



# Sage XRT Business Exchange

Version 12.2.100

Sage Rest Api



# Sommaire



<b>Présentation .....</b>	<b>3</b>
<b>Installation.....</b>	<b>4</b>
<b>Fichier de configuration.....</b>	<b>5</b>
<b>Mode debug et fichier de log .....</b>	<b>9</b>

## Présentation

Le service **Sage Rest Api** (SRA) vous permet d'échanger des données avec l'application **Sage XRT Business Exchange** à l'aide de l'**Api Rest**.

Trois types d'Api existent :

- **Api Rest d'administration**

Elles permettent d'administrer la plate-forme (création d'une entité ou d'un contrat bancaire, etc.).

- **Api Rest de production simple**

Elles permettent de suivre le parcours des flux bancaires (ajout d'un fichier dans le poste de signature, envoi ou réception d'un fichier, suivi des statuts des fichiers, etc.).

- **Api Rest de production étendue**

Elles permettent de superviser le fonctionnement de la plate-forme et de certains traitements (monitoring des services, des règles de signature serveurs, récupérations des logs, etc.).

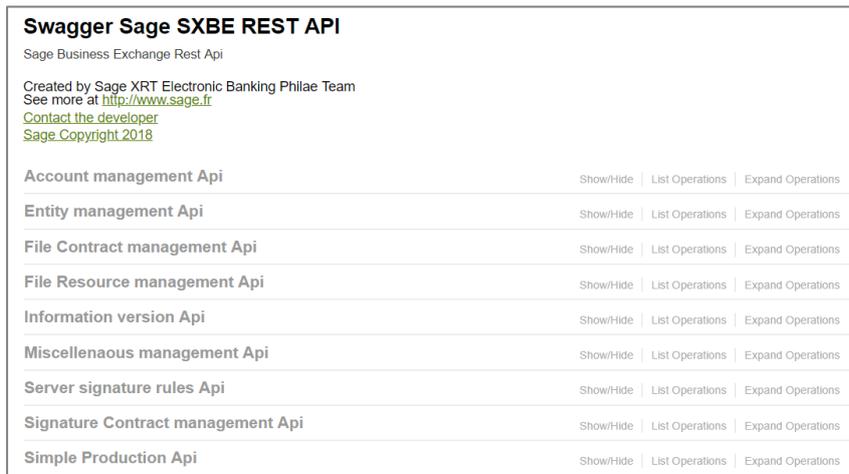
# Installation

L'installation du service **Sage Rest Api** nécessite l'exécution du package *Sage.Eb.Admin.Rest.Api.Installer.exe*.



**Sage Rest Api** doit être démarré avec un compte de service.

La documentation des **Api Rest** est disponible sur *http(s)://Hostname/sra/swagger*. Vous pouvez consulter le détail des Api déjà disponibles dans cette version.



L'accès aux Api est soumis aux droits suivants dans **Sage XRT Common Services**.



L'utilisation de l'Api **POST/v1/pdssa/geturlwpage** nécessite de paramétrer la variable **Allow Authentication Redirection** sur le **Service de transaction**, dispositif **OnlineBanking**.

## Fichier de configuration

Certaines informations nécessaires au fonctionnement du service, sont automatiquement récupérées lors de son installation.

Parfois, l'architecture souhaitée nécessite de définir certains paramètres (modifier le DSN, l'adresse de la machine, etc.).

Le tableau ci-dessous décrit le fichier de configuration *Sage.Eb.Admin.Rest.Api.exe.config*.

<appSettings>	Commentaires
<add key="UseSecureChannel" value="true" />	https ou http (par défaut https)
<add key="SecureChannelCertificateName" value="" />	Si non renseigné, par défaut True
<add key="DefaultAuthScheme" value="Ntlm" />	Méthode d'authentification : <ul style="list-style-type: none"> <li>▪ Ntlm (Par défaut)</li> <li>▪ SageXRT (basée sur le service SCAS)</li> <li>▪ Negotiate (Ntlm et/ou Kerberos)</li> <li>▪ IntegratedWindowsAuthentication</li> <li>▪ Basic</li> <li>▪ Anonymous</li> <li>▪ SageID</li> <li>▪ OAuth (Version OAuth2)</li> <li>▪ Saml (Version SamlV2)</li> <li>▪ Jwt (Json Web Token)</li> </ul>
<add key="Address" value="" />	Nom du serveur, par défaut nom de la machine
<add key="AdditionnalPath" value="" />	Chemin d'accès à l'Api Rest par défaut sra
<add key="Port" value="443" />	Port d'accès de l'Api Rest par défaut 443
<add key="LogFile" value="C:\temp\sage.eb.admin.rest.api.log" />	Chemin et log du service par défaut non activés si aucune valeur définie
<b>Paramètres de l'authentification SageXRT</b>	
<add key="SCAS" value="http://NomMachine:8760" />	Si méthode d'authentification = SageXRT
<add key="SCPS" value="http://NomMachine:8733" />	Si méthode d'authentification = SageXRT

<appSettings>	Commentaires
<b>Paramètres de l'authentification SageID</b>	
<pre>&lt;add key="SageIDAccessTokenEncryptionKey" value="Hhlnk2r3dYXtJouX6Zb223TCVMfD1fN1//g nmj6nZYU=" /&gt;</pre>	Clé de déchiffrement du token d'accès SageID
<pre>&lt;add key="SageIDAccessTokenEncryptionInitialisationVector" value="OwJAAKjcpt1sEQF/qTrU/g==" /&gt;</pre>	Vecteur d'initialisation de la clé de déchiffrement du token d'accès SageID
<pre>&lt;add key="SageIDSSORootCertificateFindValue" value="CN=Sage SSO Identity Root (Pre-Production), O=Sage (UK) Limited, C=United Kingdom" /&gt;</pre>	Nom du certificat racine (SageID)
<pre>&lt;add key="SageIDSSORootCertificateFindType" value="FindBySubjectDistinguishedName" /&gt;</pre>	Mode de récupération du certificat (SageID)
<b>Paramètres de l'authentification OAuth2 / Bearer</b>	
<pre>&lt;add key="OAuthDecryption" value="Auto" /&gt;</pre>	Clé de décryptage autogénérée
<pre>&lt;add key="OAuthValidationAlgorithm" value="HMACSHA256" /&gt;</pre>	Algorithme de validation autogénérée
<pre>&lt;add key="OAuthValidationKey" value="AutoGenerate,IsolateApps" /&gt;</pre>	Clé de validation autogénérée
<pre>&lt;add key="OAuthDecryptionKey" value="AutoGenerate,IsolateApps" /&gt;</pre>	Clé de déchiffrement autogénérée
<pre>&lt;add key="OAuthAccessTokenExpire" value="30" /&gt;</pre>	Valeur en minute de la durée de vie du token d'accès
<pre>&lt;add key="OAuthModeSupport" value="TokenEndpointServer" /&gt;</pre>	Quand la valeur TokenEndPoint est renseignée le SRA devient serveur d'identité et de token d'accès. Pour récupérer un token OAuth2 valide il faut appeler l'adresse du SRA + /token. Si cette valeur n'est pas renseignée, le SRA n'est que serveur de ressources.

<appSettings>	Commentaires
<b>Paramètres de l'authentification JWT / Bearer</b>	
<add key="JWTRealm" value="" />	Domaine du JWT
<add key="JWTIssuer" value="" />	Valeur de l'émetteur
<add key="JWTAudience" value="" />	Valeur de l'audience
<add key="JWTSecret" value="" />	Valeur du secret
<add key="JWTCertificateFindValue" value="" />	Nom du certificat
<add key="JWTCertificateFindType" value="FindBySubjectDistinguishedName" />	Mode de recherche du certificat, par défaut DN du nom de l'objet du certificat
<b>Paramètres de l'authentification SAMLV2 / Bearer</b>	
<add key="SAMLAudience" value="" />	Valeur de l'audience
<add key="SAMLIssuerThumbPrint" value="" />	Valeur de l'empreinte de l'émetteur
<add key="SAMLIssuerName" value="" />	Valeur du nom de l'émetteur
<!-- Tenant MASTER-->	
<add key="DsnType" value="1" />	Type de base de données 0 pour Oracle et 1 pour SQL Server Par défaut celle définie dans SXBE
<add key="Dsn" value="" />	Chaine de connexion à la BDD Par défaut celle définie dans SXBE
<add key="UmapiWorkGroup" value="WORKGROUP" />	Workgroup UMAPI Par défaut celui défini dans SXBE
<add key="UmapiLogin" value="" />	Login UMAPI Par défaut celui défini dans SXBE
<add key="UmapiPassword" value="" />	Password UMAPI Par défaut celui défini dans SXBE
<add key="OlbUrl" value="" />	URL du site web Par défaut celui défini dans SXBE
<add key="UmapiProfil" value=" " />	Groupe UMAPI dans lequel les signataires sont définis

## Fichier de configuration

<appSettings>	Commentaires
<add key="ComComputerName">	Nom de machine pour la localisation du service de transfert de fichier
<!-- Autre Tenant XXXX-->	Plan produit
<add key="DsnType[XXXX]" value="" />	Voir informations sur Tenant Master
<add key="Dsn[XXXX]" value="" />	Voir informations sur Tenant Master
<add key="UmapiWorkGroup[XXXX]" value="" />	Voir informations sur Tenant Master
<add key="UmapiLogin[XXXX]" value="" />	Voir informations sur Tenant Master
<add key="UmapiPassword[XXXX]" value="" />	Voir informations sur Tenant Master
<add key="OlbUrl" value="" />	Voir informations sur Tenant Master
<add key="UmapiProfil[XXXX]" value="" />	Voir informations sur Tenant Master
<add key="ComComputerName">	Voir informations sur Tenant Master

## Mode debug et fichier de log

Le service peut être utilisé en mode debug via :

**C:\Program Files\Sage\Sra\Sage.Eb.Admin.Rest.Api.exe NoService**

Un fichier log est disponible à l'endroit indiqué sur la variable du fichier de configuration *Sage.Eb.Admin.Rest.Api.exe.config* :

```
<add key="LogFile" value="C:\temp\sage.eb.admin.rest.api.log" />
```