

sage

# Sage XRT Communication & Signature

Version 4.2

Nouveautés



# Sommaire



<b>Présentation .....</b>	<b>3</b>
<b>Gestion de l'authentification .....</b>	<b>4</b>
<b>Api d'exploitation.....</b>	<b>6</b>
<b>Support de l'enveloppe personnalisée .....</b>	<b>10</b>
<b>Gestion des protocoles cryptographiques .....</b>	<b>11</b>
<b>Divers .....</b>	<b>13</b>

## Présentation

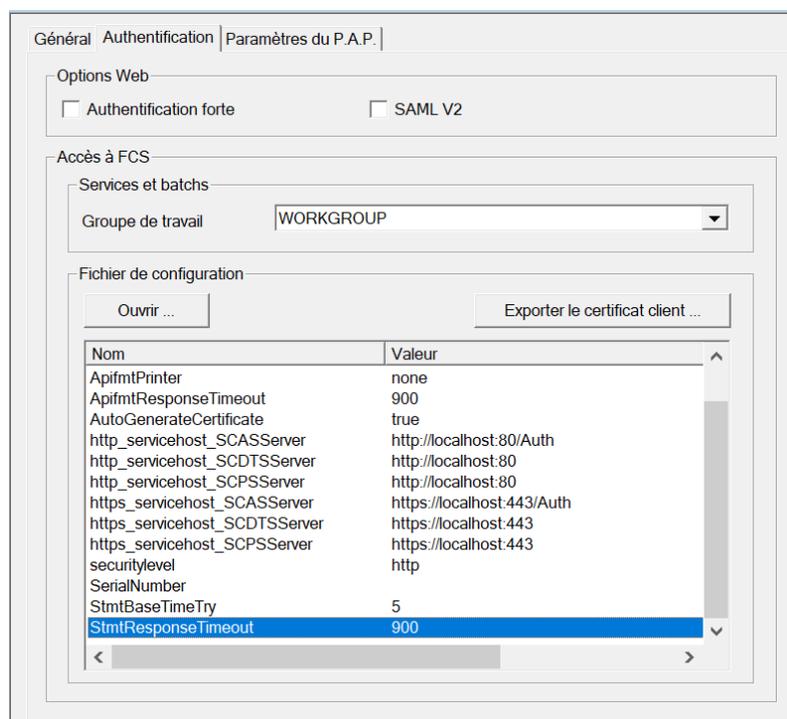
Ce document liste les nouvelles fonctionnalités disponibles dans la version 4.2 de **Sage XRT Communication & Signature**.

Cette version a été réalisée pour faciliter les échanges de fichiers entre l'application **Sage XRT Advanced** et l'application **Sage XRT communication & signature**.

**Important !** Cette version n'est pas compatible avec les versions 4.1 et inférieures de **Sage XRT Treasury**.

## Gestion de l'authentification

### Paramètres/Configuration – onglet Authentification



L'onglet **Authentification** regroupe :

- les options d'affichage de la page de connexion web (**Authentification forte** ou **SAML V2**)
- les informations du fichier de configuration *wrapper*

**Sage.Fcs.Client** permet de consommer de façon transparente un ensemble d'**API Rest** hébergé par les services d'authentification (**SCASServer**), d'administration (**SCPSServer**) et de fonctionnalités (**SCDTSServer**) de **Sage XRT Communication & Signature**.

**Sage XRT Communication & Signature 4.2** intègre cette librairie et appelle des méthodes.

Le serveur **Sage XRT Communication & Signature** est localisé via le paramétrage du fichier de configuration *Sage.Fcs.Client.dll.config*.

Les paramètres indiqués sont prédéfinis. Vous pouvez les modifier en fonction de votre configuration, dans cette interface.

## Gestion de l'authentification

Nom	Valeur	Commentaire
ApiFmtBaseTimeTry	2	Temporisation pour la partie <i>API</i> des formats
ApifmtPdfViewer	None	Outil d'affichage par défaut des Pdf.
ApifmtPrinter	None	Imprimante par défaut.
ApifmtResponseTimeout	900	Temps maximum de réponse de l' <i>Api</i> des formats.
AutoGenerateCertificate	true	Certificat autogénéré pour sécuriser les échanges
http_servicehost_SCASServer	<a href="http://localhost:80/Auth">http://localhost:80/Auth</a>	Localisation du service d'authentification en http
http_servicehost_SCPSSServer	<a href="http://localhost:80">http://localhost:80</a>	Localisation du service d'administration en http
http_servicehost_SCDTSServer	<a href="http://localhost:80">http://localhost:80</a>	Localisation du service de fonctionnalité en http
https_servicehost_SCASServer	<a href="https://localhost:443/Auth">https://localhost:443/Auth</a>	Localisation du service d'authentification en https
https_servicehost_SCPSSServer	<a href="https://localhost:443">https://localhost:443</a>	Localisation du service d'administration en https
https_servicehost_SCDTSServer	<a href="https://localhost:443">https://localhost:443</a>	Localisation du service de fonctionnalité en https
Securitylevel	http	Secure channel Http ou https
SerialNumber		Numéro de série du certificat si certificat autogénéré non utilisé
StmtBaseTimeTry	5	Non utilisé
StmtResponseTimeout	900	Non utilisé

# Api d'exploitation

Le service **XRT ComSign Rest Api** vous permet d'échanger des données avec l'application **Sage XRT Communication & Signature** à l'aide de l'**Api Rest**.

Les **Api Rest** de production simple disponibles dans cette version permettent de suivre le parcours des flux bancaires en émission (ajout d'un fichier dans le poste de signature, envoi d'un fichier, suivi des statuts des fichiers).

Le service **XRT ComSign Rest Api** est installé avec l'application **Sage XRT Communication** et doit être démarré avec un compte de service.

Si elle est activée dans le fichier de configuration, la documentation des **Api Rest** est disponible sur [http\(s\)://Hostname:8888/comsign/swagger](http(s)://Hostname:8888/comsign/swagger). Vous pouvez consulter le détail des **Api** déjà disponibles dans cette version.

Information version Api		Show/Hide	List Operations	Expand Operations
<b>Simple Production Api</b>		Show/Hide	List Operations	Expand Operations
POST	/v1/pdssa/addfile	Add a file payment's orders using SimpleApi		
POST	/v1/pdssa/getstatus	Get Job status into the pds using SimpleApi		
POST	/v1/pdssa/getticket	Get signature ticket using SimpleApi (NOT IMPLEMENTED)		
POST	/v1/pdssa/geturlwkpage	Get interactive url Page using SimpleApi		
POST	/v1/commsa/sendfile	Send a file payment's orders using SimpleApi		
POST	/v1/commsa/recvfile	Receive a file using SimpleApi (NOT IMPLEMENTED)		
POST	/v1/commsa/getstatus	Get Job status into the Comm using SimpleApi		
POST	/v1/commsa/getfilelist	Get file list using SimpleApi (NOT IMPLEMENTED)		
POST	/v1/commsa/getfiledata	Get file's data using SimpleApi (NOT IMPLEMENTED)		
POST	/v1/commsa/delfile	Delete file using SimpleApi (NOT IMPLEMENTED)		
POST	/v1/commsa/getremittanceslip	Get remittance slip using SimpleApi (NOT IMPLEMENTED)		

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

Parfois, l'architecture souhaitée nécessite de définir certains paramètres (modification du *DSN*, de l'adresse de la machine, etc.).

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

## Api d'exploitation

<appSettings>	Commentaires
<add key="UseSecureChannel" value="false" />	https ou http (par défaut http = false)
<add key="SecureChannelCertificateName" value="" />	Si non renseigné, par défaut <b>True</b>
<add key="DefaultAuthScheme" value="Ntlm" />	Méthode d'authentification : <ul style="list-style-type: none"> <li>▪ Par défaut, <b>SageXrt</b> (basée sur le service SCAS)</li> <li>▪ <b>Negotiate</b> (<i>Ntlm</i> et/ou <i>Kerberos</i>)</li> <li>▪ <b>IntegratedWindowsAuthentication</b></li> <li>▪ <b>Basic</b></li> <li>▪ <b>Anonymous</b></li> <li>▪ <b>OAuth</b> (Version <i>OAuth2</i>)</li> <li>▪ <b>Saml</b> (Version <i>SamlV2</i>)</li> <li>▪ <b>Jwt</b> (<i>Json Web Token</i>)</li> <li>▪ <b>Ntlm</b></li> </ul>
<add key="Address" value="" />	Nom du serveur, par défaut nom de la machine
<add key="AdditionalPath" value="comsign" />	Chemin d'accès à l' <i>Api Rest</i> par défaut <b>comsign</b>
<add key="Port" value="8888" />	Port d'accès de l' <i>Api Rest</i> par défaut 8888
<b>Paramètres de l'authentification FCS</b>	
<add key="SCAS" value="http://localhost " />	Si méthode d'authentification = <b>SageXRT</b>
<add key="SCPS" value="http:// localhost" />	Si méthode d'authentification = <b>SageXRT</b>

## Api d'exploitation

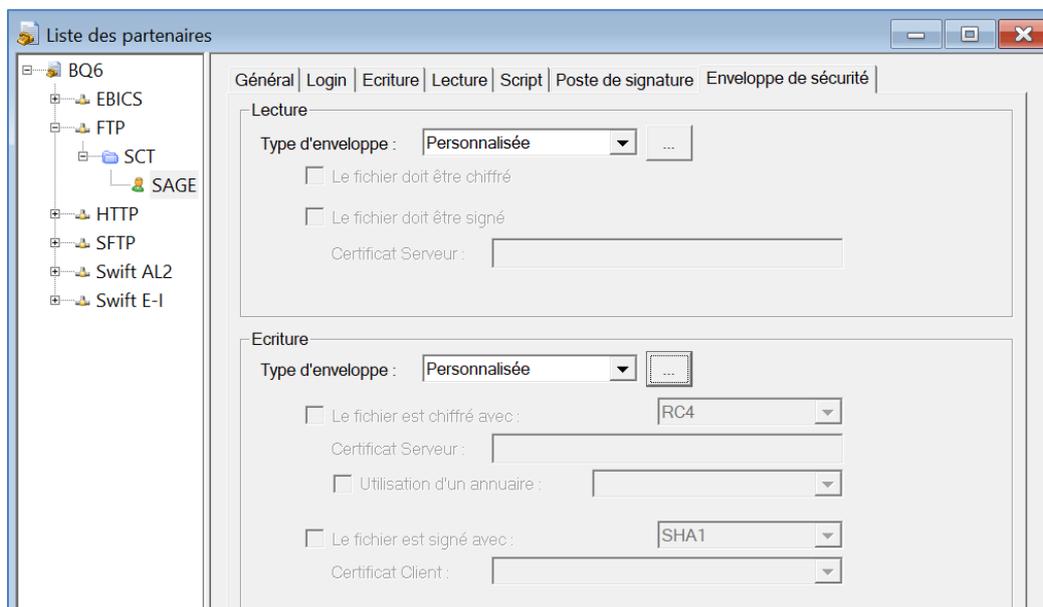
<appSettings>	Commentaires
<b>Paramètres de l'authentification OAuth2 / Bearer</b>	
<add key="OAuthDecryption" value="Auto" />	Clé de décryptage autogénérée
<add key="OAuthValidationAlgorithm" value="HMACSHA256" />	Algorithme de validation autogénérée
<add key="OAuthValidationKey" value="AutoGenerate,IsolateApps" />	Clé de validation autogénérée
<add key="OAuthDecryptionKey" value="AutoGenerate,IsolateApps" />	Clé de déchiffrement autogénérée
<add key="OAuthAccessTokenExpire" value="30" />	Valeur en minute de la durée de vie du <i>token</i> d'accès
<add key="OAuthModeSupport" value="TokenEndpointServer" />	Quand la valeur <b>TokenEndPoint</b> est renseignée, le <i>SRA</i> devient serveur d'identité et de <i>tokens</i> d'accès. Pour récupérer un <i>token OAuth2</i> valide il faut appeler l'adresse du <i>SRA</i> + <i>/token</i> . Si cette valeur n'est pas renseignée, le <i>SRA</i> se limite à un serveur de ressources.
<b>Paramètres de l'authentification JWT / Bearer</b>	
<add key="JWTRealm" value="" />	Domaine du <i>JWT</i>
<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 <i>DN</i> du nom de l'objet du certificat

## Api d'exploitation

<appSettings>	Commentaires
<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
<b>Log activation parameter</b>	
<add key="LogFile" value="" />	Chemin et nom du log de l'application. Non activé par défaut
<b>Workgroup</b>	
<add key="eBankingUrl" value="" />	Non utilisé
<add key="UmapiWorkGroup" value="WORKGROUP" />	Nom du <i>Workgroup UMAPI</i> Par défaut <b>Workgroup</b>

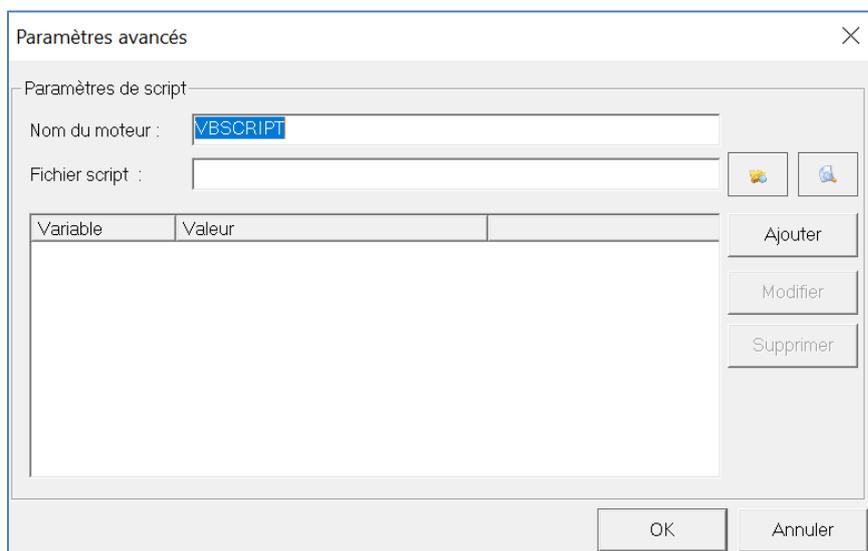
## Support de l'enveloppe personnalisée

Sur les contrats bancaires, dans l'onglet **Enveloppe de Sécurité**, le type d'enveloppe **Personnalisée** a été ajouté.



Cliquez sur le bouton  pour accéder aux paramètres avancés.

Vous pouvez sélectionner ou créer un fichier script.



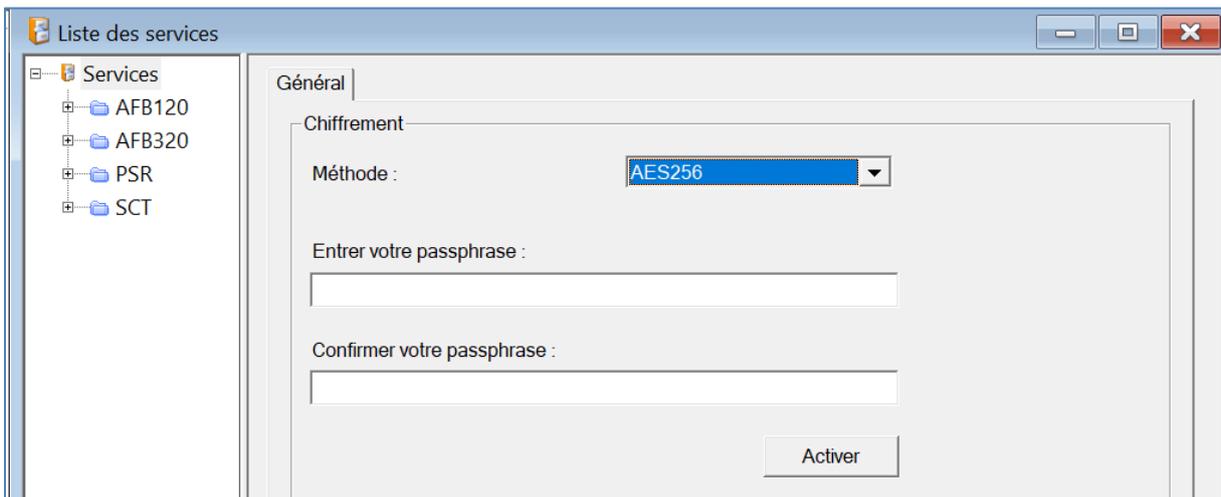
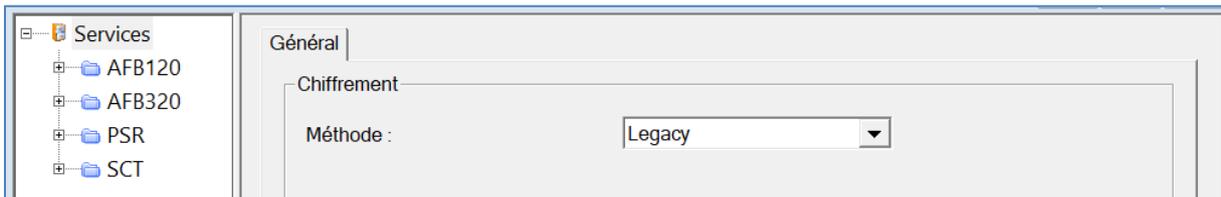
Si vous créez un fichier à partir du bouton , un *template* avec la fonction **décode** ou **encode** est disponible. Le fichier *template enveloppe.vbs* est livré dans le répertoire `\Workspace\Templates\`.

## Gestion des protocoles cryptographiques

Dans le *WORKSPACE*, les fichiers peuvent désormais être cryptés selon la norme **AES256**.

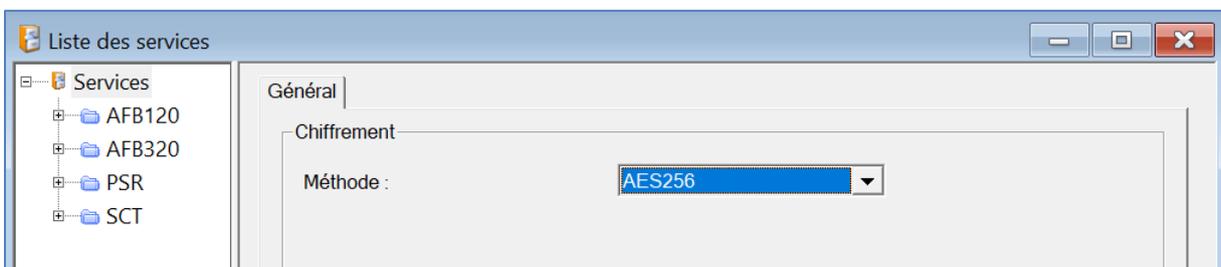
Pour les calculs de sceaux et la vérification des doublons, la fonction **SHA2-256** est utilisée.

Pour paramétrer le chiffrement **AES256**, la méthode **AES256** doit être sélectionnée au niveau du paramétrage des services.



Vous devez définir un *passphrase*, puis cliquer sur **Activer**.

**Important !** Ce *passphrase* doit être conservé de manière sécurisée.



A partir de cette activation, tous les fichiers sont désormais chiffrés en **AES256**.

**Note :** Pour activer le chiffrement au niveau de chaque service concerné, sélectionnez les options de sécurité **Chiffrement des fichiers** et **Chiffrement des archives** dans l'onglet **Propriétés** du paramétrage.

The screenshot shows the configuration window for the 'SCT' service, specifically the 'Propriétés' (Properties) tab. The left sidebar shows a tree view of services: Services, AFB120, AFB320, PSR, SCT, and under SCT, there are 'Définition', 'Interfaces', 'Fichier', and 'Archive'. The main area is divided into three sections:

- Edition:** Contains four fields: 'Projet' (dropdown menu with 'SCT'), 'Libellé' (text input with 'Format SCT SEPA'), 'Visualisation' (dropdown menu with 'SCT\_VISU\_DET'), and 'Libellé' (text input with 'Edition detaille du SCT SEPA').
- Conservation des données:** Contains three rows of settings: 'Nombre de jours pour les fichiers reçus' (input '10' followed by 'jours'), 'Nombre de jours pour les fichiers émis' (input '10' followed by 'jours'), and 'Archivage sur' (input '120' followed by 'jours').
- Sécurité:** Contains two checked checkboxes: 'Chiffrement des fichiers' and 'Chiffrement des archives'.

Vous pouvez rétablir le chiffrement *Legacy* en modifiant la méthode de chiffrement.

La modification ne s'appliquera qu'aux fichiers à venir.

L'utilitaire *sigcrypt* utilisé pour déchiffrer les fichiers a été modifié pour prendre en compte cette nouvelle fonctionnalité.

## Divers

Pour l'application **Sage XRT Treasury – Communication** la gestion des droits a été améliorée :

- Droits **Session/Create** appliqués aux connexions
- Droits **Fonction COM** appliqués aux paramètres d'Identification EBICS (gestion des droits du contrats gérés dans l'application **Sage XRT Common Services**)
- Pour toutes les interfaces (**Trésorerie, Rapprochement, Rapprochement LCR, flux5, sepamail**), ajout du droit **Delete** (géré dans l'application **Sage XRT Common Services**)

The screenshot displays the 'Sage XRT Treasury - Communication' application interface. On the left, there is a navigation menu with three main sections: 'Sage XRT Treasury - Signature', 'Sage XRT Treasury - Communication' (which is highlighted), and 'Sage XRT Functional Service'. The main area shows a list of permissions, each with a right-pointing arrow and a checked checkbox. The permissions are: Services, Clients, Dispositifs, Actions, Messages, Sessions, Interface trésorerie, Interface rappro, Interface rappro LCR, Historique des transferts, Log, Porteurs, Boîte de réception, Gestionnaire des traitements, SepaMail Interface, and Flux5 Interface. Under 'SepaMail Interface' and 'Flux5 Interface', there are sub-permissions for 'Generate', 'Report', and 'Delete', all of which are checked. At the bottom right, there are two buttons: 'Enregistrer' (blue) and 'Annuler' (white with blue border).

Section	Permission	Generate	Report	Delete
Sage XRT Treasury - Communication	Services	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Clients	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Dispositifs	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Actions	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Messages	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Sessions	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Interface trésorerie	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Interface rappro	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Interface rappro LCR	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Historique des transferts	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Log	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Porteurs	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Boîte de réception	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Gestionnaire des traitements	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
SepaMail Interface	Generate	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Report	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Delete	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Flux5 Interface	Generate	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Report	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Delete	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>