

Sterling B2B Integrator



Guide d'utilisation du client EBICS

Version 5.2.5

Sterling B2B Integrator



Guide d'utilisation du client EBICS

Version 5.2.5

Remarque

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations figurant à la section «Remarques», à la page 165.

Copyright

LE PRESENT DOCUMENT EST LIVRE EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFACON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE.

Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. Les informations qui y sont fournies sont susceptibles d'être modifiées avant que les produits décrits ne deviennent eux-mêmes disponibles. En outre, il peut contenir des informations ou des références concernant certains produits, logiciels ou services non annoncés dans ce pays. Cela ne signifie cependant pas qu'ils y seront annoncés.

Pour plus de détails, pour toute demande d'ordre technique, ou pour obtenir des exemplaires de documents IBM, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial.

Vous pouvez également consulter les serveurs Internet suivants :

- <http://www.fr.ibm.com> (serveur IBM en France)
- <http://www.ibm.com/ca/fr> (serveur IBM au Canada)
- <http://www.ibm.com> (serveur IBM aux Etats-Unis)

*Compagnie IBM France
Direction Qualité
17, avenue de l'Europe
92275 Bois-Colombes Cedex*

© Copyright IBM France 2016. Tous droits réservés.

© **Copyright IBM Corporation 2000, 2015.**

Table des matières

Avis aux lecteurs canadiens	v	Extraction des détails d'une commande VEU en attente	69
Utilisateur du client EBICS (V5.2.5 ou ultérieure)	1	Signer une commande VEU en attente	72
Présentation d'EBICS	1	Annuler une commande VEU en attente.	75
Installation manuelle du module du client EBICS	2	Mise à jour des valeurs des propriétés système	77
Conditions requises pour la configuration	3	Mon profil.	80
Créer un enregistrement d'identité	4	Importation et exportation des ressources du client EBICS	81
Créer des comptes utilisateur	6	Exporter les ressources du client EBICS	82
Configurer un adaptateur de système de fichiers	8	Importer les ressources du client EBICS	84
Création d'une boîte aux lettres et affectation de droits d'accès	16	Droits d'accès à l'interface utilisateur du client EBICS	85
Activer le planning	17	Récupération de transactions en envoi et en réception	87
Création d'un certificat autosigné	17	Soumission et signature d'un type de commande FUL	88
Enregistrer un certificat d'autorité de certification	18	Types de commande	91
Enregistrer un certificat de système de confiance	20	Type de commande FUL	91
Enregistrer des certificats de système de clé	21	Type de commande FDL	94
Configuration du client EBICS	21	Type de commande INI	96
Gestion de profils dans le client EBICS	22	Type de commande HIA	98
Configurer un utilisateur existant en tant qu'utilisateur du client EBICS	22	Type de commande H3K	99
Rechercher un profil utilisateur	27	Type de commande HPB	100
Modifier un profil utilisateur	28	Type de commande HKD	102
Supprimer un profil utilisateur	32	Type de commande HTD	103
Créer un profil de banque	33	Type de commande HEV	105
Rechercher un profil de banque.	35	Type de commande PUB	106
Modifier un profil de banque	35	Type de commande HCS	108
Supprimer un profil de banque.	37	Type de commande HCA	111
Validation d'une clé bancaire	38	Type de commande HPD	114
Créer une offre	38	Type de commande SPR	115
Rechercher une offre	39	Type de commande HVD	117
Modifier une offre	39	Type de commande HVE	118
Supprimer une offre	40	Type de commande HVS	120
Créer un format de fichier	40	Type de commande HVT	123
Rechercher un format de fichier	41	Type de commande HVU	125
Modifier un format de fichier	41	Type de commande HVZ	126
Supprimer un format de fichier.	42	Action de tâche en attente	128
Configuration des droits d'utilisateur.	42	Traitement HAC	129
Créer un droit d'utilisateur	43	Planning HAC	134
Rechercher un droit d'utilisateur	44	Création d'un planning HAC	134
Modifier un droit d'utilisateur	44	Recherche d'un planning HAC	136
Supprimer un droit d'utilisateur	46	Visualisation d'un planning HAC.	137
Initialisation d'un utilisateur.	46	Modification d'un planning HAC.	137
Soumission de commandes	48	Suppression d'un planning HAC	139
Soumission d'une commande en tant qu'utilisateur technique	52	Codes de retour	140
Configurer un utilisateur technique	54	Index	163
Afficheurs	59	Remarques	165
Recherche d'événements	59	Marques	167
Recherche de commandes	62	Dispositions applicables à la documentation du produit	168
Tâches en attente	66		
Rechercher des tâches VEU en attente	67		
Afficher les tâches VEU en attente.	68		

Avis aux lecteurs canadiens

Le présent document a été traduit en France. Voici les principales différences et particularités dont vous devez tenir compte.

Illustrations

Les illustrations sont fournies à titre d'exemple. Certaines peuvent contenir des données propres à la France.

Terminologie

La terminologie des titres IBM peut différer d'un pays à l'autre. Reportez-vous au tableau ci-dessous, au besoin.

IBM France	IBM Canada
ingénieur commercial	représentant
agence commerciale	succursale
ingénieur technico-commercial	informaticien
inspecteur	technicien du matériel

Claviers

Les lettres sont disposées différemment : le clavier français est de type AZERTY, et le clavier français-canadien de type QWERTY.








OS/2 et Windows - Paramètres canadiens

Au Canada, on utilise :

- les pages de codes 850 (multilingue) et 863 (français-canadien),
- le code pays 002,
- le code clavier CF.

Nomenclature

Les touches présentées dans le tableau d'équivalence suivant sont libellées différemment selon qu'il s'agit du clavier de la France, du clavier du Canada ou du clavier des États-Unis. Reportez-vous à ce tableau pour faire correspondre les touches françaises figurant dans le présent document aux touches de votre clavier.

France	Canada	Etats-Unis
 (Pos1)		Home
Fin	Fin	End
 (PgAr)		PgUp
 (PgAv)		PgDn
Inser	Inser	Ins
Suppr	Suppr	Del
Echap	Echap	Esc
Attn	Intrp	Break
Impr écran	ImpEc	PrtSc
Verr num	Num	Num Lock
Arrêt défil	Défil	Scroll Lock
 (Verr maj)	FixMaj	Caps Lock
AltGr	AltCar	Alt (à droite)

Brevets

Il est possible qu'IBM détienne des brevets ou qu'elle ait déposé des demandes de brevets portant sur certains sujets abordés dans ce document. Le fait qu'IBM vous fournisse le présent document ne signifie pas qu'elle vous accorde un permis d'utilisation de ces brevets. Vous pouvez envoyer, par écrit, vos demandes de renseignements relatives aux permis d'utilisation au directeur général des relations commerciales d'IBM, 3600 Steeles Avenue East, Markham, Ontario, L3R 9Z7.

Assistance téléphonique

Si vous avez besoin d'assistance ou si vous voulez commander du matériel, des logiciels et des publications IBM, contactez IBM direct au 1 800 465-1234.

Utilisateur du client EBICS (V5.2.5 ou ultérieure)

À l'aide du client EBICS, un partenaire ou un utilisateur partenaire peut configurer et gérer plusieurs banques, partenaires et utilisateurs. Plusieurs utilisateurs peuvent interagir avec plusieurs banques (serveurs EBICS Banking Server) via HTTP ou HTTPS et échanger des messages de transaction compatibles EBICS.

Le client EBICS de Sterling B2B Integrator est une application client-serveur qui fournit une solution EBICS de bout en bout pour permettre à une organisation d'effectuer des transactions avec les banques.

Les partenaires peuvent exécuter des tâches dans l'interface de tableau de bord du client EBICS :

- Configurer des utilisateurs
- Configurer des banques
- Configurer les paramètres de sécurité pour les utilisateurs
- Vérifier les paramètres de sécurité d'une banque
- Créer et gérer des formats de fichiers
- Créer et gérer des droits d'utilisateur
- Créer et gérer des offres
- Configurer des commandes
- Soumettre des commandes
- Afficher les événements et rapports associés à une commande
- Rechercher les commandes en attente dans le magasin de gestion VEU sur le serveur
- Afficher et surveiller les tâches en attente

Le client EBICS Sterling B2B Integrator prend en charge la spécification EBICS version 2.5 pour les implémentations en français et en allemand.

Présentation d'EBICS

EBICS (Electronic Banking Internet Communication Standard) est une norme de communication et de sécurité basée sur Internet. EBICS est une norme européenne dans le secteur bancaire. EBICS est principalement utilisée pour le transfert de données à distance, par exemple les transactions des paiements de l'entreprise, entre une organisation et une banque.

EBICS permet l'échange de fichiers de données quels que soient les normes et les formats des messages. EBICS utilise des procédures de signature et de chiffrement numériques établies. Ses fonctions sont basées sur des normes internationales pour la communication Internet et la sécurité améliorée comme, par exemple, XML, HTTPS, TLS et SSL. EBICS possède également des capacités multi-bancaires, dans lesquelles les clients de l'entreprise dans les pays qui ont adopté EBICS peuvent effectuer des transactions avec n'importe quelle banque dans ces pays qui utilisent le même logiciel.

Les entités suivantes sont impliquées dans les transactions du client EBICS :

Organisation

L'organisation ou entreprise qui utilise le client EBICS des transactions avec la banque.

Banque

Les institutions financières avec lesquelles l'organisation effectue des transactions. EBICS Banking Server est installé dans la banque.

Partenaire

Le département ou l'unité de l'organisation qui interagit avec la banque.

Utilisateur ou abonné

Personnel du département, qui effectue les transactions EBICS.

Une organisation doit remplir une série de conditions pour pouvoir implémenter des transactions EBICS techniques bancaires avec une banque donnée. Le prérequis de base pour implémenter les transactions EBICS est la signature d'un contrat entre le partenaire et la banque. Le protocole EBICS définit les transactions bancaires (les types de commande) nécessaires pour la communication. Les détails suivants sont convenus dans le présent contrat :

- Type des transactions commerciales.
- Informations sur les comptes bancaires de l'utilisateur.
- Informations sur les utilisateurs partenaires utilisant le système de la banque.
- Autorisations et droits d'accès des utilisateurs.

Le partenaire reçoit les données d'accès de la banque (paramètres bancaires) après la signature du contrat. La banque configure les données maître du partenaire et de l'utilisateur dans le système bancaire conformément aux accords contractuels. Les autres prérequis incluent l'initialisation de l'abonné, le téléchargement des certificats publics de la banque par l'utilisateur et la vérification des certificats de la banque par le partenaire commercial.

IBM® Sterling B2B Integrator offre une solution EBICS complète grâce à une plateforme sécurisée, souple et efficace, qui permet aux banques et aux organisations d'effectuer des transactions. L'implémentation de cette solution est divisée en deux composants principaux : le serveur EBICS Banking Server et le client EBICS. Le serveur EBICS Banking Server représente une banque et le client EBICS représente une organisation. Le serveur et le client sont déployés sur Sterling B2B Integrator.

Installation manuelle du module du client EBICS

Lors de l'installation de Sterling B2B Integrator 5.2.5 ou de la mise à niveau à partir d'une version précédente de Sterling B2B Integrator vers Sterling B2B Integrator 5.2.5, si vous aviez sélectionné l'option **Module de services financiers** à partir d'Installation Manager, le module du client EBICS est installé automatiquement.

Avant de commencer

Vous devez avoir installé Sterling B2B Integrator. Pour plus d'informations sur l'installation et la mise à niveau de Sterling B2B Integrator, consultez les *guides d'installation et de mise à niveau* dans le centre de documentation de Sterling B2B Integrator 5.2.

Pourquoi et quand exécuter cette tâche

Vous devez installer manuellement le module du client EBICS si l'un des critères suivants est respecté :

- Vous n'avez pas sélectionné l'option **Module de services financiers** à partir d'Installation Manager lors de l'installation de Sterling B2B Integrator 5.2.5.
- Vous n'avez pas sélectionné l'option **Module de services financiers** à partir d'Installation Manager lors de la mise à niveau à partir d'une version précédente de Sterling B2B Integrator vers Sterling B2B Integrator 5.2.5.
- Vous souhaitez appliquer Sterling B2B Integrator 5.2.5 comme correctif sur la version précédente de Sterling B2B Integrator 5.2.x.

Pour installer manuellement le module du client EBICS, procédez comme suit après avoir effectué une mise à niveau vers Sterling B2B Integrator 5.2.5 ou après avoir installé ce dernier :

Remarque : Si vous installez le module du client EBICS dans un environnement groupé, procédez comme suit sur chaque noeud de l'instance d'installation.

Procédure

1. Arrêtez Sterling B2B Integrator.
2. Fermez toutes les fenêtres d'invite de commande.
3. Si votre mot de passe de base de données est chiffré, déchiffrez-le.
4. Fermez toutes les fenêtres d'invite de commande.
5. Mettez à jour le fichier de licence de sorte à inclure la licence pour le client EBICS :
 - a. Ouvrez une fenêtre d'invite de commande.
 - b. Exécutez la commande suivante :
 - Microsoft Windows : `rép_install\bin\AddLicenseSet.cmd rép_install\properties\licensefiles\Fin_Serv_License.xml`
 - UNIX : `rép_install\bin\AddLicenseSet.sh rép_install\properties\licensefiles\Fin_Serv_License.xml`
6. Installez le fichier JAR du client EBICS :
 - a. Ouvrez une fenêtre d'invite de commande.
 - b. Exécutez la commande suivante :
 - Microsoft Windows : `rép_install\bin\InstallService.cmd rép_install\packages\v_ebics_client_numéro version_numéro compilation.jar`
 - UNIX : `rép_install\bin\InstallService.sh rép_install\packages\v_ebics_client_numéro version_numéro compilation.jar`
7. Si vous avez déchiffré le mot de passe de la base de données, rechiffrez-le.
8. Démarrez Sterling B2B Integrator.

Conditions requises pour la configuration

Pourquoi et quand exécuter cette tâche

Vous devez configurer les éléments suivants lors de l'accès à Sterling B2B Integrator avant d'utiliser le client EBICS :

Procédure

1. Enregistrez les parties publique et privée des certificats dans le système et dans le magasin de confiance de Sterling B2B Integrator. Enregistrez les certificats d'autorité de certification requis dans le magasin d'autorités de certification de Sterling B2B Integrator ou créez un certificat autosigné. Les types de certificat suivants sont utilisés pour configurer un utilisateur :
 - Identification et authentification
 - Chiffrement
 - Signature
2. Dans le menu **Identités** de Sterling B2B Integrator, créez un enregistrement d'identité pour votre organisation, en définissant votre organisation comme identité de base. Ce nom d'identité doit correspondre au nom de partenaire EBICS.
3. Dans le menu **Comptes utilisateur** de Sterling B2B Integrator, créez un compte utilisateur et affectez des droits à l'utilisateur. Ce nom d'utilisateur doit correspondre au nom d'utilisateur EBICS.
4. Dans Sterling B2B Integrator, configurez un adaptateur tel un adaptateur de système de fichiers, un adaptateur HTTP(S), un adaptateur SFTP ou un adaptateur FTP(S), qui vous permette d'envoyer et de recevoir des fichiers et qui appelle le processus technique EBClientOrderPreProcess. Par exemple, configurez un adaptateur de système de fichiers pour appeler le processus technique EBClientOrderPreProcess.
5. Configurez les boîtes aux lettres suivantes et associez-les à chaque utilisateur.
 - EBClientOrderMetadata (préconfigurée)
 - Download (boîte de réception)
 - Upload (boîte d'envoi)
6. Vérifiez que le processus technique EBClientMailboxArrivedMessage est associé à la boîte aux lettres EBClientOrderMetadata. La règle de routage automatique déclenche le processus technique qui exécute des fonctions automatisées, telles que la notification d'un prospect lorsqu'un message arrive dans la boîte aux lettres.

Remarque : Il est conseillé de ne pas modifier la configuration existante pour les règles de routage du client EBICS. Toute modification de la règle de routage est susceptible de créer des sous-ensembles et des commandes en double pour une soumission de commande.
7. Vérifiez que le planning MailboxEvaluateAllAutomaticRulesSubMin est activé.

Créer un enregistrement d'identité

Pourquoi et quand exécuter cette tâche

Un partenaire commercial est représenté par un enregistrement d'identité. Un enregistrement d'identité décrit le partenaire commercial et contient des informations référencées lorsqu'un processus technique qui implique un partenaire commercial est exécuté. Pour plus d'informations sur les enregistrements d'identité et les partenaires commerciaux, consultez la documentation sur la *Gestion des partenaires commerciaux de Sterling B2B Integrator*. Pour créer un enregistrement d'identité :

Procédure

1. Connectez-vous à Sterling B2B Integrator.

2. Dans le menu **Administration**, sélectionnez **Partenaire commercial > Avancé > Identité**.
3. Sous Créer en regard de Nouvelle identité, cliquez sur **OK**
4. Sur la page Identité, procédez comme suit :
 - Pour créer un enregistrement d'identité qui hérite de tous les composants d'un profil commercial existant, sélectionnez un enregistrement d'identité à partir de **Sélectionner une identité de base**, puis cliquez sur **Suivant**.
 - Pour spécifier des propriétés, laissez la zone **Sélectionner une identité de base** vide, puis cliquez sur **Suivant**.
5. Indiquez les paramètres pour Informations. Sur la page Informations, renseignez les zones suivantes, puis cliquez sur **Suivant** :

Zones d'information	Description
Nom	Obligatoire. Nom de l'enregistrement d'identité à créer pour ce profil commercial.
URL de référence	Facultatif. L'adresse URL est l'adresse Internet du partenaire commercial.
DUNS	Facultatif. Le DUNS (Data Universal Numbering System) est un numéro d'identification de société unique à neuf caractères émis par Dun & Bradstreet Corporation.
Identificateur	Obligatoire. ID principal de cet enregistrement d'identité. Il peut s'agir d'un numéro DUNS, d'un ID d'échange EDI, d'une adresse électronique ou d'une autre chaîne unique.
Ligne d'adresse 1	Obligatoire. Adresse postale conventionnelle de l'organisation du partenaire commercial.
Ligne d'adresse 2	Facultatif. Informations d'adresse postale supplémentaires de l'organisation du partenaire commercial.
Ville	Obligatoire. Ville dans laquelle le partenaire commercial se trouve.
Département ou région	Facultatif. Département ou région où l'organisation du partenaire commercial représenté par l'identité se trouve.
Code postal	Obligatoire. Code postal correspondant à la ville dans laquelle le partenaire commercial se trouve.
Adresse e-mail	Facultatif. Adresse électronique du partenaire commercial.
Numéro de téléphone	Facultatif. Numéro de téléphone du partenaire commercial.
Fuseau horaire	Facultatif. Fuseau horaire dans lequel le partenaire commercial se trouve.
Pays	Facultatif. Pays dans lequel le partenaire commercial se trouve.

6. Cliquez sur **Terminer** pour ajouter l'identité.
7. Cliquez sur **Retour** pour continuer.

Créer des comptes utilisateur

Pourquoi et quand exécuter cette tâche

Avant de commencer, vous devez savoir si vous utilisez une authentification locale ou externe :

- Local – L'authentification est exécutée auprès de la base de données d'application (par défaut).
- Externe – L'authentification est exécutée auprès d'un serveur LDAP. L'authentification externe ne requiert pas l'adaptateur LDAP, qui est utilisé avec les processus techniques et permet au système de communiquer avec les serveurs LDAP local ou distant à l'aide d'une interface JNDI.

Si vous affectez une ou plusieurs clés d'utilisateur autorisé à ce compte, les clés doivent être obtenues auprès de votre partenaire commercial et être enregistrées avant de créer le compte utilisateur.

Vous devez également connaître les informations suivantes :

Tableau 1. Créer des comptes utilisateur

Zone	Description
ID utilisateur	Obligatoire. ID utilisateur du compte utilisateur que vous créez. L'ID utilisateur doit contenir au moins 5 caractères. L'identifiant n'est pas sensible à la casse pour la base de données MySQL uniquement. Vous devez toujours utiliser des ID portant un nom unique, de sorte qu'un utilisateur n'utilise pas l'ID d'un autre par inadvertance.
Mot de passe (authentification locale uniquement)	Obligatoire pour les utilisateurs locaux. Mot de passe du compte utilisateur que vous créez. Le mot de passe doit contenir au moins 6 caractères. Cette zone ne s'affiche pas pour les utilisateurs externes.
Confirmer le mot de passe (authentification locale uniquement)	Obligatoire pour les utilisateurs locaux. Entrez le mot de passe une deuxième fois. Cette zone ne s'affiche pas pour les utilisateurs externes.
Règles (authentification locale uniquement)	Facultatif. Règles sur les mots de passe à associer à ce compte utilisateur. Sélectionnez la règle que vous souhaitez associer dans la liste. Cette zone ne s'affiche pas pour les utilisateurs externes. Le système calcule la date d'expiration à partir de la première date à laquelle l'utilisateur se connecte avec ce mot de passe.
Hôte d'authentification (authentification externe uniquement)	Serveur LDAP (Lightweight Directory Access Protocol) sur lequel l'utilisateur est en cours d'authentification. Les serveurs répertoriés dans cette zone sont spécifiés dans le fichier <code>authentication_policy.properties.in</code> .
Délai d'attente de session	Obligatoire. Durée en minutes pendant laquelle vous pouvez être inactif avant d'avoir à vous reconnecter. La durée est en minutes.

Tableau 1. Créer des comptes utilisateur (suite)

Zone	Description
Accessibilité	<p>Facultatif. Portion de l'interface utilisateur du tableau de bord à laquelle le compte utilisateur a accès.</p> <p>Les options suivantes sont des options d'accessibilité :</p> <ul style="list-style-type: none"> • Interface utilisateur d'administration – Permet d'accéder au panneau Console d'administration dans le tableau de bord uniquement. • UI AS2 – Permet d'accéder à l'interface de l'édition AS2 uniquement. • UI UCCNET – Permet d'accéder à l'interface de l'édition UCCnet uniquement. • UI Dashboard – Permet d'accéder à l'interface du tableau de bord. Pour personnaliser le tableau de bord, choisissez un thème.
Thème de tableau de bord	<p>Obligatoire si l'accessibilité est définie sur UI Dashboard. Tableau de bord prédéfini auquel le compte utilisateur a accès.</p> <p>Les options suivantes sont des options de thème de tableau de bord :</p> <ul style="list-style-type: none"> • Par défaut • Opérateur • Participant • Commanditaire de participant • Commanditaire • AFT
Prénom	Obligatoire. Nom utilisé pour identifier l'utilisateur.
Nom	Obligatoire. Nom de l'utilisateur.
E-mail	Adresse électronique de l'utilisateur.
Messageur	Numéro de messenger de poche de l'utilisateur.
Langue préférée	Langue préférée de l'utilisateur. Choisissez parmi : Anglais, Français, Japonais ou Espagnol.
ID de gestionnaire	ID utilisateur du gestionnaire de l'utilisateur.
Identité	<p>Identité du partenaire commercial à associer au compte utilisateur. Un seul partenaire commercial peut être associé à un compte utilisateur. Un compte utilisateur peut être associé à plusieurs groupes, chacun avec sa propre association d'identité de partenaire commercial. Cela permet à un compte utilisateur d'être associé à plusieurs partenaires commerciaux. La zone Identité est utilisée pour le routage des messages dans la boîte aux lettres. Sélectionnez une identité de partenaire commercial dans la liste.</p> <p>La valeur par défaut est Hub Organization.</p>

Pour plus d'informations sur la création d'utilisateurs et l'attribution de droits d'accès aux utilisateurs, consultez la documentation sur la *Sécurité de Sterling B2B Integrator*.

Pour créer un compte utilisateur :

Procédure

1. Connectez-vous à Sterling B2B Integrator.
2. Dans le menu **Administration**, sélectionnez **Comptes > Comptes utilisateur**.
3. En regard de **Créer un nouveau compte**, cliquez sur **OK**
4. Sur la page Nouveau compte, sélectionnez le **Type d'authentification**.
5. Entrez l'**ID utilisateur** et le **Mot de passe**.
6. Confirmez le mot de passe.
7. Sélectionnez les **Règles**.
8. Entrez le **Délai d'attente de session**.
9. Sélectionnez l'**Accessibilité**.
10. Sélectionnez le **Thème de tableau de bord**.
11. Cliquez sur **Suivant**.
12. Sur la page Clés d'utilisateur autorisé SSH, affectez une ou plusieurs clés publiques. Déplacez les clés du panneau **Disponible** vers le panneau **Affecté(s)**, puis cliquez sur **Suivant**.
13. Sur la page Groupes, affectez des groupes de droits d'accès. Déplacez les noms de groupe du panneau **Disponible** vers le panneau **Affecté(s)**, puis cliquez sur **Suivant**.
14. Sur la page Droits, affectez des droits d'accès individuels. Déplacez les droits d'accès du panneau **Disponible** vers le panneau **Affecté(s)**, puis cliquez sur **Suivant**. Par défaut, les droits associés aux groupes auxquels cet utilisateur est affecté sont déjà sélectionnés.
15. Sur la page Informations utilisateur, entrez le **Prénom**.
16. Entrez le **Nom**.
17. Entrez l'**Adresse électronique**.
18. Entrez le numéro de **Messageur**.
19. Sélectionnez la **Langue préférée**.
20. Entrez l'**ID de gestionnaire**.
21. Sélectionnez l'**Identité**.
22. Cliquez sur **Suivant**.
23. Passez en revue les paramètres du compte utilisateur.
24. Cliquez sur **Terminer**. Le compte utilisateur est créé et ce message s'affiche :
Mise à jour du système terminée.

Si vous avez créé un utilisateur externe, déconnectez-vous du système, puis reconnectez-vous avec l'ID utilisateur ou le compte externe. Le système authentifie l'ID utilisateur externe sur le serveur LDAP externe.

Configurer un adaptateur de système de fichiers

Utilisez l'adaptateur de système de fichiers pour collecter (importer) des fichiers à partir d'un système de fichiers dans un processus technique et extraire (exporter) des fichiers à partir d'un processus technique dans un système de fichiers. Vous pouvez configurer l'adaptateur de système de fichiers pour démarrer un processus technique une fois les fichiers collectés à partir du système de fichiers ou inclure l'adaptateur de système de fichiers dans un flux de processus technique. Vous pouvez en outre planifier l'adaptateur de système de fichiers de sorte qu'il s'exécute à des intervalles de temps spécifiques.

Vous pouvez créer plusieurs configurations d'adaptateur de système de fichiers, une pour chaque dossier de collecte. Vous pouvez également utiliser une configuration d'adaptateur de système de fichiers unique à faire pointer vers différents répertoires en spécifiant les répertoires pour la collecte et l'extraction des fichiers dans un processus technique. Pour plus d'informations sur la configuration de l'adaptateur de système de fichiers, consultez la documentation sur *l'adaptateur de système de fichiers*.

Configurez l'adaptateur de système de fichiers de sorte à appeler le processus technique EBClientOrderPreProcess.

Pour créer une configuration d'adaptateur de système de fichiers, indiquez les paramètres de zone dans Sterling B2B Integrator et dans Graphical Process Modeler (GPM).

Le tableau ci-dessous décrit les zones utilisées pour configurer l'adaptateur de système de fichiers dans Sterling B2B Integrator.

Remarque : Les noms de zone entre parenthèses représentent les noms de zone correspondants dans GPM. Ces informations sont fournies à titre de référence.

Zone	Description
Nom	Obligatoire. Nom unique et significatif pour la configuration de service.
Description	Obligatoire. Description significative pour la configuration de service, à titre de référence.
Sélectionner un groupe	Groupe à associer à l'adaptateur. Valeurs admises : <ul style="list-style-type: none"> • Aucun : aucun groupe n'est sélectionné. • Créer un nouveau groupe : permet de créer un groupe. • Sélectionner un groupe : permet d'effectuer une sélection dans une liste de groupes disponibles.
Dossier de collecte (collectionFolder)	Obligatoire. Il s'agit du nom du dossier ou du sous-dossier de l'ordinateur sur lequel Sterling B2B Integrator est installé et où il collecte (ou récupère) les fichiers dans le cadre d'un processus technique. Si le chemin d'accès au dossier n'est pas inclus dans le nom, le dossier est supposé se trouver dans le répertoire de travail de Sterling B2B Integrator. <p>Remarque :</p> <ul style="list-style-type: none"> • La valeur par défaut du paramètre deleteAfterCollect dans l'application GPM est Oui. Si vous ne modifiez pas la valeur par défaut sur Non, les fichiers collectés sont supprimés du dossier de collecte. L'adaptateur de système de fichiers ne copie pas les fichiers qu'il collecte pour traitement. Voir <i>Configuration de Graphical Process Modeler</i> pour plus d'informations sur le paramètre deleteAfterCollect. • Le paramètre collectionFolder est en lecture seule dans GPM. Vous pouvez toutefois remplacer ce paramètre à l'aide de Business Process Modeling Language (BPML).

Zone	Description
Filtre de nom de fichier (filter)	<p>Facultatif. Collectez uniquement les fichiers qui correspondent à un filtre spécifié dans le dossier de collecte. Par exemple :</p> <ul style="list-style-type: none"> • *.txt (collecte uniquement les fichiers .txt). • *.dat (collecte uniquement les fichiers .dat). • EDI.* (collecte uniquement les fichiers nommés EDI, quelle que soit leur extension de fichier). • EDI.txt (collecte uniquement les fichiers nommés EDI avec l'extension de fichier .txt). <p>Remarque : S'il existe plusieurs fichiers dans le dossier de collecte et si vous laissez cette zone vide, l'une des situations suivantes se produit :</p> <ul style="list-style-type: none"> • Si l'adaptateur est configuré pour démarrer un processus technique, il traite tous les fichiers placés dans le dossier de collecte. • Si l'adaptateur se trouve au sein d'un processus technique, il collecte uniquement le premier fichier dans le dossier de collecte. <p>Remarque : Si vous spécifiez cette option à l'aide de la configuration de l'adaptateur de système de fichiers, vous ne pouvez pas remplacer la valeur à l'aide du paramètre filter de GPM. Vous pouvez toutefois remplacer ce paramètre à l'aide de BPML.</p>
Collecter les fichiers dans le dossier de collecte et ses sous-dossiers ? (useSubFolders)	<p>Obligatoire. Indique si vous souhaitez rechercher des fichiers dans les sous-dossiers du dossier de collecte. Valeurs admises :</p> <ul style="list-style-type: none"> • Oui : collecte les fichiers dans le dossier spécifié et dans tous les sous-dossiers. • Non : collecte les fichiers dans le dossier spécifié uniquement. <p>Remarque : Ce paramètre est en lecture seule dans GPM.</p>
Utiliser le nom de chemin de fichier absolu pour le nom de document ? (keepPath)	<p>Obligatoire. Indique si vous souhaitez conserver le nom de chemin absolu des fichiers collectés lorsque vous attribuez un nom au document. Valeurs admises :</p> <ul style="list-style-type: none"> • Oui : le nom de chemin de fichier absolu est conservé avec le document dans le processus technique. Choisissez cette valeur si votre processus technique nécessite que les informations de chemin précèdent le nom du fichier. • Non : seul le nom du fichier est conservé avec le document dans le processus technique. <p>Remarque : Un chemin d'accès absolu est un chemin qui pointe vers le même emplacement indépendamment du répertoire de travail ou des chemins d'accès combinés. Il est écrit en référence à un répertoire racine. Ainsi, c:\dir1\subdir1\somefile.txt (Windows) et /home/dir1/subdir1/somefile.txt (UNIX) sont des exemples de chemins d'accès absolu au fichier somefile.txt.</p> <p>Remarque : Ce paramètre est en lecture seule dans GPM.</p>

Zone	Description
Démarrer un processus technique une fois les fichiers collectés ? (bootstrap)	<p>Obligatoire. Indique si vous souhaitez démarrer un processus technique à l'aide de l'adaptateur de système de fichiers une fois les fichiers collectés.</p> <p>Valeurs admises :</p> <ul style="list-style-type: none"> • Oui : démarre le processus technique sélectionné dans la liste déroulante des processus techniques pour tous les fichiers correspondant aux critères de filtrage. Une instance du processus technique est démarrée pour chaque fichier correspondant aux critères de filtrage indiqués pour la collecte de fichiers jusqu'à ce que le nombre d'unités d'exécution spécifié dans le paramètre <code>maxThreads</code> soit atteint. • Non : aucun processus technique n'est démarré. Ce paramètre est en lecture seule dans GPM.
Processus technique (initialWorkflowId)	<p>Obligatoire si Démarrer un processus technique est défini sur Oui. Le processus technique est démarré une fois les fichiers collectés. Sélectionnez <code>EBCClientOrderPreProcess</code> dans la liste déroulante des processus techniques.</p> <p>Remarque : Cette zone ne s'affiche que si Démarrer un processus technique une fois les fichiers collectés est défini sur Oui. Si vous indiquez un processus technique à l'aide de la configuration, vous ne pouvez pas remplacer cette valeur à l'aide de l'option <code>initialWorkflowId</code> de GPM. Si vous sélectionnez Non applicable, un processus technique peut être sélectionné dans GPM. Dans les deux cas, vous pouvez remplacer ce paramètre à l'aide de BPML.</p>
Type de stockage de documents (docStorageType)	<p>Obligatoire. Définit la manière dont le document est stocké dans le système. Valeurs admises :</p> <ul style="list-style-type: none"> • Valeur par défaut du système • Base de données • Système de fichiers <p>Remarque : Cette zone ne s'affiche que si Démarrer un processus technique une fois les fichiers collectés est défini sur Oui. Si vous indiquez ce paramètre à l'aide de la configuration, vous ne pouvez pas remplacer cette valeur à l'aide de l'option <code>DocStorageType</code> de GPM. Vous pouvez toutefois remplacer ce paramètre à l'aide de BPML.</p>
Rendre illisible le contenu du fichier ? (obscure)	<p>Indique si vous souhaitez rendre illisible le contenu du fichier lors de la collecte. Ne fonctionne pas avec <code>attachFile</code> ou <code>importFile</code>.</p> <ul style="list-style-type: none"> • Oui : le contenu du fichier est rendu illisible. • Non : le contenu du fichier n'est pas rendu illisible. <p>Remarque : Cette zone ne s'affiche que si Démarrer un processus technique une fois les fichiers collectés est défini sur Oui. Si vous indiquez ce paramètre à l'aide de la configuration, vous ne pouvez pas remplacer cette valeur à l'aide de l'option <code>Obscure</code> de GPM. Vous pouvez toutefois remplacer ce paramètre à l'aide de BPML.</p>

Zone	Description
Paramètre utilisateur 1 (userParm1)	<p>Paramètre utilisateur transmis au flux de travail amorcé et placé dans les données du processus en tant que UserParm1.</p> <p>Remarque : Cette zone ne s'affiche que si Démarrer un processus technique une fois les fichiers collectés est défini sur Oui. Si vous indiquez ce paramètre à l'aide de la configuration, vous ne pouvez pas remplacer cette valeur à l'aide de l'option userParm1 de GPM. Vous pouvez toutefois remplacer ce paramètre à l'aide de BPML.</p>
Paramètre utilisateur 2 (userParm2)	<p>Paramètre utilisateur transmis au flux de travail amorcé et placé dans les données du processus en tant que UserParm2.</p> <p>Remarque : Cette zone ne s'affiche que si Démarrer un processus technique une fois les fichiers collectés est défini sur Oui. Si vous indiquez ce paramètre à l'aide de la configuration, vous ne pouvez pas remplacer cette valeur à l'aide de l'option userParm2 de GPM. Vous pouvez toutefois remplacer ce paramètre à l'aide de BPML.</p>
Paramètre utilisateur 3 (userParm3)	<p>Paramètre utilisateur transmis au flux de travail amorcé et placé dans les données du processus en tant que UserParm3.</p> <p>Remarque : Cette zone ne s'affiche que si Démarrer un processus technique une fois les fichiers collectés est défini sur Oui. Si vous indiquez ce paramètre à l'aide de la configuration, vous ne pouvez pas remplacer cette valeur à l'aide de l'option userParm3 de GPM. Vous pouvez toutefois remplacer ce paramètre à l'aide de BPML.</p>
Paramètre utilisateur 4 (userParm4)	<p>Paramètre utilisateur transmis au flux de travail amorcé et placé dans les données du processus en tant que UserParm4.</p> <p>Remarque : Cette zone ne s'affiche que si Démarrer un processus technique une fois les fichiers collectés est défini sur Oui. Si vous indiquez ce paramètre à l'aide de la configuration, vous ne pouvez pas remplacer cette valeur à l'aide de l'option userParm4 de GPM. Vous pouvez toutefois remplacer ce paramètre à l'aide de BPML.</p>
Paramètre utilisateur 5 (userParm5)	<p>Paramètre utilisateur transmis au flux de travail amorcé et placé dans les données du processus en tant que UserParm5.</p> <p>Remarque : Cette zone ne s'affiche que si Démarrer un processus technique une fois les fichiers collectés est défini sur Oui. Si vous indiquez ce paramètre à l'aide de la configuration, vous ne pouvez pas remplacer cette valeur à l'aide de l'option userParm5 de GPM. Vous pouvez toutefois remplacer ce paramètre à l'aide de BPML.</p>

Zone	Description
Exécuter en tant qu'utilisateur	<p>S'applique à la planification du processus technique. Cette zone ne s'affiche que si Démarrer un processus technique une fois les fichiers collectés est défini sur Oui. Entrez l'ID utilisateur à associer au planning ou cliquez sur l'icône de liste et sélectionnez un ID utilisateur dans la liste. Les valeurs admises incluent tout ID utilisateur Sterling B2B Integrator authentique.</p> <p>Remarque : Ce paramètre permet à un utilisateur qui ne dispose pas des droits d'accès à un processus technique spécifique de l'exécuter. Si vous sélectionnez Admin comme ID utilisateur, vous héritez des droits d'administration (pour cette exécution du processus technique uniquement) et vous pouvez activer l'exécution planifiée.</p>
Utiliser l'affichage dans un format 24 heures	Si cette option est sélectionnée, l'adaptateur utilise une horloge dans un format 24 heures au lieu du format 12 heures par défaut.

Zone	Description
Planning	<p>Informations sur la planification du processus technique une fois que l'adaptateur de système de fichiers a collecté les fichiers. Cette zone ne s'affiche que si Démarrer un processus technique une fois les fichiers collectés est défini sur Oui. Valeurs admises :</p> <ul style="list-style-type: none"> • Ne pas utiliser le planning. Si vous sélectionnez cette zone, l'adaptateur ne démarre pas de processus technique et ne s'exécute pas en fonction d'un planning. • Exécuter selon le registre d'horloge. Les valeurs admises incluent l'heure et les minutes qui indiquent à quel moment exécuter l'adaptateur. Si vous choisissez de sélectionner un intervalle de temps, les valeurs admises incluent l'heure et les minutes des intervalles. Ajoutez ou supprimez des sélections lorsque cela est nécessaire. Indiquez les éventuelles exclusions de date. Indiquez si vous souhaitez exécuter l'adaptateur au démarrage. • Exécuter quotidiennement. Les valeurs admises incluent l'heure et les minutes qui indiquent à quel moment exécuter l'adaptateur quotidiennement. Si vous choisissez de sélectionner un intervalle de temps, les valeurs admises incluent l'heure et les minutes de l'intervalle. Ajoutez ou supprimez des sélections lorsque cela est nécessaire. Indiquez les éventuelles exclusions de date. Indiquez si vous souhaitez exécuter l'adaptateur au démarrage. • Exécuter en fonction du ou des jours de la semaine. Les valeurs admises incluent le jour de la semaine, l'heure et les minutes qui indiquent à quel moment exécuter l'adaptateur. Si vous choisissez de sélectionner un intervalle de temps, les valeurs admises incluent l'heure et les minutes des intervalles. Ajoutez ou supprimez des sélections lorsque cela est nécessaire. Indiquez les éventuelles exclusions de date. • Exécuter en fonction du ou des jours du mois. Les valeurs admises incluent le jour du mois, l'heure et les minutes qui indiquent à quel moment exécuter l'adaptateur. Si vous choisissez de sélectionner un intervalle de temps, les valeurs admises incluent l'heure et les minutes des intervalles. Ajoutez ou supprimez des sélections lorsque cela est nécessaire. Indiquez les éventuelles exclusions de date.

Zone	Description
Dossier d'extraction (extractionFolder)	<p>Obligatoire. Il s'agit du nom du dossier ou du sous-dossier sur l'ordinateur sur lequel Sterling B2B Integrator est installé et où il extrait (ou écrit) les données provenant du document principal dans le cadre d'un processus technique. Si le chemin d'accès au dossier n'est pas inclus dans le nom, le dossier est supposé se trouver dans le répertoire de travail de Sterling B2B Integrator.</p> <p>Remarque : Ce paramètre est en lecture seule dans GPM.</p>
Rendre lisible le contenu du fichier ? (unobscure)	<p>Indique si vous souhaitez rendre lisible le contenu du fichier lors de l'extraction. Ne fonctionne pas avec <i>exportFile</i>. Valeurs admises :</p> <ul style="list-style-type: none"> • Oui : le contenu du fichier est rendu lisible. • Non : le contenu du fichier n'est pas rendu lisible. <p>Remarque : Ce paramètre est en lecture seule dans GPM.</p>
Convention applicable aux noms de fichier (assignFilename)	<p>Obligatoire. Indique si vous souhaitez remplacer le nom de fichier du document et utiliser le nom de fichier attribué ou non. Valeurs admises :</p> <ul style="list-style-type: none"> • Utilisez le nom de fichier d'origine comme nom du fichier extrait : conserve les noms des fichiers. <p>Remarque : Si le document principal ne porte pas de nom, l'adaptateur utilise un nom de fichier par défaut sous la forme <i>nomnoeud_aaaaMMjjHHmssSSS.dat</i>.</p> <ul style="list-style-type: none"> • Assigner un nom spécifique : permet d'accéder à un écran et d'indiquer un nom de fichier différent pour le fichier extrait dans le système de fichiers. <p>Remarque : Ce paramètre est en lecture seule dans GPM.</p>
Nom du fichier (assignedFilename)	<p>Obligatoire. Nom que vous souhaitez affecter au fichier, avec l'extension de nom de fichier. La zone Nom du fichier s'affiche uniquement si <i>Convention applicable aux noms de fichier</i> est défini de sorte à affecter un nom spécifique. Cette zone ne peut pas être vide. Vous pouvez utiliser "%" pour affecter un nom de fichier unique dans un format <i>nomnoeud_yyyyMMddHHmssSSS</i>.</p> <p>Par exemple, lorsque vous spécifiez %^.dat comme nom de fichier, le nom <i>nomnoeud_20040203114020982.dat</i> est affecté au fichier.</p> <p>Remarque : Cette zone peut également être affectée dans GPM. Si vous sélectionnez un nom de fichier à l'aide de la configuration de l'adaptateur de système de fichiers, vous ne pouvez pas le remplacer à l'aide du paramètre assignedFilename de GPM. Vous pouvez toutefois le remplacer à l'aide de BPML.</p>
Activer le service pour les processus techniques	<p>Indique si vous souhaitez activer le service pour être utilisé par les processus techniques. Si cette option n'est pas sélectionnée, le service est désactivé. Pour plus d'informations sur l'activation d'un service, voir <i>Gestion des services et des adaptateurs</i>.</p>

Création d'une boîte aux lettres et affectation de droits d'accès

Vous devez associer chaque utilisateur du client EBICS à la boîte aux lettres EBClientOrderMetadata préconfigurée.

Pourquoi et quand exécuter cette tâche

Vous devez créer deux boîtes aux lettres de téléchargement (Boîte de réception et Boîte d'envoi) et associer chaque utilisateur aux boîtes aux lettres.

Pour plus d'informations sur la configuration des boîtes aux lettres et l'attribution de droits d'accès aux groupes et aux utilisateurs, consultez la documentation sur *l'Aide de la boîte aux lettres de Sterling B2B Integrator*.

Pour créer une boîte aux lettres et attribuer des droits d'accès aux groupes et aux utilisateurs sur cette boîte aux lettres :

Procédure

1. Connectez-vous à Sterling B2B Integrator.
2. Dans le menu **Administration**, sélectionnez **Déploiement > Boîtes aux lettres > Configuration**.
3. En regard de **Créer une nouvelle boîte aux lettres**, cliquez sur **OK**
4. Sur la page Boîte aux lettres : Nom, sélectionnez la boîte aux lettres parente dans laquelle la boîte aux lettres que vous créez sera intégrée. Vous pouvez entrer une partie du nom dans la zone **Filtrer par nom** et cliquer sur le bouton de filtre pour afficher une liste filtrée. La boîte aux lettres racine est représentée par une barre oblique (/).
5. Dans la zone **Nom**, entrez un nom pour la boîte aux lettres que vous souhaitez créer. Ce nom est utilisé pour identifier la boîte aux lettres dans l'application, par exemple, EBClientOrderMetadata.
6. Obligatoire. Dans la zone **Description**, entrez une brève description pour la boîte aux lettres, puis cliquez sur **Suivant**. Utilisez cette zone pour décrire la boîte aux lettres. Cette zone n'est utilisée par aucune autre ressource dans le système.
7. Sur la page Affecter des groupes, utilisez les flèches pour ajouter les groupes à la liste **Groupes sélectionnés**, puis cliquez sur **Suivant**. Tous les groupes de la liste **Groupes sélectionnés** se verront affecter des droits d'accès à cette boîte aux lettres. Cliquez sur la première flèche double pour ajouter tous les groupes disponibles à la liste **Groupes sélectionnés**.
8. Dans la zone **Filtrer par nom**, entrez un nom de groupe partiel, puis cliquez sur le bouton de filtre pour afficher une liste filtrée.
9. Dans le menu **Comptes**, plusieurs groupes peuvent être ajoutés. Aucun groupe n'est obligatoire.
10. Utilisez les flèches pour ajouter des utilisateurs à la liste **Utilisateurs sélectionnés**, puis cliquez sur **Suivant**. Tous les utilisateurs de la liste **Utilisateurs sélectionnés** se verront affecter des droits d'accès à cette boîte aux lettres. Cliquez sur la flèche double pour ajouter tous les utilisateurs disponibles à la liste Utilisateurs sélectionnés.
11. Dans la zone **Filtrer par ID**, entrez un nom partiel, puis cliquez sur le bouton de filtre pour afficher une liste filtrée.

Activer le planning

Pourquoi et quand exécuter cette tâche

L'activation d'un planning active celui-ci et permet à l'activité associée de s'exécuter en fonction des paramètres du planning. Un planning doit être activé pour s'exécuter. Pour plus d'informations sur la configuration des plannings afin d'automatiser les activités manuelles, consultez la documentation sur la *Planification de Sterling B2B Integrator*.

Le planning MailboxEvaluateAllAutomaticRulesSubMin est automatiquement activé.

Pour activer un planning, procédez comme suit :

Procédure

1. Connectez-vous à Sterling B2B Integrator.
2. Dans le menu **Administration**, sélectionnez **Déploiement > Plannings**.
3. Utilisez les options **Rechercher** ou **Liste** pour localiser le planning MailboxEvaluateAllAutomaticRulesSubMin, puis cliquez sur **OK**
4. Sur la page Plannings, recherchez le planning MailboxEvaluateAllAutomaticRulesSubMin et vérifiez que la case de la colonne **Activé** est cochée.

Création d'un certificat autosigné

Pourquoi et quand exécuter cette tâche

Enregistrez la partie publique du certificat autosigné dans le magasin de confiance de Sterling B2B Integrator. Pour créer un certificat autosigné :

Procédure

1. Sélectionnez l'une des options suivantes :
 - Si vous utilisez Sterling B2B Integrator, sélectionnez **Partenaire commercial > Certificats numériques > Système** à partir du menu **Administration**.
 - Si vous utilisez l'édition AS2, à partir du menu **Administration AS2**, sélectionnez **Certificats**.
2. En regard de **Créer certificat autosigné**, cliquez sur **OK**
3. Entrez le **Nom** du certificat autosigné.
4. Entrez le nom de l'**Organisation**.
5. Sélectionnez le **Pays** ou l'origine du certificat autosigné.
6. Entrez une **Adresse électronique** de contact pour la personne responsable des certificats dans l'organisation, puis cliquez sur **Suivant**.
7. Entrez le **Numéro de série** du certificat. Le numéro de série est le numéro que vous souhaitez affecter au certificat autosigné.
8. Entrez la **Durée** (nombre de jours) pendant laquelle le certificat autosigné est valide.
9. Entrez les **Adresses IP** des interfaces réseau que vous souhaitez associer au certificat dans la zone SubjectAltName.
10. Entrez les **Noms DNS** des interfaces réseau que vous souhaitez associer au certificat dans la zone SubjectAltName.
11. Sélectionnez la **longueur de clé**. Sélectionnez une des longueurs de clé suivantes :

- 512
- 1024
- 2048

Remarque : La longueur de clé 1024 constitue un bon équilibre entre la sécurité, l'interopérabilité et l'efficacité. La longueur de clé 2048 est la plus sécurisée, mais aussi la plus lente ; elle risque de ne pas fonctionner avec certaines applications. Pour plus d'informations sur la définition des longueurs de clé spécifiques à EBICS pour la signature électronique, le chiffrement et l'authentification, voir la *Spécification EBICS, version 2.5*.

Remarque : Si vous sélectionnez la longueur de clé 512, vous devez également vérifier les restrictions JDK sur la longueur de clé dans le fichier `java.security` du kit JDK.

12. Sélectionnez l'**Algorithme de signature**.

Remarque : Vous devez utiliser l'algorithme de signature SHA256withRSA pour les certificats utilisés avec les transactions EBICS.

13. Sélectionnez l'option **Valider lors de l'utilisation**. Les options de validation sont les suivantes :

- Validité – Vérifie si les dates comprises dans la période de validité du certificat sont toujours en cours. Si les dates ne sont pas en cours, le certificat ne pourra pas être utilisé.

Remarque : Avant de définir une valeur pour la période de validité du certificat, vous devez lire et appliquer les recommandations de meilleures pratiques contenues dans Microsoft PKI Quick Guide. Pour plus d'informations sur les recommandations de meilleures pratiques d'utilisation de ces certificats, voir <http://www.windowsecurity.com/articles/Microsoft-PKI-Quick-Guide-Part3.html>.

- Chaîne d'authentification – Construit une chaîne de confiance pour les certificats qui ne sont pas autosignés. Si une chaîne de confiance ne peut pas être construite en utilisant des certificats valides, le certificat n'est pas utilisé. Si le certificat est autosigné, cette option vérifie uniquement la signature du certificat.

14. Cochez la case **Définir le bit de signature du certificat**.

15. Cliquez sur **Suivant**.

16. Consultez les informations sur le certificat autosigné.

17. Cliquez sur **Terminer**.

Enregistrer un certificat d'autorité de certification

En fonction des règles de sécurité de votre site, les certificats d'autorité de certification du fichier de clés Java (JKS) peuvent également être enregistrés via la console.

Pourquoi et quand exécuter cette tâche

Avant de commencer, sauvegardez tout certificat d'autorité de certification obtenu en externe dans un fichier local.

Enregistrez tous les certificats (identification et authentification, signature et chiffrement) dont l'utilisateur du client EBICS a besoin pour effectuer des transactions avec la banque. Si un certificat signé par une autorité de certification

est utilisé pour configurer un utilisateur, enregistrez le certificat d'autorité de certification racine. Si 3SKey est utilisé pour la signature, enregistrez le certificat 3SKey racine. Enregistrez la partie publique du certificat HTTPS du serveur dans le magasin d'autorités de certification de Sterling B2B Integrator. Pour plus d'informations sur la gestion des certificats numériques, consultez la documentation sur la *Sécurité de Sterling B2B Integrator*.

Pour enregistrer un certificat d'autorité de certification :

Procédure

1. Connectez-vous à Sterling B2B Integrator.
2. Dans le menu **Administration**, sélectionnez **Partenaire commercial > Certificats numériques > CA**.
3. En regard de **Nouveau certificat**, cliquez sur **OK**
4. Sélectionnez une méthode d'importation des certificats :

Méthode d'importation	Procédure à suivre
Importer à partir de la machine virtuelle Java – Importe à partir du fichier de clés JKS	<ol style="list-style-type: none"> 1. Cliquez sur Importer depuis la machine virtuelle Java. 2. Acceptez le mot de passe par défaut qui s'affiche dans la zone de mot de passe, puis cliquez sur Suivant. <p>Si la zone du mot de passe est vide, le système utilise le mot de passe par défaut.</p>
Importer à partir d'un fichier - Importe les certificats sauvegardés dans un fichier sur une unité locale	<ol style="list-style-type: none"> 1. Cliquez sur Fichier > Importer. 2. Entrez le nom de fichier ou cliquez sur Parcourir pour sélectionner un fichier de certificat d'autorité de certification. Cliquez sur Suivant. <p>Vous pouvez ignorer le mot de passe qui s'affiche dans la zone de mot de passe. Vous n'avez pas besoin d'effacer l'entrée.</p>

Les certificats disponibles sont répertoriés avec un récapitulatif des informations d'identification. Tous les certificats sont sélectionnés par défaut.

5. Cochez les cases situées à gauche de chaque entrée pour importer les certificats.
6. Pour chaque certificat sélectionné, acceptez le nom du certificat proposé ou le modifier en fonction des conventions de dénomination de votre fichier.
7. Sélectionnez l'option **Valider lors de l'utilisation**, puis cliquez sur **Suivant**. Les options de validation sont les suivantes :
 - Validité – Vérifie si les dates comprises dans la période de validité du certificat sont toujours en cours. Si les dates ne sont pas en cours, le certificat ne pourra pas être utilisé.
 - Chaîne d'authentification – Tente de construire une chaîne de confiance pour les certificats qui ne sont pas autosignés. Si une chaîne de confiance ne peut pas être construite en utilisant des certificats valides, le certificat n'est pas utilisé. Si le certificat est autosigné, cette option vérifie uniquement la signature du certificat.
8. Si vous recevez un message indiquant que le certificat duplique un certificat déjà dans la base de données, entrez O ou N pour indiquer si vous souhaitez importer le doublon ou non.

Cette vérification n'est effectuée que sur les certificats uniques. Elle n'a pas lieu lors de l'enregistrement d'un ou de plusieurs certificats à partir d'un fichier.

Les certificats sont identifiés par hachage SHA1 ou SHA256 pour déterminer des doublons. Plusieurs copies d'un certificat peuvent être présentes dans la base de données, car chaque certificat renseigne une ligne différente et possède un ID objet distinct. Le certificat existant n'est pas remplacé.

9. Passez en revue les informations du certificat d'autorité de certification.
10. Cliquez sur **Terminer**.

Enregistrer un certificat de système de confiance

Pourquoi et quand exécuter cette tâche

Enregistrez la partie publique du certificat de l'utilisateur dans le magasin de confiance de Sterling B2B Integrator.

Avant de commencer, sauvegardez le certificat de système de confiance dans un fichier sur votre ordinateur local.

Pour enregistrer un certificat de système de confiance :

Procédure

1. Sélectionnez l'une des options suivantes :
 - Si vous utilisez Sterling B2B Integrator, dans le **Menu Administration**, sélectionnez **Partenaire commercial** > **Certificats numériques** > **Trusted**.
 - Si vous utilisez l'édition AS2, à partir du menu **Administration AS2**, sélectionnez **Certificats**.
2. En regard de **Nouveau certificat**, cliquez sur **OK**
3. Entrez le **Nom de fichier** ou cliquez sur **Parcourir** pour sélectionner le nom de fichier du certificat de confiance, puis cliquez sur **Suivant**.
4. Entrez le **Nom du certificat**.
5. Vérifiez le nom du certificat de confiance que vous enregistrez. Pour chaque certificat sélectionné, la zone Nom du certificat indique un nom proposé, suivi d'un récapitulatif des informations d'identification dans le certificat. Vous pouvez modifier le nom en fonction des conventions de dénomination de votre fichier.
6. Si vous possédez plusieurs certificats de confiance figurant dans le fichier sélectionné, cochez la case à gauche de chaque certificat pour enregistrer le certificat.
7. Sélectionnez l'option **Valider lors de l'utilisation**, puis cliquez sur **Suivant**. Les options de validation sont les suivantes :
 - Validité – Vérifie si les dates comprises dans la période de validité du certificat sont toujours en cours. Si les dates ne sont pas en cours, le certificat ne pourra pas être utilisé.
 - Chaîne d'authentification – Tente de construire une chaîne de confiance pour les certificats qui ne sont pas autosignés. Si une chaîne de confiance ne peut pas être construite en utilisant des certificats valides, le certificat n'est pas utilisé. Si le certificat est autosigné, cette option vérifie uniquement la signature du certificat.
 - Cache CRL - Vérifie si la liste de révocation de certificat est consultée chaque fois que le certificat du système est utilisé.

8. Passez en revue les informations du certificat de confiance.
9. Cliquez sur **Terminer**.

Enregistrer des certificats de système de clé

Pourquoi et quand exécuter cette tâche

Avant de commencer, sauvegardez le certificat de système de clé dans un fichier sur votre ordinateur local. Enregistrez la partie privée du certificat signé par une autorité de certification dans les certificats de système de clé de Sterling B2B Integrator.

Pour enregistrer un certificat de système de clé :

Procédure

1. Sélectionnez l'une des options suivantes :
 - Si vous utilisez Sterling B2B Integrator, sélectionnez **Partenaire commercial > Certificats numériques > Système** à partir du menu **Administration**.
 - Si vous utilisez l'édition AS2, à partir du menu **Administration AS2**, sélectionnez **Certificats**.
2. En regard de **Certificat de clé**, cliquez sur **OK**
3. Entrez le **Nom du certificat**.
4. Entrez le **Mot de passe de la clé privée**. Ce mot de passe est utilisé pour chiffrer la clé privée.
5. Entrez le **Nom de fichier** ou cliquez sur **Parcourir** pour sélectionner le nom de fichier du certificat de clé, puis cliquez sur **Suivant**.
6. Sélectionnez l'option **Valider lors de l'utilisation**, puis cliquez sur **Suivant**. Les options de validation sont les suivantes :
 - Validité – Vérifie si les dates comprises dans la période de validité du certificat sont toujours en cours. Si les dates ne sont pas en cours, le certificat ne pourra pas être utilisé.
 - Chaîne d'authentification – Construit une chaîne de confiance pour les certificats qui ne sont pas autosignés. Si une chaîne de confiance ne peut pas être construite en utilisant des certificats valides, le certificat n'est pas utilisé. Si le certificat est autosigné, cette option vérifie uniquement la signature du certificat.
7. Passez en revue les informations du certificat de clé.
8. Cliquez sur **Terminer**.

Configuration du client EBICS

Vous devez configurer le client EBICS Client dans Sterling B2B Integrator.

Avant de commencer

Effectuez la configuration du partenaire commercial, du compte utilisateur, des boîtes aux lettres et des certificats dans Sterling B2B Integrator, qui sont répertoriés dans la rubrique *Conditions requises pour la configuration*.

Pourquoi et quand exécuter cette tâche

Pour configurer le client EBICS, suivez la procédure ci-dessous :

Procédure

1. Configurez l'utilisateur Sterling B2B Integrator existant en tant qu'utilisateur du client EBICS.
2. Créez un profil de banque afin d'inclure les informations d'hôte EBICS.
3. Créez une offre et associez-la à une banque.
4. Associez les formats de fichier à l'offre.
5. Affectez le droit d'utilisateur aux utilisateurs afin de signer et de soumettre les commandes.
6. Initialisez les utilisateurs à l'aide de l'une des méthodes suivantes :
 - Soumettez une commande H3K.
 - Utilisez INI et HIA ensemble.
Soumettez des commandes INI et HIA.
Générez et signez les lettres d'initialisation INI et HIA. Adressez les lettres signées à la banque.

Pour plus d'informations, voir «Initialisation d'un utilisateur», à la page 46.
7. Utilisez le type de commande système HPB afin de recevoir par téléchargement les certificats publics de la banque.
8. Validez la valeur hachée des certificats reçus de la banque.
9. Soumettez une commande.
10. Affichez le statut des événements, des commandes et des tâches en attente.

Gestion de profils dans le client EBICS

L'option Gestion de profil du client EBICS vous permet de configurer les profils suivants. Un superadministrateur ou un administrateur du client EBICS peut configurer les profils.

- banque
- Utilisateur
- Offre
- Format de fichier

Remarque : Un superadministrateur est le rôle administrateur par défaut créé lorsque le client EBICS est installé. Un utilisateur autorisé peut se connecter à l'interface de tableau de bord du client EBICS à l'aide des données d'identification superadministrateur et configurer un administrateur du client EBICS, un opérateur du client EBICS et un utilisateur du client EBICS et d'autres profils. Un administrateur du client EBICS peut également configurer un administrateur du client EBICS, un opérateur du client EBICS, un utilisateur du client EBICS et d'autres profils.

Configurer un utilisateur existant en tant qu'utilisateur du client EBICS

Avant de commencer

Procédez comme suit dans Sterling B2B Integrator :

- Créez des entités de partenaire commercial.
- Créez des comptes utilisateur à l'aide des entités de partenaire commercial ; définissez des droits d'accès et des règles sur les mots de passe.
- Configurez les boîtes aux lettres de téléchargement pour chaque utilisateur.

Pourquoi et quand exécuter cette tâche

Un utilisateur peut être en-dessous d'un ou plusieurs partenaires. Un utilisateur est toujours associé à un partenaire pour pouvoir échanger des messages EBICS. Pour configurer un utilisateur Sterling B2B Integrator existant en tant qu'utilisateur du client EBICS, procédez comme suit :

Procédure

1. Connectez-vous au client EBICS de Sterling B2B Integrator.
2. Dans le menu **Gestion de profil**, sélectionnez **Utilisateur**.
3. Sur la page Configuration de l'utilisateur, en regard de **Configurer l'utilisateur existant en tant qu'utilisateur EBICS**, cliquez sur **OK**.
4. Sur la page Configuration de l'utilisateur, indiquez les valeurs des zones conformément aux instructions du tableau ci-après, puis cliquez sur **Suivant** :

Zone	Description
ID utilisateur	Obligatoire. Identifiant unique de l'utilisateur dans le système de la banque, qui correspond à l'utilisateur créé dans le tableau de bord du client EBICS. Dans la liste déroulante ID utilisateur , sélectionnez l'ID utilisateur.
Type d'utilisateur	Obligatoire. Dans la liste déroulante Type d'utilisateur , sélectionnez le rôle de l'utilisateur. Les valeurs admises sont : administrateur du client EBICS, opérateur du client EBICS et utilisateur du client EBICS.
Fuseau horaire	Facultatif. Indiquez le fuseau horaire de l'utilisateur.
Utilisateur technique	Facultatif. Un utilisateur technique est un système configuré pour soumettre des commandes à la place d'un utilisateur physique ou non technique. Cette option est valide si vous avez sélectionné le type d'utilisateur Utilisateur du client EBICS. Cochez cette case pour configurer un utilisateur technique.
Type de certificat	Obligatoire si vous avez sélectionné le type d'utilisateur Utilisateur du client EBICS. Sélectionnez X509 si vous utilisez le certificat de clé publique X.509 pour autoriser les certificats. Sélectionnez Clés si vous utilisez des clés RSA pour autoriser les certificats. Remarque : Le client EBICS prend en charge les clés non chiffrées uniquement.

5. Si vous avez sélectionné le type de certificat X509, indiquez les valeurs des zones conformément aux instructions du tableau ci-après sur la page Informations techniques, puis cliquez sur **Suivant** :

Zone	Description
Certificat privé d'authentification	Obligatoire. Sélectionnez la clé privée que le client EBICS utilise pour créer une signature numérique pour l'utilisateur dans la demande envoyée à la banque. La banque doit posséder la partie publique de la clé pour valider l'autorisation. La liste déroulante contient les certificats configurés dans le magasin de certificats de système Sterling B2B Integrator.
Certificat public d'authentification	Obligatoire. Sélectionnez la clé publique que l'utilisateur fournit à la banque pour valider l'autorisation de l'utilisateur dans la demande du client EBICS. Le partenaire commercial ou l'utilisateur partage la clé avec la banque. La clé doit être une partie publique du certificat de système Sterling B2B Integrator sélectionné comme certificat privé d'authentification.
Version de clé d'authentification	La version de la clé du certificat d'authentification s'affiche. La valeur X002 est admise.
Certificat privé de chiffrement	Obligatoire. Sélectionnez la clé privée que le client EBICS utilise pour déchiffrer la réponse reçue du serveur EBICS Banking Server. La liste déroulante contient les certificats configurés dans le magasin de certificats de système Sterling B2B Integrator.
Certificat public de chiffrement	Obligatoire. Sélectionnez la partie publique du certificat de système Sterling B2B Integrator sélectionné comme certificat privé de chiffrement. Le partenaire commercial ou l'utilisateur partage la clé avec la banque.
Version de clé de chiffrement	La version de la clé du certificat de chiffrement s'affiche. La valeur E002 est admise.
Utiliser le magasin de clés matérielles pour la signature électronique	Facultatif. Sélectionnez cette option si vous disposez d'un jeton de clé 3S activé.
Type de clé matérielle	Clé 3S s'affiche en tant que type de clé matérielle. Cette clé est une clé de signature sécurisée SWIFT utilisée pour l'identité numérique. Vous devez activer le jeton de clé 3S et enregistrer la clé auprès de la banque pour pouvoir signer et envoyer des messages à la banque.
Clé privée de signature électronique	Facultatif. Sélectionnez la clé privée du certificat de signature électronique (ES) si vous n'utilisez pas de clé matérielle pour la signature électronique.
Clé publique de signature électronique	Obligatoire. Sélectionnez la clé publique du certificat de signature électronique (ES) utilisé pour vérifier la signature des données de commande. La valeur de la clé publique d'un certificat de signature électronique ne doit pas être identique à celle d'un certificat d'authentification ou de chiffrement.

Zone	Description
Version de clé de signature électronique	Obligatoire si vous n'utilisez pas de magasin de clés matérielles pour la signature électronique. Sélectionnez la version de la clé du certificat de signature électronique. Les valeurs valides sont A005 et A006. Si vous utilisez un magasin de clés matérielles pour la signature électronique, la version de la clé est définie sur A005 et ne peut pas être modifiée.

6. Si vous avez sélectionné le type de certificat Clés, indiquez les valeurs des zones conformément aux instructions du tableau ci-après sur la page Informations techniques, puis cliquez sur **Suivant** :

Zone	Description
Clé privée d'authentification	Obligatoire. Cliquez sur Parcourir pour sélectionner le fichier contenant la partie privée de la clé d'authentification dans votre ordinateur.
Clé publique d'authentification	Obligatoire. Cliquez sur Parcourir pour sélectionner le fichier contenant la partie publique de la clé d'authentification dans votre ordinateur.
Version de clé d'authentification	Obligatoire. Sélectionnez la version de la clé du certificat d'authentification. La valeur X002 est admise.
Clé privée de chiffrement	Obligatoire. Cliquez sur Parcourir pour sélectionner le fichier contenant la partie privée de la clé de chiffrement dans votre ordinateur.
Clé publique de chiffrement	Obligatoire. Cliquez sur Parcourir pour sélectionner le fichier contenant la partie publique de la clé de chiffrement dans votre ordinateur.
Version de clé de chiffrement	Obligatoire. Sélectionnez la version de la clé du certificat de chiffrement. La valeur E002 est admise.
Clé privée de signature électronique	Obligatoire. Cliquez sur Parcourir pour sélectionner le fichier contenant la partie privée de la clé de signature électronique dans votre ordinateur.
Clé publique de signature électronique	Obligatoire. Cliquez sur Parcourir pour sélectionner le fichier contenant la partie publique de la clé de signature électronique dans votre ordinateur.
Version de clé de signature électronique	Obligatoire. Sélectionnez la version de la clé du certificat de signature électronique. Les valeurs valides sont A005 et A006.

7. Sur la page Partenaires associés, effectuez l'une des actions suivantes, puis cliquez sur **Suivant**.
- Cliquez sur l'icône d'ajout pour associer un nouveau partenaire à l'utilisateur.

- Cliquez sur l'icône de mise à jour en regard du partenaire que vous souhaitez modifier.
 - Cliquez sur l'icône de suppression pour dissocier un partenaire de l'utilisateur.
8. Cette étape est applicable uniquement si vous avez choisi d'ajouter un nouveau partenaire ou de modifier un partenaire existant. La banque affecte un ensemble de droits, de types de commande et de formats de fichier à un utilisateur en fonction de l'offre. Sur la page Partenaire associé : Paramètres utilisateur, indiquez les valeurs des zones conformément aux instructions du tableau ci-après, puis cliquez sur **Ajouter un partenaire**.

Zone	Description
Nom du partenaire	<p>Obligatoire. Dans la liste déroulante Nom du partenaire, sélectionnez le partenaire auquel un utilisateur est associé. Un utilisateur peut être associé à plusieurs partenaires.</p> <p>Remarque : Utilisez le tableau de bord Sterling B2B Integrator pour créer des entités de partenaire commercial.</p>
Chemin d'accès à la boîte d'envoi par téléchargement	<p>Obligatoire. Configurez la boîte aux lettres de téléchargement et affectez des utilisateurs pour faire fonctionner la boîte aux lettres dans Sterling B2B Integrator. Indiquez le chemin de la boîte aux lettres pour les messages téléchargés. Vous devez affecter un chemin de boîte aux lettres pour stocker les messages décompressés d'une demande EBICS.</p> <p>Si la boîte aux lettres (ID utilisateur, Nom du partenaire, Boîte de réception) existe déjà dans Sterling B2B Integrator et si vous laissez cette zone vide, un message d'erreur vous invite à indiquer le chemin d'accès par défaut à la boîte aux lettres.</p> <p>Remarque : Assurez-vous que le chemin de boîte aux lettres commence par une barre oblique (/).</p>
Chemin d'accès à la boîte de réception par téléchargement	<p>Obligatoire. Configurez la boîte aux lettres de téléchargement et affectez des utilisateurs pour faire fonctionner la boîte aux lettres dans Sterling B2B Integrator. Indiquez le chemin de la boîte aux lettres pour les messages téléchargés. Vous devez affecter un chemin de boîte aux lettres pour stocker les messages qui sont compressés dans une réponse EBICS.</p> <p>Si la boîte aux lettres (ID utilisateur, Nom du partenaire, Boîte d'envoi) existe déjà dans Sterling B2B Integrator et si vous laissez cette zone vide, un message d'erreur vous invite à indiquer le chemin d'accès par défaut à la boîte aux lettres.</p> <p>Remarque : Assurez-vous que le chemin de boîte aux lettres commence par une barre oblique (/).</p>

9. Cette étape n'est applicable que si vous avez choisi de configurer les paramètres de délégation des utilisateurs pour un utilisateur technique. Sur la page Partenaires associés, effectuez l'une des actions suivantes, puis cliquez sur **Suivant**.
 - Cliquez sur l'icône d'ajout pour associer un nouveau partenaire à l'utilisateur technique.
 - Cliquez sur l'icône de mise à jour en regard du partenaire que vous souhaitez modifier.
 - Cliquez sur l'icône de suppression pour dissocier un partenaire de l'utilisateur technique.
10. Cette étape n'est applicable que si vous configurez les paramètres de délégation des utilisateurs pour un utilisateur technique. Sur la page Partenaire associé : Paramètres utilisateur, indiquez les valeurs des zones conformément aux instructions du tableau ci-après, puis cliquez sur **Ajouter un partenaire**.

Zone	Description
Nom du partenaire	Obligatoire. Dans la liste déroulante Nom du partenaire , sélectionnez le partenaire auquel un utilisateur est associé. Un utilisateur peut être associé à plusieurs partenaires. Remarque : Utilisez le tableau de bord Sterling B2B Integrator pour créer des entités de partenaire commercial.
Délégué de	Obligatoire. Sélectionnez l'utilisateur qui déléguera ses tâches à l'utilisateur technique.

11. Sur la page Partenaires associés, cliquez sur **Suivant**.
12. Sur la page Confirmer, vérifiez les paramètres de configuration de l'utilisateur, puis cliquez sur **Terminer**. Vous pouvez également cliquer sur le lien **Afficher tout** en regard des **Partenaires associés** pour afficher la liste des partenaires associés à l'utilisateur.

Rechercher un profil utilisateur

Pourquoi et quand exécuter cette tâche

Pour rechercher un profil utilisateur, procédez comme suit :

Procédure

1. Connectez-vous au client EBICS de Sterling B2B Integrator.
2. Dans le menu **Gestion de profil**, sélectionnez **Utilisateur**.
3. Sur la page Configuration de l'utilisateur, effectuez l'une des actions suivantes, puis cliquez sur **OK**.
 - Dans la zone **ID utilisateur** sous **Rechercher**, entrez tout ou partie de l'ID utilisateur du profil utilisateur que vous recherchez.
 - Dans la liste déroulante **Par ordre alphabétique**, sélectionnez la lettre par laquelle commence l'ID de l'utilisateur que vous recherchez.

Modifier un profil utilisateur

Pourquoi et quand exécuter cette tâche

Vous devez être connecté à l'interface de tableau de bord du client EBICS en tant qu'administrateur pour mettre à jour un profil utilisateur, supprimer un profil utilisateur ou afficher le récapitulatif d'un utilisateur. Pour modifier un profil utilisateur, procédez comme suit :

Procédure

1. Connectez-vous au client EBICS de Sterling B2B Integrator.
2. Dans le menu **Gestion de profil**, sélectionnez **Utilisateur**.
3. Sur la page Configuration de l'utilisateur, en utilisant **Rechercher** ou **Liste**, localisez et sélectionnez l'ID utilisateur que vous souhaitez modifier, puis cliquez sur **OK**. Vous pouvez cliquer sur l'ID utilisateur pour afficher les paramètres du profil utilisateur.
4. Cliquez sur l'icône Mettre à jour en regard de l'ID utilisateur que vous souhaitez modifier.
5. Sur la page Mettre à jour : Configuration de l'utilisateur, indiquez les valeurs des zones conformément aux instructions du tableau suivant, puis cliquez sur **Suivant** :

Zone	Description
Fuseau horaire	Facultatif. Sélectionnez le fuseau horaire de l'utilisateur.
Utilisateur technique	Facultatif. Un utilisateur technique est un système configuré pour soumettre des commandes à la place d'un utilisateur physique ou non technique. Cette option est valide si vous avez sélectionné le type d'utilisateur Utilisateur du client EBICS. Cochez cette case pour configurer un utilisateur technique.
Type de certificat	Obligatoire si vous avez sélectionné le type d'utilisateur Utilisateur du client EBICS. Sélectionnez X509 si vous utilisez le certificat de clé publique X.509 pour autoriser les certificats. Sélectionnez Clés si vous utilisez des clés RSA pour autoriser les certificats. Remarque : Le client EBICS prend en charge les clés non chiffrées uniquement.

6. Si vous avez sélectionné le type de certificat X509, indiquez les valeurs des zones conformément aux instructions du tableau ci-après sur la page Informations techniques, puis cliquez sur **Suivant** :

Zone	Description
Certificat privé d'authentification	Obligatoire. Sélectionnez la clé privée que le client EBICS utilise pour créer une signature numérique pour l'utilisateur dans la demande envoyée à la banque. La banque doit posséder la partie publique de la clé pour valider l'autorisation. La liste déroulante contient les certificats configurés dans le magasin de certificats de système Sterling B2B Integrator.

Zone	Description
Certificat public d'authentification	Obligatoire. Sélectionnez la clé publique que l'utilisateur fournit à la banque pour valider l'autorisation de l'utilisateur dans la demande envoyée par le client EBICS. Le partenaire commercial ou l'utilisateur partage la clé avec la banque. La clé doit être une partie publique du certificat de système Sterling B2B Integrator sélectionné comme certificat privé d'authentification.
Version de clé d'authentification	La version de la clé du certificat d'authentification s'affiche. La valeur X002 est admise.
Certificat privé de chiffrement	Obligatoire. Sélectionnez la clé privée que le client EBICS utilise pour déchiffrer la réponse reçue du serveur EBICS Banking Server. La liste déroulante contient les certificats configurés dans le magasin de certificats de système Sterling B2B Integrator.
Certificat public de chiffrement	Obligatoire. Sélectionnez la partie publique du certificat de système Sterling B2B Integrator sélectionné comme certificat privé de chiffrement. Le partenaire commercial ou l'utilisateur partage la clé avec la banque.
Version de clé de chiffrement	La version de la clé du certificat de chiffrement s'affiche. La valeur E002 est admise.
Utiliser le magasin de clés matérielles pour la signature électronique	Facultatif. Sélectionnez cette option si vous disposez d'un jeton de clé 3S activé, enregistré auprès de la banque.
Type de clé matérielle	Clé 3S s'affiche en tant que type de clé matérielle. Cette clé est une clé de signature sécurisée SWIFT utilisée pour l'identité numérique. Vous devez activer le jeton de clé 3S et enregistrer la clé auprès de la banque pour pouvoir signer et envoyer des messages à la banque.
Clé privée de signature électronique	Facultatif. Sélectionnez la clé privée du certificat de signature électronique (ES) si vous n'utilisez pas de clé matérielle pour la signature électronique.
Clé publique de signature électronique	Obligatoire. Sélectionnez la clé publique du certificat de signature électronique (ES) utilisé pour vérifier la signature des données de commande. La valeur de la clé publique d'un certificat de signature électronique ne doit pas être identique à celle d'un certificat d'authentification ou de chiffrement.

Zone	Description
Version de clé de signature électronique	Obligatoire si vous n'utilisez pas de magasin de clés matérielles pour la signature électronique. Sélectionnez la version de la clé du certificat de signature électronique. Les valeurs valides sont A005 et A006. Si vous utilisez un magasin de clés matérielles pour la signature électronique, la version de la clé est définie sur A005 et ne peut pas être modifiée.

7. Si vous avez sélectionné le type de certificat Clés, indiquez les valeurs des zones conformément aux instructions du tableau ci-après sur la page Informations techniques, puis cliquez sur **Suivant** :

Zone	Description
Clé privée d'authentification	Obligatoire. Cliquez sur Parcourir pour sélectionner le fichier contenant la partie privée de la clé d'authentification dans votre ordinateur.
Clé publique d'authentification	Obligatoire. Cliquez sur Parcourir pour sélectionner le fichier contenant la partie publique de la clé d'authentification dans votre ordinateur.
Version de clé d'authentification	Obligatoire. Sélectionnez la version de la clé du certificat d'authentification. La valeur X002 est admise.
Clé privée de chiffrement	Obligatoire. Cliquez sur Parcourir pour sélectionner le fichier contenant la partie privée de la clé de chiffrement dans votre ordinateur.
Clé publique de chiffrement	Obligatoire. Cliquez sur Parcourir pour sélectionner le fichier contenant la partie publique de la clé de chiffrement dans votre ordinateur.
Version de clé de chiffrement	Obligatoire. Sélectionnez la version de la clé du certificat de chiffrement. La valeur E002 est admise.
Clé privée de signature électronique	Obligatoire. Cliquez sur Parcourir pour sélectionner le fichier contenant la partie privée de la clé de signature électronique dans votre ordinateur.
Clé publique de signature électronique	Obligatoire. Cliquez sur Parcourir pour sélectionner le fichier contenant la partie publique de la clé de signature électronique dans votre ordinateur.
Version de clé de signature électronique	Obligatoire. Sélectionnez la version de la clé du certificat de signature électronique. Les valeurs valides sont A005 et A006.

8. Sur la page Partenaires associés, effectuez l'une des actions suivantes, puis cliquez sur **Suivant**.
- Cliquez sur l'icône d'ajout pour associer un nouveau partenaire à l'utilisateur.

- Cliquez sur l'icône de mise à jour en regard du partenaire que vous souhaitez modifier.
 - Cliquez sur l'icône de suppression pour dissocier un partenaire de l'utilisateur.
9. Cette étape est applicable uniquement si vous avez choisi d'ajouter un nouveau partenaire ou de modifier un partenaire existant. La banque affecte un ensemble de droits, de types de commande et de formats de fichier à un utilisateur en fonction de l'offre. Sur la page Partenaires associés : Paramètres utilisateur, indiquez les valeurs des zones conformément aux instructions du tableau ci-après, puis cliquez sur **Ajouter un partenaire**.

Zone	Description
Nom du partenaire	<p>Obligatoire. Dans la liste déroulante Nom du partenaire, sélectionnez le partenaire auquel un utilisateur est associé. Un utilisateur peut être associé à plusieurs partenaires.</p> <p>Remarque : Utilisez le tableau de bord Sterling B2B Integrator pour créer des entités de partenaire commercial.</p>
Chemin d'accès à la boîte d'envoi par téléchargement	<p>Obligatoire. Configurez la boîte aux lettres de téléchargement et affectez des utilisateurs pour faire fonctionner la boîte aux lettres dans Sterling B2B Integrator. Indiquez le chemin de la boîte aux lettres pour les messages téléchargés. Vous devez affecter un chemin de boîte aux lettres pour stocker les messages décompressés d'une demande EBICS.</p> <p>Si la boîte aux lettres (ID utilisateur, Nom du partenaire, Boîte de réception) existe déjà dans Sterling B2B Integrator et si vous laissez cette zone vide, un message d'erreur vous invite à indiquer le chemin d'accès par défaut à la boîte aux lettres.</p> <p>Remarque : Assurez-vous que le chemin de boîte aux lettres commence par une barre oblique (/).</p>
Chemin d'accès à la boîte de réception par téléchargement	<p>Obligatoire. Configurez la boîte aux lettres de téléchargement et affectez des utilisateurs pour faire fonctionner la boîte aux lettres dans Sterling B2B Integrator. Indiquez le chemin de la boîte aux lettres pour les messages téléchargés. Vous devez affecter un chemin de boîte aux lettres pour stocker les messages qui sont compressés dans une réponse EBICS.</p> <p>Si la boîte aux lettres (ID utilisateur, Nom du partenaire, Boîte d'envoi) existe déjà dans Sterling B2B Integrator et si vous laissez cette zone vide, un message d'erreur vous invite à indiquer le chemin d'accès par défaut à la boîte aux lettres.</p> <p>Remarque : Assurez-vous que le chemin de boîte aux lettres commence par une barre oblique (/).</p>

10. Cette étape n'est applicable que si vous avez choisi de configurer les paramètres de délégation des utilisateurs pour un utilisateur technique. Sur la page Partenaires associés, effectuez l'une des actions suivantes, puis cliquez sur **Suivant**.
 - Cliquez sur l'icône d'ajout pour associer un nouveau partenaire à l'utilisateur technique.
 - Cliquez sur l'icône de mise à jour en regard du partenaire que vous souhaitez modifier.
 - Cliquez sur l'icône de suppression pour dissocier un partenaire de l'utilisateur technique.
11. Cette étape n'est applicable que si vous configurez les paramètres de délégation des utilisateurs pour un utilisateur technique. Sur la page Partenaire associé : Paramètres utilisateur, indiquez les valeurs des zones conformément aux instructions du tableau ci-après, puis cliquez sur **Ajouter un partenaire**.

Zone	Description
Nom du partenaire	Obligatoire. Dans la liste déroulante Nom du partenaire , sélectionnez le partenaire auquel un utilisateur est associé. Un utilisateur peut être associé à plusieurs partenaires. Remarque : Utilisez le tableau de bord Sterling B2B Integrator pour créer des entités de partenaire commercial.
Délégué de	Obligatoire. Sélectionnez l'utilisateur qui déléguera ses tâches à l'utilisateur technique.

12. Sur la page Partenaires associés, cliquez sur **Suivant**.
13. Sur la page Confirmer, vérifiez les paramètres de configuration de l'utilisateur, puis cliquez sur **Terminer**. Vous pouvez également cliquer sur le lien **Afficher tout** en regard des **Partenaires associés** pour afficher la liste des partenaires associés à l'utilisateur.

Supprimer un profil utilisateur

Pourquoi et quand exécuter cette tâche

Vous devez être connecté à l'interface de tableau de bord du client EBICS en tant qu'administrateur pour mettre à jour un profil utilisateur, supprimer un profil utilisateur ou afficher le récapitulatif d'un utilisateur. Pour supprimer un profil utilisateur, procédez comme suit :

Procédure

1. Connectez-vous au client EBICS de Sterling B2B Integrator.
2. Dans le menu **Gestion de profil**, sélectionnez **Utilisateur**.
3. En utilisant **Rechercher** ou **Liste**, localisez l'ID utilisateur que vous souhaitez supprimer, puis cliquez sur **OK**.
4. Cliquez sur l'icône Supprimer en regard de l'ID utilisateur que vous souhaitez supprimer.

Remarque : Le fait de supprimer un profil utilisateur ne supprime pas les boîtes aux lettres correspondantes qui ont déjà été créées.

Créer un profil de banque

Vous pouvez créer un profil de banque afin de fournir les informations relatives à l'hôte EBICS pour une banque.

Pourquoi et quand exécuter cette tâche

Pour créer un profil de banque :

Procédure

1. Connectez-vous au client EBICS de Sterling B2B Integrator.
2. Dans le menu **Gestion de profil**, sélectionnez **Banque > Profil**.
3. Sur la page Configuration de la banque, cliquez sur **OK** en regard de **Créer une banque**.
4. Sur la page Informations bancaires, indiquez les valeurs des zones conformément aux instructions du tableau suivant, puis cliquez sur **Suivant**.

Zone	Description
ID de banque (ID hôte)	Obligatoire. Entrez l'ID de la banque ou l'ID de l'hôte fourni par la banque. Il s'agit d'un identifiant unique pour la banque dans le système de la banque.
Nom de la banque	Obligatoire. Indiquez le nom de la banque.
Statut	Le statut de la banque est défini sur Nouveau avant de valider les clés bancaires. Une fois la validation terminée, le statut passe à Activé. Le statut ne peut pas être modifié.
RSA préféré ?	Facultatif. Si vous souhaitez que le client EBICS utilise les valeurs de clé RSA pour la signature électronique, l'authentification et le chiffrement, cochez cette case. Le client EBICS utilise uniquement les valeurs associées à RSA pour la signature électronique, l'authentification et le chiffrement quel que soit le type de clé de téléchargement.
Utiliser l'espace de nom ESIG	Facultatif. Si vous souhaitez que le client EBICS utilise un espace de nom ESIG, cochez cette case.
Insérer des éléments facultatifs dans la balise xml KeyManagement request	Facultatif. Si vous souhaitez que le client EBICS utilise des éléments facultatifs dans le fichier xml KeyManagement request, cochez cette case.
Ligne d'adresse 1	Facultatif. Indiquez l'adresse de la banque.
Ligne d'adresse 2	Facultatif. Indiquez l'adresse de la banque.
Ville	Facultatif. Indiquez le nom de la ville où se situe la banque.
Département ou région	Facultatif. Indiquez le nom de l'état ou de la province.
Pays/région	Facultatif. Sélectionnez le pays ou la région.
Code postal	Facultatif. Indiquez le code postal.

Zone	Description
Adresse e-mail	Facultatif. Indiquez l'adresse e-mail de la banque.
Numéro de téléphone	Facultatif. Indiquez le numéro de téléphone avec l'indicatif du pays.

5. Sur la page Associer l'URL, cliquez sur l'icône Ajouter en regard de Associer l'URL, indiquez les valeurs des zones conformément aux instructions du tableau suivant, puis cliquez sur **Ajouter l'URL**.

Alias d'URL	Obligatoire. Indiquez un nom abrégé pour l'adresse URL de la banque. Pour accéder au site Web de la banque, entrez le nom abrégé ou l'alias dans la barre d'adresse du navigateur. Par exemple, si vous avez indiqué <i>bs</i> comme alias pour l'adresse URL http://www.banksystem.com , entrez <i>bs</i> dans la barre d'adresse du navigateur pour accéder au site Web de la banque.
Est la valeur par défaut	Facultatif. Cochez cette case pour indiquer que l'adresse URL spécifiée dans la zone URL est l'adresse URL par défaut. Si aucune adresse URL n'est spécifiée dans la zone URL de la banque sur la page Informations de commande lors de la soumission d'une commande, le client EBICS renseigne l'adresse URL par défaut dans la zone URL de la banque . Si l'alias de l'URL d'une banque n'est pas spécifié, l'URL par défaut est utilisée lorsqu'une commande est soumise par un utilisateur technique.
URL de la banque	Obligatoire. Indiquez l'URL HTTP que la banque héberge. Une banque peut avoir plusieurs adresses URL dont une au minimum. L'adresse URL est configurée dans l'adaptateur du serveur HTTP pour écouter le port et recevoir les demandes EBICS, le cas échéant. Remarque : Chaque ID de banque doit avoir un numéro de port ou une adresse URL unique.
Certificat https de la banque	Facultatif. Sélectionnez le certificat HTTPS approprié de la banque dans la liste déroulante. Le certificat HTTPS garantit que toutes les transactions avec la banque sont chiffrées et sécurisées.

Une fois ajoutés, les détails de l'adresse URL de la banque s'affichent dans un format tabulaire dans la page Associer l'URL.

6. Cliquez sur **Suivant**.
7. Sur la page Sélectionnez la version du protocole, cliquez sur **Extraire les versions de protocole prises en charge à partir de la banque**. Sélectionnez la version de protocole appropriée dans la liste déroulante et cliquez sur **Suivant**.
8. Sur la page Confirmer, vérifiez les paramètres de configuration de la banque, puis cliquez sur **Terminer**.

Rechercher un profil de banque

Pourquoi et quand exécuter cette tâche

Pour rechercher un profil de banque, procédez comme suit :

Procédure

1. Connectez-vous au client EBICS de Sterling B2B Integrator.
2. Dans le menu **Gestion de profil**, sélectionnez **Banque > Profil**.
3. Sur la page Configuration de la banque, effectuez l'une des actions suivantes, puis cliquez sur **OK** :
 - Dans la zone **ID de banque (ID hôte)** sous **Rechercher**, entrez tout ou partie de l'ID banque du profil de banque que vous recherchez.
 - Dans la liste déroulante **Par ordre alphabétique** sous **Liste**, sélectionnez la lettre par laquelle commence l'ID de la banque que vous recherchez.

Modifier un profil de banque

Vous pouvez modifier un profil de banque afin de réviser les informations relatives à l'hôte EBICS pour une banque.

Pourquoi et quand exécuter cette tâche

Pour modifier un profil de banque, procédez comme suit :

Procédure

1. Connectez-vous au client EBICS de Sterling B2B Integrator.
2. Dans le menu **Gestion de profil**, sélectionnez **Banque > Profil**.
3. Sur la page Configuration de la banque, en utilisant **Rechercher** ou **Liste**, localisez et sélectionnez l'ID de la banque que vous souhaitez modifier, puis cliquez sur **OK**.
4. Cliquez sur l'icône Mettre à jour en regard de l'ID de la banque que vous souhaitez modifier.
5. Sur la page Informations bancaires, indiquez les valeurs des zones conformément aux instructions du tableau suivant, puis cliquez sur **Suivant**.

Zone	Description
ID de banque (ID hôte)	Obligatoire. Entrez l'ID de la banque ou l'ID de l'hôte fourni par la banque. Il s'agit d'un identifiant unique pour la banque dans le système de la banque.
Nom de la banque	Obligatoire. Indiquez le nom de la banque.
Statut	Le statut de la banque est défini sur Nouveau avant de valider les clés bancaires. Une fois la validation terminée, le statut passe à Activé. Le statut ne peut pas être modifié.

Zone	Description
RSA préféré ?	Facultatif. Si vous souhaitez que le client EBICS utilise les valeurs de clé RSA pour la signature électronique, l'authentification et le chiffrement, cochez cette case. Le client EBICS utilise uniquement les valeurs associées à RSA pour la signature électronique, l'authentification et le chiffrement quel que soit le type de clé de téléchargement.
Utiliser l'espace de nom ESIG	Facultatif. Si vous souhaitez que le client EBICS utilise un espace de nom ESIG, cochez cette case.
Insérer des éléments facultatifs dans la balise xml KeyManagement request	Facultatif. Si vous souhaitez que le client EBICS utilise des éléments facultatifs dans le fichier xml KeyManagement request, cochez cette case.
Ligne d'adresse 1	Facultatif. Indiquez l'adresse de la banque.
Ligne d'adresse 2	Facultatif. Indiquez l'adresse de la banque.
Ville	Facultatif. Indiquez le nom de la ville où se situe la banque.
Département ou région	Facultatif. Indiquez le nom de l'état ou de la province.
Pays/région	Facultatif. Sélectionnez le pays ou la région.
Code postal	Facultatif. Indiquez le code postal.
Adresse e-mail	Facultatif. Indiquez l'adresse e-mail de la banque.
Numéro de téléphone	Facultatif. Indiquez le numéro de téléphone avec l'indicatif du pays.

6. Sur la page Associer l'URL, cliquez sur l'icône Mettre à jour en regard de l'ID de la banque que vous souhaitez modifier, indiquez les valeurs des zones conformément aux instructions du tableau ci-après, puis cliquez sur **Ajouter l'URL**.

Alias d'URL	Obligatoire. Indiquez un nom abrégé pour l'adresse URL de la banque. Pour accéder au site Web de la banque, entrez le nom abrégé ou l'alias dans la barre d'adresse du navigateur. Par exemple, si vous avez indiqué <i>bs</i> comme alias pour l'adresse URL http://www.banksystem.com , entrez <i>bs</i> dans la barre d'adresse du navigateur pour accéder au site Web de la banque.
-------------	---

Est la valeur par défaut	Facultatif. Cochez cette case pour indiquer que l'adresse URL spécifiée dans la zone URL est l'adresse URL par défaut. Si aucune adresse URL n'est spécifiée dans la zone URL de la banque sur la page Informations de commande lors de la soumission d'une commande, le client EBICS renseigne l'adresse URL par défaut dans la zone URL de la banque . Si l'alias de l'URL d'une banque n'est pas spécifié, l'URL par défaut est utilisée lorsqu'une commande est soumise par un utilisateur technique.
URL de la banque	Obligatoire. Indiquez l'URL HTTP que la banque héberge. Une banque peut avoir plusieurs adresses URL dont une au minimum. L'adresse URL est configurée dans l'adaptateur du serveur HTTP pour écouter le port et recevoir les demandes EBICS, le cas échéant. Remarque : Chaque ID de banque doit avoir un numéro de port ou une adresse URL unique.
Certificat https de la banque	Facultatif. Sélectionnez le certificat HTTPS approprié de la banque dans la liste déroulante. Le certificat HTTPS garantit que toutes les transactions avec la banque sont chiffrées et sécurisées.

Une fois ajoutés, les détails de l'adresse URL de la banque s'affichent dans un format tabulaire dans la page Associer l'URL.

7. Cliquez sur **Suivant**.
8. Sur la page Sélectionnez la version du protocole, cliquez sur **Suivant**. La version du protocole ne peut pas être mise à jour en raison des dépendances sur la configuration de l'offre et des signataires.
9. Sur la page Confirmer, vérifiez les paramètres de configuration de la banque, puis cliquez sur **Terminer**.

Supprimer un profil de banque

Pourquoi et quand exécuter cette tâche

Pour supprimer un profil de banque, procédez comme suit :

Procédure

1. Connectez-vous au client EBICS de Sterling B2B Integrator.
2. Dans le menu **Gestion de profil**, sélectionnez **Banque > Profil**.
3. Sur la page Configuration de la banque, en utilisant **Rechercher** ou **Liste**, localisez et sélectionnez l'ID de la banque (ID hôte) que vous souhaitez supprimer, puis cliquez sur **OK**.
4. Cliquez sur l'icône Supprimer en regard de l'ID de banque que vous souhaitez supprimer.

Validation d'une clé bancaire

Avant de commencer

Soumettez la commande HPB avant la validation des clés bancaires.

Pourquoi et quand exécuter cette tâche

Pour déterminer l'authenticité d'identification et d'authentification de la banque, ainsi que les clés de chiffrement, le client EBICS vous permet de valider la valeur hachée des certificats envoyés par la banque. Une fois les clés bancaires validées, le statut de la banque passe à Activé. Pour valider une clé bancaire, procédez comme suit :

Procédure

1. Connectez-vous au client EBICS de Sterling B2B Integrator.
2. Dans le menu **Gestion de profil**, sélectionnez **Banque > Validation des clés bancaires**.
3. Sur la page Validation des clés bancaires, indiquez les valeurs des zones conformément aux instructions du tableau suivant :

Zone	Description
ID de banque (ID hôte)	Obligatoire. Sélectionnez l'ID de la banque dans la liste déroulante.
Valeur de hachage de la clé d'identification et d'authentification (format hexadécimal)	Obligatoire. Indiquez la valeur hachée de la clé d'identification et d'authentification fournie par la banque.
Algorithme de hachage	Obligatoire. Sélectionnez l'algorithme haché de la valeur hachée clé d'identification et d'authentification. Les valeurs valides sont : <ul style="list-style-type: none">• SHA1 (par défaut)• SHA256
Valeur de hachage de la clé de chiffrement (format hexadécimal)	Obligatoire. Indiquez la valeur hachée de la clé de chiffrement fournie par la banque.
Algorithme de hachage	Obligatoire. Sélectionnez l'algorithme haché de la valeur hachée de clé de chiffrement. Les valeurs valides sont : <ul style="list-style-type: none">• SHA1 (par défaut)• SHA256

4. Cliquez sur **Réinitialiser** si vous souhaitez supprimer les valeurs existantes et entrer de nouvelles valeurs.
5. Cliquez sur **Valider**.

Créer une offre

Pourquoi et quand exécuter cette tâche

Une offre permet à un partenaire de regrouper un ensemble de types de commande et de formats de fichier et de les traiter ensemble. Une offre doit être associée à un ID de banque spécifique. Une seule offre est autorisée par banque. Pour créer une offre, procédez comme suit :

Procédure

1. Connectez-vous au client EBICS de Sterling B2B Integrator.
2. Dans le menu **Gestion de profil**, sélectionnez **Banque > Configurations des offres**.
3. Sur la page Configuration de l'offre, cliquez sur **OK** en regard de **Créer une nouvelle offre**.
4. Sur la page Créer : Offre, indiquez les valeurs des zones conformément aux instructions du tableau suivant, puis cliquez sur **Terminer**.

Zone	Description
Nom de l'offre	Obligatoire. Indiquez un nom pour l'offre.
ID de banque (ID hôte)	Obligatoire. Sélectionnez un identifiant de banque dans la liste déroulante.
Associer/dissocier le type de commande de la configuration du format de fichier	Facultatif. Cochez la case en regard du type de commande. Les types de commande sélectionnés et les formats de fichier correspondants sont regroupés pour former une offre.

Rechercher une offre

Pourquoi et quand exécuter cette tâche

Pour rechercher une offre, procédez comme suit :

Procédure

1. Connectez-vous au client EBICS de Sterling B2B Integrator.
2. Dans le menu **Gestion de profil**, sélectionnez **Banque > Configurations des offres**.
3. Sur la page Configuration de l'offre, effectuez l'une des actions suivantes, puis cliquez sur **OK**.
 - Dans la zone **ID de banque (ID hôte)** sous **Rechercher**, entrez tout ou partie de l'ID de banque auquel l'offre que vous recherchez est associée.
 - Dans la liste déroulante **Par ordre alphabétique** sous **Liste**, sélectionnez la lettre par laquelle commence le nom de l'offre que vous recherchez.

Modifier une offre

Pourquoi et quand exécuter cette tâche

Pour modifier une offre, procédez comme suit :

Procédure

1. Connectez-vous au client EBICS de Sterling B2B Integrator.
2. Dans le menu **Gestion de profil**, sélectionnez **Banque > Configurations des offres**.
3. Sur la page Configuration de l'offre, en utilisant **Rechercher** ou **Liste**, localisez et sélectionnez l'offre que vous souhaitez modifier, puis cliquez sur **OK**.
4. Cliquez sur l'icône **Mettre à jour** en regard de l'offre que vous souhaitez modifier.
5. Sur la page **Mettre à jour : Offre**, indiquez les valeurs des zones conformément aux instructions du tableau suivant, puis cliquez sur **Terminer**.

Zone	Description
Associer/dissocier le type de commande de la configuration du format de fichier	Facultatif. Cochez la case en regard du type de commande. Les types de commande sélectionnés et les formats de fichier correspondants sont regroupés pour former l'offre.

Supprimer une offre

Pourquoi et quand exécuter cette tâche

Pour supprimer une offre, procédez comme suit :

Procédure

1. Connectez-vous au client EBICS de Sterling B2B Integrator.
2. Dans le menu **Gestion de profil**, sélectionnez **Banque > Configurations des offres**.
3. Sur la page Configuration de l'offre, en utilisant **Rechercher** ou **Liste**, localisez et sélectionnez l'offre que vous souhaitez supprimer, puis cliquez sur **OK**.
4. Cliquez sur l'icône Supprimer en regard de l'offre que vous souhaitez supprimer.

Créer un format de fichier

Pourquoi et quand exécuter cette tâche

Le client EBICS vous permet d'ajouter des formats de fichier et de les associer aux types de commande de téléchargement technique bancaire (FUL et FDL). Un type de commande peut ne contenir aucun format de fichier ou en contenir plusieurs. Les formats de fichier pour les types de commande FUL et FDL se basent sur le type de demande SWIFTNet. Pour plus d'informations sur SWIFTNet, voir <http://www.swift.com/>. Pour créer un format de fichier, procédez comme suit :

Procédure

1. Connectez-vous au client EBICS de Sterling B2B Integrator.
2. Dans le menu **Gestion de profil**, sélectionnez **Formats de fichier**.
3. Sur la page Configuration du format de fichier, cliquez sur **OK** en regard de **Créer le format de fichier**.
4. Sur la page Créer : Format de fichier, entrez les valeurs des zones répertoriées dans le tableau suivant, puis cliquez sur **Suivant**.

Zone	Description
Format de fichier	Obligatoire. Indiquez le nom du format de fichier. La première partie du nom du format de fichier doit correspondre à l'un des éléments suivants. Par exemple, pain.xxx.vcom.dda. Les éléments indiquent le type de la transaction. <ul style="list-style-type: none"> • pain. - Ordre de paiement • camt. - Gestion des liquidités • tsrv. - Services commerciaux • tsmt. - Gestion des services commerciaux

Zone	Description
Pays/région	Obligatoire. Sélectionnez un pays ou une région dans la liste déroulante.
Types de commande pris en charge	Obligatoire. Sélectionnez le type de commande pour lequel le format de fichier est pris en charge. Par exemple, FUL, FDL.

- Sur la page Confirmer, vérifiez les paramètres du format de fichier, puis cliquez sur **Terminer**.

Rechercher un format de fichier

Pourquoi et quand exécuter cette tâche

Pour rechercher un format de fichier, procédez comme suit :

Procédure

- Connectez-vous au client EBICS de Sterling B2B Integrator.
- Dans le menu **Gestion de profil**, sélectionnez **Formats de fichier**.
- Sur la page Configuration du format de fichier, effectuez l'une des actions suivantes, puis cliquez sur **OK**.
 - Dans la zone **Format de fichier** sous **Rechercher**, entrez tout ou partie du nom du format de fichier que vous recherchez.
 - Dans la liste déroulante **Par ordre alphabétique** sous **Liste**, sélectionnez la lettre par laquelle commence le format de fichier que vous recherchez.
- Cliquez sur le lien de format de fichier pour afficher les paramètres de format de fichier.

Modifier un format de fichier

Pourquoi et quand exécuter cette tâche

Pour modifier un format de fichier, procédez comme suit :

Procédure

- Connectez-vous au client EBICS de Sterling B2B Integrator.
- Dans le menu **Gestion de profil**, sélectionnez **Formats de fichier**.
- Sur la page Configuration du format de fichier, en utilisant **Rechercher** ou **Liste**, localisez et sélectionnez le format de fichier que vous souhaitez modifier, puis cliquez sur **OK**.
- Cliquez sur l'icône Mettre à jour en regard du format de fichier que vous souhaitez modifier.
- Sur la page Mettre à jour : Format de fichier, indiquez les valeurs des zones conformément aux instructions du tableau suivant, puis cliquez sur **Suivant**.

Zone	Description
Pays/région	Obligatoire. Sélectionnez un pays ou une région dans la liste déroulante.
Types de commande pris en charge	Obligatoire. Sélectionnez le type de commande pour lequel le format de fichier est pris en charge.

- Sur la page Confirmer, vérifiez les valeurs, puis cliquez sur **Terminer**.

Supprimer un format de fichier

Pourquoi et quand exécuter cette tâche

Pour supprimer un format de fichier, procédez comme suit :

Procédure

1. Connectez-vous au client EBICS de Sterling B2B Integrator.
2. Dans le menu **Gestion de profil**, sélectionnez **Formats de fichier**.
3. Sur la page Configuration du format de fichier, à l'aide de **Rechercher** ou de **Liste**, localisez et sélectionnez l'offre que vous souhaitez supprimer, puis cliquez sur **OK**.
4. Cliquez sur l'icône Supprimer en regard du format de fichier que vous souhaitez supprimer.

Configuration des droits d'utilisateur

Les droits d'utilisateur définissent les offres, les types de commande et les formats de fichier qu'un utilisateur du client EBICS peut traiter dans le client EBICS. Les droits d'utilisateur sont dérivés de l'offre créée pour la banque. Vous pouvez affecter l'un des types de droit suivants à un utilisateur :

- **Signataire** : un signataire signe ou rejette une commande. Un émetteur peut soumettre la commande uniquement après l'obtention des signatures requises. Un signataire ne peut pas soumettre la commande qu'il a signée.
- **Émetteur** : un émetteur peut soumettre une commande une fois que le signataire désigné a signé la commande.

Tableau 2. Niveaux d'autorisation

Niveau d'autorisation	Type de droit	Description
E	Signataire	Signature unique. E est le niveau d'autorisation le plus élevé.
A	Signataire	Signature principale
B	Signataire	Signature secondaire
T	Émetteur	Signature de transport. Les signatures de transport ne sont pas utilisées pour autoriser les commandes techniques bancaires, mais pour la soumission autorisée au système de la banque.

Si la valeur de la signature électronique est définie sur 1, une signature unique dont le niveau d'autorisation est E ou A est suffisante pour traiter une commande. Si la valeur de la signature électronique est définie sur 2, une combinaison de E ou A et de B est nécessaire pour traiter la commande. Seuls les niveaux d'autorisation T et E sont toutefois pris en charge dans les banques françaises. La valeur de la signature électronique est définie sur 0 dans le cas d'une commande de gestion de clés.

Remarque : La spécification EBICS ne permet pas de combiner deux niveaux d'autorisation de signature électronique secondaire (c'est-à-dire, le niveau d'autorisation B) pour traiter une commande.

Créer un droit d'utilisateur

Pourquoi et quand exécuter cette tâche

Pour créer un droit d'utilisateur, procédez comme suit :

Procédure

1. Connectez-vous au client EBICS de Sterling B2B Integrator.
2. Dans le menu **Droits**, sélectionnez **Droits d'utilisateur**.
3. Sur la page Configuration du droit d'utilisateur, cliquez sur **OK** en regard de **Créer un nouveau droit**.
4. Sur la page Créer : Informations sur le droit, dans la liste déroulante **Nom d'offre**, sélectionnez le nom de l'offre pour laquelle vous souhaitez configurer les droits d'utilisateur. L'ID de la banque associé à l'offre s'affiche. L'icône Ajouter qui permet d'ajouter le droit s'affiche également.
5. Cliquez sur l'icône Ajouter. La page Ajouter un droit s'affiche.
6. Sur la page Ajouter un droit, indiquez les valeurs des zones conformément aux instructions du tableau suivant, puis cliquez sur l'icône Ajouter située en regard de Ajouter des signataires :

Zone	Description
Type de commande et format de fichier	Obligatoire. Les types de commande et le format de fichier associé à l'offre sont sélectionnés par défaut. Pour empêcher un utilisateur de traiter certains types de commande et certains formats de fichier, décochez la case en regard du type de commande et du format de fichier associé.
Nombre minimal de signatures requises	Obligatoire. Indiquez le nombre de signatures requises pour traiter la commande.

7. Sur la page Ajouter un signataire, indiquez les valeurs des zones conformément aux instructions du tableau suivant, puis cliquez sur **Ajouter un signataire** :

Zone	Description
ID utilisateur	Obligatoire. Dans la liste déroulante, sélectionnez l'ID de l'utilisateur auquel vous souhaitez affecter le droit.
Nom du partenaire	Obligatoire. Dans la liste déroulante, sélectionnez le nom du partenaire associé à l'utilisateur.
Type de droit	Obligatoire. Sélectionnez l'un des types de droit suivants : <ul style="list-style-type: none">• Signataire• Émetteur

Zone	Description
Niveau d'autorisation	<p>Obligatoire. Si vous avez sélectionné le type de droit Émetteur, le niveau d'autorisation T est affecté à l'utilisateur. Vous n'avez pas besoin de sélectionner un niveau d'autorisation dans la liste déroulante.</p> <p>Si vous avez sélectionné le type de droit Signataire, sélectionnez l'un des niveaux d'autorisation suivants dans la liste déroulante :</p> <ul style="list-style-type: none"> • E : signature unique • A : signature principale • B : signature secondaire

8. Cliquez sur **Sauvegarder**, puis sur **Terminer**.

Rechercher un droit d'utilisateur

Pourquoi et quand exécuter cette tâche

Pour rechercher un droit d'utilisateur, procédez comme suit :

Procédure

1. Connectez-vous au client EBICS de Sterling B2B Integrator.
2. Dans le menu **Droits**, sélectionnez **Droits d'utilisateur**.
3. Sur la page Configuration du droit d'utilisateur, effectuez l'une des actions suivantes, puis cliquez sur **OK** :
 - Dans la zone **Nom d'offre** ou **ID de banque (ID hôte)**, sous **Rechercher**, entrez tout ou partie du nom de l'offre ou de l'ID de banque pour lequel le droit d'utilisateur est configuré.
 - Dans la liste déroulante **Par ordre alphabétique**, sous **Liste**, sélectionnez la lettre par laquelle commence le nom de l'offre ou l'ID de banque pour lequel le droit d'utilisateur est configuré.

Modifier un droit d'utilisateur

Pourquoi et quand exécuter cette tâche

Pour modifier un droit d'utilisateur, procédez comme suit :

Procédure

1. Connectez-vous au client EBICS de Sterling B2B Integrator.
2. Dans le menu **Droits**, sélectionnez **Droits d'utilisateur**.
3. Sur la page Configuration du droit d'utilisateur, en utilisant **Rechercher** ou **Liste**, localisez et sélectionnez l'offre pour laquelle vous souhaitez modifier le droit d'utilisateur, puis cliquez sur **OK**.
4. Cliquez sur l'icône **Mettre à jour** en regard du droit d'utilisateur que vous souhaitez modifier.
5. Sur la page **Mettre à jour : Informations sur le droit**, procédez comme suit :
 - Cliquez sur l'icône **Ajouter** située en regard de **Ajouter un droit** pour ajouter un format de fichier au droit d'utilisateur.
 - Cliquez sur l'icône **Mettre à jour** située en regard du format de fichier.

- Cliquez sur l'icône Supprimer située en regard du format de fichier.
6. Cette étape est applicable si vous avez choisi d'ajouter un droit. Sur la page Ajouter un droit, indiquez les valeurs des zones conformément aux instructions du tableau suivant, puis cliquez sur l'icône Ajouter située en regard de Ajouter des signataires :

Zone	Description
Type de commande et format de fichier	Obligatoire. Les types de commande et le format de fichier associé à l'offre sont sélectionnés par défaut. Pour empêcher un utilisateur de traiter certains types de commande et formats de fichier, décochez la case en regard du type de commande et du format de fichier associé.
Nombre minimal de signatures requises	Obligatoire. Indiquez le nombre de signatures requises pour traiter la commande.

Sur la page Ajouter un signataire, indiquez les valeurs des zones conformément aux instructions du tableau suivant, puis cliquez sur **Ajouter un signataire** :

Zone	Description
ID utilisateur	Obligatoire. Dans la liste déroulante, sélectionnez l'ID de l'utilisateur auquel vous souhaitez affecter le droit.
Nom du partenaire	Obligatoire. Dans la liste déroulante, sélectionnez le nom du partenaire associé à l'utilisateur.
Type de droit	Obligatoire. Sélectionnez l'un des types de droit suivants : <ul style="list-style-type: none"> • Signataire • Émetteur
Niveau d'autorisation	Obligatoire. Si vous avez sélectionné le type de droit Émetteur, le niveau d'autorisation T est affecté à l'utilisateur. Vous n'avez pas besoin de sélectionner un niveau d'autorisation dans la liste déroulante. Si vous avez sélectionné le type de droit Signataire, sélectionnez l'un des niveaux d'autorisation suivants dans la liste déroulante : <ul style="list-style-type: none"> • E - Signature unique • A - Signature principale • B - Signature secondaire

7. Cette étape est applicable si vous avez choisi de modifier un droit. Sur la page Modifier un droit, indiquez les valeurs des zones conformément aux instructions du tableau suivant, puis cliquez sur **Sauvegarder** :

Zone	Description
Nombre minimal de signatures requises	Facultatif. Indiquez le nombre de signatures requises pour traiter la commande.

Zone	Description
Icône Ajouter située en regard de Ajouter des signataires	Facultatif. Cliquez sur l'icône Ajouter située en regard de Ajouter des signataires pour ajouter un signataire au droit d'utilisateur.
Icône Mettre à jour	Facultatif. Cliquez sur l'icône Mettre à jour située en regard d'un signataire pour modifier les paramètres du signataire.
Icône Supprimer	Facultatif. Cliquez sur l'icône Supprimer située en regard d'un signataire pour supprimer le signataire.

8. Cliquez sur **Terminer**.

Supprimer un droit d'utilisateur

Pourquoi et quand exécuter cette tâche

Pour supprimer un droit d'utilisateur, procédez comme suit :

Procédure

1. Connectez-vous au client EBICS de Sterling B2B Integrator.
2. Dans le menu **Droits**, sélectionnez **Droits d'utilisateur**.
3. Sur la page Configuration du droit d'utilisateur, en utilisant **Rechercher** ou **Liste**, localisez et sélectionnez l'offre pour laquelle vous souhaitez supprimer le droit d'utilisateur, puis cliquez sur **OK**.
4. Cliquez sur l'icône Supprimer en regard du droit d'utilisateur que vous souhaitez supprimer.

Initialisation d'un utilisateur

Une banque conclut un contrat avec ses partenaires commerciaux. Le contrat définit les dispositions des transactions commerciales convenues entre la banque et le partenaire commercial.

La banque n'a pas encore les certificats publics de l'utilisateur. La transmission des certificats publics de l'utilisateur au système de la banque est obligatoire pour initialiser l'utilisateur.

Il existe trois types de commande pour l'initialisation des abonnés : H3K, INI et HIA. H3K est le plus simple et transmet les trois certificats publics simultanément. Cependant, H3K n'est pas utilisable dans tous les cas, comme lorsque des clés certifiées ou le protocole version H003 sont utilisés. Si vous ne pouvez pas utiliser H3K (ou préférez ne pas l'utiliser), optez pour INI et HIA afin de transmettre les certificats.

Tableau 3. Types de commande pour l'initialisation d'abonné

Types de commande	Protocole	Clés/certificats
H3K	H004	<ul style="list-style-type: none"> • Clé technique bancaire pour la signature électronique (ES) • Certificat d'identification et d'authentification • Certificat de chiffrement

Tableau 3. Types de commande pour l'initialisation d'abonné (suite)

Types de commande	Protocole	Clés/certificats
INI	H003, H004	Clé technique bancaire
HIA	H003, H004	<ul style="list-style-type: none"> • Clé d'identification et d'authentification • Clé de chiffrement

H3K

Avec la version de protocole H004, vous pouvez utiliser le type de commande H3K, qui simplifie et automatise la procédure en regroupant les demandes INI et HIA dans une seule étape. Les clés sécurisées ne sont pas prises en charge pour la commande H3K. Par ailleurs, il faut au moins que la clé technique bancaire utilisée pour la signature numérique soit un certificat émis par une autorité de certification (CA). Les deux autres certificats utilisés pour l'identification et l'autorisation et pour le chiffrement peuvent être des certificats autosignés. H3K ne requiert pas de lettres d'initialisation.

Utilisez INI et HIA pour effectuer l'initialisation avec des certificats ou des clés sécurisées non émis par des autorités de certification ou avec le protocole de version H003.

INI et HIA

Les versions de la signature électronique (ES) prises en charge, à savoir le chiffrement, l'identification et l'authentification, sont les composantes des paramètres bancaires. La clé technique bancaire de l'utilisateur doit avoir été générée récemment si l'utilisateur n'a pas une clé technique bancaire appropriée ou ne veut pas utiliser une clé technique bancaire existante pour la nouvelle connexion à la banque. La même chose s'applique pour la clé de chiffrement et la clé d'identification et d'authentification.

L'utilisateur transmet les certificats publics à l'institution financière via deux voies de communication indépendantes :

- INI - Envoie la clé technique bancaire publique
- HIA - Envoie la clé d'identification et d'authentification publique et la clé de chiffrement public

Lorsque l'utilisateur est d'abord assigné à un partenaire, le statut de l'utilisateur est Nouveau. Si l'utilisateur envoie uniquement une demande INI à la banque, le statut est modifié en Partiellement Initialisé (INI). Si l'utilisateur envoie uniquement une demande HIA à la banque, le statut est modifié en Partiellement Initialisé (HIA). Après l'envoi à la banque des deux demandes (INI et HIA) par l'utilisateur, le statut passe à Initialisé dans le système de la banque.

L'utilisateur génère les lettres INI et HIA avec la valeur hachée des clés à l'aide de l'interface du tableau de bord du client EBICS de Sterling B2B Integrator, les signe manuellement et envoie les lettres à la banque. Lorsque la banque reçoit les lettres d'initialisation de INI et HIA, elle vérifie les valeurs hachées dans les lettres par rapport à sa base de données. Une fois la vérification terminée, le statut de l'utilisateur passe à Prêt dans le système de la banque, ce qui signifie que l'utilisateur peut désormais effectuer des transactions avec la banque. L'utilisateur télécharge ensuite les certificats publics de la banque à l'aide du type de

commande système HPB et les valide à l'aide de l'interface de tableau de bord du client EBICS de Sterling B2B Integrator. Une fois la validation terminée, le statut de la banque est défini sur **Activé**, ce qui indique que la transaction avec la banque est désormais possible.

Les abonnés peuvent extraire les informations stockées par la banque et applicables à la société de l'abonné et à tous les abonnés associés à l'aide des types de commande HKD et HTD, une fois que le statut de l'utilisateur est **Prêt** (indiquant que l'utilisateur peut effectuer des transactions avec la banque).

Soumission de commandes

Les utilisateurs du client EBICS de Sterling B2B Integrator peuvent soumettre des commandes à l'aide de la fonction **Soumission de commande** à partir du menu **Utilisateur**.

Pourquoi et quand exécuter cette tâche

Si la commande qui est soumise doit être signée, une tâche en attente est créée pour le signataire. Une fois le nombre de signatures requis obtenu, la commande est soumise à la banque. La page **Soumission de commande** vous aide à configurer les paramètres de votre commande et à soumettre une commande.

Procédure

1. Connectez-vous au client EBICS de Sterling B2B Integrator.
2. À partir du menu **Utilisateur**, sélectionnez **Soumission de commande**.
Indiquez les valeurs des zones conformément aux instructions du tableau suivant, puis cliquez sur **Suivant**.

Zone	Description
Nom du partenaire	Obligatoire. Sélectionnez un nom de partenaire dans la liste déroulante.
ID de banque (ID hôte)	Obligatoire. Sélectionnez un ID de banque associé au partenaire dans la liste déroulante.
URL de la banque	Obligatoire. Sélectionnez l'adresse URL requise dans la liste déroulante. L'adresse URL sélectionnée est utilisée pour établir une session HTTP ou HTTPS avec le serveur EBICS Banking Server.
Filtre de type de commande	Obligatoire. Dans la liste déroulante, sélectionnez le type de commande approprié : <ul style="list-style-type: none">• Commandes de gestion de clés• Commandes techniques bancaires• Commandes de gestion VEU• Autres types de commande
Type de commande	Obligatoire. Dans la liste déroulante, sélectionnez le type de commande requis. Les types de commande sont affectés à l'offre et sont représentés par un code alphanumérique à 3 chiffres qui identifie le type de la commande.

Les types de commande s'affichent en fonction des droits d'utilisateur configurés pour l'utilisateur du client EBICS.

Remarque : Les zones qui apparaissent dans la page **Configuration du type de commande** varient en fonction du type de commande que vous avez

sélectionné dans la liste déroulante **Type de commande**. Il est donc important de sélectionner un type de commande approprié. Par exemple, si vous sélectionnez le type de commande INI, les zones spécifiques à INI s'affichent pour la configuration de la commande.

3. Si vous avez sélectionné le type de commande de gestion de clés, indiquez les valeurs des zones conformément aux instructions du tableau suivant, puis cliquez sur **Envoyer**.

Zone	Description
Préfixe d'ID de commande	Facultatif. Dans la liste déroulante, sélectionnez le préfixe de l'ID de commande. Le client EBICS alloue un ID de commande unique pour chaque commande en fonction de la banque, de l'ID utilisateur et du type de commande. Le client génère l'ID de commande conformément aux spécifications EBICS. L'ID de commande est un identifiant alphanumérique à 4 chiffres. Vous pouvez indiquer le premier caractère de l'ID de commande. Les deuxième, troisième et quatrième caractères de l'ID de commande sont des caractères alphanumériques dans l'ordre croissant (A-Z ou 0-9). Cette zone est applicable à tous les types de commande de gestion de clés.
Moyen de sécurité	Un numéro de sécurité à 4 chiffres s'affiche par défaut. La valeur ne peut pas être modifiée pour les types de commande INI, HIA et HPB.
ID de produit	Entrez l'ID de produit pour l'application client EBICS.
Langue de produit	Entrez le paramètre linguistique de l'application client EBICS que vous utilisez. Par exemple, entrez EN si la langue est définie sur Anglais.
Certificat privé d'authentification	Obligatoire. Dans la liste déroulante, sélectionnez le certificat privé d'authentification approprié.
Certificat public d'authentification	Obligatoire. Dans la liste déroulante, sélectionnez le certificat public d'authentification approprié.
Version de clé d'authentification	La version de la clé du certificat d'authentification s'affiche. La valeur X002 est admise.
Certificat privé de chiffrement	Obligatoire. Dans la liste déroulante, sélectionnez le certificat privé de chiffrement approprié.
Certificat public de chiffrement	Obligatoire. Dans la liste déroulante, sélectionnez le certificat public de chiffrement approprié.
Version de clé de chiffrement	La version de la clé du certificat de chiffrement s'affiche. La valeur E002 est admise.
Clé privée de signature électronique	Obligatoire. Dans la liste déroulante, sélectionnez la clé privée de signature électronique appropriée.
Clé publique de signature électronique	Obligatoire. Dans la liste déroulante, sélectionnez la clé publique de signature électronique appropriée.
Version de clé de signature électronique	Obligatoire. Dans la liste déroulante, sélectionnez la version de la clé de signature électronique appropriée.

4. Si vous avez sélectionné le type de commande technique bancaire, indiquez les valeurs des zones conformément aux instructions du tableau suivant, puis cliquez sur **Envoyer**.

Préfixe d'ID de commande	Facultatif. Dans la liste déroulante, sélectionnez le préfixe de l'ID de commande. Le client EBICS alloue un ID de commande unique pour chaque commande en fonction de la banque, de l'ID utilisateur et du type de commande. Le client génère l'ID de commande conformément aux spécifications EBICS. L'ID de commande est un identifiant alphanumérique à 4 chiffres. Vous pouvez indiquer le premier caractère de l'ID de commande. Les deuxième, troisième et quatrième caractères de l'ID de commande sont des caractères alphanumériques dans l'ordre croissant (A-Z ou 0-9).
Moyen de sécurité	Obligatoire. Entrez un numéro de sécurité à 4 chiffres compris entre 0499 et 0100.
ID de produit	Entrez l'ID de produit pour l'application client EBICS.
Langue de produit	Entrez le paramètre linguistique de l'application client EBICS que vous utilisez. Par exemple, entrez EN si la langue est définie sur Anglais.
Soumission auto	Facultatif. Cette case à cocher s'applique uniquement pour le type de commande FUL ; elle est cochée par défaut. Si l'option de soumission automatique est sélectionnée, une commande est soumise automatiquement une fois que le nombre de signatures requis a été obtenu. Si l'option de soumission automatique n'est pas sélectionnée, un utilisateur du client EBICS doit se connecter à l'interface de tableau de bord du client EBICS, accéder à l'écran des tâches en attente et soumettre la commande une fois le nombre de signatures requis obtenu.
Lire le fichier depuis la boîte aux lettres	Obligatoire. Cette option n'est applicable qu'au type de commande FUL. Pour télécharger le fichier de charge à partir de la boîte aux lettres, sélectionnez Oui . Cliquez sur Sélectionnez le fichier en regard de Télécharger le fichier. Dans la liste Sélectionnez un fichier à télécharger depuis la boîte aux lettres, sélectionnez le fichier requis, puis cliquez sur Terminer . Pour télécharger le fichier de charge depuis un emplacement de fichier, sélectionnez Non . Cliquez sur Parcourir en regard de Télécharger le fichier, accédez à l'emplacement du fichier, puis sélectionnez le fichier requis.
Format de fichier	Obligatoire uniquement pour les types de commande FUL et FDL. Dans la liste déroulante, sélectionnez le format de fichier approprié.
Date de début	Facultatif. Cliquez sur la zone, puis sélectionnez la date de début dans le calendrier. Cette option n'est applicable qu'au type de commande FDL.
Date de fin	Facultatif. Cliquez sur la zone, puis sélectionnez la date de fin dans le calendrier. Cette option n'est applicable qu'au type de commande FDL.

Liste des paramètres de commande	<p>Facultatif. Cliquez sur Ajouter un paramètre pour définir les variables d'une commande. Renseignez les informations des zones de paramètre de commande suivantes, puis cliquez sur Ajouter un paramètre. Cette option n'est applicable qu'au type de commande FDL.</p> <ul style="list-style-type: none"> • Nom : obligatoire. Entrez un nom unique pour le paramètre. N'utilisez ni espace ni caractère spécial dans le nom du paramètre. • Valeur : obligatoire. Entrez une valeur pour le paramètre. • Type : facultatif. Sélectionnez le type de paramètre. Les valeurs disponibles sont les suivantes : <ul style="list-style-type: none"> - Chaîne - Numéro - Booléen
----------------------------------	---

5. Si vous avez sélectionné le type de commande de gestion VEU, indiquez les valeurs des zones conformément aux instructions du tableau suivant, puis cliquez sur **Envoyer**.

Préfixe d'ID de commande	Facultatif. Dans la liste déroulante, sélectionnez le préfixe de l'ID de commande. Le client EBICS alloue un ID de commande unique pour chaque commande en fonction de la banque, de l'ID utilisateur et du type de commande. Le client génère l'ID de commande conformément aux spécifications EBICS. L'ID de commande est un identifiant alphanumérique à 4 chiffres. Vous pouvez indiquer le premier caractère de l'ID de commande. Les deuxième, troisième et quatrième caractères de l'ID de commande sont des caractères alphanumériques dans l'ordre croissant (A-Z ou 0-9).
Moyen de sécurité	Obligatoire. Entrez un numéro de sécurité à 4 chiffres compris entre 0499 et 0100.
ID de produit	Entrez l'ID de produit pour l'application client EBICS.
Langue de produit	Entrez le paramètre linguistique de l'application client EBICS que vous utilisez. Par exemple, entrez EN si la langue est définie sur Anglais.
Types de commande VEU	Obligatoire. Sélectionnez le type de commande VEU approprié dans la liste des types de commande VEU.
ID de commande	Obligatoire. Indiquez l'ID de la commande pour lequel vous soumettez le type de commande HVE ou HVS.
PartnerID	Obligatoire. Indiquez l'ID du partenaire associé à l'utilisateur qui a soumis la commande pour lequel vous soumettez le type de commande HVE ou HVS.
Type de commande	Obligatoire. Sélectionnez le type de la commande pour laquelle vous soumettez le type de commande HVE ou HVS.
Résumé du message	<p>Facultatif. Sélectionnez cette option pour soumettre la valeur hachée des données de commande.</p> <p>Remarque : Pour demander la valeur hachée, appelez la banque ou envoyez un courrier. La banque envoie la valeur hachée des données de commande via un autre mode de communication, par exemple, par l'envoi d'un courrier électronique.</p>

PayloadMsgID	<p>Facultatif. Sélectionnez PayloadMsgID pour soumettre la charge complète à partir de votre boîte aux lettres. Effectuez les actions suivantes :</p> <ol style="list-style-type: none"> 1. Cliquez sur Sélectionner. 2. Sélectionnez la charge requise dans la liste. 3. Cliquez sur Terminer. <p>Remarque : Pour demander la charge, appelez la banque ou envoyez un courrier. La banque envoie la charge par courrier électronique à votre boîte aux lettres du client EBICS.</p>
--------------	--

6. Si vous avez sélectionné un autre type de commande, indiquez les valeurs des zones conformément aux instructions du tableau suivant, puis cliquez sur **Envoyer**.

Préfixe d'ID de commande	Facultatif. Dans la liste déroulante, sélectionnez le préfixe de l'ID de commande. Le client EBICS alloue un ID de commande unique pour chaque commande en fonction de la banque, de l'ID utilisateur et du type de commande. Le client génère l'ID de commande conformément aux spécifications EBICS. L'ID de commande est un identifiant alphanumérique à 4 chiffres. Vous pouvez indiquer le premier caractère de l'ID de commande. Les deuxième, troisième et quatrième caractères de l'ID de commande sont des caractères alphanumériques dans l'ordre croissant (A-Z ou 0-9).
Moyen de sécurité	Obligatoire. Entrez un numéro de sécurité à 4 chiffres compris entre 0499 et 0100.
ID de produit	Entrez l'ID de produit pour l'application client EBICS.
Langue de produit	Entrez le paramètre linguistique de l'application client EBICS que vous utilisez. Par exemple, entrez EN si la langue est définie sur Anglais.

Soumission d'une commande en tant qu'utilisateur technique

Un utilisateur technique est configuré sur la machine pour soumettre des commandes à la place d'un utilisateur du client EBICS non technique (utilisateur physique) à l'aide d'un système de fichiers d'arrière-plan. L'utilisateur technique est associé à un utilisateur non technique.

Pour soumettre une commande en tant qu'utilisateur technique, vous devez configurer :

- Un utilisateur en tant qu'abonné technique
- Un adaptateur de système de fichiers ou un adaptateur technique similaire

Le scénario illustre l'utilisation d'un adaptateur de système de fichiers configuré sous Sterling B2B Integrator.

Un utilisateur technique soumet les ordres en plaçant un fichier compressé qui contient un fichier XML, ordermetadata.xml et, en option, les données de charge, dans un dossier de collecte indiqué lors de la configuration d'un adaptateur de système de fichiers.

Le diagramme suivant illustre le flux de processus lorsqu'un utilisateur technique soumet des ordres. Le processus d'arrière-plan génère le fichier ordermetadata.xml, conditionne les métadonnées de charge dans un format compressé et place celles-ci

dans un répertoire pour qu'un adaptateur technique, tel que l'adaptateur de système de fichiers, puisse sélectionner le fichier et l'envoyer au client EBICS pour traiter les données. Les composants de l'Environnement d'exécution du client EBICS incluent la Boîte aux lettres d'utilisateur, le Processeur OrderPreProcessor, la Boîte aux lettres du client EBICS et l'Environnement d'exécution EBICS. Le Processeur OrderPreProcessor extrait le contenu du fichier compressé, puis transfère les métadonnées XML dans la Boîte aux lettres du client EBICS qui, à son tour, envoie les métadonnées à l'Environnement d'exécution EBICS pour traitement. Le Processeur OrderPreProcessor envoie les données de charge dans la boîte aux lettres de l'utilisateur du client EBICS. À partir des valeurs indiquées dans le fichier XML, le client EBICS envoie la demande de commande au serveur de la banque.

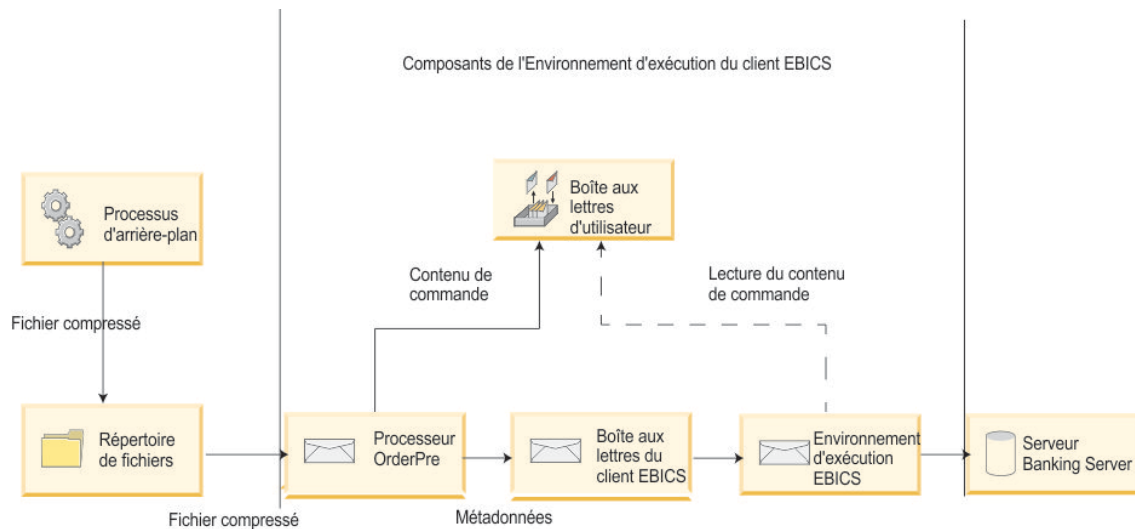


Figure 1. Flux de processus de la soumission de commande par un utilisateur technique

Si le type de commande est FUL, le fichier ordermetadata.xml contient les informations détaillées suivantes :

HostID

Informations détaillées sur la banque participant à l'opération

UserID

Utilisateur non technique qui souhaite soumettre la commande FUL

SystemID

Utilisateur technique qui est un délégué de l'utilisateur non technique

PartnerID

Informations détaillées sur le partenaire associé à l'utilisateur

OrderType

Informations détaillées sur le type de commande et le format de fichier

Attributs personnalisés

Dans Sterling B2B Integrator version 5.2.6.1_2 ou ultérieure, les utilisateurs peuvent ajouter des attributs personnalisés avant de soumettre une commande EBICS. Ces attributs sont enregistrés dans le fichier ordermetadata.xml, puis s'affichent dans l'interface utilisateur de la commande. Pour définir des attributs personnalisés, utilisez la balise <ebicsUserAttribute> du fichier ordermetadata.xml.

L'exemple suivant décrit de manière détaillée le format d'un fichier XML lorsque vous soumettez une commande FUL en tant qu'utilisateur technique.

```
<?xml version="1.0" encoding="UTF-8"?>
<orderMetaData xmlns:xsi='http://www.w3.org/2001/XMLSchema-instance'
xsi:nonNamespaceSchemaLocation='new_omd.xsd'>
<HostID>TESTBNKPK12</HostID>
<PartnerID>PARTNERPK12</PartnerID>
<UserID>USERPK12</UserID>
<SystemID>TECHUSER</SystemID>
<orderIdPrefix>D</orderIdPrefix>
<SecurityMedium>0200</SecurityMedium>
<OrderType>FUL</OrderType>
<FileFormat>pain.001.001.02.ict</FileFormat>
<autoSubmit>TRUE</autoSubmit>
<ebicsUserAttribute value="123456" name="totalamount"/>
<ebicsUserAttribute value="AAA" name="accountid"/>
</orderMetaData>
```

Si le type de commande est INI ou HIA, l'ID système et l'ID utilisateur ont la même valeur dans le fichier ordermetadata.xml.

L'exemple suivant illustre le format d'un fichier XML lorsque vous soumettez une commande INI en tant qu'utilisateur technique :

```
<?xml version="1.0" encoding="UTF-8"?>
<orderMetaData xmlns:xsi='http://www.w3.org/2001/XMLSchema-instance'
xsi:nonNamespaceSchemaLocation='new_omd.xsd'>
<HostID>TESTBNKPK12</HostID>
<PartnerID>PARTNERPK12</PartnerID>
<UserID>TECHUSER</UserID>
<SystemID>TECHUSER</SystemID>
<orderIdPrefix>W</orderIdPrefix>
<SecurityMedium>0200</SecurityMedium>
<OrderType>INI</OrderType>
</orderMetaData>
```

Si le nom de fichier du contenu contient des caractères non ASCII, l'utilitaire jar fourni avec le kit Java Development Kit installé conjointement avec Sterling B2B Integrator vous permet de créer un fichier compressé. Vous devez exécuter l'utilitaire jar à partir de l'invite de commande sous Windows ou du terminal sous UNIX en indiquant les paramètres suivants : `jar cFM <nom_fichier_zip> ordermetadata.xml <nom_fichier_contenu contenant des caractères non ASCII>`.

Remarque : Le répertoire de base de Java doit être défini sur l'emplacement du kit JDK.

Si le nom de fichier du contenu ne contient que des caractères ASCII, l'utilitaire jar ou toute autre application, par exemple WinZip ou WinRAR, peut être utilisé pour créer un fichier compressé.

Configurer un utilisateur technique

Pourquoi et quand exécuter cette tâche

Vous devez configurer un utilisateur non technique avant de configurer un utilisateur technique pour associer un utilisateur technique à un utilisateur non technique. Pour configurer un utilisateur non technique, procédez comme suit :

Procédure

1. Connectez-vous au client EBICS de Sterling B2B Integrator.
2. Dans le menu **Gestion de profil**, sélectionnez **Utilisateur**.

3. Sur la page Configuration de l'utilisateur, en regard de **Configurer l'utilisateur existant en tant qu'utilisateur EBICS**, cliquez sur **OK**.
4. Sur la page Configuration de l'utilisateur, indiquez les valeurs des zones conformément aux instructions du tableau ci-après, puis cliquez sur **Suivant** :

Zone	Description
ID utilisateur	Obligatoire. Identifiant unique de l'utilisateur dans le système de la banque, qui correspond à l'utilisateur créé dans le tableau de bord du client EBICS. Dans la liste déroulante ID utilisateur , sélectionnez l'ID utilisateur.
Type d'utilisateur	Obligatoire. Dans la liste déroulante Type d'utilisateur , sélectionnez le rôle de l'utilisateur Utilisateur du client EBICS.
Fuseau horaire	Facultatif. Indiquez le fuseau horaire de l'utilisateur.
Utilisateur technique	Cochez cette case pour configurer un utilisateur technique. Un utilisateur technique est un système de fichiers configuré pour soumettre des commandes.
Type de certificat	Obligatoire si vous avez sélectionné le type d'utilisateur Utilisateur du client EBICS. Sélectionnez X509 si vous utilisez le certificat de clé publique X.509 pour autoriser les certificats. Sélectionnez Clés si vous utilisez des clés RSA pour autoriser les certificats. Remarque : Le client EBICS prend en charge les clés non chiffrées uniquement.

5. Si vous avez sélectionné le type de certificat X509, indiquez les valeurs des zones conformément aux instructions du tableau ci-après sur la page Informations techniques, puis cliquez sur **Suivant** :

Zone	Description
Certificat privé d'authentification	Obligatoire. Sélectionnez la clé privée que le client EBICS utilise pour créer une signature numérique pour l'utilisateur dans la demande envoyée à la banque. La banque doit posséder la partie publique de la clé pour valider l'autorisation. La liste déroulante contient les certificats configurés dans le magasin de certificats de système Sterling B2B Integrator.
Certificat public d'authentification	Obligatoire. Sélectionnez la clé publique que l'utilisateur fournit à la banque pour valider l'autorisation de l'utilisateur dans la demande du client EBICS. Le partenaire commercial ou l'utilisateur partage la clé avec la banque. La clé doit être une partie publique du certificat de système Sterling B2B Integrator sélectionné comme certificat privé d'authentification.
Version de clé d'authentification	La version de la clé du certificat d'authentification s'affiche. La valeur X002 est admise.

Zone	Description
Certificat privé de chiffrement	Obligatoire. Sélectionnez la clé privée que le client EBICS utilise pour déchiffrer la réponse reçue du serveur EBICS Banking Server. La liste déroulante contient les certificats configurés dans le magasin de certificats de système Sterling B2B Integrator.
Certificat public de chiffrement	Obligatoire. Sélectionnez la partie publique du certificat de système Sterling B2B Integrator sélectionné comme certificat privé de chiffrement. Le partenaire commercial ou l'utilisateur partage la clé avec la banque.
Version de clé de chiffrement	La version de la clé du certificat de chiffrement s'affiche. La valeur E002 est admise.
Utiliser le magasin de clés matérielles pour la signature électronique	Facultatif. Sélectionnez cette option si vous disposez d'un jeton de clé 3S activé.
Type de clé matérielle	Clé 3S s'affiche en tant que type de clé matérielle. Cette clé est une clé de signature sécurisée SWIFT utilisée pour l'identité numérique. Vous devez activer le jeton de clé 3S et enregistrer la clé auprès de la banque pour pouvoir signer et envoyer des messages à la banque.
Clé privée de signature électronique	Facultatif. Sélectionnez la clé privée du certificat de signature électronique (ES) si vous n'utilisez pas de clé matérielle pour la signature électronique.
Clé publique de signature électronique	Obligatoire. Sélectionnez la clé publique du certificat de signature électronique (ES) utilisé pour vérifier la signature des données de commande. La valeur de la clé publique d'un certificat de signature électronique ne doit pas être identique à celle d'un certificat d'authentification ou de chiffrement.
Version de clé de signature électronique	Obligatoire si vous n'utilisez pas de magasin de clés matérielles pour la signature électronique. Sélectionnez la version de la clé du certificat de signature électronique. Les valeurs valides sont A005 et A006. Si vous utilisez un magasin de clés matérielles pour la signature électronique, la version de la clé est définie sur A005 et ne peut pas être modifiée.

6. Si vous avez sélectionné le type de certificat Clés, indiquez les valeurs des zones conformément aux instructions du tableau ci-après sur la page Informations techniques, puis cliquez sur **Suivant** :

Zone	Description
Clé privée d'authentification	Obligatoire. Cliquez sur Parcourir pour sélectionner le fichier contenant la partie privée de la clé d'authentification dans votre ordinateur.

Zone	Description
Clé publique d'authentification	Obligatoire. Cliquez sur Parcourir pour sélectionner le fichier contenant la partie publique de la clé d'authentification dans votre ordinateur.
Version de clé d'authentification	Obligatoire. Sélectionnez la version de la clé du certificat d'authentification. La valeur X002 est admise.
Clé privée de chiffrement	Obligatoire. Cliquez sur Parcourir pour sélectionner le fichier contenant la partie privée de la clé de chiffrement dans votre ordinateur.
Clé publique de chiffrement	Obligatoire. Cliquez sur Parcourir pour sélectionner le fichier contenant la partie publique de la clé de chiffrement dans votre ordinateur.
Version de clé de chiffrement	Obligatoire. Sélectionnez la version de la clé du certificat de chiffrement. La valeur E002 est admise.
Clé privée de signature électronique	Obligatoire. Cliquez sur Parcourir pour sélectionner le fichier contenant la partie privée de la clé de signature électronique dans votre ordinateur.
Clé publique de signature électronique	Obligatoire. Cliquez sur Parcourir pour sélectionner le fichier contenant la partie publique de la clé de signature électronique dans votre ordinateur.
Version de clé de signature électronique	Obligatoire. Sélectionnez la version de la clé du certificat de signature électronique. Les valeurs valides sont A005 et A006.

7. Cette étape est applicable uniquement si vous avez choisi d'ajouter un nouveau partenaire ou de modifier un partenaire existant pour un utilisateur non technique ou physique. Sur la page Partenaires associés : Paramètres utilisateur, indiquez les valeurs des zones conformément aux instructions du tableau ci-après, puis cliquez sur **Ajouter un partenaire**.

Zone	Description
Nom du partenaire	Obligatoire. Dans la liste déroulante Nom du partenaire , sélectionnez le partenaire auquel un utilisateur est associé. Un utilisateur peut être associé à plusieurs partenaires. Remarque : Utilisez le tableau de bord Sterling B2B Integrator pour créer des entités de partenaire commercial.

Zone	Description
Chemin d'accès à la boîte d'envoi par téléchargement	<p>Obligatoire. Configurez la boîte aux lettres de téléchargement et affectez des utilisateurs pour faire fonctionner la boîte aux lettres dans Sterling B2B Integrator. Indiquez le chemin de la boîte aux lettres pour les messages téléchargés. Vous devez affecter un chemin de boîte aux lettres pour stocker les messages décompressés d'une demande EBICS.</p> <p>Si la boîte aux lettres (ID utilisateur, Nom du partenaire, Boîte de réception) existe déjà dans Sterling B2B Integrator et si vous laissez cette zone vide, un message d'erreur vous invite à indiquer le chemin d'accès par défaut à la boîte aux lettres.</p> <p>Remarque : Assurez-vous que le chemin de boîte aux lettres commence par une barre oblique (/).</p>
Chemin d'accès à la boîte de réception par téléchargement	<p>Obligatoire. Configurez la boîte aux lettres de téléchargement et affectez des utilisateurs pour faire fonctionner la boîte aux lettres dans Sterling B2B Integrator. Indiquez le chemin de la boîte aux lettres pour les messages téléchargés. Vous devez affecter un chemin de boîte aux lettres pour stocker les messages qui sont compressés dans une réponse EBICS.</p> <p>Si la boîte aux lettres (ID utilisateur, Nom du partenaire, Boîte d'envoi) existe déjà dans Sterling B2B Integrator et si vous laissez cette zone vide, un message d'erreur vous invite à indiquer le chemin d'accès par défaut à la boîte aux lettres.</p> <p>Remarque : Assurez-vous que le chemin de boîte aux lettres commence par une barre oblique (/).</p>

8. Sur la page Partenaires associés, effectuez l'une des actions suivantes, puis cliquez sur **Suivant**.
 - Cliquez sur l'icône d'ajout pour associer un nouveau partenaire à l'utilisateur technique.
 - Cliquez sur l'icône de mise à jour en regard du partenaire que vous souhaitez modifier.
 - Cliquez sur l'icône de suppression pour dissocier un partenaire de l'utilisateur technique.
9. Un utilisateur non technique délègue un utilisateur technique pour exécuter les transactions. Sur la page Partenaires associés : Paramètres utilisateur, indiquez les valeurs des zones conformément aux instructions du tableau ci-après, puis cliquez sur **Ajouter un partenaire**.

Zone	Description
Nom du partenaire	Obligatoire. Dans la liste déroulante Nom du partenaire , sélectionnez le partenaire auquel un utilisateur est associé. Un utilisateur peut être associé à plusieurs partenaires. Un utilisateur technique et un utilisateur non technique doivent appartenir au même partenaire. L'utilisateur technique hérite tous les droits de l'utilisateur non technique associé. Remarque : Utilisez le tableau de bord Sterling B2B Integrator pour créer des entités de partenaire commercial.
Délégué de	Obligatoire. Sélectionnez l'utilisateur qui déléguera ses tâches à l'utilisateur technique.

10. Sur la page Partenaires associés, cliquez sur **Suivant**.
11. Sur la page Confirmer, vérifiez les paramètres de configuration de l'utilisateur, puis cliquez sur **Terminer**. Vous pouvez également cliquer sur le lien **Afficher tout** en regard de **Partenaires associés** pour afficher les informations suivantes :
 - La liste des partenaires associés à l'utilisateur.
 - Les détails de configuration correspondants, tels que le chemin d'accès de la boîte d'envoi ou de réception par téléchargement pour un utilisateur non technique.
 - L'utilisateur technique qui est un délégué de l'utilisateur non technique.

Afficheurs

La rubrique suivante décrit comment vous pouvez afficher et rechercher des (transactions), des ordres de recherche et l'exécution de vos tâches en attente.

Remarque : Dans l'application client EBICS, l'heure de transaction des événements et des commandes est stockée au format GMT. Par exemple, si l'utilisateur du client EBICS est hébergé dans le fuseau horaire Central (GMT+1) et qu'une commande est soumise le 3 février 2011 à 9:00 (GMT), indiquez "3 février 2011, 10:00" comme date et heure de début dans l'écran Recherche de commande pour rechercher la commande.

Recherche d'événements

À l'aide de l'observateur d'événements, un utilisateur peut rechercher des événements ou des transactions et obtenir des détails récapitulatifs d'événement par le biais des options de la recherche simple et avancée.

Pourquoi et quand exécuter cette tâche

Vous pouvez effectuer une recherche simple ou une recherche avancée, dans laquelle vous pouvez utiliser plusieurs paramètres pour affiner votre recherche. En fonction des besoins de votre recherche, vous pouvez :

- Indiquer si vous souhaitez rechercher les enregistrements d'événements dans les tables actives ou dans les tables historiques (archivées).
- Sélectionner des plages de dates et d'heures.
- Indiquer des paramètres supplémentaires pour affiner les résultats de la recherche.

La procédure suivante vous permet de rechercher les enregistrements d'événements et d'obtenir un récapitulatif de l'événement qui répond à vos critères de recherche :

Procédure

1. Connectez-vous au client EBICS de Sterling B2B Integrator.
2. Dans le menu **Afficheurs**, sélectionnez **Afficheur d'événements**.
3. Renseignez les informations relatives à la recherche d'événements dans le tableau suivant :

Zone	Description
Emplacement de la recherche	Obligatoire. Sélectionnez l'emplacement de recherche approprié. Les options sont les suivantes : <ul style="list-style-type: none"> • Tables actives : cette option est sélectionnée par défaut. Lorsque cette option est sélectionnée, les événements sont recherchés dans la base de données des tables actives (en cours). • Tables restaurées : lorsque cette option est sélectionnée, les événements sont recherchés dans la base de données de restauration.
Date de début	Obligatoire. La date en cours par défaut est renseignée dans cette zone en fonction du fuseau horaire indiqué lors de la configuration de l'utilisateur. Cliquez sur la zone Date de début pour afficher le calendrier et sélectionnez la date de début dans le calendrier.
Date de fin	Obligatoire. La date en cours par défaut est renseignée dans cette zone en fonction du fuseau horaire indiqué lors de la configuration de l'utilisateur. Cliquez sur la zone Date de fin pour afficher le calendrier et sélectionnez la date de fin dans le calendrier.
Type d'événement	Facultatif. Sélectionnez un type d'événement approprié dans la liste déroulante. Les types d'événement disponibles sont : <ul style="list-style-type: none"> • Tout (par défaut) • Info • Avertissement • Erreur • Critique
ID utilisateur	Facultatif. Dans la liste déroulante, sélectionnez l'ID de l'utilisateur du client EBICS qui a passé la commande associée à l'événement que vous recherchez. Cette option n'est pas disponible pour un utilisateur qui dispose du rôle et des droits Utilisateur du client EBICS.
Heure de début	Obligatoire. L'heure système par défaut s'affiche dans la zone en fonction du fuseau horaire spécifié lors de la configuration de l'utilisateur. Cliquez sur la zone Heure de début pour sélectionner l'heure de début.
Heure de fin	Obligatoire. L'heure système par défaut s'affiche dans la zone en fonction du fuseau horaire spécifié lors de la configuration de l'utilisateur. Cliquez sur la zone Heure de fin pour sélectionner l'heure de fin.

Zone	Description
Trier par	Facultatif. Vous pouvez trier les résultats de la recherche en fonction des options suivantes : <ul style="list-style-type: none"> • Date-heure (par défaut) • Type d'événement • Code d'événement • Type de commande • ID de commande Vous pouvez également trier les résultats de la recherche par ordre croissant ou décroissant. Sélectionnez l'option ASC ou DESC dans la liste déroulante. DESC est l'option par défaut.
Fréquence de rafraîchissement	Facultatif. À l'aide des flèches vers le haut ou vers le bas, indiquez la fréquence à laquelle vous souhaitez que les résultats de la recherche soient actualisés.
Icône Actualiser	Facultatif. Par défaut, l'actualisation des résultats de la recherche est désactivée (Off). Cliquez sur cette icône pour activer l'actualisation des résultats de la recherche (On).

4. Cliquez sur **Rechercher**. Le récapitulatif des événements s'affiche dans un format tabulaire, comme suit :

Zone	Description
Code d'événement	Cliquez sur le lien du code d'événement pour afficher les détails de l'événement.
Type d'événement	Le type d'événement généré s'affiche. Les types d'événement disponibles sont : <ul style="list-style-type: none"> • Tout • Info • Avertissement • Erreur • Critique
Nom de l'événement	Le nom de l'événement s'affiche.
Horodatage	La date et l'heure auxquelles l'événement a été généré s'affichent.
Type de commande	Le type de commande pour lequel l'événement a été généré s'affiche.
ID séq. de commande	L'ID de séquence de la commande pour lequel l'événement a été généré s'affiche. Cliquez sur ce lien pour afficher les détails de la commande. Remarque : Un administrateur et un opérateur du client EBICS ne peuvent pas afficher le lien du document de commande dans la page Détails de la commande. Le lien du document s'affiche uniquement pour un utilisateur du client EBICS.
ID de commande	L'ID de la commande pour lequel l'événement a été généré s'affiche. Cliquez sur le lien de l'ID de commande pour afficher les détails de la commande. Remarque : Un administrateur et un opérateur du client EBICS ne peuvent pas afficher le lien du document de commande dans la page Détails de la commande. Le lien du document s'affiche uniquement pour un utilisateur du client EBICS.

Zone	Description
ID utilisateur	Lorsqu'un administrateur du client EBICS lance une recherche d'événement, l'ID de l'utilisateur du client EBICS chargé du déclenchement de l'événement (soumission d'une commande, modification de la configuration de la commande, etc.) s'affiche. Lorsqu'un utilisateur du client EBICS lance une recherche d'événement, l'ID de l'utilisateur qui a lancé la recherche s'affiche.

5. Cliquez sur **Réinitialiser** pour effacer les paramètres de recherche d'événements. Réinitialisation des paramètres de recherche ne pas effacer les résultats de la recherche précédente.

Recherche de commandes

Le client EBICS Sterling B2B Integrator vous permet de rechercher des commandes et d'en obtenir un récapitulatif à l'aide des options de recherche simple et avancée.

Pourquoi et quand exécuter cette tâche

Vous pouvez effectuer une recherche simple ou une recherche avancée, dans laquelle vous pouvez utiliser plusieurs paramètres pour affiner votre recherche. En fonction de vos besoins de recherche, vous pouvez :

- Indiquer si vous souhaitez rechercher les enregistrements de commandes dans les tables actives ou dans les tables restaurées (archivées).
- Sélectionner des plages de dates et d'heures.
- Indiquer des paramètres supplémentaires pour affiner les résultats de la recherche.

Pour rechercher les enregistrements de commandes et obtenir un récapitulatif des commandes qui répond à vos critères de recherche, procédez comme suit :

Procédure

1. Connectez-vous au client EBICS de Sterling B2B Integrator.
2. Dans le menu **Afficheurs**, sélectionnez **Recherche de commande**.
3. Entrez vos critères de recherche en vous référant au tableau suivant :

Tableau 4. Recherche de commandes

Zone	Description
Emplacement de la recherche	Obligatoire. Sélectionnez l'emplacement de recherche approprié. Les options sont les suivantes : <ul style="list-style-type: none"> • Tables actives : cette option est sélectionnée par défaut. Lorsque cette option est sélectionnée, les commandes sont recherchées dans la base de données des tables actives (en cours). • Tables restaurées : lorsque cette option est sélectionnée, les commandes sont recherchées dans la base de données de restauration.
Date de début	Obligatoire. La date en cours par défaut est renseignée dans cette zone en fonction du fuseau horaire indiqué lors de la configuration de l'utilisateur. Cliquez sur la zone Date de début pour afficher le calendrier et sélectionnez la date de début dans le calendrier.
Date de fin	Obligatoire. La date en cours par défaut est renseignée dans cette zone en fonction du fuseau horaire indiqué lors de la configuration de l'utilisateur. Cliquez sur la zone Date de fin pour afficher le calendrier et sélectionnez la date de fin dans le calendrier.

Tableau 4. Recherche de commandes (suite)

Zone	Description
ID de banque (ID hôte)	Facultatif. Sélectionnez l'ID de banque requis.
ID de commande	Facultatif. Entrez l'ID de la commande dans la zone ID de commande .
Type de commande	Facultatif. Sélectionnez un type de commande approprié dans la liste déroulante Type de commande .
Statut	Facultatif. Sélectionnez le statut approprié de la commande dans la liste déroulante Statut : <ul style="list-style-type: none"> • Tout (par défaut) • Tout complet • Tout incomplet • Succès • Échec • En cours • En attente sur le client • En attente sur le serveur
ID utilisateur	Facultatif. Dans la liste déroulante, sélectionnez l'ID de l'utilisateur du client EBICS qui a passé la commande que vous recherchez. Cette option n'est pas disponible pour un utilisateur du client EBICS.
Type de droit	Facultatif. Sélectionnez le type de droit approprié. Les options sont les suivantes : <ul style="list-style-type: none"> • Émetteur : cette option est sélectionnée par défaut. Les commandes sont recherchées en fonction de l'émetteur de la commande. • Signataire : sélectionnez cette option pour rechercher les commandes en fonction du signataire de la commande. Cliquez sur le lien de l'ID de commande pour afficher les détails de la commande. Les onglets Événements de commande, Activités et Signatures en attente ne s'affichent pas lorsque les commandes sont recherchées par signataire.
Heure de début	Obligatoire. L'heure système par défaut s'affiche dans la zone en fonction du fuseau horaire spécifié lors de la configuration de l'utilisateur. Cliquez sur la zone Heure de début pour sélectionner l'heure de début.
Heure de fin	Obligatoire. L'heure système par défaut s'affiche dans la zone en fonction du fuseau horaire spécifié lors de la configuration de l'utilisateur. Cliquez sur la zone Heure de fin pour sélectionner l'heure de fin.
Nom du partenaire	Facultatif. Sélectionnez le nom de partenaire requis.
ID séq. de commande	Facultatif. Entrez l'ID de séquence de commande dans la zone ID séq. de commande .
Format de fichier	Facultatif. Sélectionnez un format de fichier approprié dans la liste déroulante Format de fichier .
Statut d'accusé de réception FUL	Facultatif. Entrez le statut d'accusé de réception FUL dans la zone Statut d'accusé de réception FUL .

Tableau 4. Recherche de commandes (suite)

Zone	Description
Trier par	<p>Facultatif. Vous pouvez trier les résultats de la recherche en fonction de l'une des options suivantes :</p> <ul style="list-style-type: none"> • Date-heure (par défaut) • Date-heure de la dernière activité • ID de commande • Type de commande • Nom du partenaire • ID de banque (ID hôte) • ID utilisateur <p>Vous pouvez également trier les résultats de la recherche par ordre croissant ou décroissant. Sélectionnez l'option ASC ou DESC dans la liste déroulante. DESC est l'option par défaut.</p>
Fréquence de rafraîchissement	<p>Facultatif. À l'aide des flèches vers le haut ou vers le bas, indiquez la fréquence à laquelle vous souhaitez que les résultats de la recherche soient actualisés.</p>
Icône Actualiser	<p>Facultatif. Par défaut, l'actualisation des résultats de la recherche est désactivée (Off). Cliquez sur cette icône pour activer l'actualisation des résultats de la recherche (On).</p>

4. Cliquez sur **Rechercher**. Le récapitulatif de la commande affiche les informations suivantes dans un format tabulaire :

Tableau 5. Zones d'informations sur la commande

Zone	Description
<p>ID séq. de commande</p> <p>ID de commande</p>	<p>Cliquez sur le lien ID de commande ou ID séq. de commande pour afficher les détails de la commande. La page des détails du récapitulatif de commande est divisée en deux sections : Données de commande et Détails de commande. La section Données de commande fournit les informations suivantes sur la commande sélectionnée :</p> <ul style="list-style-type: none"> • ID séq. de commande • Type de commande • Format de fichier • Nombre de signatures (signatures requises pour soumettre la commande) • Date et heure de début • Date et heure de la dernière activité • ID de commande • Nom du partenaire • ID utilisateur • ID de banque (ID hôte) • Statut de la commande • Date et heure de fin • ID flux de travail • Document (charge de commande). Le lien de document de commande s'affiche uniquement pour l'utilisateur du client EBICS. Cliquez sur le lien pour afficher les données utiles (pour télécharger des interventions techniques) ou la demande de commande XML (pour d'autres types de commande). <p>La section Détails de commande contient trois onglets :</p> <p>Événements de commande Fournit des informations sur les événements liés à une commande, par exemple les données compressées, les données codées et le groupage EBICS réussi.</p> <p>Activités Fournit des informations sur les activités liées à une commande, par exemple En attente de signature chez le client et Action de soumission par l'émetteur. Les activités peuvent se trouver dans l'un des états suivants :</p> <ul style="list-style-type: none"> • En cours • Terminé • Échec <p>Les activités ne sont pas générées pour les types de commande INI, HIA et HPB.</p> <p>Tâches en attente Répertorie les utilisateurs dont les signatures sont en attente pour la commande sélectionnée.</p> <p>États HAC Indique le statut et les détails de traitement de toutes les commandes soumises.</p>
ID utilisateur	L'ID utilisateur de l'utilisateur du client EBICS qui a soumis la commande.
Nom du partenaire	Le nom du partenaire auquel un utilisateur est associé s'affiche.

Tableau 5. Zones d'informations sur la commande (suite)

Zone	Description
ID de banque (ID hôte)	ID de banque ou ID hôte de la banque à laquelle l'utilisateur du client EBICS a soumis la commande. Il s'agit d'un identifiant unique pour la banque dans le système de la banque.
Type de commande	Le type de commande s'affiche.
Statut	Le statut de la commande s'affiche. Par exemple : Succès, Échec, En cours et En attente sur le client.
Statut d'accusé de réception FUL	Le statut d'accusé de réception FUL de la commande s'affiche.
Action HAC	L'action HAC s'affiche. Pour obtenir des informations, voir «Traitement HAC», à la page 129.
Raison HAC	Le code Raison HAC s'affiche. Pour obtenir des informations, voir «Traitement HAC», à la page 129.
Date-heure de début	La date et l'heure de début s'affichent.
Date-heure de fin	La date et l'heure de fin s'affichent.

5. Cliquez sur **Réinitialiser** pour effacer les paramètres de recherche de commandes. Réinitialisation des paramètres de recherche ne pas effacer les résultats de la recherche précédente.

Tâches en attente

En fonction des paramètres de configuration définis dans une offre, plusieurs signataires peuvent avoir à signer la commande pour traiter les données qu'elle contient. Si une commande est soumise pour être traitée sans toutes les signatures requises, le client EBICS ne la traitera pas. Les notifications de signature en attente sont envoyées aux boîtes aux lettres des signataires concernés pour leur demander de signer la commande. Si la commande est en attente de signature, le signataire voit le lien **Signer**. Si toutes les signatures requises ont été obtenues et que la commande est prête à être soumise, l'émetteur voit le lien **Soumettre**.

La page Tâches en attente est la page d'accueil pour les utilisateurs du client EBICS de Sterling B2B Integrator. Cette page vous permet d'afficher et de signer ou de soumettre des commandes en attente. Pour signer ou soumettre une commande en attente, procédez comme suit :

1. Connectez-vous au client EBICS de Sterling B2B Integrator.
2. Dans le menu **Afficheurs**, sélectionnez **Tâches en attente**. Les tâches en attente s'affichent dans un format tabulaire.

Noms de colonne	Description
ID de commande	Affiche l'ID de la commande. Cliquez sur l'ID de la commande pour afficher le récapitulatif de la commande et signer la commande. Cliquez sur le lien du document de commande dans la page des détails de la commande pour consulter la charge.
ID émetteur	Affiche l'ID de l'émetteur.

Noms de colonne	Description
ID de banque (ID hôte)	Affiche l'ID de la banque.
Type de commande	Affiche le type de la commande.
Date-heure	Affiche l'horodatage dans un format date et heure.
Statut	Affiche le statut de la commande. Par exemple, Succès, En attente sur le serveur, En attente sur le client, etc. En fonction de l'action requise, les liens Signer ou Soumettre s'affichent en regard du statut.

- Pour signer une commande en attente, cliquez sur **Signer**. Pour la soumettre, cliquez sur **Soumettre**.
- Si la clé de sécurité matérielle pour la signature électronique est configurée pour un utilisateur EBICS Client, alors la page Signatures électroniques s'affiche lorsque vous cliquez sur **Signer**. Entrez les valeurs des zones répertoriées dans le tableau suivant, puis cliquez sur **Signer** :

Zone	Description
Nom du fournisseur	Le nom du fournisseur du module de signature matérielle (HSM) s'affiche.
Sélectionner le fichier DLL	Cliquez sur Parcourir , accédez à l'emplacement approprié et sélectionnez le fichier DLL du module HSM.
Sélectionner le fournisseur PKCS11	Cliquez sur Charger les fournisseurs , accédez à l'emplacement approprié et sélectionnez le fichier du fournisseur de services PKCS11. Une fois les fichiers fournisseur chargés, sélectionnez le fichier approprié dans la liste déroulante.
Entrer le code confidentiel	Spécifiez le code de sécurité dans la zone Entrer le code confidentiel .
Sélectionner la clé privée	Cliquez sur Charger les clés , accédez à l'emplacement approprié et sélectionnez les clés. Une fois les clés chargées, sélectionnez la clé appropriée dans la liste déroulante.

Rechercher des tâches VEU en attente

La signature électronique distribuée (VEU) vous permet de transmettre des données à distance à plusieurs abonnés. Plusieurs abonnés peuvent autoriser des commandes à distance, indépendamment de l'heure et de l'espace.

Avant de commencer

Pour rechercher les tâches VEU en attente, un utilisateur du client EBICS doit soumettre un type de commande HVU (télécharger la présentation VEU) ou HVZ (télécharger la présentation VEU avec des informations supplémentaires, par exemple la valeur hachée).

Pourquoi et quand exécuter cette tâche

Procédez comme suit pour rechercher les tâches VEU en attente :

Procédure

1. Connectez-vous au client EBICS de Sterling B2B Integrator.
2. À partir du menu **Utilisateur**, sélectionnez **Afficheurs > Tâches VEU en attente**.
3. Dans la page Tâches VEU en attente, indiquez les valeurs des zones répertoriées dans le tableau suivant, puis cliquez sur **Rechercher**.

Zone	Description
Nom du partenaire	Obligatoire. Sélectionnez un nom de partenaire dans la liste déroulante.
ID de banque (ID hôte)	Obligatoire. Sélectionnez un ID de banque associé au partenaire dans la liste déroulante.
URL de la banque	Obligatoire. Sélectionnez l'adresse URL requise dans la liste déroulante. L'adresse URL sélectionnée est utilisée pour établir une session HTTP ou HTTPS avec le serveur EBICS Banking Server.

Une demande est envoyée à la banque afin de récupérer les détails des commandes VEU en attente.

4. Cliquez sur **Recherche avancée** pour spécifier des critères de recherche supplémentaires pour les commandes de gestion VEU dans la page Soumission de commande.
5. Si la réponse de la banque tarde à venir, cliquez sur **Annuler**.
6. Cliquez sur **Réinitialiser** pour entrer à nouveau les critères de recherche.

Afficher les tâches VEU en attente

Pourquoi et quand exécuter cette tâche

Procédez comme suit pour afficher les tâches VEU en attente :

Procédure

1. Connectez-vous au client EBICS de Sterling B2B Integrator.
2. À partir du menu **Utilisateur**, sélectionnez **Afficheurs > Tâches VEU en attente**.
3. Dans la page Tâches VEU en attente, indiquez les valeurs des zones répertoriées dans le tableau suivant, puis cliquez sur **Rechercher**.

Zone	Description
Nom du partenaire	Obligatoire. Sélectionnez un nom de partenaire dans la liste déroulante.
ID de banque (ID hôte)	Obligatoire. Sélectionnez un ID de banque associé au partenaire dans la liste déroulante.

Zone	Description
URL de la banque	Obligatoire. Sélectionnez l'adresse URL requise dans la liste déroulante. L'adresse URL sélectionnée est utilisée pour établir une session HTTP ou HTTPS avec le serveur EBICS Banking Server.

Une demande est envoyée à la banque afin de récupérer les détails des commandes VEU en attente.

4. Dans la section Résultats de la recherche de la page Tâches VEU en attente, vous pouvez afficher les informations suivantes dans les résultats de la recherche :

Zone	Description
Type de commande	Type de la commande VEU en attente. Par exemple, FUL.
ID de commande	ID de la commande VEU en attente. Cliquez sur le lien ID de commande pour afficher des informations sur les données de commande.
Taille des données de commande	Taille des données de commande non compressées en kilooctets.
Signatures requises	Nombre total de signatures électroniques requis pour l'activation dans le serveur.
Signatures effectuées	Nombre de signatures déjà fournies pour la validation de la commande.
Statut	Le statut de la commande s'affiche. Les valeurs admises sont En attente et Terminé. Par exemple, si un utilisateur a signé une commande mais qu'elle nécessite des signatures supplémentaires pour valider la commande, le statut de la commande est En attente dans le magasin VEU. L'utilisateur qui a déjà signé la commande ne peut ni signer ni annuler la commande au statut En attente. Toutefois, cet utilisateur peut soumettre des types de commande HVT ou HVD.
Date-heure	L'horodatage s'affiche dans un format date et heure.

Extraction des détails d'une commande VEU en attente

Pourquoi et quand exécuter cette tâche

Procédez comme suit pour extraire les détails d'une commande VEU en attente :

Procédure

1. Connectez-vous au client EBICS de Sterling B2B Integrator.
2. À partir du menu **Utilisateur**, sélectionnez **Afficheurs > Tâches VEU en attente**.
3. Dans la page Tâches VEU en attente, indiquez les valeurs des zones répertoriées dans le tableau suivant, puis cliquez sur **Rechercher**.

Zone	Description
Nom du partenaire	Obligatoire. Sélectionnez un nom de partenaire dans la liste déroulante.
ID de banque (ID hôte)	Obligatoire. Sélectionnez un ID de banque associé au partenaire dans la liste déroulante.
URL de la banque	Obligatoire. Sélectionnez l'adresse URL requise dans la liste déroulante. L'adresse URL sélectionnée est utilisée pour établir une session HTTP ou HTTPS avec le serveur EBICS Banking Server.

Une demande est envoyée à la banque afin de récupérer les détails des commandes VEU en attente.

4. Dans la section Résultats de la recherche de la page Tâches VEU en attente, cliquez sur le lien ID de commande. Les détails des données de commande s'affichent.

Zone	Description
ID de commande	ID de la commande VEU en attente. Cliquez sur le lien ID de commande pour afficher des informations sur les données de commande.
Type de commande	Type de la commande VEU en attente. Par exemple, FUL.
ID partenaire de l'émetteur	ID du partenaire associé à l'utilisateur qui a soumis le type de commande d'envoi par téléchargement.
ID utilisateur de l'émetteur	ID abonné de l'utilisateur qui a soumis le type de commande de réception par téléchargement.
Données de commande disponibles	Après avoir soumis un type de commande HVZ, indiquez si les données de commande peuvent être téléchargées dans le format d'origine.
Détails de commande disponibles	Informations sur la commande pour le type de commande HVU.
Taille des données de commande	Taille des données de commande non compressées en kilooctets.
Date-heure	L'horodatage s'affiche dans un format date et heure.
Prêt pour la signature	Indique si la commande est déjà signée par l'utilisateur. Faux indique que la commande est déjà signée par l'utilisateur. Vrai indique que la commande est prête à être signée par l'utilisateur.
Signatures requises	Affiche le nombre minimum de signatures requises pour autoriser la commande.

Zone	Description
Signatures effectuées	<p>Nombre de signatures qui ont clôturé la validation de la commande. Indique le nombre de signatures électroniques déjà fournies, ainsi que les informations sur les signataires précédents. Cliquez sur le lien Informations du signataire pour visualiser les détails du signataire :</p> <ul style="list-style-type: none"> • Nom du partenaire : nom du partenaire commercial • ID utilisateur • Nom : nom du signataire • Horodatage • Niveau d'autorisation : niveau d'autorisation du signataire
Lien Informations sur la commande	<p>Cliquez sur le lien Informations sur la commande pour visualiser les détails de la commande :</p> <ul style="list-style-type: none"> • Compte : cliquez sur le lien Informations sur le compte pour afficher le nom du détenteur du compte, le code de devise, la description du compte, le rôle du détenteur du compte, le numéro de compte et le code de la banque. • Montant : affichez le montant de la transaction de commande. • Code de devise : affichez le code de devise de la transaction de commande. • Débit • Date d'exécution : affichez la date de l'exécution de la commande. • Description : cliquez sur le lien Description pour afficher la description et le type de description du signataire.

5. Dans la fenêtre Données de commande, sélectionnez l'une des options suivantes pour extraire les détails d'une commande VEU en attente :
 - À partir de la liste déroulante **Soumettre**, sélectionnez HVT - détails de la commande pour extraire les détails de transaction des données de commande
 - À partir de la liste déroulante **Soumettre**, sélectionnez HVT – données de commande complètes pour extraire les données de commande complètes
 - À partir de la liste déroulante **Soumettre**, sélectionnez HVD pour extraire l'état d'une commande actuellement en cours de traitement VEU et pour laquelle l'abonné est autorisé en tant que signataire. L'abonné reçoit des informations sur la commande avec une note complémentaire électronique (DisplayFile), la valeur hachée de la commande (DataDigest) et les signataires précédents (SignerInfo).
6. Dans la fenêtre Détails de la commande VEU, indiquez les valeurs des paramètres suivants :

Zone	Description
Préfixe d'ID de commande	Sélectionnez une lettre de l'alphabet dans la liste déroulante.

Zone	Description
Moyen de sécurité	Moyen de sécurité pour la clé technique bancaire de l'utilisateur. Entrez un numéro de sécurité à quatre chiffres, compris entre 0100 et 0499.
URL de la banque	Sélectionnez l'URL de la banque dans la liste déroulante.
Limite d'extraction	Valide si vous avez sélectionné HVT - détails de la commande. Il s'agit du nombre maximal de détails de la commande à transmettre si l'attribut completeOrderData est défini sur faux. La valeur par défaut est 100. La valeur admise doit être un nombre entier non négatif. Indiquez 0 pour extraire un nombre illimité de détails. Même s'il est possible d'extraire plus de 100 détails à la fois, cela n'est pas recommandé.
Décalage d'extraction	Valide si vous avez sélectionné HVT - détails de la commande. Il s'agit de la position de décalage dans le fichier de commande d'origine qui marque le point de départ des détails de transaction à transmettre. Si l'attribut completeOrderData est défini sur faux, la position de décalage s'applique au nombre séquentiel d'une commande spécifique. La valeur par défaut est 0. La valeur admise doit être un nombre entier non négatif. Pour extraire plus de 100 enregistrements, définissez Décalage d'extraction sur 0 afin d'extraire les 100 premiers, puis sur 101 afin d'extraire les 100 suivants. Continuez si nécessaire.

7. Cliquez sur **Soumettre**.

Signer une commande VEU en attente

Avant de commencer

Pour signer une commande VEU en attente, vérifiez que les conditions suivantes sont respectées :

- Le paramètre Prêt pour la signature affiche Vrai
- Une des commandes VEU suivantes est soumise :
 - HVZ
 - HVU et HVD
 - HVU et HVT - données de commande complètes

Pourquoi et quand exécuter cette tâche

Procédez comme suit pour signer une commande VEU en attente :

Procédure

1. Connectez-vous au client EBICS de Sterling B2B Integrator.
2. À partir du menu **Utilisateur**, sélectionnez **Afficheurs > Tâches VEU en attente**.

3. Dans la page Tâches VEU en attente, indiquez les valeurs des zones répertoriées dans le tableau suivant, puis cliquez sur **Rechercher**.

Zone	Description
Nom du partenaire	Obligatoire. Sélectionnez un nom de partenaire dans la liste déroulante.
ID de banque (ID hôte)	Obligatoire. Sélectionnez un ID de banque associé au partenaire dans la liste déroulante.
URL de la banque	Obligatoire. Sélectionnez l'adresse URL requise dans la liste déroulante. L'adresse URL sélectionnée est utilisée pour établir une session HTTP ou HTTPS avec le serveur EBICS Banking Server.

Une demande est envoyée à la banque afin de récupérer les détails des commandes VEU en attente.

4. Dans la page Tâches VEU en attente, cliquez sur le lien ID de commande. Les détails des données de commande s'affichent.

Zone	Description
ID de commande	ID de la commande VEU en attente. Cliquez sur le lien ID de commande pour afficher des informations sur les données de commande.
Type de commande	Type de la commande VEU en attente. Par exemple, FUL.
ID partenaire de l'émetteur	ID du partenaire associé à l'utilisateur qui a soumis le type de commande d'envoi par téléchargement.
ID utilisateur de l'émetteur	ID abonné de l'utilisateur qui a soumis le type de commande de réception par téléchargement.
Données de commande disponibles	Après avoir soumis un type de commande HVZ, indiquez si les données de commande peuvent être téléchargées dans le format d'origine.
Détails de commande disponibles	Informations sur la commande pour le type de commande HVU.
Taille des données de commande	Taille des données de commande non compressées en kilooctets.
Date-heure	L'horodatage s'affiche dans un format date et heure.
Prêt pour la signature	Indique si la commande est déjà signée par l'utilisateur. Faux indique que la commande est déjà signée par l'utilisateur. Vrai indique que la commande est prête à être signée par l'utilisateur.
Signatures requises	Affiche le nombre minimum de signatures requises pour autoriser la commande.

Zone	Description
Signatures effectuées	<p>Nombre de signatures qui ont clôturé la validation de la commande. Indique le nombre de signatures électroniques déjà fournies, ainsi que les informations sur les signataires précédents. Cliquez sur le lien Informations du signataire pour visualiser les détails du signataire :</p> <ul style="list-style-type: none"> • Nom du partenaire : nom du partenaire commercial • ID utilisateur • Nom : nom du signataire • Horodatage • Niveau d'autorisation : niveau d'autorisation du signataire
Lien Informations sur la commande	<p>Cliquez sur le lien Informations sur la commande pour visualiser les détails de la commande :</p> <ul style="list-style-type: none"> • Compte : cliquez sur le lien Informations sur le compte pour afficher le nom du détenteur du compte, le code de devise, la description du compte, le rôle du détenteur du compte, le numéro de compte et le code de la banque. • Montant : affichez le montant de la transaction de commande. • Code de devise : affichez le code de devise de la transaction de commande. • Débit • Date d'exécution : affichez la date de l'exécution de la commande. • Description : cliquez sur le lien Description pour afficher la description et le type de description du signataire.

5. Cliquez sur **Signer la commande**.
6. Dans la fenêtre Détails de la commande VEU, indiquez les valeurs des paramètres suivants :

Zone	Description
Préfixe d'ID de commande	Sélectionnez une lettre de l'alphabet dans la liste déroulante.
Moyen de sécurité	Moyen de sécurité pour la clé technique bancaire de l'utilisateur. Entrez un numéro de sécurité à quatre chiffres, compris entre 0100 et 0499.
URL de la banque	Sélectionnez l'URL de la banque dans la liste déroulante.

7. Cliquez sur **Soumettre**.

Annuler une commande VEU en attente

Avant de commencer

Pour annuler une commande VEU en attente, vérifiez que les conditions suivantes sont respectées :

- Le paramètre Prêt pour la signature affiche Vrai
- Une des commandes VEU suivantes est soumise :
 - HVZ
 - HVU et HVD
 - HVU et HVT - données de commande complètes

Pourquoi et quand exécuter cette tâche

Procédez comme suit pour annuler une commande VEU en attente :

Procédure

1. Connectez-vous au client EBICS de Sterling B2B Integrator.
2. À partir du menu **Utilisateur**, sélectionnez **Afficheurs > Tâches VEU en attente**.
3. Dans la page Tâches VEU en attente, indiquez les valeurs des zones répertoriées dans le tableau suivant, puis cliquez sur **Rechercher**.

Zone	Description
Nom du partenaire	Obligatoire. Sélectionnez un nom de partenaire dans la liste déroulante.
ID de banque (ID hôte)	Obligatoire. Sélectionnez un ID de banque associé au partenaire dans la liste déroulante.
URL de la banque	Obligatoire. Sélectionnez l'adresse URL requise dans la liste déroulante. L'adresse URL sélectionnée est utilisée pour établir une session HTTP ou HTTPS avec le serveur EBICS Banking Server.

Une demande est envoyée à la banque afin de récupérer les détails des commandes VEU en attente.

4. Dans la section Résultats de la recherche de la page Tâches VEU en attente, cliquez sur le lien ID de commande. Les détails des données de commande s'affichent.

Zone	Description
ID de commande	ID de la commande VEU en attente. Cliquez sur le lien ID de commande pour afficher des informations sur les données de commande.
Type de commande	Type de la commande VEU en attente. Par exemple, FUL.
ID partenaire de l'émetteur	ID du partenaire associé à l'utilisateur qui a soumis le type de commande d'envoi par téléchargement.

Zone	Description
ID utilisateur de l'émetteur	ID abonné de l'utilisateur qui a soumis le type de commande de réception par téléchargement.
Données de commande disponibles	Après avoir soumis un type de commande HVZ, indiquez si les données de commande peuvent être téléchargées dans le format d'origine.
Détails de commande disponibles	Informations sur la commande pour le type de commande HVU.
Taille des données de commande	Taille des données de commande non compressées en kilooctets.
Date-heure	L'horodatage s'affiche dans un format date et heure.
Prêt pour la signature	Indique si la commande est déjà signée par l'utilisateur. Faux indique que la commande est déjà signée par l'utilisateur. Vrai indique que la commande est prête à être signée par l'utilisateur.
Signatures requises	Affiche le nombre minimum de signatures requises pour autoriser la commande.
Signatures effectuées	<p>Nombre de signatures qui ont clôturé la validation de la commande. Indique le nombre de signatures électroniques déjà fournies, ainsi que les informations sur les signataires précédents. Cliquez sur le lien Informations du signataire pour visualiser les détails du signataire :</p> <ul style="list-style-type: none"> • Nom du partenaire : nom du partenaire commercial • ID utilisateur • Nom : nom du signataire • Horodatage • Niveau d'autorisation : niveau d'autorisation du signataire

Zone	Description
Lien Informations sur la commande	<p>Cliquez sur le lien Informations sur la commande pour visualiser les détails de la commande :</p> <ul style="list-style-type: none"> • Compte : cliquez sur le lien Informations sur le compte pour afficher le nom du détenteur du compte, le code de devise, la description du compte, le rôle du détenteur du compte, le numéro de compte et le code de la banque. • Montant : affichez le montant de la transaction de commande. • Code de devise : affichez le code de devise de la transaction de commande. • Débit • Date d'exécution : affichez la date de l'exécution de la commande. • Description : cliquez sur le lien Description pour afficher la description et le type de description du signataire.

5. Cliquez sur **Annuler la commande**.
6. Dans la fenêtre Détails de la commande VEU, indiquez les valeurs des paramètres suivants :

Zone	Description
Préfixe d'ID de commande	Sélectionnez une lettre de l'alphabet dans la liste déroulante.
Moyen de sécurité	Moyen de sécurité pour la clé technique bancaire de l'utilisateur. Entrez un numéro de sécurité à quatre chiffres, compris entre 0100 et 0499.
URL de la banque	Sélectionnez l'URL de la banque dans la liste déroulante.

7. Cliquez sur **Soumettre**.

Mise à jour des valeurs des propriétés système

Après avoir configuré le client EBICS, un administrateur du client EBICS peut mettre à jour les valeurs des propriétés système.

Pourquoi et quand exécuter cette tâche

Pour mettre à jour les valeurs des propriétés système :

Procédure

1. Connectez-vous au client EBICS de Sterling B2B Integrator.
2. À partir du menu **Administration**, sélectionnez **Valeurs des propriétés système**.
3. Cliquez sur **Mettre à jour** pour mettre à jour les valeurs des propriétés système répertoriées dans le tableau suivant :

Zone	Description
Afficher le code de réponse	Chaque service client renvoie un code de réponse à partir du serveur. Si ce code est un code d'erreur, le processus technique renvoie une erreur. Si le code d'erreur est attendu, utilisez un service OnFault pour continuer à interagir avec le partenaire commercial.
Nouvelles tentatives de connexion	Indiquez le nombre de fois où l'adaptateur client HTTP tente de se connecter au serveur. Les valeurs admises incluent tout entier compris entre 0 et 50. La valeur par défaut est 3.
Délai entre les tentatives	Indiquez le nombre de secondes pendant lesquelles l'adaptateur client HTTP attend entre deux tentatives. La valeur par défaut est 60. Les valeurs admises incluent tout entier compris entre 1 et 7200.
Délai d'attente d'E-S	Indiquez le nombre de secondes à attendre pour que le transfert des données se termine avant de passer à l'état WAITING_ON_IO. Si -1 est indiqué, le service fonctionne en mode blocage. Les valeurs admises incluent toute valeur numérique.
Initialiser une nouvelle session HTTP pour chaque demande	Si vous souhaitez initialiser une nouvelle session HTTP pour chaque demande envoyée par le client EBICS au serveur, définissez ce paramètre sur true (vrai). La valeur par défaut est false. Si vous téléchargez un grand volume de données (par ex., 200 Mo) vers le serveur EBICS en utilisant le type de commande FUL, ce paramètre doit être défini sur true.
Nombre de segments de persistance	Nombre de segments après lequel l'exécution journalise un événement. Ce paramètre n'est valide que pour les types de commande d'envoi et de réception par téléchargement. Supposons que vous avez indiqué cinq pour cette propriété. Après l'envoi de dix segments sur le serveur, deux points de données de la transaction (le cinquième et le dixième) sont conservés dans la base de données du client. Si l'instance du client cesse de fonctionner après l'envoi du douzième segment sur le serveur, le client renvoie le dixième segment de données de la transaction. Si le serveur a déjà reçu douze segments de données de la transaction, le serveur informe le client qu'il va effectuer un nouvel envoi à partir du treizième segment.
Taille du cache de génération de l'ID de commande	Indiquez la taille de la mémoire cache interne pour la génération d'ID de commande. La valeur par défaut est 30.
Temps d'attente de l'unité d'exécution en cas d'échec en mémoire cache de l'ID de commande (en ms)	Indiquez la durée pendant laquelle l'unité d'exécution doit attendre si celle-ci subit un échec en mémoire cache. La valeur par défaut est 1000 millisecondes.
Nombre de tentatives en cas d'échec en mémoire cache de l'ID de commande	Indiquez le nombre de fois où l'unité d'exécution doit attendre entre chaque échec en mémoire cache. La valeur par défaut est 5.
ID de produit	Entrez l'ID de produit pour l'application client EBICS.

Zone	Description
Langue de produit	Entrez le paramètre linguistique de l'application client EBICS que vous utilisez. Par exemple, entrez EN si la langue est définie sur Anglais.
Durée de conservation des commandes qui ont des tâches en attente (en jours)	Indiquez le nombre de jours pendant lesquels les commandes associées à des tâches en attente doivent être conservées dans le système sans être purgées. La valeur par défaut est 1000.
Vérifier l'utilisation de la clé du certificat	Spécifiez s'il faut contrôler l'utilisation de la clé dans les certificats. Les valeurs valides sont : <ul style="list-style-type: none"> • true - Contrôler l'utilisation de la clé. • false - Ne pas contrôler l'utilisation de la clé.
Utiliser un modulo et un exposant avec un espace pour l'entrée de hachage dans la lettre d'initialisation	Indiquez vrai si le hachage de la lettre d'initialisation doit être calculé à l'aide d'une entrée de hachage sous la forme d'un modulo et d'un exposant avec espace. Indiquez faux si le hachage de la lettre d'initialisation doit être calculé à l'aide du certificat complet ou de la clé publique. La valeur par défaut est faux.
Utiliser un modulo et un exposant avec un espace pour l'entrée de hachage dans la validation de clé bancaire	Indiquez vrai si le hachage de la validation de clé bancaire doit être calculé à l'aide d'une entrée de hachage sous la forme d'un modulo et d'un exposant avec espace. Indiquez faux si le hachage de la validation de clé bancaire doit être calculé à l'aide du certificat complet ou de la clé publique. La valeur par défaut est faux.
Chemin d'accès aux métadonnées de la boîte aux lettres	Indiquez la boîte aux lettres qui contient le message OrderMetadata.
Fréquence de purge HAC (en minutes)	Spécifiez le nombre de minutes entre les opérations de purge automatique dans lesquelles EBICS analyse la base de données à la recherche d'enregistrements HAC et purge ces enregistrements. La valeur par défaut est 720. Pour plus d'informations sur l'expiration d'enregistrement HAC, consultez le paramètre Expiration de purge dans «Création d'un planning HAC», à la page 134.
Puissance de chiffrement	Indiquez le taux de chiffrement. Les valeurs valides sont Fort, Tout et Faible.
Adaptateur client	Indiquez un adaptateur client permettant d'envoyer des demandes aux partenaires commerciaux. Par exemple, configurez un adaptateur client HTTP pour envoyer des demandes HTTP aux partenaires commerciaux.
Demande brute	Spécifiez vrai pour indiquer si un message de demande brut est remis à un processus technique. Sinon, indiquez faux.
Réponse brute	Spécifiez vrai pour indiquer si une réponse brute est renvoyée par un processus technique. Sinon, indiquez faux.
Réinitialiser la connexion en cas d'erreur	Indiquez Activer pour réinitialiser la connexion au serveur si le client rencontre une erreur lors de la tentative de connexion au serveur.
Délai d'attente de réponse	Indiquez le nombre de secondes que le serveur prend pour répondre. La valeur par défaut est 300. Les valeurs admises incluent tout entier compris entre 1 et 999 999.

Zone	Description
Utiliser l'espace de nom 'esig' dans la balise xml KeyOrderData	Indiquez vrai si vous souhaitez utiliser 'esig' comme espace de nom supplémentaire plutôt que de l'utiliser comme espace de nom par défaut dans la balise XML KeyOrderData. La valeur par défaut est vrai.
Insérer des éléments facultatifs dans la balise xml KeyManagement request	Indiquez vrai si vous souhaitez insérer des éléments facultatifs spécifiés dans le schéma de demande de gestion des clés EBICS de la balise XML KeyManagement request. La valeur par défaut est vrai.

4. Cliquez sur **Terminer** pour sauvegarder les modifications que vous avez mises à jour.

Mon profil

Pourquoi et quand exécuter cette tâche

La page Mon profil vous permet d'afficher les paramètres utilisateur. Les paramètres sont différents en fonction du type d'utilisateur.

Procédure

1. Connectez-vous au client EBICS de Sterling B2B Integrator.
2. Dans le menu **Administration, Opérateur** ou **Utilisateur**, sélectionnez **Mon profil**. Les tableaux ci-dessous répertorient les paramètres affichés pour différents types d'utilisateur.

Tableau 6. Utilisateur du client EBICS

Paramètres utilisateur	Description
ID utilisateur	L'ID utilisateur s'affiche.
Nom d'utilisateur	Le nom d'utilisateur s'affiche.
Type d'utilisateur	Le type d'utilisateur s'affiche.
Fuseau horaire	Le fuseau horaire de l'utilisateur s'affiche.
Utilisateur technique	Indique si l'utilisateur est un utilisateur technique. Les valeurs admises sont : <ul style="list-style-type: none"> • Vrai • Faux
Type de certificat	Le type de certificat utilisé par l'utilisateur pour autoriser les certificats d'identification et d'authentification, de chiffrement et de signature électronique s'affiche.
Certificat privé d'authentification	Le certificat privé d'authentification de l'utilisateur s'affiche.
Certificat public d'authentification	Le certificat public d'authentification de l'utilisateur s'affiche.
Version de clé d'authentification	La version de la clé d'authentification s'affiche.
Certificat privé de chiffrement	Le certificat privé de chiffrement de l'utilisateur s'affiche.
Certificat public de chiffrement	Le certificat public de chiffrement de l'utilisateur s'affiche.

Tableau 6. Utilisateur du client EBICS (suite)

Paramètres utilisateur	Description
Version de clé de chiffrement	La version de la clé de chiffrement s'affiche.
Utiliser le magasin de clés matérielles pour la signature électronique	Indique si un fichier de clés matériel est utilisé pour la signature électronique (ES). Les valeurs admises sont : <ul style="list-style-type: none"> • Oui • Non
Clé privée de signature électronique	Le certificat privé de signature électronique de l'utilisateur s'affiche.
Clé publique de signature électronique	Le certificat public de signature électronique de l'utilisateur s'affiche.
Version de clé de signature électronique	La version de la clé de signature électronique s'affiche.
Partenaire(s) associé(s)	Lorsque vous cliquez sur le lien Tout afficher , les informations des partenaires associés s'affichent dans un format tabulaire. Vous pouvez afficher le nom du partenaire, le chemin d'accès à la boîte d'envoi par téléchargement et le chemin d'accès à la boîte de réception par téléchargement.
Partenaire(s) associé(s) avec les banques	Lorsque vous cliquez sur le lien Tout afficher , les partenaires associés à la banque, le nom du partenaire, l'ID de la banque et le statut s'affichent. Si un utilisateur du client EBICS est à l'état Initialisé ou Prêt, une lettre INI ou HIA peut également être générée. Si l'utilisateur du client EBICS est autorisé à soumettre le type de commande SPR, une icône de soumission du type de commande SPR s'affiche. Cliquez sur l'icône pour interrompre l'utilisateur actuel à la banque.

Tableau 7. Superadministrateur du client EBICS, Administrateur du client EBICS ou Opérateur du client EBICS

Paramètres utilisateur	Description
ID utilisateur	L'ID utilisateur s'affiche.
Nom d'utilisateur	Le nom d'utilisateur s'affiche.
Type d'utilisateur	Le type d'utilisateur s'affiche.
Fuseau horaire	Le fuseau horaire de l'utilisateur s'affiche.

Importation et exportation des ressources du client EBICS

Vous pouvez importer des ressources et exporter des données de configuration pour des ressources qui appartiennent au client EBICS à l'aide de Sterling B2B Integrator.

Par exemple, vous pouvez exporter des données de configuration pour un profil de banque, un profil d'utilisateur, des formats de fichier, une offre et un droit d'utilisateur au format XML, puis les stocker sur le système. Vous pouvez importer des données de configuration pour un profil de banque, un profil d'utilisateur, des formats de fichier, une offre et un droit d'utilisateur au format XML. Pour plus

d'informations sur la gestion des ressources, voir *Gestion des ressources* dans le centre de documentation de Sterling B2B Integrator.

Lorsque vous choisissez d'exporter un droit d'utilisateur ou une offre, tous les types de ressource dépendante (par exemple, les profils de la banque et de l'utilisateur) sont également exportés. Lors de l'importation, vérifiez que vous avez sélectionné chaque type de ressource dépendante, affiché dans une page distincte. Par exemple, si vous choisissez d'importer un droit d'utilisateur, vérifiez que vous avez sélectionné les profils d'utilisateur associés.

Remarque : Si vous exportez un profil de banque avec une adresse URL par défaut, si le profil de banque se trouve sur le système cible, mais s'il est associé à une autre URL par défaut, le profil de banque aura plusieurs URL par défaut après l'importation. Pour conserver une seule URL par défaut, connectez-vous au tableau de bord de l'application client EBICS et modifiez les paramètres de configuration de la banque. Sinon, l'exécution du client EBICS utilise la première URL par défaut extraite de la base de données pour effectuer les transactions.

Remarque : Dans le client EBICS, une banque peut posséder une seule offre. Si un système cible possède une offre dont la clé principale est identique à celle du fichier XML d'exportation et si l'option **Ressources à mettre à jour** est définie sur **Oui**, l'offre du système cible est mise à jour avec les types de commande associés à l'offre dans le fichier XML d'exportation. Toutefois, si la clé principale de l'offre sur le système cible est différente de celle du fichier XML d'exportation, l'offre et les types de commande associés dans le système cible sont remplacés par l'offre et les types de commande associés du fichier XML d'exportation.

Exporter les ressources du client EBICS

Vous pouvez utiliser le gestionnaire de ressources dans Sterling B2B Integrator pour exporter des ressources du client EBICS.

Pourquoi et quand exécuter cette tâche

Pour exporter des ressources du client EBICS :

Procédure

1. Connectez-vous à Sterling B2B Integrator.
2. Dans le menu **Administration**, sélectionnez **Déploiement > Gestionnaire des ressources > Importer/Exporter des ressources**.
3. En regard de **Exporter des ressources**, cliquez sur **OK**.
4. Sur la page Type du format de sortie :
 - a. Sélectionnez le type de format utilisé pour exporter vos données :
 - **Document XML (.xml)**
 - **Module d'installation (.jar)**
 - b. Cliquez sur **Suivant**.
5. Sur la page Groupe de ressources, indiquez si vous souhaitez exporter les ressources en fonction du nom d'un indicateur.
 - Sélectionnez **Non** pour indiquer que vous ne souhaitez pas exporter les ressources en fonction du nom d'un indicateur.
 - Sélectionnez **Oui** pour exporter un groupe de ressources complet en fonction du nom d'un indicateur. Sélectionnez le nom d'indicateur dans la liste.

Cliquez sur **Suivant**.

6. Sur la page Type d'exportation, sélectionnez **Standard – exporte la version par défaut**, puis cliquez sur **Suivant**.
7. Sur la page Sélectionner des ressources, sélectionnez **Ressource(s) EBICS Client**, puis cliquez sur **Suivant**.
8. Sur la page Sélectionner des ressources EBICS Client, sélectionnez les ressources que vous souhaitez exporter :

Option	Description
Format de fichier	Informations sur les formats de fichier.
Offre bancaire	Informations sur l'offre qui incluent des détails sur le profil de la banque et les formats de fichier associés à l'offre.
Droit d'utilisateur	Informations sur l'utilisateur, le partenaire commercial (enregistrement d'identité), les détails du profil de la banque, l'offre, les types d'offre et les formats de fichier associés à l'offre.
Profil de la banque	Informations sur la banque et les certificats de confiance associés à la banque.
Profil de l'utilisateur	Informations sur l'utilisateur, le partenaire, les données associées telles que les droits de boîte aux lettres, les enregistrements d'identité et les certificats de système et de confiance.

Cliquez sur **Suivant**.

9. Sur la page correspondant à chaque type de ressource sélectionné, déplacez les éléments à exporter de la liste **Disponible** vers la liste **À exporter**.
 - a. Facultatif. Filtrez les données à l'aide de l'option **Filtrer les données**.
 - b. Dans la zone **Exporter les enregistrements dépendants**, sélectionnez **Oui** afin d'exporter les informations configurées pour le client EBICS dans Sterling B2B Integrator. Par exemple, des informations concernant la configuration des boîtes aux lettres, les certificats numériques, les enregistrements d'identité, etc. Sinon, sélectionnez **Non**.
 - c. Cliquez sur **Suivant**.Répétez cette opération pour chaque page de types de ressources supplémentaires.
10. Sur la page Sécurité, entrez et confirmez la phrase passe du système, puis cliquez sur **Suivant**.
11. Sur la page Confirmer, consultez les informations sur les ressources à exporter, puis cliquez sur **Terminer**. Le fichier d'exportation est créé.
12. Sur la page Terminer, sélectionnez l'un des paramètres suivants :
 - Cliquez sur l'icône en regard de **Afficher le rapport d'exportation** pour consulter le rapport d'exportation.
 - Cliquez sur l'icône **Télécharger** en regard de **Données d'exportation (.xml)** ou de **Données d'exportation (.jar)** pour télécharger le fichier d'exportation et l'enregistrer sur un disque dur.
13. Cliquez sur **Retourner**.

Importer les ressources du client EBICS

Vous pouvez utiliser le gestionnaire de ressources dans Sterling B2B Integrator pour importer des ressources du client EBICS.

Pourquoi et quand exécuter cette tâche

Pour importer des ressources du client EBICS :

Procédure

1. Connectez-vous à Sterling B2B Integrator.
2. Dans le menu **Administration**, sélectionnez **Déploiement > Gestionnaire des ressources > Importer/Exporter des ressources**.
3. En regard de **Importer des ressources**, cliquez sur **OK**.
4. Sur la page Importer fichier, indiquez les valeurs des zones répertoriées dans le tableau suivant, puis cliquez sur **Suivant**.

Zone	Description
Nom de fichier	Obligatoire. Cliquez sur Parcourir pour rechercher et sélectionner le fichier à importer. Le fichier doit être un document XML (.xml) ou un module d'installation (.jar).
Phrase passe	Facultatif. Indiquez une phrase passe pour le fichier lorsque vous y êtes invité.
Ignorer la génération de sauvegardes	Facultatif. Sous Options de réglage , si vous ne souhaitez <i>pas</i> générer de sauvegarde des entités mises à jour, cochez cette case.
Importer toutes les ressources	Facultatif. Sous Options de réglage , si vous souhaitez importer toutes les ressources, cochez cette case. Par exemple, les droits associés à la boîte aux lettres, les enregistrements d'identité et les certificats de clé privée sont automatiquement importés. Si vous ne sélectionnez pas cette option, vous êtes invité à sélectionner les entrées à importer pour chaque type de ressource.

5. Sur la page Créer des indicateurs de ressources :
 - a. Cette étape est facultative. Si vous souhaitez associer les données importées à un groupe de ressources, entrez un **Nom d'indicateur** et une **Description de l'indicateur**.
 - b. Cliquez sur **Suivant**.
6. Sur la page Mettre à jour les objets :
 - Sélectionnez **Oui** pour mettre à jour les objets qui se trouvent sur le système.
 - Sélectionnez **Non** pour importer les objets qui ne se trouvent pas sur le système.Cliquez sur **Suivant**.
7. Cette étape peut ne pas s'appliquer à toutes les importations. Pour chaque type de ressource sélectionné, déplacez les articles à importer de la liste **Disponible** vers la liste **À importer**. Cliquez sur **Suivant**.

8. Sur la page Confirmer, consultez les informations sur les ressources à importer, puis cliquez sur **Terminer**. Les données sont importées.
9. Sur la page Terminer, vous pouvez effectuer les actions suivantes :
 - Cliquez sur **Afficher le rapport d'importation** pour consulter le rapport d'importation.
 - Cliquez sur **Afficher le rapport de performance** pour consulter les données récapitulatives dans le rapport de performance.
 - Cliquez sur **Télécharger en regard de Données dans Sterling B2B Integrator avant l'importation (.xml)** pour obtenir une copie sauvegardée des données.

Remarque : Si vous avez sélectionné l'option Ignorer la génération de sauvegardes, le lien Télécharger ne s'affiche *pas*.

10. Cliquez sur **Retourner**.

Droits d'accès à l'interface utilisateur du client EBICS

Pour accéder à l'interface graphique du client EBICS de Sterling B2B Integrator et à ses fonctions, vous devez être affecté à l'un des groupes de droits suivants :

- Administrateur EBICSClient
- Opérateur EBICSClient
- Utilisateurs EBICSClient

Le tableau ci-dessous répertorie les éléments de menu du client EBICS de Sterling B2B Integrator, ainsi que les droits nécessaires pour accéder aux pages associées à chaque groupe :

Remarque :

Accéder à un élément de menu permet l'accès à la fonctionnalité complète de la page associée, avec la fonction de suppression limitée aux utilisateurs avec des droits administrateur.

Tableau 8. Éléments de menu du client EBICS de Sterling B2B Integrator et droits d'accès

Éléments de menu	Droits	EBICSClient		
		Administrateur	Opérateur	Utilisateurs
Gestion de profil > Utilisateur	CREATE	Oui	Non	Non
	EDIT	Oui	Non	Non
	VIEW	Oui	Oui	Non
	DELETE	Oui	Non	Non
Gestion de profil > Banque > Profil	CREATE	Oui	Non	Non
	EDIT	Oui	Non	Non
	VIEW	Oui	Oui	Non
	DELETE	Oui	Non	Non
Gestion de profil > Banque > Configurations des offres	CREATE	Oui	Non	Non
	EDIT	Oui	Non	Non
	VIEW	Oui	Oui	Non
	DELETE	Oui	Non	Non

Tableau 8. Éléments de menu du client EBICS de Sterling B2B Integrator et droits d'accès (suite)

Éléments de menu	Droits	EBICSClient		
		Administrateur	Opérateur	Utilisateurs
Gestion de profil > Banque > Validation des clés bancaires	VALIDATE	Oui	Non	Non
Gestion de profil > Formats de fichier	CREATE	Oui	Non	Non
	EDIT	Oui	Non	Non
	VIEW	Oui	Oui	Non
	DELETE	Oui	Non	Non
Gestion de profil > Clés	CREATE	Oui	Non	Non
	EDIT	Oui	Non	Non
	VIEW	Oui	Oui	Non
	DELETE	Oui	Non	Non
Droits > Droits d'utilisateur	CREATE	Oui	Non	Non
	EDIT	Oui	Non	Non
	VIEW	Oui	Oui	Non
	DELETE	Oui	Non	Non
Soumission de commande	SUBMISSION	Non	Non	Oui
Afficheurs > Afficheur d'événements	SEARCH	Oui	Oui	Oui
Afficheurs > Recherche de commande	SEARCH	Oui	Oui	Oui
Afficheurs > Tâches en attente	VIEW	Non	Non	Oui
	SIGN	Non	Non	Oui
Afficheurs > Tâches VEU en attente	VIEW	Non	Non	Oui
	SIGN	Non	Non	Oui
	SUBMIT	Non	Non	Oui
Remarque : La page Tâches VEU en attente s'affiche uniquement après la soumission des types de commande HVU et HVZ à partir du menu Soumission de commande.				
Propriété système	VIEW	Oui	Non	Non
	UPDATE	Oui	Non	Non

Tableau 8. Éléments de menu du client EBICS de Sterling B2B Integrator et droits d'accès (suite)

Éléments de menu	Droits	EBICSClient		
		Administrateur	Opérateur	Utilisateurs
Mon profil	VIEW	Oui	Oui	Oui

Récupération de transactions en envoi et en réception

Lorsque des données de transaction sont en cours d'envoi ou de réception et que le client cesse de fonctionner, il existe un risque de perte des données de transaction. Pour éviter la perte des données de transaction et, par conséquent, leur restauration, le client EBICS prend en charge la récupération des transactions en envoi et en réception.

Récupération des transactions en envoi

Le scénario suivant illustre le mécanisme de récupération d'une transaction en envoi à l'aide du type de commande FUL :

1. Vingt segments de données de la transaction sont envoyés au serveur.
2. Après l'envoi de dix segments, l'instance du client cesse de fonctionner.
3. Lorsque l'instance du client a été restaurée, le client renvoie les données de la transaction à partir du point d'interruption. Dans cet exemple, le client renvoie le onzième segment de données de la transaction.

Si le segment reçu du client après la récupération n'est pas synchronisé avec le segment existant sur le serveur, ce dernier renvoie l'événement EBICS_TX_RECOVERY_SYNC. EBICS_TX_RECOVERY_SYNC indique que le serveur synchronise les segments de la transaction avec le client. Dans la colonne Horodatage de l'observateur d'événements, vous pouvez voir la différence dans les horodatages des segments qui sont envoyés avant et après la récupération des transactions.

Conservation du nombre de segments

Vous pouvez mettre à jour la valeur de la propriété système Nombre de segments de persistance dans le menu Administration du client EBICS afin de conserver les points de données de la transaction dans la base de données du client. Supposons que vous avez indiqué cinq pour cette propriété. Après l'envoi de dix segments sur le serveur, deux points de données de la transaction (le cinquième et le dixième) sont conservés dans la base de données du client.

Si l'instance du client cesse de fonctionner après l'envoi du douzième segment sur le serveur, le client renvoie le dixième segment de données de la transaction. Si le serveur a déjà reçu douze segments de données de la transaction, le serveur informe le client qu'il va effectuer un nouvel envoi à partir du treizième segment.

Récupération des transactions en réception

Le scénario suivant illustre le mécanisme de récupération d'une transaction en réception à l'aide du type de commande FDL :

1. Dix segments de données de la transaction sont reçus du serveur.
2. L'instance du client s'arrête de fonctionner après la réception et la conservation du sixième segment dans la base de données.

3. Lorsque l'instance du client a été restaurée, le client envoie une demande au serveur concernant le septième segment.

Le scénario suivant illustre la récupération d'une transaction en réception à l'aide du type de commande FDL, lorsque l'instance du client cesse de fonctionner au cours du téléchargement d'un segment :

1. Dix segments de données de la transaction sont reçus du serveur.
2. L'instance du client cesse de fonctionner au cours de la réception du sixième segment du serveur.
3. Lorsque l'instance du client a été restaurée, le client renvoie une demande au serveur concernant le sixième segment.

Soumission et signature d'un type de commande FUL

L'exemple de scénario suivant présente la procédure de soumission et de signature ou de rejet d'un type de commande FUL, dans lequel l'émetteur et le signataire sont deux entités distinctes. Si la valeur de la signature électronique est définie sur 1, une signature unique dont le niveau d'autorisation est E ou A est suffisante pour traiter une commande.

Avant de commencer

Dans le scénario, les entités suivantes sont utilisées :

- L'émetteur est l'utilisateur EBICS USERSUBMIT
- Le signataire est l'utilisateur EBICS USERSIGN
- Le nom de la banque est BANK
- Le nom de l'offre est OFFER
- Le nom du partenaire est PARTNER

Avertissement : Si vous téléchargez un grand volume de données (par ex., 200 Mo) vers le serveur EBICS en utilisant le type de commande FUL, le paramètre **Initialiser une nouvelle session HTTP pour chaque demande** des propriétés système du client EBICS doit être défini sur true. Pour modifier les propriétés système, voir «Mise à jour des valeurs des propriétés système», à la page 77.

Pourquoi et quand exécuter cette tâche

Pour soumettre un type de commande FUL, lorsque le paramètre ES=1, effectuez les étapes suivantes dans l'interface utilisateur du client EBICS de Sterling B2B Integrator :

Procédure

1. Configurez USERSUBMIT et USERSIGN en tant qu'utilisateurs du client EBICS. Pour plus d'informations sur la configuration d'un utilisateur existant en tant qu'utilisateur du client EBICS, voir *Configurer un utilisateur existant en tant qu'utilisateur du client EBICS*.
2. Configurez un profil de banque pour BANK. Pour plus d'informations sur la configuration d'un profil de banque, voir *Créer un profil de banque*.
3. Configurez une offre pour OFFER. Pour plus d'informations sur la configuration d'une offre, voir *Créer une offre*.
4. Configurez le droit d'utilisateur pour OFFER. Pour plus d'informations sur le droit d'utilisateur, voir *Créer un droit d'utilisateur*.

5. Connectez-vous au client EBICS de Sterling B2B Integrator en tant qu'administrateur (admin).
6. Dans le menu **Droits**, sélectionnez **Droits d'utilisateur**.
7. Sur la page Configuration du droit d'utilisateur, dans la zone **Nom de l'offre**, sous **Rechercher**, entrez le nom de l'offre, OFFER, pour laquelle le droit d'utilisateur est configuré.
8. Cliquez sur **OK**.
9. Cliquez sur l'icône Mettre à jour en regard du droit d'utilisateur que vous souhaitez modifier. Le nom de l'offre du droit d'utilisateur est OFFER et l'ID de banque associé est BANK.
10. Sur la page Mettre à jour : Informations sur le droit, cliquez sur l'icône Mettre à jour en regard de n'importe quel format de fichier FUL, par exemple, pain.001.001.02.ict.
11. Sur la page Ajouter un droit, indiquez 1 dans la zone **Nombre de signatures requis**.
12. Cliquez sur **Ajouter des signataires**.
13. Sur la page Ajouter un signataire, sélectionnez USERSIGN dans la liste déroulante **ID utilisateur**. Sélectionnez Signataire comme **Type de droit**.
14. Cliquez sur **Enregistrer**.
15. Connectez-vous au client EBICS de Sterling B2B Integrator en tant qu'utilisateur USERSUBMIT.
16. Générez les lettres INI et HIA à l'aide de l'interface utilisateur de tableau de bord du client EBICS ou utilisez le type de commande H3K. Pour plus d'informations sur l'envoi de clés publiques à la banque à l'aide des commandes INI et HIA ou H3K, voir *Initialisation d'un utilisateur*.
17. Signez manuellement les lettres INI et HIA et envoyez-les par courrier électronique à la banque (BANK). Cette procédure ne s'applique pas à la commande H3K.
18. Initialisez les utilisateurs à l'aide de l'une des méthodes suivantes :
 - Soumettez une commande H3K.
 - Utilisez INI et HIA ensemble.
 - Soumettez des commandes INI et HIA.
 - Générez et signez les lettres d'initialisation INI et HIA. Adressez les lettres signées à la banque.

Pour plus d'informations, voir «Initialisation d'un utilisateur», à la page 46.
19. Une fois la vérification terminée, BANK fait passer le statut de l'utilisateur USERSUBMIT de Nouveau en Prêt. USERSUBMIT peut désormais effectuer des transactions avec la banque.
20. À l'aide du type de commande HPB, téléchargez les certificats publics de BANK.
21. Répétez les étapes 15 à 19 pour USERSIGN.
22. Connectez-vous au client EBICS de Sterling B2B Integrator en tant qu'administrateur (admin).
23. Validez la valeur hachée des certificats reçus de la banque. Pour plus d'informations sur la validation des certificats de banque, voir *Valider une clé bancaire*. Une fois les clés bancaires validées, le statut de la banque passe à Activé.
24. Connectez-vous au client EBICS de Sterling B2B Integrator en tant qu'utilisateur USERSUBMIT.

25. À partir du menu **Utilisateur**, sélectionnez **Soumission de commande**.
26. Sur la page Informations de commande, indiquez les valeurs ci-dessous, puis cliquez sur **Suivant**.
- Sélectionnez PARTNER dans la zone ID du partenaire
 - Sélectionnez BANK dans la zone ID de banque (ID hôte)
 - Sélectionnez Commandes techniques bancaires dans la zone Filtre de type de commande
 - Sélectionnez FUL dans la zone Type de commande
27. Indiquez les valeurs des zones conformément aux instructions du tableau ci-après, puis cliquez sur **Envoyer** :

Zone	Description
Préfixe d'ID de commande	Facultatif. Dans la liste déroulante, sélectionnez le préfixe d'ID de commande, par exemple, F. Le client EBICS alloue un ID de commande unique à chaque commande en fonction de la banque, de l'ID utilisateur et du type de commande. Le client génère l'ID de commande conformément aux spécifications EBICS. L'ID de commande est un identifiant alphanumérique à 4 chiffres. Vous pouvez indiquer le premier caractère de l'ID de commande. Les deuxième, troisième et quatrième caractères de l'ID de commande sont des caractères alphanumériques dans l'ordre croissant (A-Z ou 0-9).
Moyen de sécurité	Obligatoire. Entrez un numéro de sécurité à 4 chiffres compris entre 0499 et 0100. Par exemple, 0200.
Soumission auto	Facultatif. Applicable uniquement au type de commande FUL. Cochez la case. Si l'option de soumission automatique est sélectionnée, une commande est soumise automatiquement une fois que le nombre de signatures requis a été obtenu. Si l'option de soumission automatique n'est pas sélectionnée, un utilisateur du client EBICS doit se connecter à l'interface de tableau de bord du client EBICS, accéder à l'écran des tâches en attente et soumettre la commande une fois le nombre de signatures requis obtenu.
Lire le fichier depuis la boîte aux lettres	Pour télécharger le fichier de charge à partir de la boîte aux lettres, sélectionnez Oui . Pour télécharger le fichier de charge à partir d'un emplacement de fichier, sélectionnez Non .
Télécharger le fichier	Cliquez sur Parcourir en regard de la zone Télécharger le fichier, accédez à l'emplacement du fichier, puis sélectionnez le fichier à envoyer par téléchargement au serveur EBICS.

Zone	Description
Format de fichier	Sélectionnez pain.001.001.02.ict dans la liste déroulante.

Un message de confirmation de soumission de commande s'affiche.

28. Pour signer la commande, connectez-vous au client EBICS de Sterling B2B Integrator en tant qu'utilisateur USERSIGN.
29. Dans le menu **Afficheurs**, sélectionnez **Tâches en attente**. La commande FUL soumise par l'utilisateur USERSUBMIT figure dans la liste comme une tâche en attente. Pour plus d'informations sur les tâches en attente, voir *Tâches en attente*. Si la commande contient des attributs personnalisés, ces attributs sont visibles à l'écran. Pour plus d'informations sur les attributs personnalisés, voir *Soumettre une commande en tant qu'utilisateur technique*.
30. Cliquez sur **Signer** pour signer la commande FUL en attente ou sur **Rejeter** pour la rejeter. Si un signataire rejette la commande avant que le nombre obligatoire de signataires soit atteint, la commande n'est plus mentionnée comme tâche en attente pour les signataires et ne doit plus être traitée.
31. Si, lors de la soumission de la commande FUL, vous n'avez pas activé l'option de soumission automatique, connectez-vous au client EBICS en tant qu'utilisateur USERSUBMIT, accédez à l'écran **Tâches en attente**, puis soumettez la commande FUL signée par l'utilisateur USERSIGN.

Que faire ensuite

Pour afficher le statut (Succès, Échec, En cours ou En attente sur le client) de la commande soumise dans l'interface utilisateur du client EBICS, dans le menu **Afficheurs**, sélectionnez **Recherche de commande** puis indiquez les critères de recherche appropriés pour localiser la commande.

Types de commande

Une brève description du type de commande, la définition des paramètres spécifiés pour le type de commande ainsi qu'un exemple de schéma XML sont donnés pour les types de commande suivants.

Type de commande FUL

FUL est un type de commande standard utilisé pour la soumission des fichiers à la banque. Son utilisation garantit un transfert transparent des fichiers de tout format.

Accès

Boîte aux lettres

Description

Un utilisateur initie une transaction d'envoi par téléchargement à la banque en soumettant une demande via la commande FUL. FUL est un type de commande technique bancaire de réception par téléchargement.

Avertissement : Si vous téléchargez un grand volume de données (par ex., 200 Mo) vers le serveur EBICS en utilisant le type de commande FUL, le paramètre **Initialiser une nouvelle session HTTP pour chaque demande** des propriétés système du client EBICS doit être défini sur true. Pour modifier les propriétés système, voir «Mise à jour des valeurs des propriétés système», à la page 77.

Paramètres

Tableau 9. Paramètres de FUL

Paramètre	Description et valeur
HostID	ID de banque ou ID hôte de la banque à laquelle l'utilisateur du client EBICS a soumis la commande. Il s'agit d'un identifiant unique pour la banque dans le système de la banque.
HostUrlAlias	Lorsque vous configurez un profil de banque, vous pouvez indiquer plusieurs adresses URL d'hôte et en définir une par défaut. Si vous souhaitez envoyer une demande à une adresse URL d'hôte qui n'est pas celle par défaut, indiquez une valeur pour ce paramètre.
PartnerID	ID de partenaire associé à l'ID utilisateur.
UserID	Identifiant unique de l'utilisateur dans le système de la banque, qui correspond à l'utilisateur créé dans le tableau de bord du client EBICS.
SystemID	ID utilisateur de l'utilisateur technique. Un utilisateur technique est un délégué de l'utilisateur non technique ou physique.
orderIdPrefix	<p>Le client EBICS alloue un ID de commande unique pour chaque commande en fonction de la banque, de l'ID utilisateur et du type de commande. Le client génère l'ID de commande en fonction des spécifications EBICS. L'ID de commande est un identifiant alphanumérique à 4 chiffres. Vous pouvez indiquer le premier caractère de l'ID de commande. Les deuxième, troisième et quatrième caractères de l'ID de commande sont des caractères alphanumériques dans l'ordre croissant (A-Z ou 0-9).</p> <p>Ce paramètre est utilisé uniquement avec le protocole EBICS version H003.</p>
SecurityMedium	Numéro de sécurité à 4 chiffres compris entre 0000 et 0499.
OrderType	Type de la commande que vous soumettez. Dans ce cas, FUL est le type de commande.
FileFormat	Format de fichier associé au type de commande. Un type de commande peut ne contenir aucun format de fichier ou en contenir plusieurs. Les formats de fichier pour les types de commande FUL et FDL se basent sur le type de demande SWIFTNet.

Tableau 9. Paramètres de FUL (suite)

Paramètre	Description et valeur
autoSubmit	Ce paramètre n'est applicable qu'au type de commande FUL. Si ce paramètre est défini sur true, une commande est soumise automatiquement une fois que le nombre de signatures requis a été obtenu. Si ce paramètre est défini sur false, un utilisateur du client EBICS doit se connecter à l'interface de tableau de bord du client EBICS, accéder à l'écran des tâches en attente et soumettre la commande une fois le nombre de signatures requis obtenu.

Schéma XML

```
<?xml version="1.0" encoding="UTF-8"?>
<orderMetaData xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="new_omd.xsd">
  <HostID>SUBNKPK12</HostID>
  <HostUrlAlias>SUBNKPK12_URL_ALIAS</HostUrlAlias>
  <PartnerID>SUPKID</PartnerID>
  <UserID>SUUSER1</UserID>
  <SystemID>TECHUSER</SystemID>
  <orderIdPrefix>L</orderIdPrefix>
  <SecurityMedium>0200</SecurityMedium>
  <OrderType>FUL</OrderType>
  <FileFormat>pain.xxx.cfonb160.dtg</FileFormat>
  <autoSubmit>true</autoSubmit>
</orderMetaData>
```

Liste de paramètres

Le document *EBICS - Guide de mise en oeuvre en France* préconise d'effectuer des tests de l'échange de fichiers avant tout transfert de fichiers réels à la banque. De ce fait, le poste de travail du client doit disposer d'un paramétrage permettant le transfert de fichiers tant dans les environnements de test que dans les environnements de production. Pour distinguer les fichiers de test des fichiers de production, le nom du paramètre TEST est inclus dans la balise OrderParams pour les types de commande FUL et FDL. La balise OrderParams peut être définie dans le schéma XML orderMetaData. De la même façon, la banque et le client EBICS peuvent partager une liste des paramètres et leurs valeurs correspondantes en s'appuyant sur une compréhension mutuelle des paramètres définis dans les modalités contractuelles.

L'exemple suivant illustre un scénario d'échange des fichiers de test où la valeur de TEST est définie sur TRUE :

```
<OrderParams>
  <ParameterList>
    <Parameter>
      <Name>TEST</Name>
      <Value>TRUE</Value>
    </Parameter>
    <Parameter>
      <Name>param2</Name>
      <Value>value2</Value>
    </Parameter>
    <Parameter>
      <Name>param3</Name>
```

```

<Value>value3</Value>
  </Parameter>
</ParameterList>
</OrderParams>

```

Type de commande FDL

FDL est un type de commande standard utilisé pour les téléchargements de fichier. Son utilisation garantit un transfert transparent des fichiers de tout format.

Accès

Boîte aux lettres

Description

FDL est un type de commande technique bancaire de réception par téléchargement. Pour initier une transaction de réception par téléchargement avec la banque, un utilisateur soumet une demande de commande de réception par téléchargement (FDL).

Paramètres

Tableau 10. Paramètres de FDL

Paramètre	Description et valeur
HostID	ID de banque ou ID hôte de la banque à laquelle l'utilisateur du client EBICS a soumis la commande. Il s'agit d'un identifiant unique pour la banque dans le système de la banque.
HostUrlAlias	Lorsque vous configurez un profil de banque, vous pouvez indiquer plusieurs adresses URL d'hôte et en définir une par défaut. Si vous souhaitez envoyer une demande à une adresse URL d'hôte qui n'est pas celle par défaut, indiquez une valeur pour ce paramètre.
PartnerID	ID de partenaire associé à l'ID utilisateur.
UserID	Identifiant unique de l'utilisateur dans le système de la banque, qui correspond à l'utilisateur créé dans le tableau de bord du client EBICS.
SystemID	ID utilisateur de l'utilisateur technique. Un utilisateur technique est un délégué de l'utilisateur non technique ou physique.

Tableau 10. Paramètres de FDL (suite)

Paramètre	Description et valeur
orderIdPrefix	Le client EBICS alloue un ID de commande unique pour chaque commande en fonction de la banque, de l'ID utilisateur et du type de commande. Le client génère l'ID de commande conformément aux spécifications EBICS. L'ID de commande est un identifiant alphanumérique à 4 chiffres. Vous pouvez indiquer le premier caractère de l'ID de commande. Les deuxième, troisième et quatrième caractères de l'ID de commande sont des caractères alphanumériques dans l'ordre croissant (A-Z ou 0-9). Ce paramètre est utilisé uniquement avec le protocole EBICS version H003.
SecurityMedium	Numéro de sécurité à 4 chiffres compris entre 0000 et 0499.
OrderType	Type de la commande que vous soumettez. Dans ce cas, FDL est le type de commande.
FileFormat	Format de fichier associé au type de commande. Un type de commande peut ne contenir aucun format de fichier ou en contenir plusieurs. Les formats de fichier pour les types de commande FUL et FDL se basent sur le type de demande SWIFTNet.
DownloadDateRangeStart	Date de début du téléchargement des données de commande. Ce paramètre n'est applicable qu'au type de commande FDL.
DownloadDateRangeEnd	Date de fin du téléchargement des données de commande. Ce paramètre n'est applicable qu'au type de commande FDL.

Schéma XML

```
<?xml version="1.0" encoding="UTF-8"?>
<orderMetaData xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="new_omd.xsd">
  <HostID>BNKLCMC1</HostID>
  <HostUrlAlias>BNKLCMC1_URL_ALIAS</HostUrlAlias>
  <PartnerID>PH2LCMC1</PartnerID>
  <UserID>USERPK12</UserID>
  <SystemID>UH2LCMC1</SystemID>
  <orderIdPrefix>U</orderIdPrefix>
  <SecurityMedium>0000</SecurityMedium>
  <OrderType>FDL</OrderType>
  <FileFormat>pain.002.001.02.ack</FileFormat>
  <DownloadDateRangeStart></DownloadDateRangeStart>
  <DownloadDateRangeEnd></DownloadDateRangeEnd>
</orderMetaData>
```

Liste de paramètres

Le document *EBICS - Guide de mise en oeuvre en France* préconise d'effectuer des tests de l'échange de fichiers avant tout transfert de fichiers réels à la banque. De ce fait, le poste de travail du client doit disposer d'un paramétrage permettant le transfert de fichiers tant dans les environnements de test que dans les

environnements de production. Pour distinguer les fichiers de test des fichiers de production, le nom du paramètre TEST est inclus dans la balise OrderParams pour les types de commande FUL et FDL. La balise OrderParams peut être définie dans le schéma XML orderMetaData. De la même façon, la banque et le client EBICS peuvent partager une liste des paramètres et leurs valeurs correspondantes en s'appuyant sur une compréhension mutuelle des paramètres définis dans les modalités contractuelles.

L'exemple suivant illustre un scénario d'échange des fichiers de test où la valeur de TEST est définie sur TRUE :

```
<OrderParams>
<ParameterList>
  <Parameter>
    <Name>TEST</Name>
    <Value>TRUE</Value>
  </Parameter>
  <Parameter>
    <Name>param2</Name>
    <Value>value2</Value>
  </Parameter>
  <Parameter>
    <Name>param3</Name>
    <Value>value3</Value>
  </Parameter>
</ParameterList>
</OrderParams>
```

Type de commande INI

L'utilisateur du client EBICS partage les clés publiques pour la signature électronique avec la banque via le type de commande INI (Initialisation).

Accès

Boîte aux lettres

Description

INI est un type de commande de gestion de clés d'envoi par téléchargement, utilisé pour l'initialisation de l'abonné. Il permet d'envoyer le certificat technique bancaire public d'un client à la banque. Les données de commande sont compressées et codées en base64.

Les certificats autosignés ne peuvent pas être utilisés pour les signatures électroniques et donc pour l'initialisation de l'utilisateur (type de commande INI). Un utilisateur du client EBICS qui utilise des certificats autosignés pour l'identification, l'authentification et le chiffrement doit utiliser des certificats d'autorité de certification pour les signatures électroniques.

Paramètres

Tableau 11. Paramètres de INI

Paramètre	Description et valeur
HostID	ID de banque ou ID hôte de la banque à laquelle l'utilisateur du client EBICS a soumis la commande. Il s'agit d'un identifiant unique pour la banque dans le système de la banque.

Tableau 11. Paramètres de INI (suite)

Paramètre	Description et valeur
HostUrlAlias	Lorsque vous configurez un profil de banque, vous pouvez indiquer plusieurs adresses URL d'hôte et en définir une par défaut. Si vous souhaitez envoyer une demande à une adresse URL d'hôte qui n'est pas celle par défaut, indiquez une valeur pour ce paramètre.
PartnerID	ID de partenaire associé à l'ID utilisateur.
UserID	Identifiant unique de l'utilisateur dans le système de la banque, qui correspond à l'utilisateur créé dans le tableau de bord du client EBICS.
SystemID	ID utilisateur de l'utilisateur technique. Le type de commande INI peut être soumis par un utilisateur technique qui est un délégué de l'utilisateur physique ou non technique. Par conséquent, la valeur du paramètre UserID est la même que celle du paramètre systemID.
orderIdPrefix	Le client EBICS alloue un ID de commande unique pour chaque commande en fonction de la banque, de l'ID utilisateur et du type de commande. Le client génère l'ID de commande conformément aux spécifications EBICS. L'ID de commande est un identifiant alphanumérique à 4 chiffres. Vous pouvez indiquer le premier caractère de l'ID de commande. Les deuxième, troisième et quatrième caractères de l'ID de commande sont des caractères alphanumériques dans l'ordre croissant (A-Z ou 0-9). Ce paramètre est utilisé uniquement avec le protocole EBICS version H003.
SecurityMedium	Numéro de sécurité à 4 chiffres compris entre 0100 et 0499. La valeur ne peut pas être modifiée pour les types de commande INI, HIA et HPB.
OrderType	Type de la commande que vous soumettez. Dans ce cas, INI est le type de commande.

Schéma XML

```
<?xml version="1.0" encoding="UTF-8"?>
<orderMetaData xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="new_omd.xsd">
  <HostID>SUBNPK12</HostID>
  <HostUrlAlias>SUBNPK12_URL_ALIAS</HostUrlAlias>
  <PartnerID>SUPKID</PartnerID>
  <UserID>TECHUSER</UserID>
  <SystemID>TECHUSER</SystemID>
  <orderIdPrefix>S</orderIdPrefix>
  <SecurityMedium>0200</SecurityMedium>
  <OrderType>INI</OrderType>
</orderMetaData>
```

Type de commande HIA

L'utilisateur du client EBICS partage les clés publiques pour l'identification, l'authentification et le chiffrement avec la banque via le type de commande HIA.

Accès

Boîte aux lettres

Description

HIA est un type de commande de gestion de clés d'envoi par téléchargement. HIA permet de transmettre des certificats publics d'utilisateur pour l'identification, l'authentification et le chiffrement afin que l'utilisateur puisse effectuer des opérations avec la banque. Les données de commande sont compressées et codées en base64.

Paramètres

Tableau 12. Paramètres de HIA

Paramètre	Description et valeur
HostID	ID de banque ou ID hôte de la banque à laquelle l'utilisateur du client EBICS a soumis la commande. Il s'agit d'un identifiant unique pour la banque dans le système de la banque.
HostUrlAlias	Lorsque vous configurez un profil de banque, vous pouvez indiquer plusieurs adresses URL d'hôte et en définir une par défaut. Si vous souhaitez envoyer une demande à une adresse URL d'hôte qui n'est pas celle par défaut, indiquez une valeur pour ce paramètre.
PartnerID	ID de partenaire associé à l'ID utilisateur.
UserID	Identifiant unique de l'utilisateur dans le système de la banque, qui correspond à l'utilisateur créé dans le tableau de bord du client EBICS.
SystemID	ID utilisateur de l'utilisateur technique. Le type de commande HIA peut être soumis par un utilisateur technique qui est un délégué de l'utilisateur physique ou non technique. Par conséquent, la valeur du paramètre UserID est la même que celle du paramètre systemID.

Tableau 12. Paramètres de HIA (suite)

Paramètre	Description et valeur
orderIdPrefix	Le client EBICS alloue un ID de commande unique pour chaque commande en fonction de la banque, de l'ID utilisateur et du type de commande. Le client génère l'ID de commande conformément aux spécifications EBICS. L'ID de commande est un identifiant alphanumérique à 4 chiffres. Vous pouvez indiquer le premier caractère de l'ID de commande. Les deuxième, troisième et quatrième caractères de l'ID de commande sont des caractères alphanumériques dans l'ordre croissant (A-Z ou 0-9). Ce paramètre est utilisé uniquement avec le protocole EBICS version H003.
SecurityMedium	Numéro de sécurité à 4 chiffres compris entre 0100 et 0499. La valeur ne peut pas être modifiée pour les types de commande INI, HIA et HPB.
OrderType	Type de la commande que vous soumettez. Dans ce cas, HIA est le type de commande.

Schéma XML

```
<?xml version="1.0" encoding="UTF-8"?>
<orderMetaData xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="new_omd.xsd">
  <HostID>SUBNKPK12</HostID>
  <HostUrlAlias>SUBNKPK12_URL_ALIAS</HostUrlAlias>
  <PartnerID>SUPKID</PartnerID>
  <UserID>TECHUSER</UserID>
  <SystemID>TECHUSER</SystemID>
  <orderIdPrefix>W</orderIdPrefix>
  <SecurityMedium>0000</SecurityMedium>
  <OrderType>HIA</OrderType>
</orderMetaData>
```

Type de commande H3K

Le type de commande H3K permet de partager les certificats publics pour la signature électronique, l'identification et l'authentification, et le chiffrement avec la banque.

Accès

Boîte aux lettres

Description

H3K est un type de commande de gestion de clés d'envoi par téléchargement. H3K permet de transmettre des certificats publics d'utilisateur pour la signature publique, l'identification, l'authentification et le chiffrement afin que l'utilisateur puisse effectuer des opérations avec la banque.

Paramètres

Tableau 13. Paramètres H3K

Paramètre	Description et valeur
HostID	ID de banque ou ID hôte de la banque à laquelle l'utilisateur du client EBICS a soumis la commande. Il s'agit d'un identifiant unique pour la banque dans le système de la banque.
HostUrlAlias	Lorsque vous configurez un profil de banque, vous pouvez indiquer plusieurs adresses URL d'hôte et en définir une par défaut. Si vous souhaitez envoyer une demande à une adresse URL d'hôte qui n'est pas celle par défaut, indiquez une valeur pour ce paramètre.
PartnerID	ID de partenaire associé à l'ID utilisateur.
UserID	Identifiant unique de l'utilisateur dans le système de la banque, qui correspond à l'utilisateur créé dans le tableau de bord du client EBICS.
SystemID	ID utilisateur de l'utilisateur technique. Le type de commande H3K peut être soumis par un utilisateur technique qui est un délégué de l'utilisateur physique ou non technique. Par conséquent, la valeur du paramètre UserID est la même que celle du paramètre SystemID.
SecurityMedium	Numéro de sécurité à 4 chiffres compris entre 0000 et 0499.
OrderType	Type de la commande que vous soumettez. Dans ce cas, H3K est le type de commande.

Schéma XML

```
<?xml version="1.0" encoding="UTF-8"?>
<orderMetaData xmlns:ns2="partnerInfo">
  <HostID>SUBNPK12</HostID>
  <HostUrlAlias>SUBNPK12_URL_ALIAS</HostUrlAlias>
  <PartnerID>SUPKID</PartnerID>
  <UserID>TECHUSER</UserID>
  <SystemID>TECHUSER</SystemID>
  <SecurityMedium>0200</SecurityMedium>
  <OrderType>H3K</OrderType>
</orderMetaData>
```

Type de commande HPB

Le type de commande HPB permet à l'utilisateur du client EBICS de recevoir par téléchargement les certificats publics de la banque.

Accès

Boîte aux lettres

Description

HPB est un type de commande de gestion de clés par téléchargement (download). L'utilisateur soumet une demande de commande HPB pour recevoir, par téléchargement, les certificats publiques de la banque. Après avoir validé les clés d'authentification et d'identification de l'utilisateur, la banque envoie une réponse HPB. Cette réponse contient les clés bancaires publiques. L'utilisateur valide les clés bancaires par rapport aux valeurs de hachage générées en interne. À l'issue de la validation, le statut de la banque passe à Activé, ce qui indique que le partenaire et ses utilisateurs associés peuvent désormais effectuer des opérations avec la banque.

Les données de commande sont compressées, chiffrées et codées en base64. Le message de réponse et les données de commande ne sont pas signés.

Paramètres

Tableau 14. Paramètres de HPB

Paramètre	Description et valeur
HostID	ID de banque ou ID hôte de la banque à laquelle l'utilisateur du client EBICS a soumis la commande. Il s'agit d'un identifiant unique pour la banque dans le système de la banque.
HostUrlAlias	Lorsque vous configurez un profil de banque, vous pouvez indiquer plusieurs adresses URL d'hôte et en définir une par défaut. Si vous souhaitez envoyer une demande à une adresse URL d'hôte qui n'est pas celle par défaut, indiquez une valeur pour ce paramètre.
PartnerID	ID de partenaire associé à l'ID utilisateur.
UserID	Identifiant unique de l'utilisateur dans le système de la banque, qui correspond à l'utilisateur créé dans le tableau de bord du client EBICS.
SystemID	ID utilisateur de l'utilisateur technique. Un utilisateur technique est un délégué de l'utilisateur non technique ou physique.
orderIdPrefix	<p>Le client EBICS alloue un ID de commande unique pour chaque commande en fonction de la banque, de l'ID utilisateur et du type de commande. Le client génère l'ID de commande conformément aux spécifications EBICS. L'ID de commande est un identifiant alphanumérique à 4 chiffres. Vous pouvez indiquer le premier caractère de l'ID de commande. Les deuxième, troisième et quatrième caractères de l'ID de commande sont des caractères alphanumériques dans l'ordre croissant (A-Z ou 0-9).</p> <p>Ce paramètre est utilisé uniquement avec le protocole EBICS version H003.</p>

Tableau 14. Paramètres de HPB (suite)

Paramètre	Description et valeur
SecurityMedium	Numéro de sécurité à 4 chiffres compris entre 0100 et 0499. La valeur ne peut pas être modifiée pour les types de commande INI, HIA et HPB. Le moyen de sécurité utilisé pour la clé technique bancaire de l'abonné est 0000 puisque les commandes HPB ne nécessitent pas de signatures électroniques et ne transmettent pas les clés techniques bancaires de l'abonné.
OrderType	Type de la commande que vous soumettez. Dans ce cas, HPB est le type de commande.

Schéma XML

```
<?xml version="1.0" encoding="UTF-8"?>
<orderMetaData xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="new_omd.xsd">
  <HostID>BNKLCMC1</HostID>
  <HostUrlAlias>BNKLCMC1_URL_ALIAS</HostUrlAlias>
  <PartnerID>PH2LCMC1</PartnerID>
  <UserID>UH2LCMC1</UserID>
  <SystemID>UH2LCMC1</SystemID>
  <orderIdPrefix>C</orderIdPrefix>
  <SecurityMedium>0000</SecurityMedium>
  <OrderType>HPB</OrderType>
</orderMetaData>
```

Type de commande HKD

Le type de commande HKD permet à l'utilisateur de recevoir par téléchargement les données du client et les données de l'abonné.

Accès

Boîte aux lettres

Description

HKD est un type de commande de gestion de clés par téléchargement (download). Il permet de recevoir par téléchargement des informations concernant un partenaire et les abonnés associés stockés par la banque, notamment des informations sur votre société. Les données de commande sont compressées et codées en base64.

Paramètres

Tableau 15. Paramètres de HKD

Paramètre	Description et valeur
HostID	ID de banque ou ID hôte de la banque à laquelle l'utilisateur du client EBICS a soumis la commande. Il s'agit d'un identifiant unique pour la banque dans le système de la banque.

Tableau 15. Paramètres de HKD (suite)

Paramètre	Description et valeur
HostUrlAlias	Lorsque vous configurez un profil de banque, vous pouvez indiquer plusieurs adresses URL d'hôte et en définir une par défaut. Si vous souhaitez envoyer une demande à une adresse URL d'hôte qui n'est pas celle par défaut, indiquez une valeur pour ce paramètre.
PartnerID	ID de partenaire associé à l'ID utilisateur.
UserID	Identifiant unique de l'utilisateur dans le système de la banque, qui correspond à l'utilisateur créé dans le tableau de bord du client EBICS.
SystemID	ID utilisateur de l'utilisateur technique. Un utilisateur technique est un délégué de l'utilisateur non technique ou physique.
orderIdPrefix	Le client EBICS alloue un ID de commande unique pour chaque commande en fonction de la banque, de l'ID utilisateur et du type de commande. Le client génère l'ID de commande conformément aux spécifications EBICS. L'ID de commande est un identifiant alphanumérique à 4 chiffres. Vous pouvez indiquer le premier caractère de l'ID de commande. Les deuxième, troisième et quatrième caractères de l'ID de commande sont des caractères alphanumériques dans l'ordre croissant (A-Z ou 0-9). Ce paramètre est utilisé uniquement avec le protocole EBICS version H003.
SecurityMedium	Numéro de sécurité à 4 chiffres compris entre 0000 et 0499.
OrderType	Type de la commande que vous soumettez. Dans ce cas, HKD est le type de commande.

Schéma XML

```
<?xml version="1.0" encoding="UTF-8"?>
<orderMetaData>
  <HostID>BNKLCMC1</HostID>
  <HostUrlAlias>BNKLCMC1_URL_ALIAS</HostUrlAlias>
  <PartnerID>PH2LCMC1</PartnerID>
  <UserID>USERPK12</UserID>
  <SystemID>UH2LCMC1</SystemID>
  <orderIdPrefix>H</orderIdPrefix>
  <SecurityMedium>0200</SecurityMedium>
  <OrderType>HKD</OrderType>
</orderMetaData>
```

Type de commande HTD

Le type de commande HTD permet à l'utilisateur de recevoir par téléchargement les données de client et les données d'abonné.

Accès

Boîte aux lettres

Description

HTD est un type de commande de gestion de clés de réception par téléchargement. Il permet à l'abonné de récupérer des informations stockées par la banque le concernant ou concernant sa société. Cependant, à la différence de la commande HKD, l'abonné ne peut pas récupérer des informations concernant d'autres abonnés de la société. Les données de commande sont compressées et codées en base64.

Paramètres

Tableau 16. Paramètres de HTD

Paramètre	Description et valeur
HostID	ID de banque ou ID hôte de la banque à laquelle l'utilisateur du client EBICS a soumis la commande. Il s'agit d'un identifiant unique pour la banque dans le système de la banque.
HostUrlAlias	Lorsque vous configurez un profil de banque, vous pouvez indiquer plusieurs adresses URL d'hôte et en définir une par défaut. Si vous souhaitez envoyer une demande à une adresse URL d'hôte qui n'est pas celle par défaut, indiquez une valeur pour ce paramètre.
PartnerID	ID de partenaire associé à l'ID utilisateur.
UserID	Identifiant unique de l'utilisateur dans le système de la banque, qui correspond à l'utilisateur créé dans le tableau de bord du client EBICS.
SystemID	ID utilisateur de l'utilisateur technique. Un utilisateur technique est un délégué de l'utilisateur non technique ou physique.
orderIdPrefix	Le client EBICS alloue un ID de commande unique pour chaque commande en fonction de la banque, de l'ID utilisateur et du type de commande. Le client génère l'ID de commande conformément aux spécifications EBICS. L'ID de commande est un identifiant alphanumérique à 4 chiffres. Vous pouvez indiquer le premier caractère de l'ID de commande. Les deuxième, troisième et quatrième caractères de l'ID de commande sont des caractères alphanumériques dans l'ordre croissant (A-Z ou 0-9). Ce paramètre est utilisé uniquement avec le protocole EBICS version H003.
SecurityMedium	Numéro de sécurité à 4 chiffres compris entre 0000 et 0499.
OrderType	Type de la commande que vous soumettez. Dans ce cas, HTD est le type de commande.

Schéma XML

```
<?xml version="1.0" encoding="UTF-8"?>
<orderMetaData>
  <HostID>BNKLCMC1</HostID>
  <HostUrlAlias>BNKLCMC1_URL_ALIAS</HostUrlAlias>
  <PartnerID>PH2LCMC1</PartnerID>
  <UserID>USERPK12</UserID>
  <SystemID>UH2LCMC1</SystemID>
  <orderIdPrefix>Z</orderIdPrefix>
  <SecurityMedium>0000</SecurityMedium>
  <OrderType>HTD</OrderType>
</orderMetaData>
```

Type de commande HEV

Le type de commande HEV permet à l'utilisateur de recevoir par téléchargement les versions EBICS prises en charge par la banque.

Accès

Boîte aux lettres

Description

HEV est un type de commande de gestion de clés par téléchargement (download). En soumettant une demande HEV à la banque, l'utilisateur souhaite recevoir la liste des versions EBICS prises en charge. La banque envoie alors une réponse contenant la liste des versions EBICS prises en charge et la version du schéma approprié.

Paramètres

Tableau 17. Paramètres de HEV

Paramètre	Description et valeur
HostID	ID de banque ou ID hôte de la banque à laquelle l'utilisateur du client EBICS a soumis la commande. Il s'agit d'un identifiant unique pour la banque dans le système de la banque.
HostUrlAlias	Lorsque vous configurez un profil de banque, vous pouvez indiquer plusieurs adresses URL d'hôte et en définir une par défaut. Si vous souhaitez envoyer une demande à une adresse URL d'hôte qui n'est pas celle par défaut, indiquez une valeur pour ce paramètre.
PartnerID	ID de partenaire associé à l'ID utilisateur.
UserID	Identifiant unique de l'utilisateur dans le système de la banque, qui correspond à l'utilisateur créé dans le tableau de bord du client EBICS.
SystemID	ID utilisateur de l'utilisateur technique. Un utilisateur technique est un délégué de l'utilisateur non technique ou physique.
OrderType	Type de la commande que vous soumettez. Dans ce cas, HEV est le type de commande.

Schéma XML

```
<?xml version="1.0" encoding="UTF-8"?>
<orderMetaData xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="new_omd.xsd">
  <HostID>BNKLCMC1</HostID>
  <HostUrlAlias>BNKLCMC1_URL_ALIAS</HostUrlAlias>
  <PartnerID>PH2LCMC1</PartnerID>
  <UserID>USERPK12</UserID>
  <SystemID>UH2LCMC1</SystemID>
  <OrderType>HEV</OrderType>
</orderMetaData>
```

Type de commande PUB

Utilisez le type de commande PUB afin d'envoyer une clé publique pour vérification de la signature.

Accès

Boîte aux lettres

Description

PUB est un type de commande de gestion de clés d'envoi par téléchargement qui permet de mettre à jour le certificat d'un client et d'envoyer le certificat public à la banque. Les données de commande sont signées, compressées, chiffrées et codées en base64.

Paramètres

Tableau 18. Paramètres de PUB

Paramètre	Description et valeur
HostID	ID de banque ou ID hôte de la banque à laquelle l'utilisateur du client EBICS a soumis la commande. Il s'agit d'un identifiant unique pour la banque dans le système de la banque.
HostUrlAlias	Lorsque vous configurez un profil de banque, vous pouvez indiquer plusieurs adresses URL d'hôte et en définir une par défaut. Si vous souhaitez envoyer une demande à une adresse URL d'hôte qui n'est pas celle par défaut, indiquez une valeur pour ce paramètre.
PartnerID	ID de partenaire associé à l>ID utilisateur.
UserID	Identifiant unique de l'utilisateur dans le système de la banque, qui correspond à l'utilisateur créé dans le tableau de bord du client EBICS.
SystemID	ID utilisateur de l'utilisateur technique. Le type de commande PUB peut être soumis par un utilisateur technique qui est un délégué de l'utilisateur physique ou non technique. Par conséquent, la valeur du paramètre UserID est la même que celle du paramètre systemID.

Tableau 18. Paramètres de PUB (suite)

Paramètre	Description et valeur
orderIdPrefix	<p>Le client EBICS alloue un ID de commande unique pour chaque commande en fonction de la banque, de l'ID utilisateur et du type de commande. Le client génère l'ID de commande conformément aux spécifications EBICS. L'ID de commande est un identifiant alphanumérique à 4 chiffres. Vous pouvez indiquer le premier caractère de l'ID de commande. Les deuxième, troisième et quatrième caractères de l'ID de commande sont des caractères alphanumériques dans l'ordre croissant (A-Z ou 0-9).</p> <p>Ce paramètre est utilisé uniquement avec le protocole EBICS version H003.</p>
SecurityMedium	<p>Numéro de sécurité à 4 chiffres compris entre 0000 et 0499. La valeur ne peut pas être modifiée pour les types de commande INI, HIA et HPB. Le moyen de sécurité utilisé pour la clé technique bancaire de l'abonné est 0000 puisque les commandes HPB ne nécessitent pas de signatures électroniques et ne transmettent pas les clés techniques bancaires de l'abonné.</p>
OrderType	<p>Type de la commande que vous soumettez. Dans ce cas, PUB est le type de commande.</p>
UserSignNewPubKeyAlias	<p>Alias de la clé publique du nouveau certificat de signature électronique à mettre à jour pour l'utilisateur.</p>
UserSignNewPubKeyID	<p>ID du nouveau certificat public de signature électronique à mettre à jour pour l'utilisateur.</p>
UserSignNewPriKeyAlias	<p>Alias de la clé privée du nouveau certificat de signature électronique à mettre à jour pour l'utilisateur. Définissez ce paramètre si vous n'utilisez pas une clé matérielle pour la signature électronique. La banque doit posséder la partie publique de la clé pour valider l'autorisation.</p>
UserSignNewPriKeyID	<p>ID du nouveau certificat privé de signature électronique (ES) à mettre à jour pour l'utilisateur. Définissez ce paramètre si vous n'utilisez pas une clé matérielle pour la signature électronique.</p>
UserNewSignatureVersion	<p>Version de la clé de la nouvelle signature électronique à mettre à jour pour l'utilisateur. Les valeurs valides sont A005 ou A006. Si vous utilisez un magasin de clés matérielles pour la signature électronique, la version de la clé est définie sur A005 et ne peut pas être modifiée.</p>

Schéma XML

```
<?xml version="1.0" encoding="UTF-8"?>
<orderMetaData xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="new_omd.xsd">
  <HostID>BNKLCMC1</HostID>
  <HostUrlAlias>BNKLCMC1_URL_ALIAS</HostUrlAlias>
  <PartnerID>PH2LCMC1</PartnerID>
  <UserID>UH2LCMC1</UserID>
  <SystemID>UH2LCMC1</SystemID>
  <orderIdPrefix>G</orderIdPrefix>
  <SecurityMedium>0200</SecurityMedium>
  <OrderType>PUB</OrderType>
  <UserSignNewPubKeyAlias>CAEBSignBSaiPub</UserSignNewPubKeyAlias>
  <UserSignNewPubKeyID>blrgislin32:node1:12e961909b2:10417097</UserSignNewPubKeyID>
  <UserSignNewPriKeyAlias>CAEBSignBSaiPriv</UserSignNewPriKeyAlias>
  <UserSignNewPriKeyID>blrgislin32:node1:12e961909b2:10415111</UserSignNewPriKeyID>
  <UserNewSignatureVersion>A005</UserNewSignatureVersion>
</orderMetaData>
```

Type de commande HCS

Le type de commande HCS permet de modifier les clés d'abonné pour la signature électronique, l'identification et l'authentification ainsi que le chiffrement.

Accès

Boîte aux lettres

Description

HCS est un type de commande de gestion de clés d'envoi par téléchargement qui a été introduit pour permettre la modification des trois clés dans une transaction unique. Ces trois clés incluent la signature électronique technique bancaire (PUB), la signature d'identification et d'authentification ainsi que le chiffrement (HCA). De ce fait, le type de commande HCS comprend les types de commande PUB et HCA. Les types de commande PUB et HCA peuvent être utilisés à la place de HCS.

Paramètres

Tableau 19. Paramètres de HCS

Paramètre	Description et valeur
HostID	ID de banque ou ID hôte de la banque à laquelle l'utilisateur du client EBICS a soumis la commande. Il s'agit d'un identifiant unique pour la banque dans le système de la banque.
HostUrlAlias	Lorsque vous configurez un profil de banque, vous pouvez indiquer plusieurs adresses URL d'hôte et en définir une par défaut. Si vous souhaitez envoyer une demande à une adresse URL d'hôte qui n'est pas celle par défaut, indiquez une valeur pour ce paramètre.
PartnerID	ID de partenaire associé à l'ID utilisateur.
UserID	Identifiant unique de l'utilisateur dans le système de la banque, qui correspond à l'utilisateur créé dans le tableau de bord du client EBICS.

Tableau 19. Paramètres de HCS (suite)

Paramètre	Description et valeur
SystemID	ID utilisateur de l'utilisateur technique. Le type de commande PUB peut être soumis par un utilisateur technique qui est un délégué de l'utilisateur physique ou non technique. Par conséquent, la valeur du paramètre UserID est la même que celle du paramètre systemID.
orderIdPrefix	Le client EBICS alloue un ID de commande unique pour chaque commande en fonction de la banque, de l'ID utilisateur et du type de commande. Le client génère l'ID de commande conformément aux spécifications EBICS. L'ID de commande est un identifiant alphanumérique à 4 chiffres. Vous pouvez indiquer le premier caractère de l'ID de commande. Les deuxième, troisième et quatrième caractères de l'ID de commande sont des caractères alphanumériques dans l'ordre croissant (A-Z ou 0-9). Ce paramètre est utilisé uniquement avec le protocole EBICS version H003.
SecurityMedium	Numéro de sécurité à 4 chiffres compris entre 0000 et 0499. La valeur ne peut pas être modifiée pour les types de commande INI, HIA et HPB. Le moyen de sécurité utilisé pour la clé technique bancaire de l'abonné est 0000 puisque les commandes HPB ne nécessitent pas de signatures électroniques et ne transmettent pas les clés techniques bancaires de l'abonné.
OrderType	Type de la commande que vous soumettez. Dans ce cas, HCS est le type de commande.
UserSignNewPubKeyAlias	Alias de la clé publique du nouveau certificat de signature électronique à mettre à jour pour l'utilisateur.
UserSignNewPubKeyID	ID du nouveau certificat public de signature électronique à mettre à jour pour l'utilisateur.
UserSignNewPriKeyAlias	Alias de la clé privée du nouveau certificat de signature électronique à mettre à jour pour l'utilisateur. Définissez ce paramètre si vous n'utilisez pas une clé matérielle pour la signature électronique. La banque doit posséder la partie publique de la clé pour valider l'autorisation.
UserSignNewPriKeyID	ID du nouveau certificat privé de signature électronique (ES) à mettre à jour pour l'utilisateur. Définissez ce paramètre si vous n'utilisez pas une clé matérielle pour la signature électronique.

Tableau 19. Paramètres de HCS (suite)

Paramètre	Description et valeur
UserAuthNewPubKeyAlias	Alias du nouveau certificat public d'authentification à mettre à jour pour l'utilisateur. Désigne la clé publique que l'utilisateur fournit à la banque pour valider l'autorisation de l'utilisateur dans la demande du client EBICS. Le partenaire commercial ou l'utilisateur partage la clé avec la banque.
UserAuthNewPubKeyID	ID du nouveau certificat public d'authentification à mettre à jour pour l'utilisateur.
UserAuthNewPriKeyAlias	Alias du nouveau certificat privé d'authentification à mettre à jour pour l'utilisateur. Désigne la clé privée que le client EBICS utilise pour créer une signature numérique pour l'utilisateur dans la demande envoyée à la banque. La banque doit posséder la partie publique de la clé pour valider l'autorisation.
UserAuthNewPriKeyID	ID du nouveau certificat privé d'authentification à mettre à jour pour l'utilisateur.
UserEncrNewPubKeyAlias	Alias du nouveau certificat public de chiffrement à mettre à jour pour l'utilisateur. Désigne la partie publique du certificat de système qui est sélectionné comme certificat privé de chiffrement. Le partenaire commercial ou l'utilisateur partage la clé avec la banque.
UserEncrNewPubKeyID	ID du nouveau certificat public de chiffrement à mettre à jour pour l'utilisateur.
UserEncrNewPriKeyAlias	Alias du nouveau certificat privé de chiffrement à mettre à jour pour l'utilisateur. Désigne la clé privée que le client EBICS utilise pour déchiffrer la réponse reçue de la banque.
UserEncrNewPriKeyID	ID du nouveau certificat privé de chiffrement à mettre à jour pour l'utilisateur.
UserNewSignatureVersion	Version de la clé de la nouvelle signature électronique à mettre à jour pour l'utilisateur. Les valeurs valides sont A005 ou A006. Si vous utilisez un magasin de clés matérielles pour la signature électronique, la version de la clé est définie sur A005 et ne peut pas être modifiée.
UserNewAuthVersion	La version de la clé du certificat d'authentification est X002.
UserNewEncVersion	La version de la clé du certificat de chiffrement est E002.

Schéma XML

```
<?xml version="1.0" encoding="UTF-8"?>
<orderMetaData xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="new_omd.xsd">
  <HostID>BNKLCMC1</HostID>
  <HostUr1Alias>BNKLCMC1_URL_ALIAS</HostUr1Alias>
  <PartnerID>PH2LCMC1</PartnerID>
  <UserID>UH2LCMC1</UserID>
  <SystemID>UH2LCMC1</SystemID>
  <orderIdPrefix>J</orderIdPrefix>
  <SecurityMedium>0200</SecurityMedium>
  <OrderType>HCS</OrderType>
  <UserSignNewPubKeyAlias>CAEBSignASaiPub</UserSignNewPubKeyAlias>
  <UserSignNewPubKeyID>b1rgis1in32:node1:12e961909b2:10416964</UserSignNewPubKeyID>
  <UserSignNewPriKeyAlias>CAEBSignASaiPriv</UserSignNewPriKeyAlias>
  <UserSignNewPriKeyID>b1rgis1in32:node1:12e961909b2:10414702</UserSignNewPriKeyID>
  <UserAuthNewPubKeyAlias>CAEBAuthSaiPub</UserAuthNewPubKeyAlias>
  <UserAuthNewPubKeyID>b1rgis1in32:node1:12e961909b2:10416444</UserAuthNewPubKeyID>
  <UserAuthNewPriKeyAlias>CAEBAuthSaiPriv</UserAuthNewPriKeyAlias>
  <UserAuthNewPriKeyID>b1rgis1in32:node1:12e961909b2:10413399</UserAuthNewPriKeyID>
  <UserEncrNewPubKeyAlias>CAEBEncrSaiPub</UserEncrNewPubKeyAlias>
  <UserEncrNewPubKeyID>b1rgis1in32:node1:12e961909b2:10416577</UserEncrNewPubKeyID>
  <UserEncrNewPriKeyAlias>CAEBEncrSaiPriv</UserEncrNewPriKeyAlias>
  <UserEncrNewPriKeyID>b1rgis1in32:node1:12e961909b2:10414316</UserEncrNewPriKeyID>
  <UserNewSignatureVersion>A005</UserNewSignatureVersion>
  <UserNewAuthVersion>X002</UserNewAuthVersion>
  <UserNewEncVersion>E002</UserNewEncVersion>
</orderMetaData>
```

Type de commande HCA

Le type de commande HCA permet d'envoyer une modification de la clé de l'abonné pour identification, authentification et chiffrement.

Accès

Boîte aux lettres

Description

HCA est un type de commande de gestion de clés d'envoi par téléchargement qui permet de mettre à jour le certificat d'un client identification, authentification et chiffrement. Les données de commande sont signées, compressées, chiffrées et codées en base64.

Paramètres

Tableau 20. Paramètres de HCA

Paramètre	Description et valeur
HostID	ID de banque ou ID hôte de la banque à laquelle l'utilisateur du client EBICS a soumis la commande. Il s'agit d'un identifiant unique pour la banque dans le système de la banque.

Tableau 20. Paramètres de HCA (suite)

Paramètre	Description et valeur
HostUrlAlias	Lorsque vous configurez un profil de banque, vous pouvez indiquer plusieurs adresses URL d'hôte et en définir une par défaut. Si vous souhaitez envoyer une demande à une adresse URL d'hôte qui n'est pas celle par défaut, indiquez une valeur pour ce paramètre.
PartnerID	ID de partenaire associé à l'ID utilisateur.
UserID	Identifiant unique de l'utilisateur dans le système de la banque, qui correspond à l'utilisateur créé dans le tableau de bord du client EBICS.
SystemID	ID utilisateur de l'utilisateur technique. Le type de commande HCA peut être soumis par un utilisateur technique qui est un délégué de l'utilisateur physique ou non technique. Par conséquent, la valeur du paramètre UserID est la même que celle du paramètre systemID.
orderIdPrefix	<p>Le client EBICS alloue un ID de commande unique pour chaque commande en fonction de la banque, de l'ID utilisateur et du type de commande. Le client génère l'ID de commande conformément aux spécifications EBICS. L'ID de commande est un identifiant alphanumérique à 4 chiffres. Vous pouvez indiquer le premier caractère de l'ID de commande. Les deuxième, troisième et quatrième caractères de l'ID de commande sont des caractères alphanumériques dans l'ordre croissant (A-Z ou 0-9).</p> <p>Ce paramètre est utilisé uniquement avec le protocole EBICS version H003.</p>
SecurityMedium	Numéro de sécurité à 4 chiffres compris entre 0000 et 0499. La valeur ne peut pas être modifiée pour les types de commande INI, HIA et HPB. Le moyen de sécurité utilisé pour la clé technique bancaire de l'abonné est 0000 puisque les commandes HPB ne nécessitent pas de signatures électroniques et ne transmettent pas les clés techniques bancaires de l'abonné.
OrderType	Type de la commande que vous soumettez. Dans ce cas, HCA est le type de commande.
UserAuthNewPubKeyAlias	Alias du nouveau certificat public d'authentification à mettre à jour pour l'utilisateur. Désigne la clé publique que l'utilisateur fournit à la banque pour valider l'autorisation de l'utilisateur dans la demande du client EBICS. Le partenaire commercial ou l'utilisateur partage la clé avec la banque.

Tableau 20. Paramètres de HCA (suite)

Paramètre	Description et valeur
UserAuthNewPubKeyID	ID du nouveau certificat public d'authentification à mettre à jour pour l'utilisateur.
UserAuthNewPriKeyAlias	Alias du nouveau certificat privé d'authentification à mettre à jour pour l'utilisateur. Désigne la clé privée que le client EBICS utilise pour créer une signature numérique pour l'utilisateur dans la demande envoyée à la banque. La banque doit posséder la partie publique de la clé pour valider l'autorisation.
UserAuthNewPriKeyID	ID du nouveau certificat privé d'authentification à mettre à jour pour l'utilisateur.
UserEncrNewPubKeyAlias	Alias du nouveau certificat public de chiffrement à mettre à jour pour l'utilisateur. Désigne la partie publique du certificat de système qui est sélectionné comme certificat privé de chiffrement. Le partenaire commercial ou l'utilisateur partage la clé avec la banque.
UserEncrNewPubKeyID	ID du nouveau certificat public de chiffrement à mettre à jour pour l'utilisateur.
UserEncrNewPriKeyAlias	Alias du nouveau certificat privé de chiffrement à mettre à jour pour l'utilisateur. Désigne la clé privée que le client EBICS utilise pour déchiffrer la réponse reçue de la banque.
UserEncrNewPriKeyID	ID du nouveau certificat privé de chiffrement à mettre à jour pour l'utilisateur.
UserNewAuthVersion	La version de la clé du certificat d'authentification est X002.
UserNewEncVersion	La version de la clé du certificat de chiffrement est E002.

Schéma XML

```
<?xml version="1.0" encoding="UTF-8"?>
<orderMetaData xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="new_omd.xsd">
  <HostID>BNKLCMC1</HostID>
  <HostUr1Alias>BNKLCMC1_URL_ALIASE</HostUr1Alias>
  <PartnerID>PH2LCMC1</PartnerID>
  <UserID>UH2LCMC1</UserID>
  <SystemID>UH2LCMC1</SystemID>
  <orderIdPrefix>E</orderIdPrefix>
  <SecurityMedium>0200</SecurityMedium>
  <OrderType>HCA</OrderType>
  <UserAuthNewPubKeyAlias>CAEBAAuthLMPub</UserAuthNewPubKeyAlias>
  <UserAuthNewPubKeyID>270:3290569:130ae100679:goldie:node1</UserAuthNewPubKeyID>
  <UserAuthNewPriKeyAlias>CAEBAAuthLMPriv</UserAuthNewPriKeyAlias>
  <UserAuthNewPriKeyID>041:3289243:130ae100679:goldie:node1</UserAuthNewPriKeyID>
  <UserEncrNewPubKeyAlias>CAEBEncrLMPub</UserEncrNewPubKeyAlias>
  <UserEncrNewPubKeyID>694:3292683:130ae100679:goldie:node1</UserEncrNewPubKeyID>
  <UserEncrNewPriKeyAlias>CAEBEncrLMPriv</UserEncrNewPriKeyAlias>
```

```

<UserEncrNewPriKeyID>167:3288453:130ae100679:goldie:node1</UserEncrNewPriKeyID>
<UserNewAuthVersion>X002</UserNewAuthVersion>
<UserNewEncVersion>E002</UserNewEncVersion>
</orderMetaData>

```

Type de commande HPD

Le type de commande HEV permet à l'utilisateur de recevoir par téléchargement les paramètres de la banque.

Accès

Boîte aux lettres

Description

HPD est un type de commande de gestion de clés par téléchargement (download). L'abonné reçoit les informations d'accès à la banque (par exemple, l'adresse URL, l'adresse IP et la désignation de la banque) ainsi que les paramètres de protocole (par exemple, la prise en charge des versions de protocole EBICS, de la reprise, de la prévalidation, de X.509, et ainsi de suite). Les données de commande sont signées, compressées, chiffrées et codées en base64.

Paramètres

Tableau 21. Paramètres de HPD

Paramètre	Description et valeur
HostID	ID de banque ou ID hôte de la banque à laquelle l'utilisateur du client EBICS a soumis la commande. Il s'agit d'un identifiant unique pour la banque dans le système de la banque.
HostUrlAlias	Lorsque vous configurez un profil de banque, vous pouvez indiquer plusieurs adresses URL d'hôte et en définir une par défaut. Si vous souhaitez envoyer une demande à une adresse URL d'hôte qui n'est pas celle par défaut, indiquez une valeur pour ce paramètre.
PartnerID	ID de partenaire associé à l'ID utilisateur.
UserID	Identifiant unique de l'utilisateur dans le système de la banque, qui correspond à l'utilisateur créé dans le tableau de bord du client EBICS.
SystemID	ID utilisateur de l'utilisateur technique. Un utilisateur technique est un délégué de l'utilisateur non technique ou physique.

Tableau 21. Paramètres de HPD (suite)

Paramètre	Description et valeur
orderIdPrefix	Le client EBICS alloue un ID de commande unique pour chaque commande en fonction de la banque, de l'ID utilisateur et du type de commande. Le client génère l'ID de commande conformément aux spécifications EBICS. L'ID de commande est un identifiant alphanumérique à 4 chiffres. Vous pouvez indiquer le premier caractère de l'ID de commande. Les deuxième, troisième et quatrième caractères de l'ID de commande sont des caractères alphanumériques dans l'ordre croissant (A-Z ou 0-9). Ce paramètre est utilisé uniquement avec le protocole EBICS version H003.
SecurityMedium	Numéro de sécurité à 4 chiffres compris entre 0000 et 0499.
OrderType	Type de la commande que vous soumettez. Dans ce cas, HPD est le type de commande.

Schéma XML

```
<?xml version="1.0" encoding="UTF-8"?>
<orderMetaData xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="new_omd.xsd">
  <HostID>BNKLCMC1</HostID>
  <HostUrlAlias>BNKLCMC1_URL_ALIAS</HostUrlAlias>
  <PartnerID>PH2LCMC1</PartnerID>
  <UserID>USERPK12</UserID>
  <SystemID>UH2LCMC1</SystemID>
  <orderIdPrefix>J</orderIdPrefix>
  <SecurityMedium>0000</SecurityMedium>
  <OrderType>HPD</OrderType>
</orderMetaData>
```

Type de commande SPR

Le type de commande SPR est utilisé pour suspendre l'autorisation d'accès d'un utilisateur.

Accès

Boîte aux lettres

Description

SPR est un type de commande de gestion de clés d'envoi par téléchargement. Les raisons pour lesquelles les transactions sont suspendues entre un abonné et sa banque sont nombreuses. L'une des raisons principales est la compromission des clés de l'abonné. Face à tout soupçon de compromission, l'abonné doit immédiatement suspendre son autorisation d'accès à tous les systèmes de la banque qui utilisent les clés.

Le type de commande de SPR ne compromet aucune donnée de commande supplémentaire et, par conséquent, ne contient aucun fichier de commande. La signature électronique de l'utilisateur du client EBICS qui doit être suspendu est

envoyée à la banque. Les données de commande sont vides. La signature est compressée, chiffrée et codée en base64 comme pour un envoi par téléchargement standard.

Dès lors qu'un abonné n'est plus autorisé à réaliser des transactions, il doit soumettre un nouvel ensemble de types de commande INI et HIA à la banque. Si un abonné est suspendu par la banque, l'initialisation via les commandes INI et HIA n'est pas possible. Seule la banque peut révoquer la suspension.

Paramètres

Tableau 22. Paramètres de SPR

Paramètre	Description et valeur
HostID	ID de banque ou ID hôte de la banque à laquelle l'utilisateur du client EBICS a soumis la commande. Il s'agit d'un identifiant unique pour la banque dans le système de la banque.
HostUrlAlias	Lorsque vous configurez un profil de banque, vous pouvez indiquer plusieurs adresses URL d'hôte et en définir une par défaut. Si vous souhaitez envoyer une demande à une adresse URL d'hôte qui n'est pas celle par défaut, indiquez une valeur pour ce paramètre.
PartnerID	ID de partenaire associé à l'ID utilisateur.
UserID	Identifiant unique de l'utilisateur dans le système de la banque, qui correspond à l'utilisateur créé dans le tableau de bord du client EBICS.
SystemID	ID utilisateur de l'utilisateur technique. Le type de commande SPR peut être soumis par un utilisateur technique qui est un délégué de l'utilisateur physique ou non technique. Par conséquent, la valeur du paramètre UserID est la même que celle du paramètre systemID.
orderIdPrefix	Le client EBICS alloue un ID de commande unique pour chaque commande en fonction de la banque, de l'ID utilisateur et du type de commande. Le client génère l'ID de commande conformément aux spécifications EBICS. L'ID de commande est un identifiant alphanumérique à 4 chiffres. Vous pouvez indiquer le premier caractère de l'ID de commande. Les deuxième, troisième et quatrième caractères de l'ID de commande sont des caractères alphanumériques dans l'ordre croissant (A-Z ou 0-9). Ce paramètre est utilisé uniquement avec le protocole EBICS version H003.
SecurityMedium	Numéro de sécurité à 4 chiffres compris entre 0000 et 0499.
OrderType	Type de la commande que vous soumettez. Dans ce cas, SPR est le type de commande.

Schéma XML

```
<?xml version="1.0" encoding="UTF-8"?>
<orderMetaData xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="new_omd.xsd">
  <HostID>BNKLCMC1</HostID>
  <HostUrlAlias>BNKLCMC1_URL_ALIAS</HostUrlAlias>
  <PartnerID>PH2LCMC1</PartnerID>
  <UserID>UH2LCMC1</UserID>
  <SystemID>UH2LCMC1</SystemID>
  <orderIdPrefix>K</orderIdPrefix>
  <SecurityMedium>0200</SecurityMedium>
  <OrderType>SPR</OrderType>
</orderMetaData>
```

Type de commande HVD

Le type de commande HVD permet à l'utilisateur de récupérer l'état d'une commande VEU.

Accès

Boîte aux lettres

Description

HVD est un type de commande de réception par téléchargement pour la signature distribuée. Il permet d'extraire l'état d'une commande actuellement en cours de traitement VEU et pour laquelle l'abonné est autorisé en tant que signataire. Avec HVD, la valeur hachée de la commande est récupérée.

Paramètres

Tableau 23. Paramètres de HVD

Paramètre	Description et valeur
OrderType	Type de la commande que vous soumettez. Dans ce cas, HVD est le type de commande.
SecurityMedium	Numéro de sécurité à 4 chiffres compris entre 0000 et 0499.
VEUOrderSeqID	ID de séquence de la transaction pour laquelle vous extrayez les détails à l'aide de HVD. Le client EBICS affecte un ID de séquence à une transaction.
orderIdPrefix	Le client EBICS alloue un ID de commande unique pour chaque commande en fonction de la banque, de l'ID utilisateur et du type de commande. Le client génère l'ID de commande conformément aux spécifications EBICS. L'ID de commande est un identifiant alphanumérique à 4 chiffres. Vous pouvez indiquer le premier caractère de l'ID de commande. Les deuxième, troisième et quatrième caractères de l'ID de commande sont des caractères alphanumériques dans l'ordre croissant (A-Z ou 0-9). Ce paramètre est utilisé uniquement avec le protocole EBICS version H003.

Schéma XML

```
<?xml version="1.0" encoding="UTF-8"?>
<orderMetaData>
  <OrderType>HVD</OrderType>
  <SecurityMedium>0200</SecurityMedium>
  <VEUOrderSeqID>39132G7e0939003jffj34535536657</VEUOrderSeqID>
  <orderIdPrefix>V</orderIdPrefix>
</orderMetaData>
```

Type de commande HVE

Le type de commande HEV permet à l'utilisateur d'ajouter une signature VEU.

Accès

Boîte aux lettres

Description

HVE est un type de commande d'envoi par téléchargement pour la signature distribuée. Il permet d'ajouter à une commande une signature technique bancaire pour autorisation en vue du traitement VEU. Les données de signature sont compressées, chiffrées et codées en base64.

Paramètres

Tableau 24. Paramètres de HVE

Paramètre	Description et valeur
PartnerID	ID de partenaire associé à l'ID utilisateur.
HostID	ID de banque ou ID hôte de la banque à laquelle l'utilisateur du client EBICS a soumis la commande. Il s'agit d'un identifiant unique pour la banque dans le système de la banque.
HostUrlAlias	Lorsque vous configurez un profil de banque, vous pouvez indiquer plusieurs adresses URL d'hôte et en définir une par défaut. Si vous souhaitez envoyer une demande à une adresse URL d'hôte qui n'est pas celle par défaut, indiquez une valeur pour ce paramètre.
OrderType	Type de la commande que vous soumettez. Dans ce cas, HVE est le type de commande.
orderIdPrefix	Le client EBICS alloue un ID de commande unique pour chaque commande en fonction de la banque, de l'ID utilisateur et du type de commande. Le client génère l'ID de commande conformément aux spécifications EBICS. L'ID de commande est un identifiant alphanumérique à 4 chiffres. Vous pouvez indiquer le premier caractère de l'ID de commande. Les deuxième, troisième et quatrième caractères de l'ID de commande sont des caractères alphanumériques dans l'ordre croissant (A-Z ou 0-9). Ce paramètre est utilisé uniquement avec le protocole EBICS version H003.

Tableau 24. Paramètres de HVE (suite)

Paramètre	Description et valeur
Product	Produit de l'application client EBICS.
productLang	Paramètre linguistique de l'application client EBICS que vous utilisez. Par exemple, saisissez EN si la langue définie est l'anglais.
SecurityMedium	Numéro de sécurité à 4 chiffres compris entre 0000 et 0499.
UserID	Identifiant unique de l'utilisateur dans le système de la banque, qui correspond à l'utilisateur créé dans le tableau de bord du client EBICS.
OrigPartnerID	ID du partenaire associé à l'utilisateur qui a soumis le type de commande d'envoi par téléchargement.
OrigOrderID	ID de la commande pour laquelle la signature est appliquée.
OrigOrderType	Type de la commande pour laquelle la signature est appliquée.
VeUMessageDigest	Spécifiez le résumé du message pour soumettre la valeur hachée des données de commande. Pour demander la valeur hachée, appelez la banque ou envoyez un courrier. La banque envoie la valeur hachée des données de commande par un autre mode de communication, tel que le courrier électronique.
PAYLOADMSGID	Spécifiez l'ID du message de charge pour soumettre la charge complète à partir de votre boîte aux lettres. Pour demander la charge, appelez la banque ou envoyez un courrier. La banque envoie la charge par courrier électronique à votre boîte aux lettres du client EBICS.
VEUOrderSeqID	ID de séquence de la transaction pour laquelle vous appliquez la signature à l'aide de la commande HVE. Le client EBICS affecte un ID de séquence à une transaction.

Schéma XML

Le schéma XML suivant montre l'utilisation de la commande HVE avec un résumé du message VEU :

```
<?xml version="1.0" encoding="UTF-8"?>
<orderMetaData xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="new_omd.xsd">
  <PartnerID>PARTNERPK55</PartnerID>
  <HostID>HOSTBNKPK12</HostID>
  <HostUrlAlias>HOSTBNKPK12_URL_ALIAS</HostUrlAlias>
  <OrderType>HVE</OrderType>
  <orderIdPrefix>V</orderIdPrefix>
  <Product>IBM EBICS Client</Product>
  <productLang>EN</productLang>
  <SecurityMedium>0200</SecurityMedium>
  <UserID>USERPK55</UserID>
```

```

<OrigPartnerID>PARTNERPK56</OrigPartnerID>
<OrigOrderID>V234</OrigOrderID>
<OrigOrderType>C2X</OrigOrderType>
<VeuMessageDigest>u0UnuZNNPgi1L1LX2n2r+sSE7+N6U4DukIj3r0Lvzek=</VeuMessageDigest>
</orderMetaData>

```

Le schéma XML suivant montre l'utilisation de la commande HVE avec un ID du message de charge lorsque la charge complète est disponible dans la boîte aux lettres :

```

<?xml version="1.0" encoding="UTF-8"?>
<orderMetaData xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="new_omd.xsd">
  <PartnerID>PARTNERPK55</PartnerID>
  <HostID>HOSTBNKPK12</HostID>
  <HostUrlAlias>HOSTBNKPK12_URL_ALIASE</HostUrlAlias>
  <OrderType>HVE</OrderType>
  <orderIdPrefix>V</orderIdPrefix>
  <Product>IBM EBICS Client</Product>
  <productLang>EN</productLang>
  <SecurityMedium>0200</SecurityMedium>
  <UserID>USERPK55</UserID>
  <PAYLOADMSGID>71</PAYLOADMSGID>
  <OrigPartnerID>PARTNERPK56</OrigPartnerID>
  <OrigOrderID>V568</OrigOrderID>
  <OrigOrderType>C2S</OrigOrderType>
</orderMetaData>

```

Le schéma XML suivant montre l'utilisation de la commande HVE avec un ID de séquence de commande VEU. Les détails de la commande sont récupérés de la banque via les types de commande de réception par téléchargement VEU avant l'exécution de la commande HVE :

```

<?xml version="1.0" encoding="UTF-8"?>
<orderMetaData>
  <OrderType>HVE</OrderType>
  <SecurityMedium>0200</SecurityMedium>
  <VEUOrderSeqID>39132G7e0939003jffj34535536657</VEUOrderSeqID>
  <orderIdPrefix>V</orderIdPrefix>
</orderMetaData>

```

Type de commande HVS

Le type de commande HVS permet à l'utilisateur d'annuler définitivement une commande existante du traitement VEU.

Accès

Boîte aux lettres

Description

HVS est un type de commande d'envoi par téléchargement pour la signature distribuée. Utilisez-le pour annuler définitivement une commande existante du traitement VEU. L'abonné envoie une demande HVS pour annuler une commande et distribue la signature technique bancaire nécessaire pour l'annulation dans la valeur hachée des données de commande. La réponse HVS ne contient pas de données spécifiques à VEU.

Paramètres

Tableau 25. Paramètres de HVS

Paramètre	Description et valeur
PartnerID	ID de partenaire associé à l'ID utilisateur.
HostID	ID de banque ou ID hôte de la banque à laquelle l'utilisateur du client EBICS a soumis la commande. Il s'agit d'un identifiant unique pour la banque dans le système de la banque.
HostUrlAlias	Lorsque vous configurez un profil de banque, vous pouvez indiquer plusieurs adresses URL d'hôte et en définir une par défaut. Si vous souhaitez envoyer une demande à une adresse URL d'hôte qui n'est pas celle par défaut, indiquez une valeur pour ce paramètre.
OrderType	Type de la commande que vous soumettez. Dans ce cas, HVS est le type de commande.
orderIdPrefix	Le client EBICS alloue un ID de commande unique pour chaque commande en fonction de la banque, de l'ID utilisateur et du type de commande. Le client génère l'ID de commande conformément aux spécifications EBICS. L'ID de commande est un identifiant alphanumérique à 4 chiffres. Vous pouvez indiquer le premier caractère de l'ID de commande. Les deuxième, troisième et quatrième caractères de l'ID de commande sont des caractères alphanumériques dans l'ordre croissant (A-Z ou 0-9). Ce paramètre est utilisé uniquement avec le protocole EBICS version H003.
Product	Produit de l'application client EBICS.
productLang	Paramètre linguistique de l'application client EBICS que vous utilisez. Par exemple, saisissez EN si la langue définie est l'anglais.
SecurityMedium	Numéro de sécurité à 4 chiffres compris entre 0000 et 0499.
UserID	Identifiant unique de l'utilisateur dans le système de la banque, qui correspond à l'utilisateur créé dans le tableau de bord du client EBICS.
OrigPartnerID	ID du partenaire associé à l'utilisateur qui a soumis le type de commande d'envoi par téléchargement.
OrigOrderID	ID de la commande pour laquelle la signature est appliquée.
OrigOrderType	Type de la commande pour laquelle la signature est appliquée.

Tableau 25. Paramètres de HVS (suite)

Paramètre	Description et valeur
VeuMessageDigest	Spécifiez le résumé du message pour soumettre la valeur hachée des données de commande. Pour demander la valeur hachée, appelez la banque ou envoyez un courrier. La banque envoie la valeur hachée des données de commande par un autre mode de communication, tel que le courrier électronique.
PAYLOADMSGID	Spécifiez l'ID du message de charge pour soumettre la charge complète à partir de votre boîte aux lettres. Pour demander la charge, appelez la banque ou envoyez un courrier. La banque envoie la charge par courrier électronique à votre boîte aux lettres du client EBICS.
VEUOrderSeqID	ID de séquence de la transaction affectée par le client, pour laquelle vous appliquez la signature à l'aide de la commande HVS.

Schéma XML

Le schéma XML suivant montre l'utilisation de la commande HVS avec un résumé du message VEU :

```
<?xml version="1.0" encoding="UTF-8"?>
<orderMetaData xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="new_omd.xsd">
  <PartnerID>PARTNERPK55</PartnerID>
  <HostID>HOSTBNKPK12</HostID>
  <HostUrlAlias>HOSTBNKPK12_URL_ALIAS</HostUrlAlias>
  <OrderType>HVS</OrderType>
  <orderIdPrefix>V</orderIdPrefix>
  <Product>IBM EBICS Client</Product>
  <productLang>EN</productLang>
  <SecurityMedium>0200</SecurityMedium>
  <UserID>USERPK55</UserID>
  <OrigPartnerID>PARTNERPK56</OrigPartnerID>
  <OrigOrderID>V234</OrigOrderID>
  <OrigOrderType>C2X</OrigOrderType>
  <VeuMessageDigest>uU0nuZNNPgilLlLX2n2r+sSE7+N6U4DukIj3r0Lvzek</VeuMessageDigest>
</orderMetaData>
```

Le schéma XML suivant montre l'utilisation de la commande HVS avec un ID du message de charge lorsque la charge complète est disponible dans la boîte aux lettres :

```
<?xml version="1.0" encoding="UTF-8"?>
<orderMetaData xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="new_omd.xsd">
  <PartnerID>PARTNERPK55</PartnerID>
  <HostID>HOSTBNKPK12</HostID>
  <HostUrlAlias>HOSTBNKPK12_URL_ALIAS</HostUrlAlias>
  <OrderType>HVS</OrderType>
  <orderIdPrefix>V</orderIdPrefix>
  <Product>IBM EBICS Client</Product>
  <productLang>EN</productLang>
  <SecurityMedium>0200</SecurityMedium>
  <UserID>USERPK55</UserID>
  <PAYLOADMSGID>71</PAYLOADMSGID>
```

```

<OrigPartnerID>PARTNERPK56</OrigPartnerID>
<OrigOrderID>V568</OrigOrderID>
<OrigOrderType>C2S</OrigOrderType>
</orderMetaData>

```

Le schéma XML suivant montre l'utilisation de la commande HVS avec un ID de séquence de commande VEU. Les détails de la commande sont récupérés de la banque via les types de commande de réception par téléchargement VEU avant l'exécution de la commande HVS :

```

<?xml version="1.0" encoding="UTF-8"?>
<orderMetaData>
  <OrderType>HVS</OrderType>
  <SecurityMedium>0200</SecurityMedium>
  <VEUOrderSeqID>39132G7e0939003jfj34535536657</VEUOrderSeqID>
  <orderIdPrefix>V</orderIdPrefix>
</orderMetaData>

```

Type de commande HVT

Le type de commande HVU permet à l'utilisateur de récupérer des informations détaillées sur une commande à partir du traitement VEU pour lequel l'utilisateur est un signataire habilité.

Accès

Boîte aux lettres

Description

HVT est un type de commande de réception par téléchargement pour la signature distribuée. Utilisez le type de commande HVT pour récupérer des détails transactionnels concernant une commande à partir du traitement VEU.

Paramètres

Tableau 26. Paramètres de HVT

Paramètre	Description et valeur
OrderType	Type de la commande que vous soumettez. Dans ce cas, HVT est le type de commande.
SecurityMedium	Numéro de sécurité à 4 chiffres compris entre 0000 et 0499.
VEUOrderSeqID	ID de séquence de la transaction pour laquelle vous téléchargez les détails de transaction à l'aide de HVT. Le client EBICS affecte un ID de séquence à une transaction.

Tableau 26. Paramètres de HVT (suite)

Paramètre	Description et valeur
orderIdPrefix	<p>Le client EBICS alloue un ID de commande unique pour chaque commande en fonction de la banque, de l'ID utilisateur et du type de commande. Le client génère l'ID de commande conformément aux spécifications EBICS. L'ID de commande est un identifiant alphanumérique à 4 chiffres. Vous pouvez indiquer le premier caractère de l'ID de commande. Les deuxième, troisième et quatrième caractères de l'ID de commande sont des caractères alphanumériques dans l'ordre croissant (A-Z ou 0-9).</p> <p>Ce paramètre est utilisé uniquement avec le protocole EBICS version H003.</p>
completeOrderData	<p>Si l'attribut completeOrderData est défini sur vrai, l'utilisateur envoie une demande pour recevoir le fichier de commande complet. Si l'attribut completeOrderData est défini sur faux, l'utilisateur envoie une demande pour recevoir des informations spécifiques telles que les détails du compte, l'échéance d'implémentation, le montant et d'autres descriptions.</p>
fetchLimit	<p>Il s'agit du nombre maximal de détails de la commande à transmettre si l'attribut completeOrderData est défini sur faux. La valeur par défaut est 100. La valeur admise doit être un nombre entier non négatif. Indiquez 0 pour extraire un nombre illimité de détails. Même s'il est possible d'extraire plus de 100 détails à la fois, cela n'est pas recommandé.</p>
fetchOffset	<p>Il s'agit de la position de décalage dans le fichier de commande d'origine qui marque le point de départ des détails de transaction à transmettre. Si l'attribut completeOrderData est défini sur faux, la position de décalage s'applique au nombre séquentiel d'une commande spécifique. La valeur par défaut est 0. La valeur admise doit être un nombre entier non négatif. Pour extraire plus de 100 enregistrements, définissez Décalage d'extraction sur 0 afin d'extraire les 100 premiers, puis sur 101 afin d'extraire les 100 suivants. Continuez si nécessaire.</p>

Schéma XML

L'exemple de schéma XML suivant montre l'utilisation du type de commande HVT lorsque l'attribut completeOrderData est défini sur true :

```
<?xml version="1.0" encoding="UTF-8"?>
<orderMetaData>
  <OrderType>HVT</OrderType>
```

```

<SecurityMedium>0200</SecurityMedium>
<VEUOrderSeqID>39132G7e0939003jffj34535536657</VEUOrderSeqID>
<orderIdPrefix>V</orderIdPrefix>
<completeOrderData>true</completeOrderData>
</orderMetaData>

```

L'exemple de schéma XML suivant montre l'utilisation du type de commande HVT lorsque l'attribut completeOrderData est défini sur false :

```

<?xml version="1.0" encoding="UTF-8"?>
<orderMetaData>
  <OrderType>HVT</OrderType>
  <SecurityMedium>0200</SecurityMedium>
  <VEUOrderSeqID>39132G7e0939003jffj34535536657</VEUOrderSeqID>
  <orderIdPrefix>V</orderIdPrefix>
  <completeOrderData>false</completeOrderData>
  <fetchLimit>5</fetchLimit>
  <fetchOffset>2</fetchOffset>
</orderMetaData>

```

Type de commande HVU

Le type de commande HVU permet à l'utilisateur de lister les commandes que l'utilisateur est autorisé à utiliser en tant que signataire.

Accès

Boîte aux lettres

Description

HVU est un type de commande de réception par téléchargement pour la signature distribuée. Utilisez-le pour recevoir par téléchargement une présentation VEU. Dans la demande HVU, l'abonné soumet sur option une liste des types de commande pour lesquels il est signataire.

Paramètres

Tableau 27. Paramètres de HVU

Paramètre	Description et valeur
PartnerID	ID de partenaire associé à l'ID utilisateur.
HostID	ID de banque ou ID hôte de la banque à laquelle l'utilisateur du client EBICS a soumis la commande. Il s'agit d'un identifiant unique pour la banque dans le système de la banque.
HostUrlAlias	Lorsque vous configurez un profil de banque, vous pouvez indiquer plusieurs adresses URL d'hôte et en définir une par défaut. Si vous souhaitez envoyer une demande à une adresse URL d'hôte qui n'est pas celle par défaut, indiquez une valeur pour ce paramètre.
OrderType	Type de la commande que vous soumettez. Dans ce cas, HVU est le type de commande.

Tableau 27. Paramètres de HVU (suite)

Paramètre	Description et valeur
orderIdPrefix	Le client EBICS alloue un ID de commande unique pour chaque commande en fonction de la banque, de l'ID utilisateur et du type de commande. Le client génère l'ID de commande conformément aux spécifications EBICS. L'ID de commande est un identifiant alphanumérique à 4 chiffres. Vous pouvez indiquer le premier caractère de l'ID de commande. Les deuxième, troisième et quatrième caractères de l'ID de commande sont des caractères alphanumériques dans l'ordre croissant (A-Z ou 0-9). Ce paramètre est utilisé uniquement avec le protocole EBICS version H003.
Product	Produit de l'application client EBICS.
productLang	Paramètre linguistique de l'application client EBICS que vous utilisez. Par exemple, saisissez EN si la langue définie est l'anglais.
SecurityMedium	Numéro de sécurité à 4 chiffres compris entre 0000 et 0499.
UserID	Identifiant unique de l'utilisateur dans le système de la banque, qui correspond à l'utilisateur créé dans le tableau de bord du client EBICS.
VEUOrderTypes	Types de commande, sous la forme d'une liste XML, pour lesquels les données HVU doivent être extraites.

Schéma XML

```
<?xml version="1.0" encoding="UTF-8"?>
<orderMetaData xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="new_omd.xsd">
  <PartnerID>PARTNERPK55</PartnerID>
  <HostID>HOSTBNKPK12</HostID>
  <HostUrlAlias>HOSTBNKPK12_URL_ALIAS</HostUrlAlias>
  <OrderType>HVU</OrderType>
  <orderIdPrefix>V</orderIdPrefix>
  <Product>IBM EBICS Client</Product>
  <productLang>EN</productLang>
  <SecurityMedium>0200</SecurityMedium>
  <UserID>USERPK55</UserID>
  <VEUOrderTypes>C2C C2S</VEUOrderTypes>
</orderMetaData>
```

Type de commande HVZ

Le type de commande HVZ permet à l'utilisateur de recevoir par téléchargement la présentation VEU avec des informations supplémentaires.

Accès

Boîte aux lettres

Description

HVZ est un type de commande de réception par téléchargement pour la signature distribuée. Utilisez-le pour recevoir par téléchargement la présentation VEU avec des renseignements supplémentaires. Dans la demande HVZ, l'abonné soumet sur option une liste des types de commande pour lesquels il est signataire par habilitation. Les données de la commande de réponse HVZ contiennent les informations complètes des données de commande de réponse HVU et HVD, sauf l'élément d'affichage de fichier.

Paramètres

Tableau 28. Paramètres de HVZ

Paramètre	Description et valeur
PartnerID	ID de partenaire associé à l'ID utilisateur.
HostID	ID de banque ou ID hôte de la banque à laquelle l'utilisateur du client EBICS a soumis la commande. Il s'agit d'un identifiant unique pour la banque dans le système de la banque.
HostUrlAlias	Lorsque vous configurez un profil de banque, vous pouvez indiquer plusieurs adresses URL d'hôte et en définir une par défaut. Si vous souhaitez envoyer une demande à une adresse URL d'hôte qui n'est pas celle par défaut, indiquez une valeur pour ce paramètre.
OrderType	Type de la commande que vous soumettez. Dans ce cas, HVZ est le type de commande.
orderIdPrefix	Le client EBICS alloue un ID de commande unique pour chaque commande en fonction de la banque, de l'ID utilisateur et du type de commande. Le client génère l'ID de commande conformément aux spécifications EBICS. L'ID de commande est un identifiant alphanumérique à 4 chiffres. Vous pouvez indiquer le premier caractère de l'ID de commande. Les deuxième, troisième et quatrième caractères de l'ID de commande sont des caractères alphanumériques dans l'ordre croissant (A-Z ou 0-9). Ce paramètre est utilisé uniquement avec le protocole EBICS version H003.
Product	Produit de l'application client EBICS.
productLang	Paramètre linguistique de l'application client EBICS que vous utilisez. Par exemple, saisissez EN si la langue définie est l'anglais.
SecurityMedium	Numéro de sécurité à 4 chiffres compris entre 0000 et 0499.
UserID	Identifiant unique de l'utilisateur dans le système de la banque, qui correspond à l'utilisateur créé dans le tableau de bord du client EBICS.

Tableau 28. Paramètres de HVZ (suite)

Paramètre	Description et valeur
VEUOrderTypes	Types de commande, sous la forme d'une liste XML, pour lesquels les données HVZ doivent être extraites.

Schéma XML

```
<?xml version="1.0" encoding="UTF-8"?>
<orderMetaData xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="new_omd.xsd">
  <PartnerID>PARTNERPK55</PartnerID>
  <HostID>HOSTBNKPK12</HostID>
  <HostUrlAlias>HOSTBNKPK12_URL_ALIAS</HostUrlAlias>
  <OrderType>HVZ</OrderType>
  <orderIdPrefix>V</orderIdPrefix>
  <Product>IBM EBICS Client</Product>
  <productLang>EN</productLang>
  <SecurityMedium>0200</SecurityMedium>
  <UserID>USERPK55</UserID>
  <VEUOrderTypes>C2X TST-Upload</VEUOrderTypes>
</orderMetaData>
```

Action de tâche en attente

Utilisez la balise XML taskMetaData pour signer ou soumettre une commande en attente.

Accès

Boîte aux lettres

Description

En fonction des paramètres de configuration définis dans une offre, plusieurs signataires peuvent avoir à signer la commande pour traiter les données qu'elle contient. Si une commande est soumise pour être traitée sans toutes les signatures requises, le client EBICS ne traitera pas la commande. L'utilisateur signataire ou autorisé à soumettre une commande peut visualiser la commande en question dans la liste des tâches en attente à l'aide de l'interface de tableau de bord du client EBICS.

Le signataire doit signer la commande en attente. Une fois que toutes les signatures requises ont été obtenues, l'émetteur soumet la commande.

Paramètres

Tableau 29. Paramètres de EBICSPendingTaskAction

Paramètre	Description et valeur
UserID	Identifiant unique de l'utilisateur dans le système de la banque, qui correspond à l'utilisateur créé dans le tableau de bord du client EBICS.
OrderSeqId	ID de séquence de la transaction pour laquelle la signature ou la soumission de la commande est en attente. Le client EBICS affecte un ID de séquence à une transaction.

Tableau 29. Paramètres de EBICSPendingTaskAction (suite)

Paramètre	Description et valeur
action	Vous pouvez signer ou soumettre la commande en attente. Si la commande en attente doit être soumise, affectez au paramètre la valeur submit. Si la commande en attente doit être signée, affectez au paramètre la valeur sign.
isHSM	Valide si le paramètre action est défini sur sign. L'utilisateur doit fournir les informations appropriées sur la clé de sécurité matérielle pour pouvoir signer la commande. Actuellement, le client EBICS prend en charge le module de signature matérielle (HSM) utilisant 3SKey uniquement. Si vous voulez envoyer HSM en utilisant une API pour signer une commande, assurez-vous que la table CEB_ORD_TASK_PEND est mise à jour avec la signature.

Schéma XML

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<taskMetaData>
  <UserID>userID</UserID>
  <OrderSeqId>orderSeqId</OrderSeqId>
  <action>submit</action>
  <isHSM>>false</isHSM>
</taskMetaData>
```

Traitement HAC

Lorsqu'un accusé de réception du client EBICS (type de commande HAC) est téléchargé dans Sterling B2B Integrator, des données comprenant des informations sur le statut et le code anomalie sont créées, tel que défini dans la spécification EBICS 2.5.

Le type de commande HAC est un accusé de réception technique envoyé au client, qui indique le statut de traitement et fournit des informations détaillées sur les commandes soumises. Ces données incluent les actions et les résultats qui se produisent lors de l'émission, de la réception ou de signature des fichiers et, le cas échéant, fournissent des informations sur le contenu des fichiers.

Les utilisateurs n'initient pas directement les demandes HAC. C'est le client EBICS Sterling B2B Integrator qui les lance automatiquement selon les plannings définis en utilisant le planificateur HAC. Chaque réponse HAC contient un historique complet des actions et du statut EBICS depuis la dernière demande HAC. Les données de chaque réponse HAC sont stockées par Sterling B2B Integrator.

Pour afficher les données de la commande HAC, utilisez soit l'afficheur **Recherche de commande** du client EBICS dans Sterling B2B Integrator, soit la fonction de **recherche EBICS** de Sterling File Gateway.

Les résultats de la recherche peuvent contenir des actions et des codes anomalie de la commande HAC comme indiqué dans le tableau suivant.

Tableau 30. Actions et codes anomalie de la commande HAC

Action HAC	Type d'action	Code anomalie	Résultat HAC
Fichier soumis à la banque	FILE_UPLOAD	DS0C	Utilisateur verrouillé/certificat révoqué
		DS08	Erreur de décompression
		DS09	Erreur de déchiffrement
		TA01	Envoi par téléchargement abandonné
		TS01	Envoi par téléchargement réussi
Fichier reçu par téléchargement de la banque	FILE_DOWNLOAD	DS0C	Utilisateur verrouillé/certificat révoqué
		DS08	Erreur de décompression
		DS09	Erreur de déchiffrement
		TA01	Réception par téléchargement abandonnée
		TD01	Aucune donnée disponible au téléchargement
		TS01	Réception par téléchargement réussie
Signature électronique soumise à la banque	ES_UPLOAD	ID01	Le dossier de commandes d'origine n'a pas été envoyé auparavant
		DS0C	Utilisateur verrouillé/certificat révoqué
		DS08	Erreur de décompression
		DS09	Erreur de déchiffrement
		TA01	Envoi par téléchargement de signature électronique abandonné
		TS01	Envoi par téléchargement de signature électronique réussi

Tableau 30. Actions et codes anomalie de la commande HAC (suite)

Action HAC	Type d'action	Code anomalie	Résultat HAC
Vérification de signature	ES_VERIFICATION	AM21	Le montant dépasse le plafond
		DS01	Signature(s) électronique(s) correcte(s)
		DS0A	Nombre de signatures électroniques insuffisant
		DS0B	Signature(s) électronique(s) incorrecte(s)
		DS0C	Certificat révoqué/utilisateur verrouillé
		DS0D	Certificat non valide/clé publique non activée
		DS0E	Certificat non présent/clé publique inexistante
		DS0F	L'autorité de certification du certificat est inconnue
		DS0G	Signataire non autorisé pour signer cette opération
		DS0H	Signataire non autorisé à signer ce compte
		DS08	Erreur de décompression
		DS09	Erreur de déchiffrement
		DS10	Certificat révoqué pour le premier signataire
		DS11	Certificat non valide pour le premier signataire
		DS12	Certificat absent pour le premier signataire
		DS13	Autorité de certification inconnue pour le premier signataire
		DS14	L'utilisateur (signataire) est inconnu sur le serveur
		DS15	La même signature électronique (ES) a déjà été envoyée à la banque
		DS16	Version de clé publique incorrecte
		DS17	Les données de commande et les signatures électroniques (ES) ne correspondent pas
		DS18	Répétition de commande (fichier non testable)
		DS19	Les droits de signature électronique du signataire sont insuffisants
		DS20	Certificat révoqué pour le second signataire
		DS21	Certificat non valide pour le second signataire
DS22	Certificat absent pour le second signataire		
DS23	Autorité de certification inconnue pour le second signataire (Utilisateur du point de vue du signataire)		
DS24	Expiration du délai d'attente et suppression du fichier par la banque		

Tableau 30. Actions et codes anomalie de la commande HAC (suite)

Action HAC	Type d'action	Code anomalie	Résultat HAC
Réacheminement vers VEU	VEU_FORWARDING	DS06	Commande transférée à la fonction VEU

Tableau 30. Actions et codes anomalie de la commande HAC (suite)

Action HAC	Type d'action	Code anomalie	Résultat HAC
Vérification de signature VEU	VEU_VERIFICATION	AM21	Le montant dépasse le plafond
		DS01	Signature(s) électronique(s) correcte(s)
		DS0B	Signature(s) électronique(s) incorrecte(s)
		DS0C	Certificat révoqué/utilisateur verrouillé
		DS0D	Certificat non valide/clé publique non activée
		DS0E	Certificat non présent/clé publique inexistante
		DS0F	L'autorité de certification du certificat est inconnue
		DS0G	Signataire non autorisé pour signer cette opération
		DS0H	Signataire non autorisé à signer ce compte
		DS10	Certificat révoqué pour le premier signataire
		DS11	Certificat non valide pour le premier signataire
		DS12	Certificat absent pour le premier signataire
		DS13	Autorité de certification inconnue pour le premier signataire
		DS14	L'utilisateur (signataire) est inconnu sur le serveur
		DS15	La même signature électronique (ES) a déjà été envoyée à la banque
		DS16	Version de clé publique incorrecte
		DS17	Les données de commande et les signatures électroniques (ES) ne correspondent pas
		DS18	Répétition de commande (fichier non testable)
		DS19	Les droits de signature électronique du signataire sont insuffisants
		DS20	Certificat révoqué pour le second signataire
		DS21	Certificat non valide pour le second signataire
		DS22	Certificat absent pour le second signataire
		DS23	Autorité de certification inconnue pour le second signataire
		DS24	Expiration du délai d'attente et suppression du fichier par la banque
		DS25	Fichier supprimé par la banque (causes multiples) Utilisateur du client EBICS (V5.2.5 ou ultérieure)
		DS26	Le même utilisateur a signé plusieurs fois
		DS27	Utilisateur (signataire) non encore

Tableau 30. Actions et codes anomalie de la commande HAC (suite)

Action HAC	Type d'action	Code anomalie	Résultat HAC
Fin de la vérification de signature VEU	VEU_VERIFICATION_END	DS05	Commande correcte, réacheminée pour post-traitement
Annulation de la commande VEU	VEU_CANCEL_ORDER	DS02	Commande annulée
		DS03	Commande non annulée
Fin de commande HAC (positif)	ORDER_HAC_FINAL_POS	Non fourni	Indication finale pour le traitement réussi de la commande.
Fin de commande HAC (négatif)	ORDER_HAC_FINAL_NEG	Non fourni	Indication finale pour l'échec du traitement de la commande.

Planning HAC

Les utilisateurs n'initient pas directement les demandes HAC. C'est le client EBICS Sterling B2B Integrator qui les lance automatiquement à l'aide de Planning HAC dans le menu Administration du client EBICS.

La planification HAC est disponible uniquement pour les utilisateurs Sterling B2B Integrator disposant d'autorisations d'administration (administrateur ou super administrateur).

Chaque planning HAC soumet une demande HAC pour un ID partenaire indiqué à un ID de banque indiqué à l'aide d'un ID utilisateur spécifique. Le planning HAC définit également la fréquence de traitement de la demande HAC et le moment où les données collectées sont purgées.

Pour que la création d'un planning HAC soit possible, il doit exister au moins un ID utilisateur par ID partenaire, à l'état "Prêt" et possédant des autorisations de soumission des commandes de type HAC.

Lorsqu'une demande HAC planifiée est traitée, les données de l'historique des commandes EBICS sont collectées et reçues dans une réponse HAC. Chaque réponse HAC contient un historique complet des actions et du statut EBICS depuis la dernière demande HAC. Les données de chaque réponse HAC sont stockées par Sterling B2B Integrator.

Création d'un planning HAC

Pour créer des plannings HAC dans Sterling B2B Integrator, utilisez l'option de planning HAC dans le menu Administration du client EBICS.

Pourquoi et quand exécuter cette tâche

Restriction : Seul un utilisateur Sterling B2B Integrator disposant d'autorisations d'administration peut créer des plannings HAC. Pour que la création d'un planning HAC soit possible, il doit exister au moins un ID utilisateur par ID partenaire, à l'état "Prêt" et possédant des autorisations de soumission des commandes de type HAC.

Pour créer un planning HAC :

Procédure

1. Connectez-vous au client EBICS de Sterling B2B Integrator.
2. Dans le menu **Administration**, sélectionnez **Planning HAC**.
3. Sur la page Configuration du planning HAC, cliquez sur **OK** en regard de **Créer un nouveau planning**.
4. Sur la page d'informations sur la création du planning HAC, indiquez les valeurs des zones conformément aux instructions du tableau suivant :

Zone	Description
ID de banque (ID hôte)	Sélectionnez un identifiant de banque dans la liste déroulante.
ID du partenaire	Sélectionnez un ID de partenaire associé à la banque dans la liste déroulante.
ID utilisateur	Dans la liste déroulante, sélectionnez l'ID utilisateur. Restriction : Il doit exister au moins un ID utilisateur par ID partenaire, à l'état "Prêt" et possédant des autorisations de soumission des commandes de type HAC.
Moyen de sécurité	Entrez le moyen de sécurité.
Intervalle entre les demandes	Dans la liste déroulante, sélectionnez l'intervalle de soumission des demandes HAC : <ul style="list-style-type: none"> • désactivé • toutes les 5 minutes • toutes les 15 minutes • toutes les 30 minutes • toutes les heures • toutes les 3 heures • toutes les 6 heures • toutes les 12 heures • tous les jours • tous les 2 jours <p>Détermine la fréquence de soumission d'une nouvelle commande HAC pour le nom du partenaire à l'ID banque avec l'ID utilisateur afin de recueillir les données d'historique du traitement des commandes.</p> <p>Chaque rapport HAC contient toutes les nouvelles activités de commande depuis les derniers résultats de commande HAC.</p>

Zone	Description
Expiration de la purge	<p>Dans la liste déroulante, sélectionnez l'expiration des données de rapport HAC collectées :</p> <ul style="list-style-type: none"> • jamais • après 1 jour • après 2 jours • après une semaine • après 2 semaines • après un mois <p>Les enregistrements de données HAC ayant expiré sont purgés automatiquement de la base de données lors de la prochaine exécution du processus de purge automatique. La fréquence d'exécution de la purge automatique est contrôlée par le paramètre Intervalle de purge HAC (en minutes) dans les priorités système du client EBICS. Pour plus d'informations sur les propriétés système, voir «Mise à jour des valeurs des propriétés système», à la page 77.</p> <p>Important : Si vous sélectionnez jamais, les enregistrements de données HAC n'expireront jamais et ne seront donc jamais purgés de la base de données. Les enregistrements s'accumuleront indéfiniment dans la base de données jusqu'à ce qu'ils soient supprimés manuellement des tables de la base de données lorsqu'ils sont devenus inutiles.</p> <p>Cette sélection s'applique uniquement aux données HAC collectées dans le futur. Si cette valeur est modifiée ultérieurement, les données HAC déjà présentes dans la base de données conservent la valeur affectée au moment de leur collecte et de leur stockage dans la base de données.</p>

5. Cliquez sur **Terminer**.

Recherche d'un planning HAC

Pour rechercher des plannings HAC dans Sterling B2B Integrator, utilisez l'option de planning HAC dans le menu Administration du client EBICS.

Pourquoi et quand exécuter cette tâche

Pour rechercher un planning HAC :

Procédure

1. Connectez-vous au client EBICS de Sterling B2B Integrator.
2. Dans le menu **Administration**, sélectionnez **Planning HAC**.
3. Sur la page Configuration de planning HAC, procédez comme suit :

- Sous **Rechercher**, dans la zone **Banque (ID hôte)** ou la zone **ID du partenaire**, entrez tout ou partie de l'ID banque ou l'ID du partenaire.
 - Sous **Liste**, dans la liste déroulante **Par ordre alphabétique**, sélectionnez la première lettre ou le premier chiffre de l'ID banque. Sélectionnez **Tous** pour dresser la liste de tous les plannings HAC.
4. Cliquez sur **OK**.

Visualisation d'un planning HAC

Pour visualiser des plannings HAC dans Sterling B2B Integrator, utilisez l'option de planning HAC dans le menu Administration du client EBICS.

Pourquoi et quand exécuter cette tâche

Pour visualiser les paramètres d'un planning HAC :

Procédure

1. Connectez-vous au client EBICS de Sterling B2B Integrator.
2. Dans le menu **Administration**, sélectionnez **Planning HAC**.
3. Sur la page Configuration du planning HAC, en utilisant **Rechercher** ou **Liste**, localisez et sélectionnez le planning HAC que vous souhaitez modifier, puis cliquez sur **OK**.
4. Cliquez sur le lien du nom du partenaire correspondant au planning HAC à afficher. Les paramètres du planning HAC s'affichent.

Modification d'un planning HAC

Pour modifier des plannings HAC dans Sterling B2B Integrator, utilisez l'option de planning HAC dans le menu Administration du client EBICS.

Pourquoi et quand exécuter cette tâche

Restriction : Seul un utilisateur Sterling B2B Integrator disposant d'autorisations d'administration peut modifier des plannings HAC.

Pour modifier un planning HAC :

Procédure

1. Connectez-vous au client EBICS de Sterling B2B Integrator.
2. Dans le menu **Administration**, sélectionnez **Planning HAC**.
3. Sur la page Configuration du planning HAC, en utilisant **Rechercher** ou **Liste**, localisez et sélectionnez le planning HAC que vous souhaitez modifier, puis cliquez sur **OK**.
4. Cliquez sur l'icône **Mettre à jour** en regard du planning HAC que vous souhaitez modifier.
5. Sur la page d'informations sur la mise à jour du planning HAC, indiquez les valeurs des zones conformément aux instructions du tableau suivant :

Zone	Description
ID de banque (ID hôte)	Affiche l'ID de banque. Il ne peut pas être modifié.
ID du partenaire	Affiche l'ID du partenaire. Il ne peut pas être modifié.

Zone	Description
ID utilisateur	<p>Dans la liste déroulante, sélectionnez l'ID utilisateur.</p> <p>Restriction : Il doit exister au moins un ID utilisateur par ID partenaire, à l'état "Prêt" et possédant des autorisations de soumission des commandes de type HAC.</p>
Moyen de sécurité	Entrez le moyen de sécurité.
Intervalle entre les demandes	<p>Dans la liste déroulante, sélectionnez l'intervalle de soumission des demandes HAC :</p> <ul style="list-style-type: none"> • désactivé • toutes les 5 minutes • toutes les 15 minutes • toutes les 30 minutes • toutes les heures • toutes les 3 heures • toutes les 6 heures • toutes les 12 heures • tous les jours • tous les 2 jours <p>Détermine la fréquence de soumission d'une nouvelle commande HAC pour le nom du partenaire à l'ID banque avec l'ID utilisateur afin de recueillir les données d'historique du traitement des commandes.</p> <p>Chaque rapport HAC contient toutes les nouvelles activités de commande depuis les derniers résultats de commande HAC.</p>

Zone	Description
Expiration de la purge	<p>Dans la liste déroulante, sélectionnez l'expiration des données de rapport HAC collectées :</p> <ul style="list-style-type: none"> • jamais • après 1 jour • après 2 jours • après une semaine • après 2 semaines • après un mois <p>Les enregistrements de données HAC ayant expiré sont purgés automatiquement de la base de données lors de la prochaine exécution du processus de purge automatique. La fréquence d'exécution de la purge automatique est contrôlée par le paramètre Intervalle de purge HAC (en minutes) dans les priorités système du client EBICS. Pour plus d'informations sur les propriétés système, voir «Mise à jour des valeurs des propriétés système», à la page 77.</p> <p>Important : Si vous sélectionnez jamais, les enregistrements de données HAC n'expireront jamais et ne seront donc jamais purgés de la base de données. Les enregistrements s'accumuleront indéfiniment dans la base de données jusqu'à ce qu'ils soient supprimés manuellement des tables de la base de données lorsqu'ils sont devenus inutiles.</p> <p>Cette sélection s'applique uniquement aux données HAC collectées dans le futur. Le changement de cette valeur ne concerne pas les enregistrements de données HAC déjà stockés dans la base de données. La modification concerne uniquement les données collectées et stockées après affectation de la nouvelle valeur. Les enregistrements de données existants conservent la valeur affectée au moment de leur collecte et de leur stockage dans la base de données.</p>

6. Cliquez sur **Terminer**.

Suppression d'un planning HAC

Pour supprimer des plannings HAC de Sterling B2B Integrator, utilisez l'option de planning HAC dans le menu Administration du client EBICS.

Pourquoi et quand exécuter cette tâche

Pour supprimer un planning HAC :

Procédure

1. Connectez-vous au client EBICS de Sterling B2B Integrator.
2. Dans le menu **Administration**, sélectionnez **Planning HAC**.
3. Sur la page Configuration du planning HAC, en utilisant **Rechercher** ou **Liste**, localisez et sélectionnez le planning HAC que vous souhaitez supprimer.
4. Cliquez sur **OK**.
5. Cliquez sur l'icône Supprimer en regard de la planification HAC que vous souhaitez supprimer.

Résultats

Le planning HAC est supprimé.

La suppression du planning HAC n'a pas d'effet sur les données d'état HAC déjà téléchargées dans la base de données. Ces enregistrements restent dans la table jusqu'à leur date d'expiration de purge définie dans le planning HAC lors de la soumission de la demande HAC.

Codes de retour

Lorsque vous utilisez le client EBICS, vous pouvez recevoir des codes d'erreur et des messages d'événement.

Codes de retour associés aux événements

Les tableaux présentés dans cette section exposent le code de retour, le message d'événement correspondant ainsi qu'une brève description du code de retour.

Tableau 31. Codes de retour associés aux événements

Code de retour	Message d'événement	Description
EBICSCL2302	Données de commande compressées	Indique que les données de commande de la transaction sont compressées. Aucune action de l'utilisateur n'est requise.
EBICSCL2303	Données de commande chiffrées	Indique que les données de commande de la transaction sont chiffrées. Aucune action de l'utilisateur n'est requise.
EBICSCL2304	Données de commande codées	Indique que les données de commande de la transaction sont codées. Aucune action de l'utilisateur n'est requise.
EBICSCL2305	Données de commande signées	Indique que les données de commande de la transaction sont signées. Aucune action de l'utilisateur n'est requise.
EBICSCL2306	Données de commande décompressées	Indique que les données de commande de la transaction sont décompressées. Aucune action de l'utilisateur n'est requise.

Tableau 31. Codes de retour associés aux événements (suite)

Code de retour	Message d'événement	Description
EBICSCL2307	Données de commande déchiffrées	Indique que les données de commande de la transaction sont déchiffrées. Aucune action de l'utilisateur n'est requise.
EBICSCL2308	Données de commande décodées	Indique que les données de commande de la transaction sont décodées. Aucune action de l'utilisateur n'est requise.
EBICSCL2309	Données de signature compressées	Indique que les données de signature de la transaction sont compressées. Aucune action de l'utilisateur n'est requise.
EBICSCL2310	Données de signature chiffrées	Indique que les données de signature de la transaction sont chiffrées. Aucune action de l'utilisateur n'est requise.
EBICSCL2311	Données de signature codées	Indique que les données de signature de la transaction sont codées. Aucune action de l'utilisateur n'est requise.
EBICSCL2312	Données de signature décompressées	Indique que les données de signature de la transaction sont décompressées. Aucune action de l'utilisateur n'est requise.
EBICSCL2313	Données de signature déchiffrées	Indique que les données de signature de la transaction sont déchiffrées. Aucune action de l'utilisateur n'est requise.
EBICSCL2314	Données de signature décodées	Indique que les données de signature de la transaction sont décodées. Aucune action de l'utilisateur n'est requise.
EBICSCL2300	Conditionnement EBICS réussi	Indique que le conditionnement des données de commande a abouti. Aucune action de l'utilisateur n'est requise.

Tableau 31. Codes de retour associés aux événements (suite)

Code de retour	Message d'événement	Description
EBICSCL2301	Échec du conditionnement EBICS	Indique que le conditionnement des données de commande a échoué. L'échec du conditionnement peut être lié à une erreur survenue lors de la compression ou du chiffrement des données de commande, ou bien à des clés erronées utilisées dans la signature ou le chiffrement. Vérifiez la liste des événements à l'aide de l'observateur d'événements dans l'interface de tableau de bord du client EBICS.
EBICSCL2500	Déconditionnement EBICS réussi	Indique que le déconditionnement des données de commande a abouti. Aucune action de l'utilisateur n'est requise.
EBICSCL2501	Échec du déconditionnement EBICS	Indique que le déconditionnement des données de commande a échoué. L'échec du déconditionnement peut être lié à une erreur survenue lors de la décompression ou du déchiffrement des données de commande, ou bien à des clés erronées utilisées dans la vérification de signature. Vérifiez la liste des événements à l'aide de l'observateur d'événements dans l'interface de tableau de bord du client EBICS.
EBICSCL2318	Réponse valide reçue	Indique que vous avez reçu une réponse valide du serveur lorsque vous avez soumis un type de commande.
EBICSCL2319	Réponse erronée reçue	Indique que le serveur a renvoyé une réponse non valide à une demande de commande particulière. Pour plus d'informations sur la réponse, examinez les codes de retour techniques et métier dans la liste des événements en utilisant l'observateur d'événements dans l'interface de tableau de bord du client EBICS.

Tableau 31. Codes de retour associés aux événements (suite)

Code de retour	Message d'événement	Description
EBICSCL2320	Demande d'initialisation EBICS transmise	Indique que la demande a été initialisée.
EBICSCL2321	Demande de transfert de données EBICS transmise	Indique que la demande de transfert de données a été acceptée par la banque.
EBICSCL2322	Aucun droit pour l'émetteur	Indique que vous ne disposez pas du droit d'utilisateur pour soumettre une commande. Configurez le droit d'utilisateur du rôle en affectant au niveau d'autorisation la valeur T et au type d'autorisation la valeur Émetteur.
EBICSCL2323	Écriture des données décompressées dans la boîte aux lettres réussie	Indique que les données ont été décompressées et stockées dans la boîte aux lettres d'utilisateur.
EBICSCL2324	Échec de l'écriture des données décompressées dans la boîte aux lettres	L'échec de l'écriture des données décompressées dans une boîte aux lettres peut être dû à des droits d'accès incorrects à cette boîte aux lettres. Pour plus d'informations, consultez le fichier journal ebicsClient.log.
EBICSCL2325	Tâches en attente créées pour les autoriseurs	Indique que des tâches en attente sont créées pour l'utilisateur. Affichez la liste des tâches en attente de signature à l'aide de l'interface de tableau de bord du client EBICS.
EBICSCL2326	Tâches en attente créées pour l'émetteur	Indique que des tâches en attente sont créées pour l'utilisateur qui est autorisé à soumettre des commandes. Affichez la liste des tâches en attente de soumission à l'aide de l'interface de tableau de bord du client EBICS.
EBICSCL2327	Génération de signature réussie pour l'autoriseur	Indique que la génération de signature a abouti quand un signataire a signé une commande en attente de signature.
EBICSCL2328	Échec de génération de signature pour l'autoriseur	Indique que la génération de signature a échoué quand un signataire a signé une commande en attente de signature.

Tableau 31. Codes de retour associés aux événements (suite)

Code de retour	Message d'événement	Description
EBICSCL2329	Le type de commande n'est pas valide	Indique que le type de commande indiqué est non valide. Indiquez un type de commande valide.
EBICSCL2330	L'ID hôte n'est pas valide	Indique que l'ID hôte ou l'ID de banque indiqué est non valide. Spécifiez un nom d'hôte valide.
EBICSCL2331	La combinaison d'ID de partenaire et d'ID utilisateur n'est pas valide	Indique que la combinaison de l'ID utilisateur et de l'ID de partenaire associé n'est pas valide. Spécifiez une combinaison valide.
EBICSCL2332	L'ID système n'est pas valide	Indique que l'ID système spécifié est non valide. Spécifiez un ID système valide.
EBICSCL2333	Paramètre obligatoire manquant dans les métadonnées de la commande	Indique qu'un paramètre obligatoire dans les métadonnées de la commande n'est pas inclus. Recherchez le paramètre manquant dans le fichier ordermetadata.xml et indiquez une valeur valide pour le paramètre.
EBICSCL2334	Le moyen de sécurité n'est pas valide	Indique que la valeur spécifiée pour le moyen de sécurité n'est pas valide. Entrez un numéro de sécurité à quatre chiffres, compris entre 0100 et 0499.
EBICSCL2335	Impossible d'analyser le document principal dans le flux de travail	Revérifiez la configuration et lancez la transaction.
EBICSCL2336	Clé publique de chiffrement non trouvée pour la banque	Envoyez par téléchargement une clé de chiffrement valide.
EBICSCL2337	Impossible d'extraire la clé pour utilisation	La clé vers l'alias n'a pas pu être extraite lors de la signature ou du chiffrement des données de commande.
EBICSCL2338	Envoi par téléchargement de segments vers l'hôte	Le segment de données de commande a été envoyé par téléchargement au serveur.
EBICSCL2339	Réception par téléchargement de segments de l'hôte	Le segment de données de commande a été reçu par téléchargement du serveur.
EBICSCL2340	Nombre total calculé de segments à envoyer par téléchargement	Le client EBICS calcule le nombre total de segments de données d'une commande à envoyer par téléchargement.

Tableau 31. Codes de retour associés aux événements (suite)

Code de retour	Message d'événement	Description
EBICSCL2341	Nombre total calculé de segments à recevoir par téléchargement	Le client EBICS reçoit le nombre total de segments de données d'une commande à recevoir par téléchargement.
EBICSCL2342	La valeur de soumission automatique n'est pas valide	Indique que la valeur définie pour la soumission automatique n'est pas valide et que la commande ne peut pas être soumise automatiquement. Entrez une valeur valide pour le paramètre autosubmit. Les valeurs valides sont true (vrai) et false (faux).
EBICSCL2343	La valeur de code pays n'est pas valide	Indique que l'abréviation d'un pays est non valide. Indiquez un format valide pour les abréviations de pays.
EBICSCL2344	L'hôte n'est pas encore actif	Indique que le serveur de la banque n'est pas encore actif. Téléchargez les clés bancaires en utilisant le type de commande HPB et validez les clés bancaires.
EBICSCL2345	L'utilisateur n'est pas encore prêt	Indique que l'initialisation de l'abonné pour l'utilisateur n'est pas encore terminée. Générez les lettres INI et HIA pour l'utilisateur associé au partenaire et envoyez-les à la banque pour validation.
EBICSCL2346	Écriture des données de réponse dans la boîte aux lettres réussie	Indique que la réponse reçue de la banque a été stockée dans la boîte aux lettres de l'utilisateur.
EBICSCL2347	Échec de l'écriture des données de réponse dans la boîte aux lettres	L'échec de l'écriture des données de réponse dans une boîte aux lettres peut être due à des droits d'accès incorrects à cette boîte aux lettres. Pour plus d'informations, consultez le fichier journal ebicsClient.log.
EBICSCL2348	Erreur d'insertion du message dans la boîte aux lettres	Indique que le message n'a pas pu être envoyé par téléchargement dans la boîte aux lettres.
EBICSCL2349	Aucune réponse du serveur	Indique que le serveur n'a pas répondu lorsqu'une demande a été envoyée au serveur.

Tableau 31. Codes de retour associés aux événements (suite)

Code de retour	Message d'événement	Description
EBICSCL2350	Réponse non valide du serveur	Indique que le serveur a renvoyé une réponse non valide lorsqu'une demande a été envoyée au serveur.
EBICSCL2392	Paramètre obligatoire pour HttpClient manquant	Indique que le nom de l'adaptateur du client HTTP configuré a la valeur nulle, que des propriétés de l'adaptateur sont manquantes, ou que l'hôte ou le port n'est pas configuré correctement. Si SSL est activé, le certificat de l'autorité de certification n'est pas configuré.
EBICSCL2393	Instance HttpClient introuvable	Indique que l'instance d'adaptateur du client HTTP est manquante.
EBICSCL2394	Erreur lors de la fermeture de la session HTTP avec le serveur	Indique qu'une erreur s'est produite lors de la fermeture de la session HTTP avec le serveur. Il est possible qu'une session valide n'ait pas été trouvée.
EBICSCL2395	Hôte introuvable	Indique que l'hôte ou le port n'est pas configuré correctement.
EBICSCL2396	Échec d'établissement d'une liaison	Lors de la connexion au serveur à l'aide de SSL, la connexion peut échouer, par exemple en raison de certificats non valides.
EBICSCL2398	La connexion à l'hôte spécifié n'a pas pu être établie	Indique que le client n'a pas pu se connecter à un hôte même si la session a démarré correctement.
EBICSCL2351	Longueur de clé non valide pour la signature	Indique que la longueur des clés techniques bancaires est non valide pour la signature. Vérifiez que la longueur de clé est égale ou supérieure à 1 536 bits et égale ou inférieure à 4 096 bits. Pour plus d'informations sur la définition des longueurs de clé spécifiques à EBICS pour la signature électronique, le chiffrement et l'authentification, voir la <i>Spécification EBICS, version 2.5</i> .

Tableau 31. Codes de retour associés aux événements (suite)

Code de retour	Message d'événement	Description
EBICSCL2352	Longueur de clé non valide pour l'authentification	Indique que la longueur des clés techniques bancaires est non valide pour l'identification et l'authentification. Vérifiez que la longueur de clé est égale ou supérieure à 1 024 bits et égale ou inférieure à 16 384 bits. Pour plus d'informations sur la définition des longueurs de clé spécifiques à EBICS pour la signature électronique, le chiffrement et l'authentification, voir la <i>Spécification EBICS, version 2.5</i> .
EBICSCL2353	Longueur de clé non valide pour le chiffrement	Indique que la longueur des clés techniques bancaires est non valide pour le chiffrement. Vérifiez que la longueur de clé est égale ou supérieure à 1 024 bits et égale ou inférieure à 16 384 bits. Pour plus d'informations sur la définition des longueurs de clé spécifiques à EBICS pour la signature électronique, le chiffrement et l'authentification, voir la <i>Spécification EBICS, version 2.5</i> .
EBICSCL2354	Erreur lors du démarrage de la session HTTP avec le serveur	Indique qu'une erreur s'est produite lors du démarrage d'une session HTTP avec le serveur.
EBICSCL2355	Erreur lors de l'analyse syntaxique du document OrderMetadata avec l'ID de message	Vérifiez si le schéma XML est bien formé ou non.
EBICSCL2356	L'abonné technique n'a pas les droits nécessaires pour être un délégué de l'utilisateur spécifié	Configurez l'utilisateur technique et associez-le à un utilisateur existant.
EBICSCL2357	Erreur lors de la tentative de récupération des messages à partir de la boîte aux lettres	Indique qu'une erreur s'est produite lors de la récupération d'un message dans la boîte aux lettres.
EBICSCL2358	Erreur lors de l'analyse syntaxique du document de métadonnées de commande	Vérifiez si le schéma XML est bien formé.

Tableau 31. Codes de retour associés aux événements (suite)

Code de retour	Message d'événement	Description
EBICSCL2359	Application de la signature rejetée	Application de signature rejetée car les conditions de signature sont déjà remplies pour la commande.
EBICSCL2360	Application de la soumission rejetée	L'application de la soumission a été rejetée car la commande a déjà été soumise à la banque.
EBICSCL2361	Le fichier de métadonnées de commande n'est pas un fichier zip ou aucun fichier n'est présent dans le zip	Assurez-vous que le format du fichier ordermetadata est compressé et que le contenu du fichier zip est valide.
EBICSCL2362	Nombre incorrect de fichiers présents dans le zip de métadonnées de commande	Indique que le nombre de fichiers présents dans le fichier ordermetadata.zip est incorrect. Par exemple, lors de la soumission d'un type de commande FUL à partir d'un système dorsal, ce message s'affiche si le fichier zip ne contient pas de données de charge et/ou de fichier ordermetadata.xml.
EBICSCL2363	Fichier nommé ordermetadata.xml manquant dans le zip de métadonnées de commande	Assurez-vous que le fichier zip contient un fichier nommé ordermetadata.xml.
EBICSCL2364	Fichier de charge manquant dans le zip de métadonnées de commande pour le type de commande FUL	Assurez-vous que le fichier zip contient les données de commande de charge pour le type de commande FUL.
EBICSCL2365	Erreur lors de la tentative de récupération de l'URL de transport ou d'autres paramètres de transport obligatoires	Indique que l'URL d'hôte est mal formée ou que le client ne peut pas récupérer les détails de configuration HTTP de la base de données.
EBICSCL2366	Erreur lors du déchiffrement des données	Une erreur s'est produite lors du déchiffrement des données. Il existe plusieurs raisons. Par exemple, les données en cours de chiffrement avec le mauvais certificat ou des données chiffrées incomplètes peuvent entraîner cette erreur.
EBICSCL2367	Erreur lors du chiffrement des données	Une erreur s'est produite lors du chiffrement des données. Il existe plusieurs raisons. Par exemple, une clé manquante ou non valide peut entraîner cette erreur.

Tableau 31. Codes de retour associés aux événements (suite)

Code de retour	Message d'événement	Description
EBICSCL2368	Erreur lors de la création de l'authentification XML	Cette erreur peut être liée, par exemple, à un certificat non configuré ou impossible à récupérer.
EBICSCL2369	Erreur lors de la vérification de l'authentification XML	Cette erreur peut être liée, par exemple, à un certificat non configuré ou impossible à récupérer.
EBICSCL2370	Code de retour inattendu du serveur	Le serveur a renvoyé une erreur non définie dans la base de données du client.
EBICSCL2371	Erreur interne EBICS Client	Une erreur interne s'est produite pendant le traitement d'une demande EBICS.
EBICSCL2403	Erreur de conformité NIST	Erreur de conformité NIST. Vérifiez si l'algorithme/la complexité de la clé utilisé(e) est conforme au NIST dans le mode de conformité NIST actuellement configuré.
EBICSCL2404	Certificat de signature non émis par une autorité de certification	Certificat de signature non émis par une autorité de certification (AC). Nom distinctif de l'émetteur : \${0}.
EBICSCL2405	Non concordance de version du protocole EBICS : le serveur répond avec une version différente de celle du type de commande pour	Non concordance de version du protocole EBICS : le type de commande INI a été émis dans la version H003 mais le serveur EBICS a envoyé une réponse pour la version du protocole H004.

Codes de retour associés à la fonction HPB

Tableau 32. Codes de retour associés à la fonction HPB

Code de retour	Message d'événement	Description
EBICSCL1701	Échec de création de la demande HPB EBICS	Une erreur s'est produite lors de la création d'une demande HPB.
EBICSCL1702	Création de la demande HPB EBICS réussie	La demande de commande HPB a été créée.
EBICSCL1703	Échec de l'analyse syntaxique de la réponse HPB EBICS	Une erreur s'est produite lors de l'analyse syntaxique d'une réponse HPB.
EBICSCL1704	Analyse syntaxique de la réponse HPB EBICS réussie	La réponse HPB a été analysée syntaxiquement.
EBICSCL1705	Décompression de la réponse HPB EBICS réussie	La réponse HPB a été décompressée.

Tableau 32. Codes de retour associés à la fonction HPB (suite)

Code de retour	Message d'événement	Description
EBICSCL1706	Échec de décompression de la réponse HPB EBICS	Une erreur s'est produite lors de la décompression d'une réponse HPB.
EBICSCL1707	Échec de sauvegarde des certificats bancaires HPB EBICS	Une erreur s'est produite lors de la sauvegarde des clés bancaires.
EBICSCL1708	Sauvegarde des certificats bancaires HPB EBICS réussie	La clés bancaires HPB ont été sauvegardées.

Codes de retour associés aux clés

Tableau 33. Codes de retour associés aux clés

Code de retour	Message d'événement	Description
EBICSCL2372 à EBICSCL2381	Impossible d'extraire la clé privée pour utilisation	<p>Les principales raisons de l'échec de la récupération des clés privées sont les suivantes :</p> <ul style="list-style-type: none"> • Certificat de système introuvable dans la base de données • Certificat expiré • Certificat pas encore valide • Certificat mis en attente • Certificat révoqué • Signature d'émetteur non valide pour un certificat dans la chaîne • Échec de validation du chemin d'accès du certificat • Erreur dans le certificat • Erreur lors de la récupération du certificat • Erreur lors de la récupération de la clé dans le magasin de clés RSA

Tableau 33. Codes de retour associés aux clés (suite)

Code de retour	Message d'événement	Description
EBICSCL2382 à EBICSCL2391	Impossible d'extraire la clé publique pour utilisation	<p>Les principales raisons de l'échec de la récupération des clés publiques sont les suivantes :</p> <ul style="list-style-type: none"> • Clé introuvable dans la base de données • Certificat expiré • Certificat pas encore valide • Certificat mis en attente • Certificat révoqué • Signature d'émetteur non valide pour un certificat dans la chaîne • Échec de validation du chemin d'accès du certificat • Erreur dans le certificat • Erreur lors de la récupération du certificat • Erreur lors de la récupération de la clé dans le magasin de clés RSA

Codes de retour associés à la génération d'ID de commande

Tableau 34. Codes de retour associés à la génération d'ID de commande

Code de retour	Message d'événement	Description
EBICSCL2399	Génération de l'ID de commande réinitialisée	Indique que les trois dernières valeurs alphanumériques de l'ID de commande, qui s'échelonnent de 000 à zzz, ont été réinitialisées à 000.
EBICSCL2400	Échec de la journalisation de la commande dans le système EBICS Client	L'ID de commande existe déjà dans le système pour l'ID de partenaire. Contactez l'administrateur pour remédier au problème.
EBICSCL2401	Échec de la génération de l'ID de commande	Dans un scénario multi-noeud, cet incident se produit quand un des noeuds ne régénère pas le cache de l'ID de commande et, par conséquent, n'arrive pas à générer un ID de commande pour une commande particulière.
EBICSCL2402	Erreur de configuration du cache de l'ID de commande	Vérifiez la configuration du cache de l'ID de commande sous Propriétés système.

Codes de retour techniques

Tableau 35. Codes de retour techniques

Code de retour	Message d'événement	Description
ESRVT011000	[t011000] EBICS_DOWNLOAD_POSTPROCESS_DONE	Accusé de réception positif de la réponse EBICS envoyée au client à partir du serveur.
ESRVT011001	[t011001] EBICS_DOWNLOAD_POSTPROCESS_SKIPPED	Accusé de réception négatif de la réponse EBICS envoyée au client à partir du serveur.
ESRVT011101	[t011101] EBICS_TX_SEGMENT_NUMBER_UNDERRUN	Le serveur met fin à la transaction si le client, dans une transaction d'envoi par téléchargement, a indiqué un nombre très élevé de segments (par rapport au nombre spécifié lors de la phase d'initialisation) devant lui être transmis.
ESRVT031001	[t031001] EBICS_ORDER_PARAMS_IGNORED	Les paramètres de commande fournis qui ne sont pas pris en charge par la banque sont ignorés.
ESRVT061001	[t061001] EBICS_AUTHENTICATION_FAILED	La banque n'a pas pu vérifier la signature d'identification et d'authentification d'une demande EBICS.
ESRVT061002	[t061002] EBICS_INVALID_REQUEST	Le message XML EBICS reçu n'est pas conforme aux spécifications EBICS.
ESRVT061099	[t061099] EBICS_INTERNAL_ERROR	Une erreur interne s'est produite pendant le traitement d'une demande EBICS.
ESRVT061101	[t061101] EBICS_TX_RECOVERY_SYNC	Si la banque prend en charge la récupération de transaction, elle vérifie si une transaction d'envoi par téléchargement peut être récupérée. Le serveur se synchronise avec le client pour récupérer la transaction.
ESRVT091002	[t091002] EBICS_INVALID_USER_OR_USER_STATE	Erreur due à une combinaison non valide d'ID utilisateur ou à un état incorrect d'abonné.
ESRVT091003	[t091003] EBICS_USER_UNKNOWN	La signature d'identification et d'authentification de l'utilisateur technique a été vérifiée avec succès mais l'abonné non technique n'est pas connu de la banque.
ESRVT091004	[t091004] EBICS_INVALID_USER_STATE	La signature d'identification et d'authentification de l'utilisateur technique a été vérifiée avec succès et l'abonné non technique est connu de la banque, mais l'utilisateur n'est pas à l'état 'Prêt'.

Tableau 35. Codes de retour techniques (suite)

Code de retour	Message d'événement	Description
ESRVT091005	[t091005] EBICS_INVALID_ORDER_TYPE	Lors de la vérification, la banque a détecté que le type de commande indiqué était non valide.
ESRVT091006	[t091006] EBICS_UNSUPPORTED_ORDER_TYPE	Lors de la vérification, la banque a détecté que le type de commande indiqué était valide mais non pris en charge par elle.
ESRVT091007	(Protocole H003) [t091007] EBICS_USER_AUTHENTICATION_REQUIRED (Protocole H004) [t091007] EBICS_DISTRIBUTED_SIGNATURE_AUTHORISATION_FAILED	L'abonné ne dispose d'aucune autorisation de signature pour la commande référencée dans l'administration VEU.
ESRVT091008	[t091008] EBICS_BANK_PUBKEY_UPDATE_REQUIRED	La banque vérifie la valeur hachée envoyée par l'utilisateur. Si la valeur hachée ne correspond pas aux clés publiques en cours, la banque met fin à l'initialisation de la transaction.
ESRVT091009	[t091009] EBICS_SEGMENT_SIZE_EXCEEDED	Si la taille du segment de données de commande transmis dépasse 1 Mo, la transaction est arrêtée.
ESRVT091010	[t091010] EBICS_INVALID_XML	Le schéma XML n'est pas conforme aux spécifications EBICS.
ESRVT091011	[t091011] EBICS_INVALID_HOST_ID	L'ID hôte transmis n'est pas connu de la banque.
ESRVT091101	[t091101] EBICS_TX_UNKNOWN_TXID	L'ID de transaction fourni n'est pas valide.
ESRVT091102	[t091102] EBICS_TX_ABORT	Si la banque prend en charge la récupération de transaction, elle vérifie si une transaction d'envoi par téléchargement peut être récupérée. Si la transaction ne peut pas être récupérée, la banque met fin à la transaction.
ESRVT091103	[t091103] EBICS_TX_MESSAGE_REPLAY	Pour empêcher la réexécution, la banque compare la valeur nonce reçue à la liste des valeurs nonce déjà reçues qui sont stockées localement. Si la valeur nonce reçue est supérieure à la période de tolérance indiquée par la banque, la réponse EBICS_TX_MESSAGE_REPLAY est renvoyée.

Tableau 35. Codes de retour techniques (suite)

Code de retour	Message d'événement	Description
ESRVT091104	[t091104] EBICS_TX_SEGMENT_NUMBER_EXCEEDED	Le numéro de série du segment de données de commande transmis doit être inférieur ou égal au nombre total de segments de données devant être transmis. La transaction est arrêtée si le nombre de segments de données de commande transmis dépasse le nombre total de segments de données.
ESRVT091112	[t091112] EBICS_INVALID_ORDER_PARAMS	Dans une demande HVT, l'abonné indique la commande pour laquelle il souhaite extraire les détails de transaction VEU. La demande HVT indique également la position de décalage dans le fichier de commande d'origine qui marque le point de départ des détails de transaction à transmettre. Les détails de la commande figurant après la position de décalage indiquée sont renvoyés. Si la valeur indiquée pour le décalage est plus élevée que le nombre total de détails de la commande, l'erreur EBICS_INVALID_ORDER_PARAMS est renvoyée.
ESRVT091113	[t091113] EBICS_INVALID_REQUEST_CONTENT	La demande EBICS n'est pas conforme à la définition de schéma XML indiquée pour chaque demande.
ESRVT091117	[t091117] EBICS_MAX_ORDER_DATA_SIZE_EXCEEDED	La banque ne prend pas en charge la taille de la commande demandée.
ESRVT091118	[t091118] EBICS_MAX_SEGMENTS_EXCEEDED	Le nombre de segments soumis pour l'envoi par téléchargement est très élevé.
ESRVT091119	[t091119] EBICS_MAX_TRANSACTIONS_EXCEEDED	Le nombre maximal de transactions parallèles par client est dépassé.
ESRVT091120	[t091120] EBICS_PARTNER_ID_MISMATCH	L'ID de partenaire du fichier de signature électronique est différent de celui de l'émetteur.

Tableau 35. Codes de retour techniques (suite)

Code de retour	Message d'événement	Description
ESRVT091121	[t091121] EBICS_INCOMPATIBLE_ORDER_ATTRIBUTE	L'attribut de commande indiqué n'est pas compatible avec la commande du système de la banque. Si la banque dispose d'un fichier avec l'attribut DZHNN ou tout autre fichier de signature électronique (par exemple, avec l'attribut UZHNN) pour la même commande, l'utilisation des attributs de commande DZHNN n'est pas autorisée. De plus, si la banque a déjà la même commande et que celle-ci a été transmise avec les attributs de commande DZHNN, là encore l'utilisation des attributs de commande DZHNN n'est pas autorisée.
(Protocole H004) ESRVT091219	[t091219] EBICS_CERTIFICATES_VALIDATION_ERROR	Le serveur ne peut pas faire correspondre automatiquement le certificat avec les informations précédemment déclarées.

Codes de retour techniques bancaires

Tableau 36. Codes de retour techniques bancaires

Code de retour	Message d'événement	Description
ESRVB011301	[b011301] EBICS_NO_ONLINE_CHECKS	La banque ne prend pas en charge la vérification préliminaire des commandes mais la demande EBICS contient des données relatives à la vérification préliminaire de la commande.
ESRVB091001	[b091001] EBICS_DOWNLOAD_SIGNED_ONLY	Le système de la banque accepte uniquement les données de commande technique bancaire de téléchargement signées pour la demande. Si l'abonné définit les attributs de commande à DZHNN et qu'il demande les données de téléchargement sans la signature électronique de la banque, l'initialisation de la transaction est arrêtée.

Tableau 36. Codes de retour techniques bancaires (suite)

Code de retour	Message d'événement	Description
ESRVB091002	[b091002] EBICS_DOWNLOAD_UNSIGNED_ONLY	Le système de la banque accepte uniquement les données de commande de téléchargement non signées pour la demande. Lorsqu'il est convenu que l'abonné peut télécharger uniquement des données de commande sans la signature électronique de la banque, s'il définit les attributs de commande à OZHNN et demande les données de téléchargement avec la signature électronique de la banque, l'initialisation de la transaction est arrêtée.
ESRVB090003	[b090003] EBICS_AUTHORISATION_ORDER_TYPE_FAILED	L'abonné n'est pas autorisé à soumettre des commandes du type de commande sélectionné. Si l'autorisation fait défaut au moment où la banque vérifie que l'abonné dispose d'une autorisation technique bancaire de signature pour la commande, la transaction est annulée.
ESRVB090004	[b090004] EBICS_INVALID_ORDER_DATA_FORMAT	Les données de commande transmises ne correspondent pas au format spécifié.
ESRVB090005	[b090005] EBICS_NO_DOWNLOAD_DATA_AVAILABLE	Si les données de réception par téléchargement ne sont pas disponibles, la transaction EBICS est arrêtée.
ESRVB090006	[b090006] EBICS_UNSUPPORTED_REQUEST_FOR_ORDER_INSTANCE	Dans certaines transactions commerciales, il n'est pas possible d'extraire les informations détaillées des données de commande.
ESRVB091105	[b091105] EBICS_RECOVERY_NOT_SUPPORTED	Si la banque ne prend pas en charge la récupération de transaction, la transaction d'envoi par téléchargement est arrêtée.
ESRVB091111	[b091111] EBICS_INVALID_SIGNATURE_FILE_FORMAT	Le fichier de signature électronique soumis n'est pas conforme au format défini.
ESRVB091114	[b091114] EBICS_ORDERID_UNKNOWN	Lors de la vérification, la banque a détecté que la commande ne faisait pas partie du système de traitement VEU.
ESRVB091115	[b091115] EBICS_ORDERID_ALREADY_EXISTS	Le numéro de commande soumis existe déjà.

Tableau 36. Codes de retour techniques bancaires (suite)

Code de retour	Message d'événement	Description
ESRVB091116	[b091116] EBICS_PROCESSING_ERROR	Des erreurs liées à l'activité se sont produites lors du traitement d'une demande EBICS.
ESRVB091201	[b091201] EBICS_KEYMGMT_UNsupported_VERSION_SIGNATURE	Lors du traitement d'une demande INI, il s'est avéré que les données de commande contenaient une version incorrecte du processus de signature technique bancaire.
ESRVB091202	[b091202] EBICS_KEYMGMT_UNsupported_VERSION_AUTHENTICATION	Lors du traitement d'une demande HIA, il s'est avéré que les données de commande contenaient une version incorrecte du processus de signature d'identification et d'authentification.
ESRVB091203	[b091203] EBICS_KEYMGMT_UNsupported_VERSION_ENCRYPTION	Lors du traitement d'une demande HIA, il s'est avéré que les données de commande contenaient une version incorrecte du processus de chiffrement.
ESRVB091204	[b091204] EBICS_KEYMGMT_KEYLENGTH_ERROR_SIGNATURE	Lors du traitement d'une demande INI, il s'est avéré que les données de commande contenaient une clé technique bancaire de longueur incorrecte.
ESRVB091205	[b091205] EBICS_KEYMGMT_KEYLENGTH_ERROR_AUTHENTICATION	Lors du traitement d'une demande HIA, il s'est avéré que les données de commande contenaient une clé d'identification et d'authentification de longueur incorrecte.
ESRVB091206	[b091206] EBICS_KEYMGMT_KEYLENGTH_ERROR_ENCRYPTION	Lors du traitement d'une demande HIA, il s'est avéré que les données de commande contenaient une clé de chiffrement de longueur incorrecte.
ESRVB091207	[b091207] EBICS_KEYMGMT_NO_X509_SUPPORT	Une clé publique de type X509 a été envoyée à la banque mais celle-ci ne prend en charge que le type de valeur de clé publique.
ESRVB091208	[b091208] EBICS_X509_CERTIFICATE_EXPIRED	Le certificat a expiré et n'est plus valide.
ESRVB091209	[b091209] EBICS_X509_CERTIFICATE_NOT_VALID_YET	Le certificat n'est pas valide car il n'est pas encore actif.

Tableau 36. Codes de retour techniques bancaires (suite)

Code de retour	Message d'événement	Description
ESRVB091210	[b091210] EBICS_X509_WRONG_ KEY_USAGE	Lors de la vérification de l'utilisation de la clé du certificat, la banque a détecté que le certificat n'avait pas été émis pour l'utilisation en cours.
ESRVB091211	[b091211] EBICS_X509_WRONG_ ALGORITHM	Lors de la vérification de l'algorithme du certificat, la banque a détecté que le certificat n'avait pas été émis pour l'utilisation en cours.
ESRVB091212	[b091212] EBICS_X509_INVALID_ THUMBPRINT	L'empreinte numérique ne correspond pas au certificat.
ESRVB091213	[b091213] EBICS_X509_CTL_INVALID	Lors de la vérification du certificat, la banque a détecté que la liste de confiance du certificat n'était pas valide.
ESRVB091214	[b091214] EBICS_X509_UNKNOWN_ CERTIFICATE_AUTHORITY	Il n'est pas possible de vérifier la chaîne car l'autorité de certification est inconnue.
ESRVB091215	[b091215] EBICS_X509_INVALID_ POLICY	Le processus de vérification de certificat a détecté que le certificat possédait une règle non valide.
ESRVB091216	[b091216] EBICS_X509_INVALID_ BASIC_CONSTRAINTS	Le processus de vérification de certificat a détecté que les contraintes de base n'étaient pas valides.
ESRVB091217	[b091217] EBICS_ONLY_X509_ SUPPORT	La banque prend en charge l'évaluation des données X.509 uniquement.
ESRVB091218	[b091218] EBICS_KEYMGMT_ DUPLICATE_KEY	La clé envoyée pour l'authentification ou le chiffrement est identique à la clé de signature.
ESRVB091301	[b091301] EBICS_SIGNATURE_ VERIFICATION_FAILED	La vérification de la signature électronique a échoué.
ESRVB091302	[b091302] EBICS_ACCOUNT_ AUTHORISATION_FAILED	La vérification préliminaire de l'autorisation de compte a échoué.
ESRVB091303	[b091303] EBICS_AMOUNT_CHECK_ FAILED	La vérification préliminaire du plafond du compte a échoué.
ESRVB091304	[b091304] EBICS_SIGNER_UNKNOWN	Le signataire de la commande n'est pas un abonné valide.
ESRVB091305	[b091305] EBICS_INVALID_ SIGNER_STATE	L'état du signataire n'est pas admissible.
ESRVB091306	[b091306] EBICS_DUPLICATE_ SIGNATURE	Le signataire a déjà signé la commande.

Codes de retour associés à la fonction VEU

Tableau 37. Codes de retour associés à la fonction VEU

Code de retour	Message d'événement	Description
EBICSCL1050	Erreur lors de la déconversion du paramètre ResponseOrderData et de sa conservation dans la base de données	Indique que les données de commande de réponse ne sont pas constituées correctement.

Codes de retour associés aux événements de console

Tableau 38. Codes de retour associés aux événements de console

Code de retour	Message d'événement	Description
EBICSCL9000	Utilisateur créé avec succès	Le profil utilisateur a été créé.
EBICSCL9001	Utilisateur mis à jour avec succès	Le profil utilisateur a été mis à jour.
EBICSCL9002	Utilisateur supprimé avec succès	Le profil utilisateur a été supprimé.
EBICSCL9003	Échec de création de l'utilisateur	La création d'un profil d'utilisateur a échoué. Le profil utilisateur existe peut-être déjà ou les paramètres de configuration de l'utilisateur sont associés à des valeurs non valides.
EBICSCL9004	Échec de mise à jour de l'utilisateur	Vérifiez si les paramètres de configuration de l'utilisateur ont des valeurs valides ou si la connexion à la base de données est arrêtée.
EBICSCL9005	Échec de suppression de l'utilisateur	Vérifiez si les paramètres de configuration de l'utilisateur ont des valeurs valides ou si la connexion à la base de données est arrêtée.

Codes de retour associés à la connexion

Tableau 39. Codes de retour associés à la connexion

Code de retour	Message d'événement	Description
EBICSCL9020	Utilisateur connecté avec succès	L'utilisateur a été connecté au système.
EBICSCL9021 et EBICSCL9022	Échec de connexion de l'utilisateur	La tentative de connexion au concentrateur a échoué en raison d'un nom ou d'un mot de passe utilisateur incorrect ou de droits insuffisants.
EBICSCL9023	L'utilisateur ne dispose pas des droits d'accès à l'identificateur URI	Vérifiez que vous disposez des droits et du rôle appropriés pour accéder à l'identificateur URI.

Tableau 39. Codes de retour associés à la connexion (suite)

Code de retour	Message d'événement	Description
EBICSCL9024	Les fonctions suivantes doivent être associées à la licence EBICS Client	Obtenez la licence auprès du Support IBM.
EBICSCL9025	Le compte a été verrouillé	Le compte a été verrouillé car le nombre maximal de connexions infructueuses a été dépassé.

Codes de retour associés au format de fichier

Tableau 40. Codes de retour associés au format de fichier

Code de retour	Message d'événement	Description
EBICSCL9050	Format de fichier créé avec succès	Le format de fichier a été créé.
EBICSCL9051	Format de fichier mis à jour avec succès	Le format de fichier a été mis à jour.
EBICSCL9052	Échec de création du format de fichier	Vérifiez que les paramètres de configuration du format de fichier ont des valeurs valides ou que la connexion à la base de données est arrêtée.
EBICSCL9053	Échec de mise à jour du format de fichier	Vérifiez que les paramètres de configuration du format de fichier ont des valeurs valides ou que la connexion à la base de données est arrêtée.
EBICSCL9054	Format de fichier supprimé avec succès	Le format de fichier a été supprimé.
EBICSCL9055	Échec de suppression du format de fichier	Vérifiez si la connexion à la base de données est opérationnelle ou que le type de commande est associé au format de fichier approprié.

Codes de retour associés à la banque

Tableau 41. Codes de retour associés à la banque

Code de retour	Message d'événement	Description
EBICSCL9070	Banque créée avec succès	Le profil de banque a été créé.
EBICSCL9071	Banque mise à jour avec succès	Le profil de banque a été mis à jour.
EBICSCL9072	Échec de création de la banque	Vérifiez que les paramètres de configuration de la banque ont des valeurs valides ou si la connexion à la base de données est arrêtée.

Tableau 41. Codes de retour associés à la banque (suite)

Code de retour	Message d'événement	Description
EBICSCL9073	Échec de mise à jour de la banque	Vérifiez que les paramètres de configuration de la banque ont des valeurs valides ou si la connexion à la base de données est arrêtée.
EBICSCL9074	Banque supprimée avec succès	Le profil de banque a été supprimé.
EBICSCL9075	Échec de suppression de la banque	Vérifiez que la connexion à la base de données est active.
EBICSCL9076	Clé bancaire validée avec succès	Le profil de banque a été validé.
EBICSCL9077	Échec de validation de la clé bancaire	La valeur hachée reçue de la banque ne correspond pas à celle qui est stockée dans le système du client EBICS.

Codes de retour associés à la soumission de commande

Tableau 42. Codes de retour associés à la soumission de commande

Code de retour	Message d'événement	Description
EBICSCL9090	Commande soumise avec succès	La commande a été soumise.
EBICSCL9095	Échec de soumission de la commande	Les raisons de cet échec sont notamment les suivantes : l'émetteur ne dispose pas des droits nécessaires, les certificats ne sont pas valides ou la validation des clés bancaires a échoué.

Codes de retour associés à l'offre

Tableau 43. Codes de retour associés à l'offre

Code de retour	Message d'événement	Description
EBICSCL9101	Offre créée avec succès	L'offre a été créée.
EBICSCL9102	Échec de création de l'offre	Vérifiez que la connexion à la base de données est active.
EBICSCL9103	Offre mise à jour avec succès	L'offre a été mise à jour.
EBICSCL9104	Échec de mise à jour de l'offre	Vérifiez que la connexion à la base de données est active.
EBICSCL9105	Offre supprimée avec succès	L'offre a été supprimée.
EBICSCL9106	Échec de suppression de l'offre	Vérifiez que la connexion à la base de données est active.

Codes de retour associés aux droits d'utilisateur

Tableau 44. Codes de retour associés aux droits d'utilisateur

Code de retour	Message d'événement	Description
EBICSCL9120	Droits d'utilisateur créés avec succès	Le droit d'utilisateur a été créé.
EBICSCL9121	Échec de création des droits d'utilisateur	Vérifiez que la connexion à la base de données est active.
EBICSCL9122	Droits d'utilisateur mis à jour avec succès	Le droit d'utilisateur a été mis à jour.
EBICSCL9123	Échec de mise à jour des droits d'utilisateur	Vérifiez que la connexion à la base de données est active.
EBICSCL9124	Droits d'utilisateur supprimés avec succès	Le droit d'utilisateur a été supprimé.
EBICSCL9125	Échec de suppression des droits d'utilisateur	Vérifiez que la connexion à la base de données est active.

Codes de retour associés à la signature en attente

Tableau 45. Codes de retour associés à la signature en attente

Code de retour	Message d'événement	Description
EBICSCL9141	Signature soumise	La signature a été soumise.
EBICSCL9142	Échec de soumission de la signature	Vérifiez que la connexion à la base de données est active ou que le message a été écrit correctement dans la boîte aux lettres.
EBICSCL9143	Signature mise à jour	La signature a été mise à jour.
EBICSCL9144	Échec de mise à jour de la signature	Vérifiez que la connexion à la base de données est active ou que le message a été écrit correctement dans la boîte aux lettres.

Codes de retour associés à la signature VEU en attente

Tableau 46. Codes de retour associés à la signature VEU en attente

Code de retour	Message d'événement	Description
EBICSCL9151	Signature VEU soumise	La signature VEU a été soumise.
EBICSCL9152	Échec de soumission de la signature VEU	Vérifiez que la connexion à la base de données est active ou que le message a été écrit correctement dans la boîte aux lettres.

Index

A

activer le planning 17
adaptateur de système de fichiers 8

B

banque 2

C

certificat autosigné 17
certificat d'autorité de certification 18
certificat de système de clé 21
certificats de système 20
chemin d'accès absolu:définition 10
commandes, recherche 62
comptes utilisateur 6
conditions requises pour la
 configuration 3, 21
configurer les droits d'utilisateur 42
configurer un adaptateur de système de
 fichiers 8
configurer un utilisateur existant 22
configurer un utilisateur existant en tant
 qu'utilisateur du client EBICS 22
configurer un utilisateur technique 54
Créer des comptes utilisateur 6
créer un certificat autosigné 17
créer un droit d'utilisateur 43
créer un enregistrement d'identité 5
créer un format de fichier 40
créer un planning HAC 134
créer un profil de banque 33
créer une boîte aux lettres et affecter des
 droits d'accès 16
créer une offre 38

D

droits 85
droits d'accès à une boîte aux lettres 16
droits pour accéder à différentes
 pages 85

E

EBICS, présentation 1
enregistrement d'identité 5
enregistrer un certificat d'autorité de
 certification 18
enregistrer un certificat de système de
 clé 21
enregistrer un certificat de système de
 confiance 20
événements, recherche 59

G

gestion de profils dans le client
 EBICS 22

I

initialiser un utilisateur 46
interface de tableau de bord du client
 EBICS 1

M

mises à jour, valeurs des propriétés
 système 77
modifier un droit d'utilisateur 44
modifier un format de fichier 41
modifier un planning HAC 137
modifier un profil de banque 35
modifier un profil utilisateur 28
modifier une offre 39
mon profil 80

O

organisation 2

P

paramètres de commande 49
partenaire 2
présentation d'EBICS 1
profil 80
profils dans le client EBICS 22

R

récapitulatif des commandes 62
récapitulatif des événements 59
recherche d'événements 59
recherche de commandes 62
rechercher un droit d'utilisateur 44
rechercher un format de fichier 41
rechercher un planning HAC 136
rechercher un profil de banque 35
rechercher un profil utilisateur 27
rechercher une offre 39

S

soumission de commandes 48
supprimer un droit d'utilisateur 46
supprimer un format de fichier 42
supprimer un planning HAC 139
supprimer un profil de banque 37
supprimer un profil utilisateur 32
supprimer une offre 40

T

tâches en attente 66

U

utilisateur, droits 85
utilisateur ou abonné 2
utilisateur technique 54

V

valeurs des propriétés système 77
valider une clé bancaire 38
visualiser un planning HAC 137

Z

zones d'information de commande 48

Remarques

Ce document a été élaboré pour des produits et services offerts aux Etats-Unis. Ce document peut être disponible dans d'autres langues auprès d'IBM. Vous pouvez toutefois devoir détenir une copie du produit ou une version du produit dans cette langue pour pouvoir y accéder.

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services IBM non annoncés dans ce pays. Pour plus de détails, référez-vous aux documents d'annonce disponibles dans votre pays ou adressez-vous à votre partenaire commercial IBM. Toute référence à un produit, logiciel ou service IBM n'implique pas que seul ce produit, logiciel ou service IBM puisse être utilisé. Tout autre élément fonctionnellement équivalent peut être utilisé, s'il n'enfreint aucun droit d'IBM. Il est de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même les installations et applications réalisées avec des produits, logiciels ou services non expressément référencés par IBM.

IBM peut détenir des brevets ou des demandes de brevet couvrant les produits mentionnés dans le présent document. La remise de ce document ne vous donne aucun droit de licence sur ces brevets ou demandes de brevet. Si vous désirez recevoir des informations concernant l'acquisition de licences, veuillez en faire la demande par écrit à l'adresse suivante :

*IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
Etats-Unis*

Les informations sur les licences concernant les produits utilisant un jeu de caractères double octet peuvent être obtenues par écrit à l'adresse suivante :

*Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japon*

LE PRESENT DOCUMENT EST LIVRE "EN L'ETAT" SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFAÇON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE. Certaines juridictions n'autorisent pas l'exclusion des garanties implicites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Le présent document peut contenir des inexactitudes ou des coquilles. Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. IBM peut, à tout moment et sans préavis, modifier les produits et logiciels décrits dans ce document.

Les références à des sites Web non IBM sont fournies à titre d'information uniquement et n'impliquent en aucun cas une adhésion aux données qu'ils

contiennent. Les éléments figurant sur ces sites Web ne font pas partie des éléments du présent produit IBM et l'utilisation de ces sites relève de votre seule responsabilité.

IBM pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie des informations qui lui seront fournies.

Les licenciés souhaitant obtenir des informations permettant : (i) l'échange des données entre des logiciels créés de façon indépendante et d'autres logiciels (dont celui-ci), et (ii) l'utilisation mutuelle des données ainsi échangées, doivent adresser leur demande à :

*IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
Etats-Unis*

Ces informations peuvent être soumises à des conditions particulières, prévoyant notamment le paiement d'une redevance.

Le logiciel sous licence décrit dans ce document et tous les éléments sous licence disponibles s'y rapportant sont fournis par IBM conformément aux dispositions de l'ICA, des Conditions internationales d'utilisation des logiciels IBM ou de tout autre accord équivalent.

Les données de performances et les exemples de clients ne sont présentés qu'à des fins d'illustration. Les performances réelles peuvent varier en fonction des configurations et des conditions d'exploitation spécifiques.

Les informations concernant des produits non IBM ont été obtenues auprès des fournisseurs de ces produits, par l'intermédiaire d'annonces publiques ou via d'autres sources disponibles. IBM n'a pas testé ces produits et ne peut confirmer l'exactitude de leurs performances ni leur compatibilité. Elle ne peut recevoir aucune réclamation concernant des produits non IBM. Toute question concernant les performances de produits non IBM doit être adressée aux fournisseurs de ces produits.

Les instructions relatives aux intentions d'IBM pour ses opérations à venir sont susceptibles d'être modifiées ou annulées sans préavis, et doivent être considérées uniquement comme un objectif.

Tous les tarifs indiqués sont les prix de vente actuels suggérés par IBM et sont susceptibles d'être modifiés sans préavis. Les tarifs appliqués peuvent varier selon les revendeurs.

Ces informations sont fournies uniquement à titre de planification. Elles sont susceptibles d'être modifiées avant la mise à disposition des produits décrits.

Le présent document peut contenir des exemples de données et de rapports utilisés couramment dans l'environnement professionnel. Ces exemples mentionnent des noms fictifs de personnes, de sociétés, de marques ou de produits à des fins illustratives ou explicatives uniquement. Toute ressemblance avec des noms de personnes et de sociétés serait purement fortuite.

LICENCE DE COPYRIGHT :

Le présent logiciel contient des exemples de programmes d'application en langage source destinés à illustrer les techniques de programmation sur différentes plateformes d'exploitation. Vous avez le droit de copier, de modifier et de distribuer ces exemples de programmes sous quelque forme que ce soit et sans paiement d'aucune redevance à IBM, à des fins de développement, d'utilisation, de vente ou de distribution de programmes d'application conformes aux interfaces de programmation des plateformes pour lesquels ils ont été écrits ou aux interfaces de programmation IBM. Ces exemples de programmes n'ont pas été rigoureusement testés dans toutes les conditions. IBM ne peut donc pas garantir expressément ou implicitement la fiabilité, la maintenabilité ou le fonctionnement de ces programmes. Les programmes exemples sont fournis "en l'état", sans garantie d'aucune sorte. IBM ne sera en aucun cas responsable des dommages liés à l'utilisation de ces programmes exemples.

Toute copie totale ou partielle de ces programmes exemples et des oeuvres qui en sont dérivées doit comprendre une notice de copyright, libellée comme indiqué dans la colonne suivante.

© 2015.

Des segments de code sont dérivés des Programmes exemples d'IBM Corp.

© Copyright IBM Corp. 2015.

Marques

IBM, le logo IBM et ibm.com sont des marques d'International Business Machines Corp. dans de nombreux pays. Les autres noms de produits et de services peuvent appartenir à IBM ou à des tiers. La liste actualisée de toutes les marques d'IBM est disponible sur la page Web "Copyright and trademark information" à l'adresse www.ibm.com/legal/copytrade.shtml.

Adobe, le logo Adobe, PostScript et le logo PostScript sont des marques d'Adobe Systems Incorporated aux États-Unis et/ou dans certains autres pays.

IT Infrastructure Library est une marque de The Central Computer and Telecommunications Agency qui fait désormais partie de The Office of Government Commerce.

Intel, le logo Intel, Intel Inside, le logo Intel Inside, Intel Centrino, le logo Intel Centrino, Celeron, Intel Xeon, Intel SpeedStep, Itanium et Pentium sont des marques d'Intel Corporation ou de ses filiales aux États-Unis et/ou dans certains autres pays.

Linux est une marque de Linus Torvalds aux États-Unis et/ou dans certains autres pays.

Microsoft, Windows, Windows NT et le logo Windows sont des marques de Microsoft Corporation aux États-Unis et/ou dans certains autres pays.

ITIL est une marque de The Office of Government Commerce et est enregistrée au bureau américain Patent and Trademark Office.

UNIX est une marque enregistrée de The Open Group aux États-Unis et/ou dans certains autres pays.

Java™ ainsi que tous les logos et toutes les marques incluant Java sont des marques d'Oracle et/ou de ses sociétés affiliées.

Cell Broadband Engine est une marque de Sony Computer Entertainment, Inc. aux États-Unis et/ou dans certains autres pays et est utilisée sous licence.

Linear Tape-Open, LTO, le logo LTO, Ultrium et le logo Ultrium sont des marques de HP, IBM Corp. et Quantum aux États-Unis et/ou dans certains autres pays.

Connect Control Center, Connect:Direct, Connect:Enterprise, Gentran, Gentran:Basic, Gentran:Control, Gentran:Director, Gentran:Plus, Gentran:Realtime, Gentran:Server, Gentran:Viewpoint, Sterling Commerce, Sterling Information Broker et Sterling Integrator sont des marques de Sterling Commerce, Inc., une filiale d'IBM Company.

Les autres noms de sociétés, de produits et de services peuvent appartenir à des tiers.

Dispositions applicables à la documentation du produit

Les droits d'utilisation relatifs à ces publications sont soumis aux dispositions suivantes.

Applicabilité

Les présentes dispositions viennent s'ajouter à toute autre condition d'utilisation applicable au site Web IBM.

Usage personnel

Vous pouvez reproduire ces informations pour votre usage personnel, non commercial, sous réserve que toutes les mentions de propriété soient conservées. Vous ne devez pas distribuer, afficher ni réaliser des oeuvres dérivées à partir de tout ou partie de ces publications, sans l'autorisation expresse par écrit d'IBM.

Usage commercial :

Vous pouvez reproduire, distribuer et afficher ces publications uniquement au sein de votre entreprise, à condition que toutes les notices propriétaires soient préservées. Vous ne pouvez reproduire, distribuer, afficher tout ou partie de ces publications en dehors de votre entreprise, ou en faire des oeuvres dérivées, sans le consentement exprès d'IBM.

Droits

Excepté les droits d'utilisation expressément accordés dans le présent document, aucun autre droit, licence ou autorisation, implicite ou explicite, n'est accordé pour ces publications ou autres informations, données, logiciels ou droits de propriété intellectuelle contenus dans ces publications.

IBM se réserve le droit de retirer les autorisations accordées ici si, à sa discrétion, l'utilisation des publications s'avère préjudiciable à ses intérêts ou que, selon son appréciation, les instructions susmentionnées n'ont pas été respectées.

Vous ne pouvez télécharger, exporter ou réexporter ces informations qu'en total accord avec toutes les lois et règlements applicables dans votre pays, y compris les lois et règlements américains relatifs à l'exportation.

IBM N'OCTROIE AUCUNE GARANTIE SUR LE CONTENU DE CES PUBLICATIONS. LES PUBLICATIONS SONT LIVREES EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE EN CAS DE CONTREFAÇON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE.



Imprimé en France