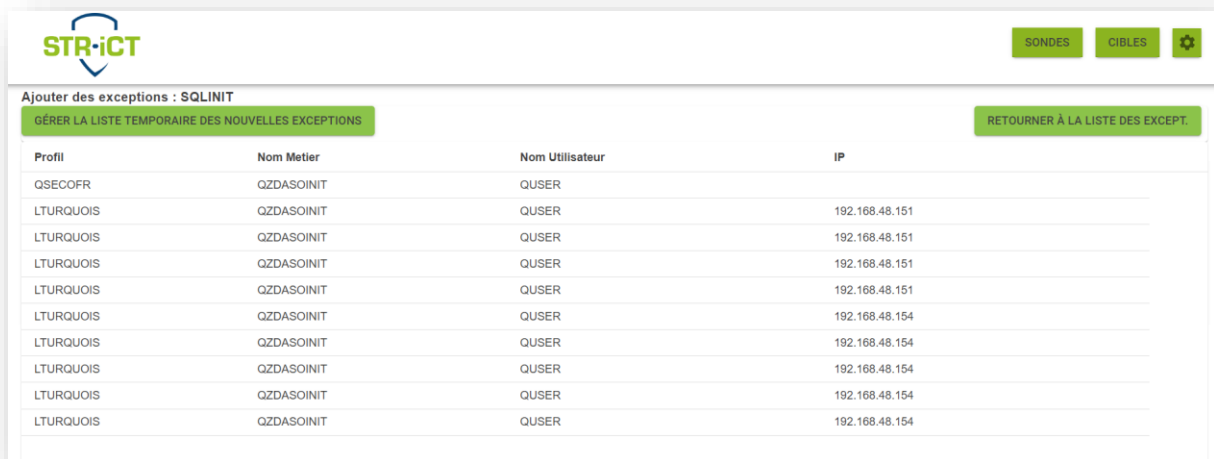
Figure 59 : Paramètre date EP

Une boîte de dialogue s'ouvre alors permettant de renseigner le paramètre « date », ce paramètre permet de récupérer les enregistrements jusqu'à la date renseignée, par défaut la date actuelle de la machine - Figure 59

A noter que ce paramétrage n'est pas nécessaire pour SQLDETAIL

Une fois la date voulue renseignée vous pouvez appuyer sur **OK** la liste (Figure 59), les enregistrements jusqu'à cette date vous sont alors présentés.

C'est à partir de cette liste que vous allez sélectionner les exceptions.

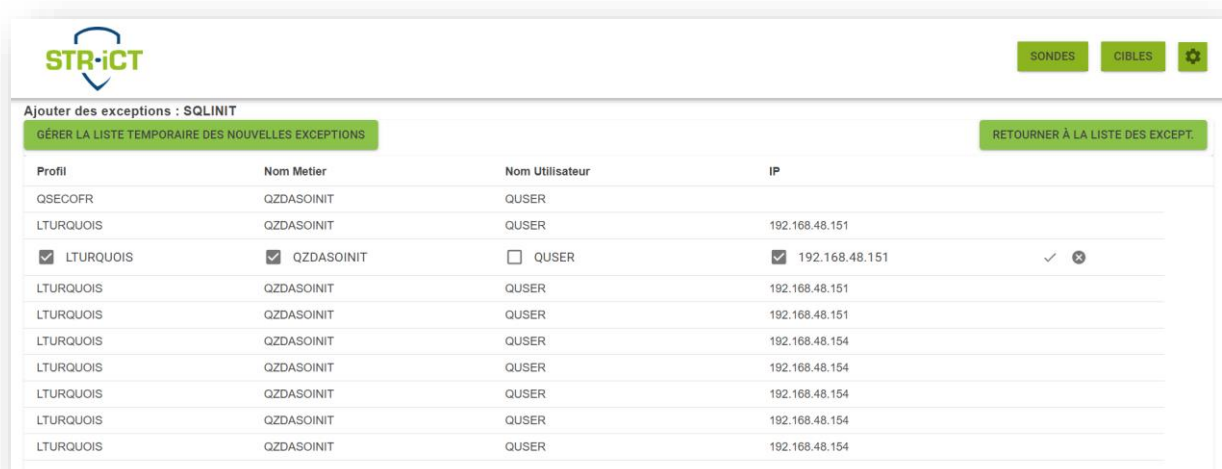


Profil	Nom Metier	Nom Utilisateur	IP
QSECOFR	QZDASOINIT	QUSER	
LTURQUOIS	QZDASOINIT	QUSER	192.168.48.151
LTURQUOIS	QZDASOINIT	QUSER	192.168.48.151
LTURQUOIS	QZDASOINIT	QUSER	192.168.48.151
LTURQUOIS	QZDASOINIT	QUSER	192.168.48.151
LTURQUOIS	QZDASOINIT	QUSER	192.168.48.154
LTURQUOIS	QZDASOINIT	QUSER	192.168.48.154
LTURQUOIS	QZDASOINIT	QUSER	192.168.48.154
LTURQUOIS	QZDASOINIT	QUSER	192.168.48.154
LTURQUOIS	QZDASOINIT	QUSER	192.168.48.154

Figure 60 : Liste des enregistrements du récepteur de journal (SQLINIT)

Pour **rajouter des exceptions** il vous suffit de **cliquer sur la ligne** comprenant l'enregistrement des valeurs à exclure dans la liste de données générées par la sonde.

Une fois la ligne cliquée vous avez la possibilité de cocher ou décocher les paramètres qui vous intéressent afin de garder seulement les valeurs à exclure - Figure 61.



Profil	Nom Metier	Nom Utilisateur	IP
QSECOFR	QZDASOINIT	QUSER	
LTURQUOIS	QZDASOINIT	QUSER	192.168.48.151
<input checked="" type="checkbox"/> LTURQUOIS	<input checked="" type="checkbox"/> QZDASOINIT	<input type="checkbox"/> QUSER	<input checked="" type="checkbox"/> 192.168.48.151
LTURQUOIS	QZDASOINIT	QUSER	192.168.48.151
LTURQUOIS	QZDASOINIT	QUSER	192.168.48.151
LTURQUOIS	QZDASOINIT	QUSER	192.168.48.154
LTURQUOIS	QZDASOINIT	QUSER	192.168.48.154
LTURQUOIS	QZDASOINIT	QUSER	192.168.48.154
LTURQUOIS	QZDASOINIT	QUSER	192.168.48.154
LTURQUOIS	QZDASOINIT	QUSER	192.168.48.154

Figure 61 : Décocher ou cocher des valeurs pour EP

Puis cliquez au bout de la ligne sur la **coche** ✓ pour valider votre choix et rajouter l'exception dans la **liste temporaire des nouvelles exceptions** ou sur la **croix** ✕ pour annuler votre sélection. Renouvelez l'opération pour une autre exception si nécessaire.

A noter qu'il est impossible de rajouter une exception sans valeur cochée.



Une fois votre sélection faite, **cliquez** sur **GERER LA LISTE TEMPORAIRE DES NOUVELLES EXCEPTIONS** (en haut à gauche de l'écran), la fenêtre des exceptions rajoutées temporairement dans la liste depuis le journal récepteur vous est alors présentée (Figure 62).

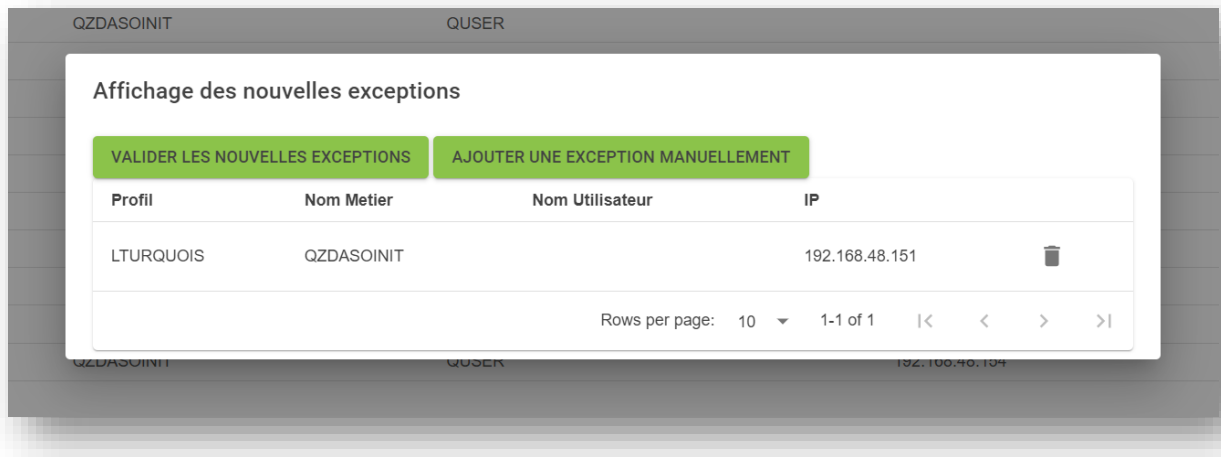


Figure 62 : Affichages des nouvelles exceptions temporaires pour SQLINIT

À partir de cet écran vous retrouvez vos exceptions rajoutées depuis la fenêtre précédente (**les valeurs décochées n'apparaissent pas**).

Vous avez la possibilité de retirer de la liste temporaire des exceptions en appuyant sur la poubelle



à droite pour chacune des lignes du tableau.

Il vous est aussi offert la possibilité de rajouter une exception manuellement en appuyant sur le bouton vert **AJOUTER UNE EXCEPTION MANUELLEMENT** vous conduit sur le formulaire d'ajout manuel, présenté sur la ci-dessus.

Affichage des nouvelles exceptions

VALIDER LES NOUVELLES EXCEPTIONS

Profil
10 caractères

Nom Metier
10 caractères

Nom Utilisateur
10 caractères

IP
45 caractères

ENVOYER

Profil	Job name	User name	IP
LTURQUOIS	QZDASOINIT		192.168.48.151

Rows per page: 10 1-1 of 1 |< < > >|

Figure 63 : Fenêtre d'ajout manuel possible d'une exception pour EP

Depuis cette fenêtre vous pouvez renseigner **manuellement** les informations à exclure selon votre machine et votre système d'information.

Ce formulaire d'ajout **est propre à chaque sonde** (Figure 63 – SQLINIT).

Une fois les informations transmises vous pouvez appuyer sur **ENVOYER** et votre exception manuelle sera **rajoutée dans la liste temporaire**.

Lorsque vous avez ajouté toutes les exceptions que vous vouliez rajouter dans la liste temporaire, vous pouvez appuyer sur le bouton vert **VALIDER LES NOUVELLES EXCEPTIONS**, qui en plus de rajouter vos exceptions vous renverra sur l'écran d'affichage des exceptions de la sonde (Figure 64).

Profil	Nom Metier	Nom Utilisateur	IP
LTURQUOIS	QZDASOINIT		192.168.48.151

Figure 64 : Affichage des exceptions retenues pour la SQLINIT

Durée d'archivage

La durée d'archivage correspond au nombre de jours durant lesquels les données de la sonde sont archivées dans l'IBM i. Elle est modifiable sur l'écran de la figure 31 en passant en mode « édition de sonde » (figure 33), une fois en édition il vous suffit de rentrer le nombre de jours de votre choix.


Il vous est aussi donné la possibilité de paramétrer la **durée de rétention cible** sur le même écran (durée d'archivage des sondes pour les cibles). Afin d'effectuer une modification cliquez au bout de la ligne sur la **coche** ✓ pour valider ou sur la **croix** ✕ pour annuler.

Sévérité & Risque

Nous définissons la **sévérité** comme le niveau d'impact d'un événement sur une organisation, en l'occurrence sur le fonctionnement de l'application sur IBM i, on pourrait aussi parler de gravité.

Le **risque** quant à lui est la possibilité qu'un événement entraîne directement ou indirectement, de manière volontaire ou involontaire, une altération du fonctionnement d'un système, en l'occurrence un IBM i. Il a pour mission d'informer sur la dangerosité potentielle d'un événement qui s'est déroulé et qui peut paraître anodin mais qui peut être une étape d'un processus dangereux.

L'interface graphique vous offre la possibilité de modifier ces 2 valeurs pour chaque type de violation et pour chaque cible

Pour commencer il vous suffit de vous rendre sur la Figure 31 puis d'appuyer sur l'icône  sur la ligne de la sonde de votre choix (Cf. Figure 49) afin d'arriver sur la Figure 50.




<input checked="" type="checkbox"/>	SQLINIT	SQL Connexion	2023-10-16 08:33:15.1780000	600	365	365	120			 Prérequis Ok	
-------------------------------------	---------	---------------	-----------------------------	-----	-----	-----	-----	---------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------

Figure 65 : Affichage des Sondes : Sévérité & Risque



Affichage des risques : SQL INIT

AJOUTER UN RISQUE RETOUR AUX EXIT POINTS

PROFIL	IP	Sévérité POSTGRE	Risque POSTGRE
-	-	20	50

Figure 66 : Affichage des risques SC

Depuis cette fenêtre vous avez plusieurs actions possibles sur les valeurs des risques par Cibles, vous pouvez **modifier** ces valeurs en passant en mode édition de ligne (le même procédé vu précédemment dans cette documentation)


Affichage des risques : SQL INIT

AJOUTER UN RISQUE RETOUR AUX EXIT POINTS

PROFIL	IP	Sévérité POSTGRE	Risque POSTGRE
-	-	20	50
	221.212.42.112	50	99

Figure 67 : Edition de risque pour la sonde SC

Puis pour valider vos modifications vous devez cliquer au bout de la ligne sur la **coche** ✓ pour valider ou sur la **croix** ✕ pour annuler.

Vous avez la possibilité de **retirer** des cas de risque en appuyant sur la poubelle  situé à droite de chaque ligne du tableau pour chaque sonde indépendamment

Vous avez à votre disposition 2 boutons :



- **AJOUTER UN CAS DE RISQUE** : Renvoie sur un formulaire d'ajout de cas de risque manuellement

Figure 68 : Ajout de risque manuellement SC

A noter que les valeurs de sévérité et risque ne peuvent dépasser 99 et que les champs IP ne peuvent contenir seulement des format d'IPv4 donc elles ne peuvent comprendre que 2 digits. Une fois vos valeurs saisies vous pouvez appuyer sur **VALIDER** afin de revenir sur l'affichage des cas de risques (Figure 50) et d'ajouter cas de risques dans la liste des risques.

- **RETOUR AUX SONDÉS** : Permet de naviguer dans l'application, renvoie à la Figure 31

Cible

Données significatives par sonde et visualisables dans le Dashboard Grafana.

Lien documentation :

OM	Gestion Objets		Type Objet, Library, Programme, type Modification
AD	Modification Attribut Audit		Type, Nouvelle Valeur, Ancienne Valeur
CP	Modification Profil Utilisateur		User concerné, Actions effectuées
IM	Tentative d'Intrusion		Programme, User, IP Locale IP distante
AF	Accès Refusé droits insuffisants		Utilisateur concerné, Cible de la tentative
DO	Suppression Objet		Objet concerné, Programme source, Utilisateur



PW	Mot De Passe		Programme et User source, Device
DS	Modification Profil SST		Programme et User Source, type de modification
NA	Modification TCP_IP		
OR	Objets Restaurés		Nom Objets, Bibliothèque, Programme
PA	Autorité Du Propriétaire		
PF	Actions PTF		Installations effectuées, Programme Source
ST	Actions SST		Type Action, Programme et user source
SV	Actions Valeurs Système		
VP	Erreur mot de Passe Réseau		
X0	Authentification Réseau		