Prérequis pour le fonctionnement de l'extension sur le poste client

Aucun prérequis pour le fonctionnement de l'extension sur le poste client pour le navigateur Mozilla Firefox

Prérequis pour le fonctionnement de l'extension sur le poste client pour les navigateurs de type Chromium (Chrome, Edge)

L'ordinateur du poste client doit forcément être géré.

Les solutions sont les suivantes :

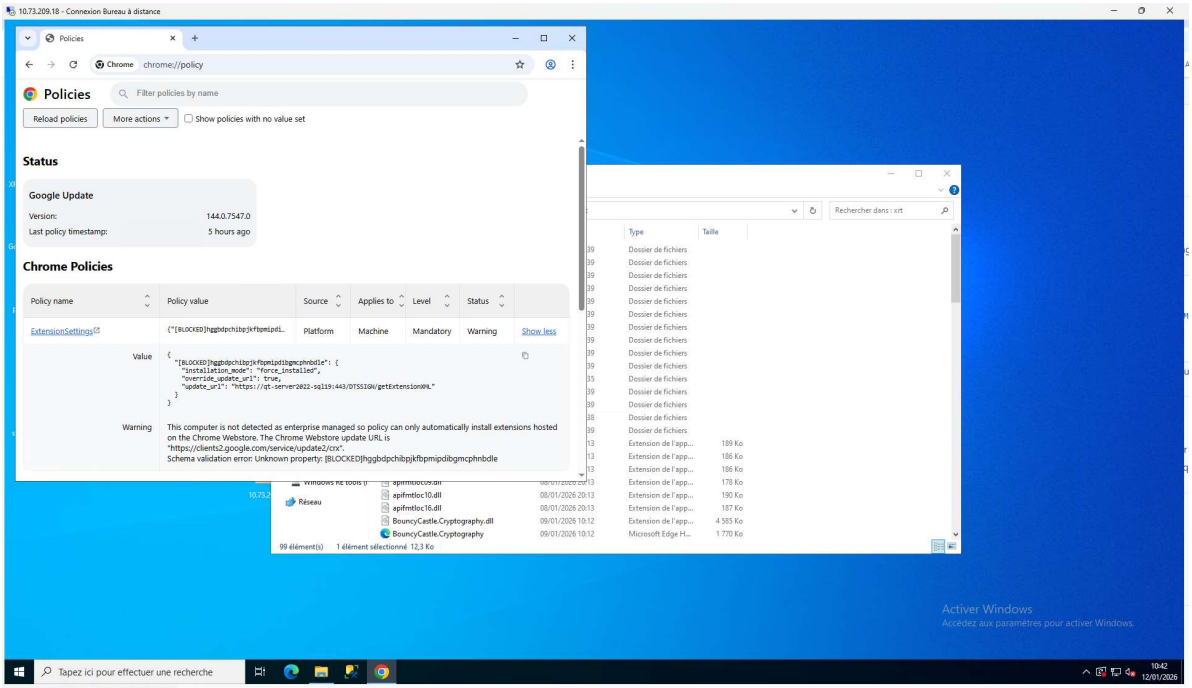
Joindre l'appareil à un domaine ou MDM

- Active Directory ou Azure AD.
- Ou utiliser une solution MDM (Google Workspace, Intune, etc.)

Activer le mode entreprise via un token de gestion

- Google propose un « enrollment token » pour marquer Chrome comme géré sans domaine.

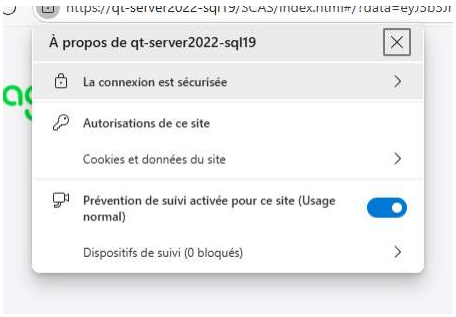
Si l'ordinateur est rattaché à un groupe de travail (workgroup) alors l'extension sera marquée comme bloquée (non fonctionnelle). Il est possible de visualiser le blocage dans le navigateur en entrant chrome://policy



L’URL d’accès au site des widgets doit être sécurisée et valide.

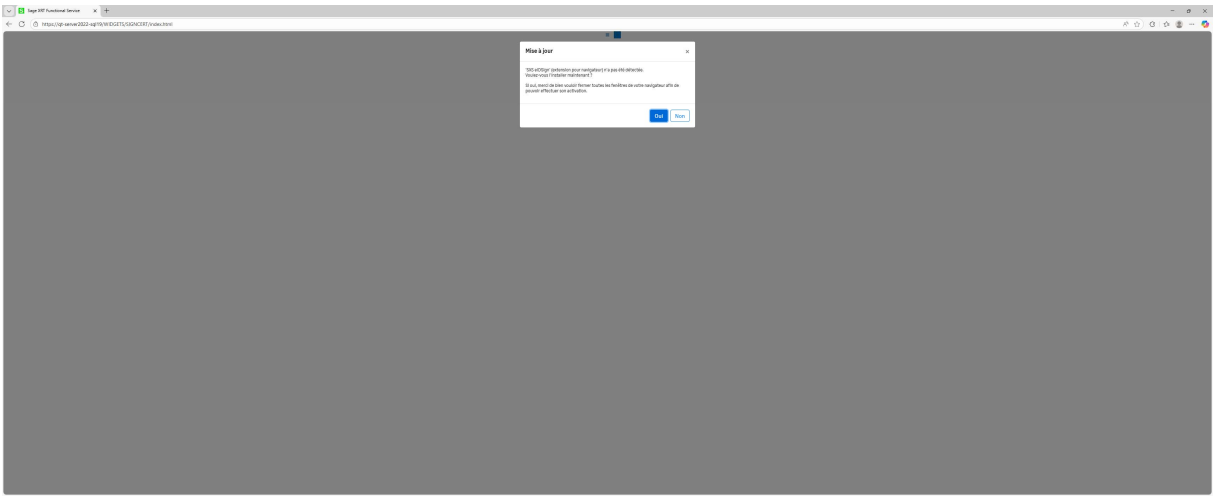
Exemple avec l’url https://qt-server2022-sql19/WIDGETS/SIGNCERT

Le site doit être sécurisé en https et le certificat du serveur sur IIS doit être valide. Si le site n’est pas sécurisé ou s’il y a une erreur ou un avertissement au niveau du certificat serveur alors l’extension ne sera pas fonctionnelle.



Installation de l’extension sur le poste client

Dans les conditions d’environnement correctes, lors de l’utilisation d’un widget de signature (SIGNCERT ou SIGNFILE), lors de la première installation de l’extension (ou mise à jour), le message suivant apparait :

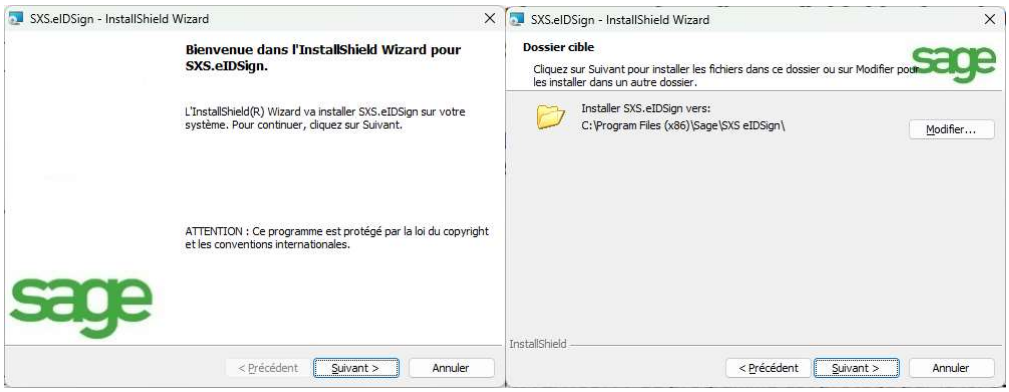


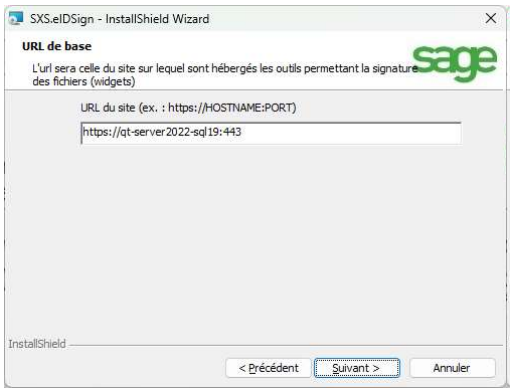
L’acceptation entraine le téléchargement d’un fichier de type SXS.eIDSign.Installer[aHR0cHM6Ly9xdC1zZXJ2ZXIyMDIyLXNxbDE5OjQ0Mw==].exe

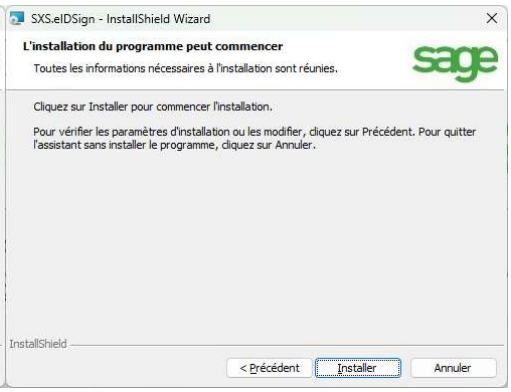
La valeur aHR0cHM6Ly9xdC1zZXJ2ZXIyMDIyLXNxbDE5OjQ0Mw== est une chaine encodée en base64 qui contient l’url de base du site des widgets afin que l’utilisateur final n’ait pas à la saisir lors de l’installation.

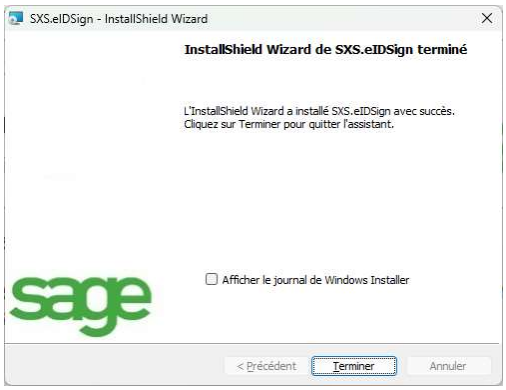
Dans ce cas, elle contient https://qt-server2022-sql19:443

L’utilisateur final peut lancer l’installation en exécutant ce fichier.



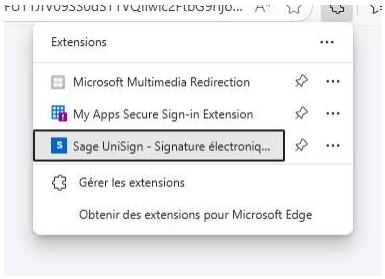






A la fin de l'installation, l'utilisateur DEVRA fermer toutes les instances de son navigateur (Edge et/ou Chrome) afin de pouvoir bénéficier de l'extension à la prochaine navigation.

A l'ouverture suivante du navigateur, l'extension devrait être ajoutée au niveau des extensions :



L'utilisateur peut à nouveau effectuer des opérations cryptographiques en utilisant les widgets.

Données techniques

Le programme va installer le module natif dans le répertoire par défaut C:\Program Files (x86)\Sage\SXS eIDSign. Ce répertoire est modifiable lors de l'installation.

Chrome / Edge

Pendant l'installation, les clés suivantes vont être ajoutées au registre :

Ordinateur\HKEY_LOCAL_MACHINE\SOFTWARE\Google\Chrome\NativeMessagingHosts\com.sage.unisign.native

Ordinateur\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Edge\NativeMessagingHosts\com.sage.unisign.native

Elles contiendront le chemin vers le fichier installé com.sage.unisign.native.json. Celui-ci indique le chemin vers l'exécutable et l'ID de l'extension du navigateur qui peut y accéder.

Afin d'autoriser le navigateur à utiliser l'extension, l'installateur va ajouter ou modifier la valeur ExtensionSettings des clés de registre dans Ordinateur\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome et Ordinateur\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge.

La valeur suivante sera ajoutée (ou mise à jour) :

"hggbdpchibpjkfbpmipdibgmcphnbdle":{"installation_mode":"force_installed","update_url":"https://qt-server2022-sql19:443/DTSSIGN/getExtensionXML","override_update_url":true}

hggbdpchibpjkfbpmipdibgmcphnbdle est l'ID de notre extension pour Chrome/Edge.

Attention, dans le cadre d'une utilisation globale de la GPO, ces valeurs peuvent être amenées à être écrasées régulièrement et donc empêcher l'extension de fonctionner sur les postes clients.

Il est donc important d'autoriser cette extension de façon globale OU de ne pas apporter de restriction au niveau des extensions.

Firefox

Contrairement aux navigateurs Chromium qui nécessitent une url sécurisée de téléchargement, l'extension signée par Mozilla sera installée sur le client sous le répertoire d'installation (C:\Program Files (x86)\Sage\SXS eIDSign par défaut). Elle a pour nom firefox_extension.xpi

Pendant l'installation, la clé suivante va être ajoutée au registre :

Ordinateur\HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\NativeMessagingHosts\com.sage.unisign.native

Elle contiendra le chemin vers le fichier installé com.sage.unisign.native.firefox.json. Celui-ci indique le chemin vers l'exécutable et l'ID de l'extension du navigateur qui peut y accéder.

Afin d'autoriser le navigateur à utiliser l'extension, l'installateur va ajouter ou modifier la valeur ExtensionSettings de la clé de registre dans Ordinateur\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Mozilla\Firefox.

La valeur suivante sera ajoutée (ou mise à jour) :

"sage-unisign@sage.com": { "installation_mode": "force_installed", "install_url": "file:///C:/Program Files (x86)/Sage/SXS eIDSign/firefox_extension.xpi"}

sage-unisign@sage.com est l'ID de notre extension pour Firefox.