



Sage XRT Business Exchange

Version 12.2.100

Sage Rest Api



Contents

Presentation	3
Installation.....	4
Configuration File.....	5
Debug Mode and Log File	9

Presentation

Sage Rest Api service (SRA) enables you to exchange data with **Sage XRT Business Exchange** through a **REST API**.

Three types of APIs exist:

- **Administration REST API**

These APIs manage the platform: entity or bank contract creations, etc.

- **Plain Production REST API**

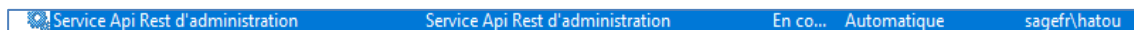
These enable you to monitor the bank flows life cycle: new file in the Signature Station, file received or sent, statuses, etc.

- **Extended Production REST API**

These enable you to supervise the smooth operation of the platform and certain processing: Services monitoring, Server Signature Rules monitoring, logs retrieval, etc.

Installation

Installing **Sage Rest Api** service requires the execution of the package *Sage.Eb.Admin.Rest.Api.Installer.exe*.

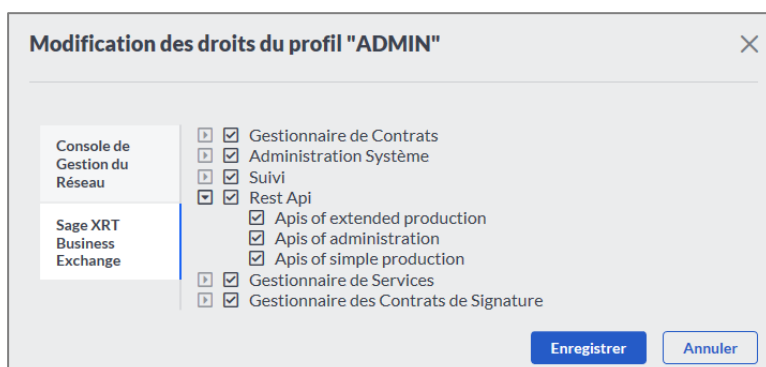


Sage Rest Api must be started with a service account.

Documentation on **REST APIs** is available on *http(s)://Hostname/sra/swagger*. You can view all the APIs that are already in this version.

Swagger Sage SXBE REST API		
Sage Business Exchange Rest Api		
Created by Sage XRT Electronic Banking Philae Team See more at http://www.sage.fr Contact the developer Sage Copyright 2018		
Account management Api	Show/Hide	List Operations Expand Operations
Entity management Api	Show/Hide	List Operations Expand Operations
File Contract management Api	Show/Hide	List Operations Expand Operations
File Resource management Api	Show/Hide	List Operations Expand Operations
Information version Api	Show/Hide	List Operations Expand Operations
Miscellenaous management Api	Show/Hide	List Operations Expand Operations
Server signature rules Api	Show/Hide	List Operations Expand Operations
Signature Contract management Api	Show/Hide	List Operations Expand Operations
Simple Production Api	Show/Hide	List Operations Expand Operations

Access to APIs is restricted to the following rights in **Sage XRT Common Services**.



Using the API **POST/v1/pdssa/geturlwpage** requires the setup of the variable **Allow Authentication Redirection** in the **Service de transaction, OnlineBanking**.

Configuration File

Some data required for the smooth operation of the service, are automatically recovered during its installation.

The intended architecture may require the definition of certain settings such as the modification of DSN or station address, etc.

The following table describes the configuration file *Sage.Eb.Admin.Rest.Api.exe.config*.

<appSettings>	Comments
<add key="UseSecureChannel" value="true" />	https or http (by default https)
<add key="SecureChannelCertificateName" value="" />	If not specified, True by default
<add key="DefaultAuthScheme" value="Ntlm" />	Authentication Method: ▪ Ntlm (default) ▪ SageXRT (based on SCAS service) ▪ Negotiate (Ntlm and/or Kerberos) ▪ IntegratedWindowsAuthentication ▪ Basic ▪ Anonymous ▪ SageID ▪ OAuth (OAuth2 version) ▪ Saml (SamlV2 version) ▪ Jwt (Json Web Token)
<add key="Address" value="" />	Server Name, Station Name by default
<add key="AdditionnalPath" value="" />	Access Path to REST API, by default SRA
<add key="Port" value="443" />	Access Port to REST API, by default 443
<add key="LogFile" value="C:\temp\sage.eb.admin.rest.api.log" />	Service path and log, by default deactivated if no value entered
SageXRT Authentication Parameters	
<add key="SCAS" value="http://NomMachine:8760" />	If Authentication Method = SageXRT
<add key="SCPS" value="http://NomMachine:8733" />	If Authentication Method = SageXRT
SageID Authentication Parameters	

<appSettings>	Comments
<add key="SageIDAccessTokenEncryptionKey" value="Hhlnk2r3dYXtJouX6Zb223TCVMfD1fN1//g nmj6nZYU=" />	Decryption key for SageID access token
<add key="SageIDAccessTokenEncryptionInitializationVector" value="OwJAAKjcpt1sEQF/qTrU/g==" />	Initialization Vector of Decryption key for SageID access token
<add key="SageIDSSORootCertificateFindValue" value="CN=Sage SSO Identity Root (Pre-Production), O=Sage (UK) Limited, C=United Kingdom" />	Root Certificate Name (SageID)
<add key="SageIDSSORootCertificateFindType" value="FindBySubjectDistinguishedName" />	Recovery Method for certificate (SageID)
OAuth2 / Bearer Authentication Parameters	
<add key="OAuthDecryption" value="Auto" />	Self-generated decryption key
<add key="OAuthValidationAlgorithm" value="HMACSHA256" />	Self-generated validation algorithm
<add key="OAuthValidationKey" value="AutoGenerate,IsolateApps" />	Self-generated validation key
<add key="OAuthDecryptionKey" value="AutoGenerate,IsolateApps" />	Self-generated decryption key
<add key="OAuthAccessTokenExpire" value="30" />	Access Token Lifetime in minutes
<add key="OAuthModeSupport" value="TokenEndpointServer" />	When TokenEndPoint is specified, SRA becomes an identity and access token server. To recover a valid OAuth2 token, SRA + /token address must be called. If not specified, SRA is just a resources server.
JWT / Bearer Authentication Parameters	
<add key="JWTRealm" value="" />	JWT domain
<add key="JWTIssuer" value="" />	Issuer value

<appSettings>	Comments
<add key="JWTAudience" value="" />	Audience value
<add key="JWTSecret" value="" />	Secret value
<add key="JWTCertificateFindValue" value="" />	Certificate Name
<add key="JWTCertificateFindType" value="FindBySubjectDistinguishedName" />	Search method for certificate, by default DN of certificate object name
SAMLV2 / Bearer Authentication Parameters	
<add key="SAMLAudience" value="" />	Audience value
<add key="SAMLIssuerThumbPrint" value="" />	Issuer Thumb Print value
<add key="SAMLIssuerName" value="" />	Issuer Name value
<!-- Tenant MASTER-->	
<add key="DsnType" value="1" />	Database type: 0 for Oracle and 1 for SQL Server By default, type defined for SXBE
<add key="Dsn" value="" />	DB connection string By default, same as for SXBE
<add key="UmapWorkGroup" value="WORKGROUP" />	UMAPI Workgroup By default, same as for SXBE
<add key="UmapLogin" value="" />	UMAPI Login By default, same as for SXBE
<add key="UmapPassword" value="" />	UMAPI Password By default, same as for SXBE
<add key="OlbUrl" value="" />	Website URL By default, same as for SXBE
<add key="UmapProfil" value="" />	UMAPI group in which signatories are defined
<add key="ComComputerName">	Station Name to locate the file transfer service
<!-- Autre Tenant XXXX-->	Product plan
<add key="DsnType[XXXX]" value="" />	See information on Tenant Master

<appSettings>	Comments
<add key="Dsn[XXXX]" value="" />	See information on Tenant Master
<add key="UmapWorkGroup[XXXX]" value="" />	See information on Tenant Master
<add key="UmapLogin[XXXX]" value="" />	See information on Tenant Master
<add key="UmapPassword[XXXX]" value="" />	See information on Tenant Master
<add key="OlbUrl" value="" />	See information on Tenant Master
<add key="UmapProfil[XXXX]" value="" />	See information on Tenant Master
<add key="ComComputerName">	See information on Tenant Master

Debug Mode and Log File

The service can be used in Debug Mode through:

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

A log file is available in the location specified in the configuration file variable *Sage.Eb.Admin.Rest.Api.exe.config*:

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