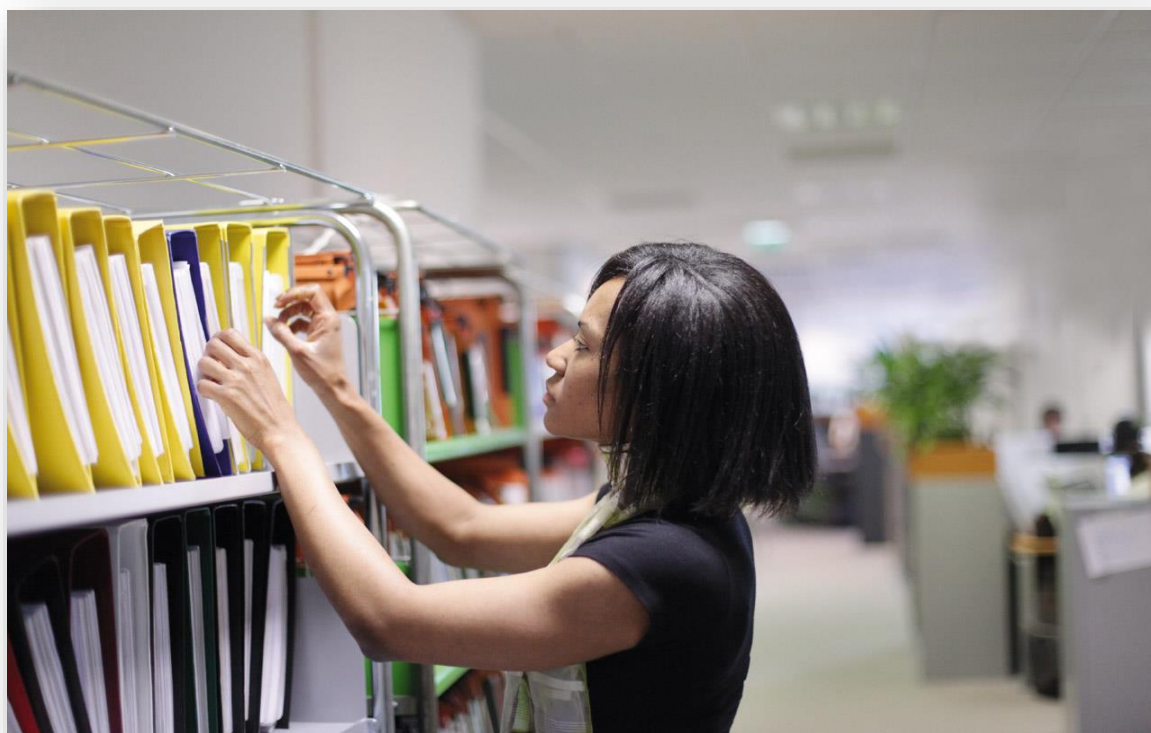


SAGE.Eb.eIDSign

version 3.00

Document Technique



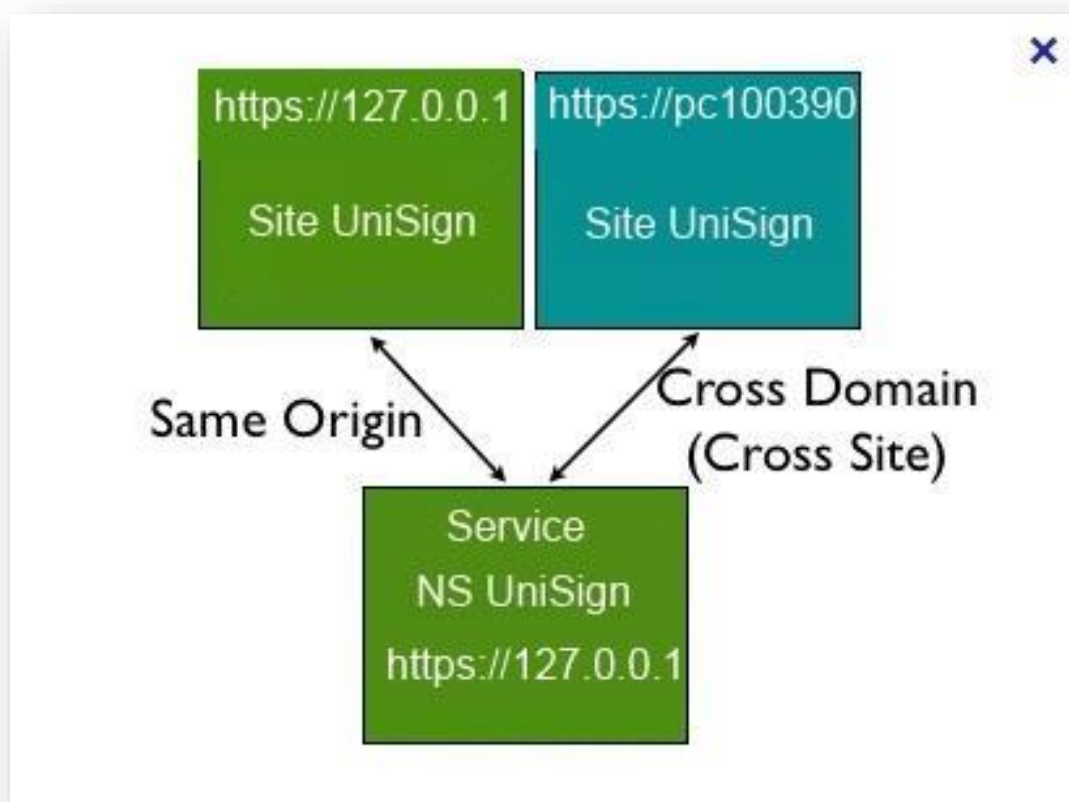
Sommaire

SUPPORT CORS	3
SUPPORT SSL	4
Internet Explorer 11.X et Google Chrome 48.X	4
Firefox 43.X.X	4
SUPPORT NTLM SSO (SINGLE-SIGN-ON)	6
IE 11.....	6
Firefox 39.X.X	6
SUPPORT ETW (EVENT TRACING FOR WINDOWS)	7
Utilisation des traces <i>UniSign</i> dans <i>Event Viewer</i>	8
Utilisation du service <i>eldSign</i> en mode Console	10
Enregistrement des canaux de Log dans ETW	10
TRADUCTION DES LIBELLES DES ECRANS <i>EIDSIGN</i>.....	11
GESTION DU CROSS-SITE REQUEST FORGERY	12
Définition.....	12
Mise en place du Jeton de validité sur SBE	12
GESTION DES FENETRES POP-UP DANS GOOGLE CHROME	15

Support CORS

Le Cross-origin resource sharing (CORS) est une spécification W3C (World Wide Web Consortium) qui autorise un site web via Ajax, à utiliser des ressources situées sur un autre domaine.

Pour le cas d'eIDSign, ce mécanisme permet de gérer le dialogue entre le site web (via le composant jquery plugin) et le service natif eIDSign lorsque ces deux éléments se trouvent sur deux serveurs distincts.



Support SSL

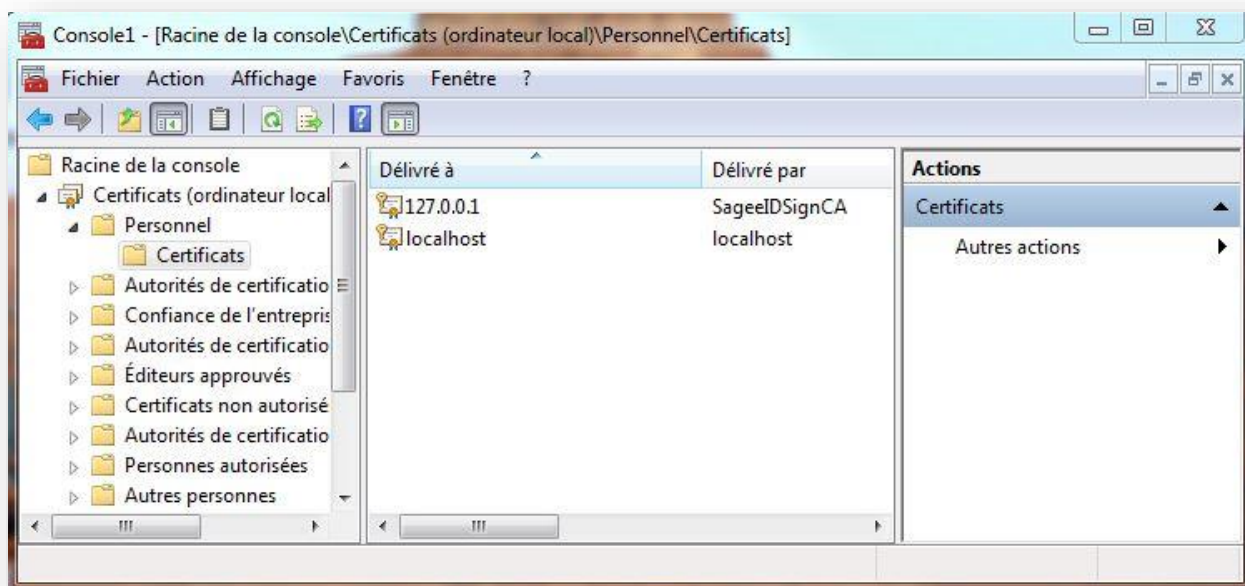
Internet Explorer 11.X et Google Chrome 48.X

Pour le cas d'IE et de Google Chrome, il faudra vérifier que le certificat du service Sage Eb eIDSign (127.0.0.1) a bien été généré dynamiquement et signé par le certificat d'autorité (SageeIDSignCA, également généré dynamiquement) et qu'ils sont bien tous les deux déclarés dans le Système d'Exploitation.

Pour ce faire il faut ouvrir la console Microsoft de gestion des certificats (mmc.exe).

On y ajoute un composant logiciel enfichable de type « compte d'ordinateur » pour l'ordinateur local.

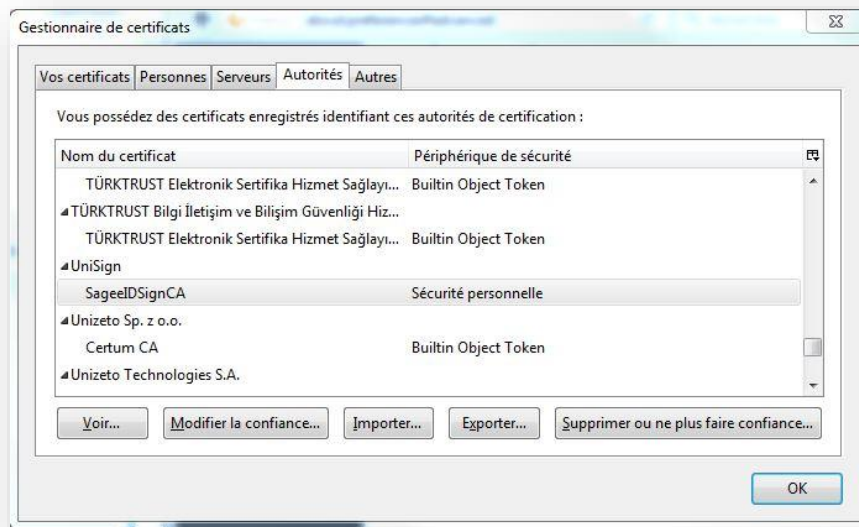
Dans le container « Certificats » du niveau « Autorités de certification racines de confiance », on vérifie la présence du certificat « 127.0.0.1 » délivré par SageeIDSignCA.



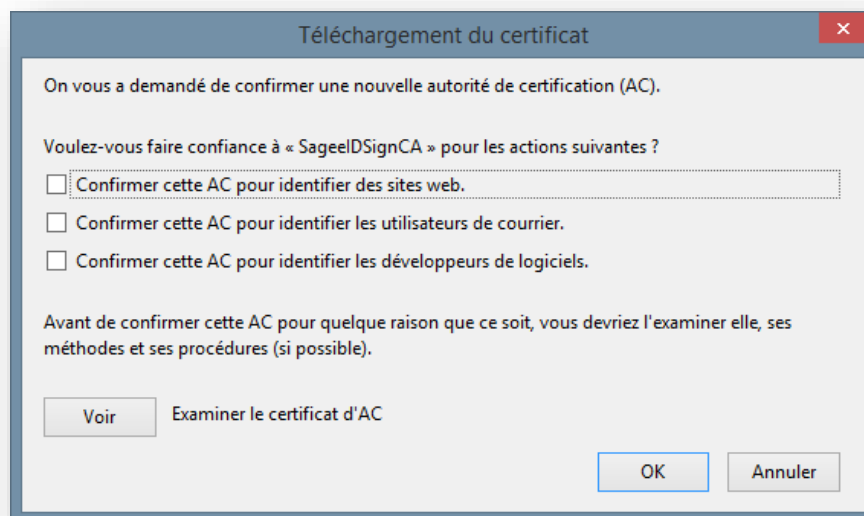
Firefox 43.X.X

Pour le cas de Firefox, il faudra importer le certificat « SageeIDSignCA » (C:\Program Files (x86)\SAGE\leIDSign) dans le container des Autorités de Certification.

- soit via le gestionnaire de certificats de Firefox



- soit en saisissant cette adresse dans Firefox : <http://127.0.0.1:48081/UniSign/ca> et en cochant toutes les cases dans la fenêtre ci-dessous



Support NTLM SSO (Single-Sign-On)

Le processus d'Authentification SSO permet à l'utilisateur d'accéder à plusieurs applications via une seule phase d'authentification, une seule saisie du couple login/password pour la session Windows et l'accès au site Web, par exemple.

IE 11

IE supporte nativement le Single-Sign-On.

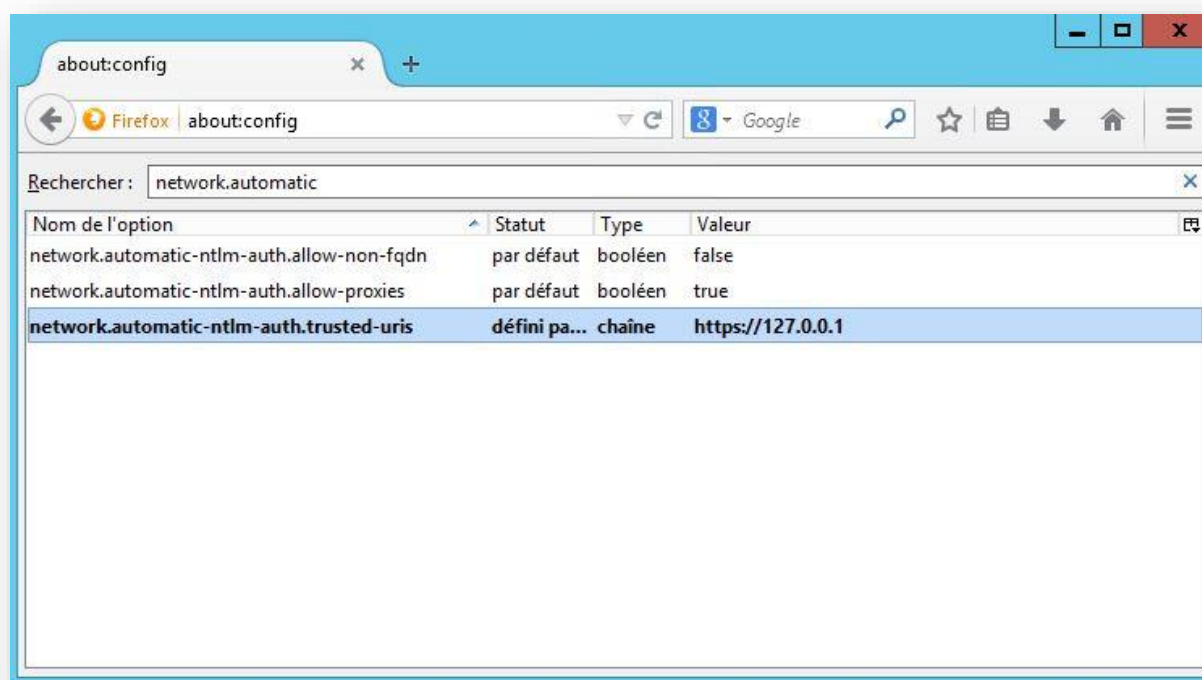
Firefox 39.X.X

Par défaut, Firefox n'utilise pas ce mode d'authentification.

C'est pourquoi, lors de l'installation du Service eIDSign, le mode d'authentification SSO sera automatiquement activé dans la configuration de Firefox.

Pour le vérifier, il faut accéder à la page de configuration de Firefox (about:config) et trouver l'option chaîne « network.automatic-ntlm-auth.trusted-uris » avec la valeur « <https://127.0.0.1> ».

Voir aussi le fichier « **user.js** » dans le dossier contenant le Profile Firefox de l'utilisateur.



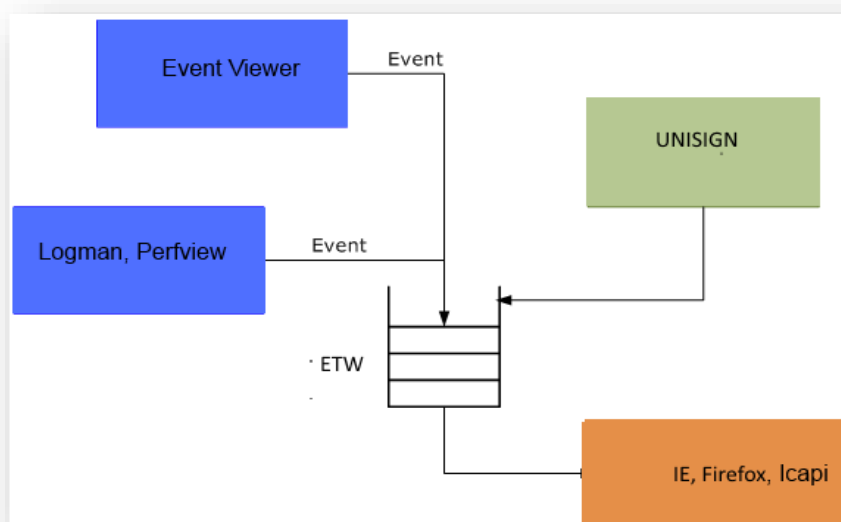
Support ETW (Event Tracing for Windows)

ETW est un outil développé par Microsoft pour analyser l'activité de tous les programmes et services Windows afin d'en optimiser les performances et les diagnostics et la maintenance.

Il permet de générer des traces conceptualisées (Administration, Analytique et Debug) sur la base du composant « eventsource ».

Le programme ou service à tracer (dans notre cas, eIDSign) implémente un ou plusieurs fournisseurs d'événements (Event provider). Lorsque ces derniers veulent écrire dans la trace, ils génèrent un événement (Event) qui sera placé dans une file d'attente (la trace) gérée par ETW.

L'application qui lit la trace est un listener. Elle se connecte sur la trace et ETW lui envoie les événements mémorisés un à un. L'application cliente reçoit chaque événement sous la forme d'une structure binaire. Elle doit alors interpréter sa signification et le décoder pour l'afficher ou l'enregistrer en fonction des besoins.



Il existe de nombreux outils qui permettent de collecter et d'analyser les traces générées.

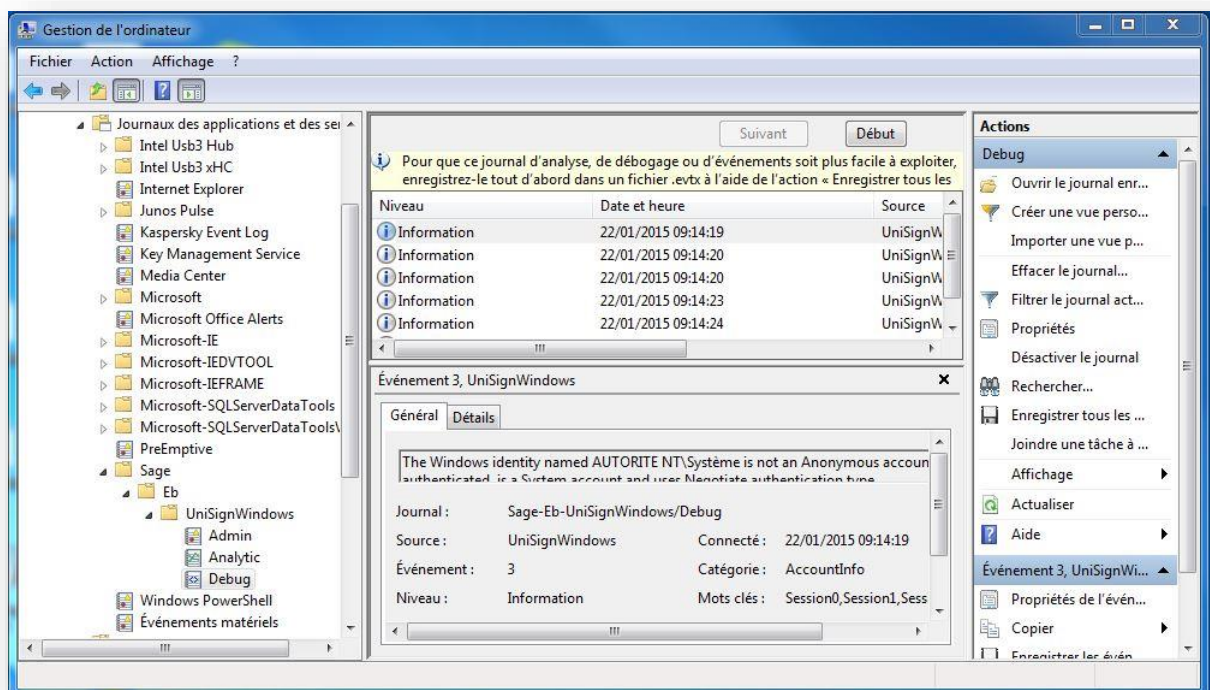
1. Logman permet entre autres, via la ligne de commande, de démarrer et arrêter une trace en créant un nouveau « *journal de traçage* ».
2. Perfview propose une interface graphique qui regroupe collecte et analyse.
3. L'Observateur d'évènement de Windows (Event Viewer) qui permet de gérer des traces applicatives sous 3 canaux différents (Admin, Analytic et Debug), le premier activé par défaut, les deux autres activables sur demande pour répondre aux besoins d'analyse ou de maintenance.

Utilisation des traces *UniSign* dans *Event Viewer*

Suite à l'installation du service de Signature, seul le canal <Admin> est affiché.

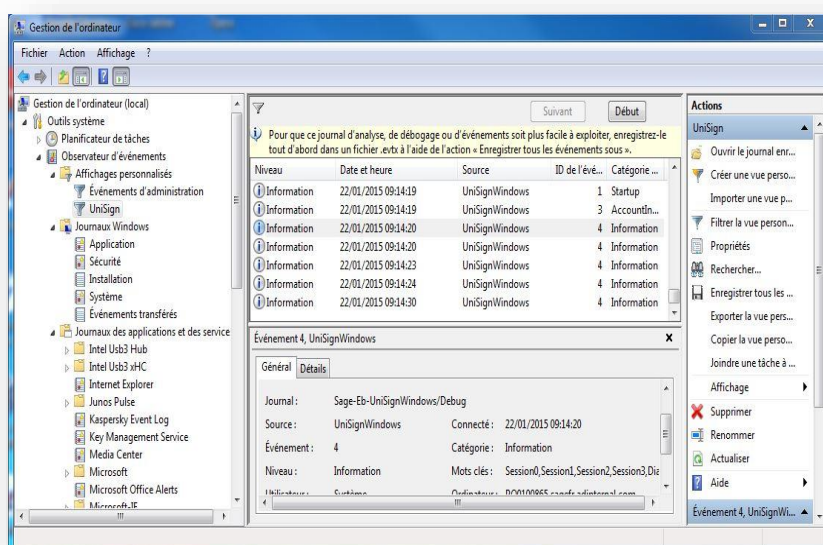
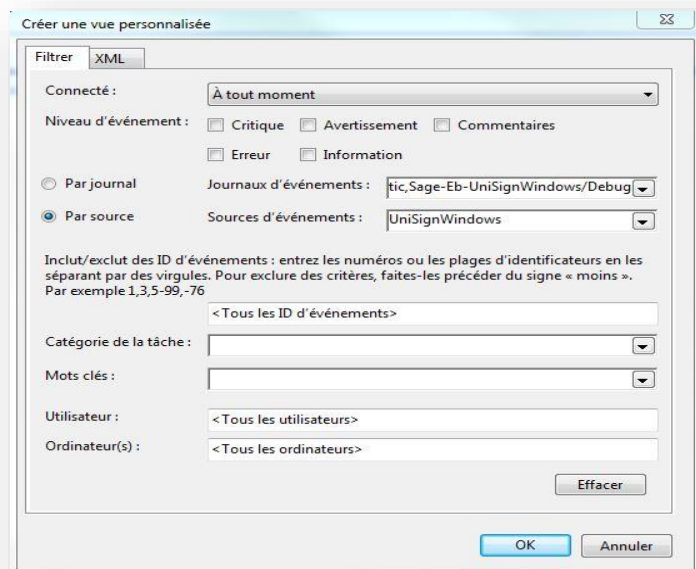
Les canaux <Analytic> et <Debug> doivent être affichés et activés manuellement.

UniSignWindows/Affichage/Afficher les journaux d'analyse et de débogage puis *clic droit* sur le canal et *activer le journal*.



Il permet aussi de créer des vues personnalisées pour afficher le résultat des différents canaux de manière unifiée.

Observateur d'évènement/Affichages personnalisés/Créer une vue personnalisée



Utilisation du service eldSign en mode Console

Dans C:\Program Files (x86)\SAGE\elDSign, lancer la commande :

Sage.Eb.UniSign.Windows.exe NoService

Enregistrement des canaux de Log dans ETW

Pour enregistrer, lancer la commande

Reg Etw

Pour désenregistrer, lancer la commande

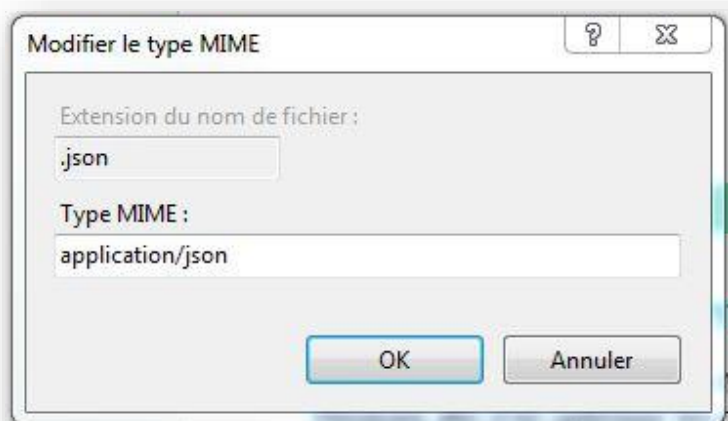
Unreg Etw

Traduction des libellés des écrans *eIDSign*

Les fichiers de langue pour les différentes versions des libellés des écrans *eIDSign* sont gérés dans des fichiers json (*unisign-dev.json*), un par langue.

Par défaut les extensions *.json* ne sont pas reconnues par IIS.

Il faut ajouter la prise en charge de cette extension dans la fonctionnalité <Type Mime> des paramètres IIS.



Gestion du Cross-Site Request Forgery

Définition

En [sécurité informatique](#), le **Cross-Site Request Forgery**, abrégé **CSRF** (parfois prononcé *sea-surfing* en anglais) ou **XSRF**, est un type de [vulnérabilité des services d'authentification web](#).

L'objet de cette attaque est de transmettre à un utilisateur authentifié une requête HTTP falsifiée qui pointe sur une action interne au site, afin qu'il l'exécute sans en avoir conscience et en utilisant ses propres droits.

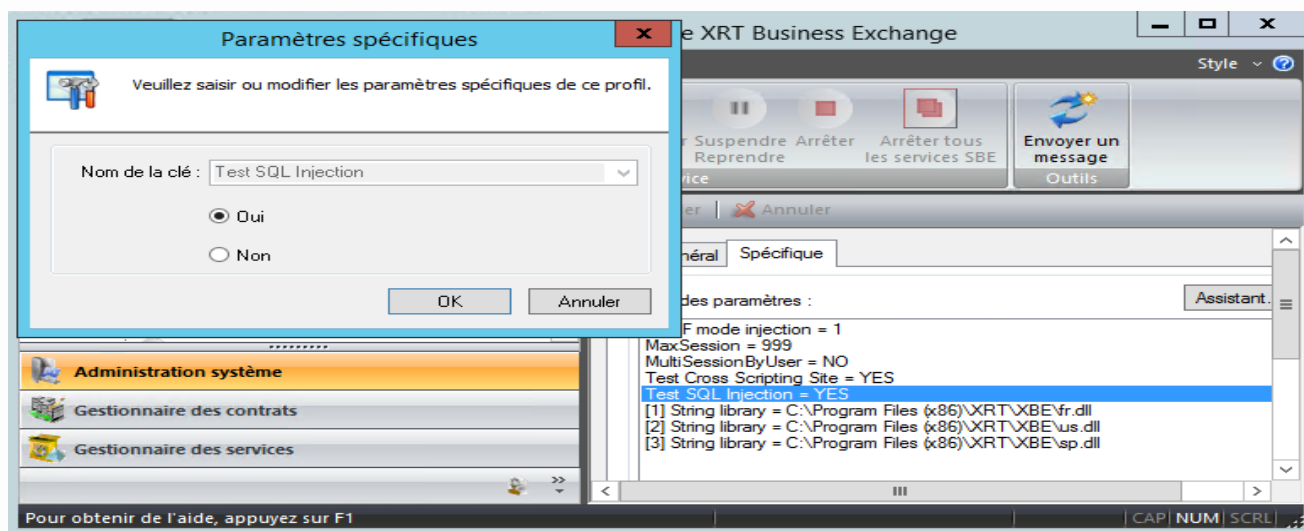
La meilleure prévention de ce type d'attaque consiste donc à sécuriser les requêtes de type POST et GET.

Pour ce faire le meilleur moyen est d'utiliser des jetons de validité dans les formulaires : faire en sorte qu'un formulaire posté ne soit accepté que s'il a été produit quelques minutes auparavant : le jeton de validité en sera la preuve. Le jeton de validité doit être transmis en paramètre et vérifié côté serveur.

Mise en place du Jeton de validité sur SBE

Dans l'interface SBE, le paramétrage adéquat se déclare dans le module d'Administration pour les propriétés spécifiques du Service Transactionnel (P5CWEB).

Il faut y activer le paramètre « Test Cross Scripting Site »



Pour vérifier la bonne prise en compte de ce paramètre et la génération du jeton de validité, il faut :

- Démarrer le service transactionnel en mode debug (p5cweb noservice /debug)
- Identifier l'élément « Test CRSF → »

```
Test CRSF ==> ref:http://sageparaphin.cloudapp.net/OnlineBanking/viewsign/
vices/paraphs/fileToSign.html,tok=696804C92D114239B1B6BB707F8C22D7
**** [768] Démarrage de l'exécution du script ActiveX sur le fichier 'fr\s
s\sbe\UpSignRp.htm'
Data send:65 bytes
 43 61 63 68 65 2D 43 6F 6E 74  Cache-Cont
 72 6F 6C 3A 20 70 72 69 76 61  rol: priva
 74 65 0D 0A 63 6F 6E 74 65 6E  te..conten
 74 2D                                t-
**** [768 : 31 ms] Fin d'exécution du script
```



Gestion des fenêtres pop-up dans Google Chrome

Toujours autoriser les pop-up sur un site spécifique

1. Ouvrez Chrome.
2. Dans l'angle supérieur droit, cliquez sur le menu Chrome ☰.
3. Cliquez sur **Paramètres**.
4. Cliquez sur **Afficher les paramètres avancés**.
5. Sous "Confidentialité", cliquez sur le bouton **Paramètres de contenu**.
6. Sous "Fenêtres pop-up", cliquez sur **Gérer les exceptions**.