Sterling B2B Integrator

EBICS Client User Guide

Version 5.2.5

Sterling B2B Integrator

EBICS Client User Guide

Version 5.2.5

Note
Before using this information and the product it supports, read the information in "Notices" on page 147.

Contents

EBICS Client User (V5.2.5 or later)

Using EBICS Client, a partner or partner user can configure and manage multiple banks, partners, and users. Multiple users can interact with multiple banks (EBICS Banking Servers) over HTTP or HTTPS and exchange EBICS-compliant transaction messages.

The Sterling B2B Integrator EBICS Client is a client server application. It provides an end-to-end EBICS solution for an organization to transact with banks

Partners can perform the following tasks in the EBICS Client dashboard interface:

- Configure users
- Configure banks
- Configure security settings for users
- Verify security settings of a bank
- Create and manage file formats
- Create and manage user permissions
- Create and manage offers
- Configure orders
- Submit orders
- View order-related events and reports
- Search for orders pending at the VEU management store in the server
- View and monitor pending tasks

The Sterling B2B Integrator EBICS Client supports EBICS Specification V2.5 for both French and German implementations.

Overview of EBICS

Electronic Banking Internet Communication Standard (EBICS) is an Internet-based communication and security standard. EBICS is a European banking standard. EBICS is primarily used for remote data transfer, such as corporate payment transactions, between an organization and a bank.

EBICS allows data file exchange independent of message standards and formats. EBICS uses an established digital signature and encryption procedures. EBICS features are based on international standards for internet communication and improved security, for example, XML, HTTPS, TLS, and SSL. EBICS also contains multi-bank capability, wherein corporate clients in countries that have adopted EBICS can transact with any bank in those countries using the same software.

The following entities are involved in EBICS Client transactions:

Organization
The organization or company that uses EBICS Client to transact with the bank.

Bank Financial institutions with which the organization transacts. The EBICS Banking Server is installed in the bank.

Partner
The department or unit in the organization that interacts with the bank.

User or Subscriber
Personnel in the department, who perform the EBICS transactions.

An organization has to fulfill a range of prerequisites for it to be able to implement bank-technical EBICS transactions with a particular bank. The basic prerequisite to implement EBICS transactions is the completion of a contract between the partner and the bank. The EBICS protocol defines bank transactions (order types) for communication. The following details are agreed upon in this contract:

- Type of business transactions.
- Information about the user's bank accounts.
- Information about the partners users working with the bank's system.
- Authorizations and permissions of the users.

The partner receives the access data of the bank (bank parameters) after the contract is signed. The bank configures the partner and user master data in the bank system in accordance with the contractual agreements. Other prerequisites include subscriber initialization, download of the bank's public certificates by the user, verification of the user's public certificates by the bank, and verification of the bank's certificates by the trading partner.

IBM® Sterling B2B Integrator offers a complete EBICS solution by providing a secure, flexible, and efficient platform to banks and organizations for performing the transactions. The implementation of this solution is divided into two major components: EBICS Banking Server and EBICS Client. EBICS Banking Server represents a bank and EBICS Client represents an organization. Both the server and the client are deployed over Sterling B2B Integrator.

Install EBICS Client Module Manually

When installing Sterling B2B Integrator 5.2.5 or when upgrading from a previous version of Sterling B2B Integrator to Sterling B2B Integrator 5.2.5, if you selected the **Financial Services Module** option from the Installation Manager, then the EBICS Client module is installed automatically.

Before you begin

You must have installed Sterling B2B Integrator. For information about installing and upgrading Sterling B2B Integrator, see the *Installation and Upgrade guides* on the Sterling B2B Integrator 5.2 Information Center.

About this task

You must manually install the EBICS Client module if one of the following criteria is met:

- You did not select the **Financial Services Module** option from the Installation Manager when installing Sterling B2B Integrator 5.2.5.
- You did not select the **Financial Services Module** option from the Installation Manager when upgrading from a previous version of Sterling B2B Integrator to Sterling B2B Integrator 5.2.5.
- You want to apply Sterling B2B Integrator 5.2.5 as a patch on the previous version of Sterling B2B Integrator 5.2.x.

To manually install the EBICS Client module, complete the following steps after installing or upgrading to Sterling B2B Integrator 5.2.5:

Note: If you are installing the EBICS Client module in a clustered environment, perform the following steps on each node of the installation instance.

Procedure

1. Stop Sterling B2B Integrator.
2. Close all command prompt windows.
3. If your database password is encrypted, decrypt the password.
4. Close all command prompt windows.
5. Update the license file to include the license for EBICS Client:
   a. Open a command prompt window.
   b. Run the following command:
      - For Microsoft Windows: *install_dir*\bin\AddLicenseSet.cmd *install_dir*\ properties\licensefiles\Fin_Serv_License.xml
      - For UNIX: *install_dir*\bin\AddLicenseSet.sh *install_dir*\ properties\licensefiles\Fin_Serv_License.xml
6. Install the EBICS Client JAR file:
   a. Open a command prompt window.
   b. Run the following command:
      - For Microsoft Windows: *install_dir*\bin\InstallService.cmd *install_dir*\packages\v_ebics_client_*version number_build number*.jar
      - For UNIX: *install_dir*\bin\InstallService.sh *install_dir*\packages\ v_ebics_client_*version number_build number*.jar
7. If you decrypted the database password, re-encrypt the password.
8. Start Sterling B2B Integrator.

Configuration Prerequisites

About this task

You must configure the following prerequisites accessing Sterling B2B Integrator before using EBICS Client:

Procedure

1. Check in the public and private part of the certificates into the System and Trusted store of Sterling B2B Integrator. Check in the required Certificate Authority (CA) certificates into the CA store of Sterling B2B Integrator or create a self-signed certificate. The following types of certificates are used for configuring a user:
   - Identification and authentication
   - Encryption
   - Signing
2. From the **Identities** menu of Sterling B2B Integrator, create an identity record for your organization, indicating your organization as the base identity. This identity name should correspond to the EBICS partner name.
3. From the **User Accounts** menu of Sterling B2B Integrator, create a User Account and assign permissions to the user. The user name should correspond to the EBICS user name.

4. Configure an adapter (such as File system adapter, HTTP(S) adapter, SFTP adapter, FTP(S) adapter) in Sterling B2B Integrator, that enables you to send and receive files and invokes the EBClientOrderPreProcess business process. For example, configure a File System Adapter to invoke the EBClientOrderPreProcess business process.
5. Configure the following mailboxes and associate them with each user.
   - EBClientOrderMetadata (preconfigured)
   - Download (Inbox)
   - Upload (Outbox)
6. Verify that the EBClientMailboxArrivedMessage business process is associated with the EBClientOrderMetadata Mailbox. The automatic routing rule triggers the business process to perform automated functions, such as notifying an interested party about an incoming message in the mailbox.

   Note: It is recommended that you do not modify the existing configuration for EBICS Client routing rules. Modifying the routing rule configuration may create duplicate subsets and duplicate orders for an order submission.
7. Ensure that the MailboxEvaluateAllAutomaticRulesSubMin Schedule is enabled.

Create an Identity Record

About this task

A trading partner is represented by an identity record. An identity record describes the trading partner and contains information referenced when a business process involving trading partners is run. For more information about identity record and trading partner, see the *Sterling B2B Integrator Trading Partner Management* documentation. To create an identity record:

Procedure

1. Log in to Sterling B2B Integrator.
2. From the **Administration Menu**, select **Trading Partner** > **Advanced** > **Identities**.
3. Under Create, next to New Identity, click **Go!**
4. On the Identities page, do one of the following:
   - To create an identity record that inherits all the components of an existing trading profile, select an identity record from **Select Base Identity**, and click **Next**.
   - To specify properties, leave **Select Base Identity** blank, and click **Next**.
5. Specify the Information settings. On the Information page, complete the following fields and click **Next**:

Information Fields	Description
Name	Required. Name for the identity record to create for this trading profile.
Reference URL	Optional. Uniform Resource Locator (URL) is the Internet address of the trading partner.
DUNS	Optional. Data Universal Numbering System (DUNS) is a unique nine-character company identification number issued by Dun & Bradstreet Corporation.

Information Fields	Description
Identifier	Required. Primary ID of this identity record. It could be a DUNS number, EDI interchange ID, e-mail address, or another unique string.
Address Line 1	Required. Conventional mailing address of the trading partner organization.
Address Line 2	Optional. Additional mailing address information of the trading partner organization.
City	Required. City where the trading partner is located.
State or Province	Optional. State or province where the organization of the trading partner represented by the identity is located.
Zip or Postal Code	Required. ZIP or postal code where the trading partner is located.
E-mail Address	Optional. E-mail address of the trading partner.
Telephone Number	Optional. Telephone number of the trading partner.
Time Zone	Optional. Time zone where the trading partner is located.
Country	Optional. Country where the trading partner is located.

6. Click **Finish** to add the identity.
7. Click **Return** to continue.

Create User Accounts

About this task

Before you begin, you need to know whether you are using local or external authentication:

- Local – Authentication is completed against the application database (default).
- External – Authentication is completed against an LDAP server. External authentication does not require the LDAP adapter, which is used with business processes and enables the system to communicate with local or remote LDAP servers using a Java Naming Directory Interface (JNDI).

If you are assigning one or more Authorized User Keys to this account, the keys must be obtained from your trading partner and checked in before creating the user account.

You also need to know the following information:

Table 1. create user accounts

Field	Description
User ID	Required. User ID for the user account you are creating. The user ID must be at least 5 characters long. For the MySQL database only, the login is not case sensitive. You should always use uniquely spelled IDs, so that one user does not accidentally use another user's ID.
Password (Local Authentication only)	Required for local users. Password for the user account you are creating. The password must be at least 6 characters long. This field does not display for external users.
Confirm Password (Local Authentication only)	Required for local users. Type the password a second time. This field does not display for external users.
Policy (Local Authentication only)	Optional. Password policy to associate with this user account. From the list, select from the policy you want to associate. This field does not display for external users. The system calculates the expiration date from the first date that the user logs on with this password.
Authentication Host (External Authentication only)	The Lightweight Directory Access Protocol (LDAP) server on which the user is being authenticated. The server or servers listed in this field are specified in the authentication_policy.properties.in file.
Session Timeout	Required. Amount of time in minutes that you can be inactive before you have to log in again. Time is in minutes.
Accessibility	Optional. Portion of the dashboard user interface that the user account has access to. The following are accessibility options: • Admin UI – Accesses the Admin Console pane in the dashboard only. • AS2 UI – Accesses the AS2 Edition interface only. • UCCNET UI – Access to the UCCnet Edition interface only. • Dashboard UI – Accesses dashboard interface. Refine by choosing a Dashboard Theme.
Dashboard Theme	Required if accessibility is set as Dashboard UI. Predefined dashboard that the user account has access to. The following are dashboard theme options: • Default • Operator • Participant • Participant Sponsor • Sponsor • AFT
Given Name	Required. Name used to identify the user.
Surname	Required. User's last name.
E-mail	User's e-mail address.
Pager	User's pager number.
Preferred Language	User's preferred language. Select from: English, French, Japanese, or Spanish.

Table 1. create user accounts (continued)

Field	Description
Manager ID	User ID of the user's manager.
Identity	Identity of the trading partner to associate with the user account. Only one trading partner can be associated with a user account. A user account can be associated with many groups, each with its own trading partner identity association. This enables a user account to be associated with more than one trading partner. The Identity field is used for routing messages in Mailbox. Select a trading partner identity from the list. The default value is Hub Organization.

For more information about creating users and assigning permissions to users, see the *Sterling B2B Integrator Security* documentation.

To create a user account:

Procedure

1. Log in to Sterling B2B Integrator.
2. From the **Administration Menu**, select **Accounts** > **User Accounts**.
3. Next to **Create a new Account**, click **Go!**
4. In the New Account page, select the **Authentication Type**.
5. Enter the **User ID** and **Password**.
6. Confirm the Password.
7. Select the **Policy**.
8. Enter the **Session Timeout**.
9. Select the **Accessibility**.
10. Select the **Dashboard Theme**.
11. Click **Next**.
12. On the SSH Authorized User Key page, assign one or more public keys. Move the keys from the **Available** pane to the **Assigned** pane and click **Next**.
13. On the Groups page, assign groups of permissions. Move the group names from the **Available** pane to the **Assigned** pane and click **Next**.
14. On the Permissions page, assign individual permissions. Move the permissions from the **Available** pane to the **Assigned** pane and click **Next**. By default, the permissions associated with the groups that this user is assigned to are already selected.
15. On the User Information page, enter the **Given Name**.
16. Enter the **Surname**.
17. Enter the **E-mail address**.
18. Enter the **Pager number**.
19. Select the **Preferred Language**.
20. Enter the **Manager ID**.
21. Select the **Identity**.
22. Click **Next.**
23. Review the user account settings.
24. Click **Finish**. The user account is created and this message is displayed:
    `The system update completed successfully.`

If you created an external user, log out of the system, and then log back in with the external user ID or account. The system authenticates the external user ID on the external LDAP server.

Configure a File System Adapter

Use the File System adapter to collect (import) files from a file system into a business process and extract (export) files from a business process to a file system. You can configure the File System adapter to start a business process after files are collected from the file system or include the File System adapter in a business process flow. In addition, you can schedule the File System adapter to run at specific time intervals.

You can create multiple File System adapter configurations, one for each of several collection folders. Alternatively, you can use a single File System adapter configuration to point to different directories by specifying the directories for file collection and extraction in a business process. For more information about configuring the File System Adapter, see the *File System Adapter* documentation.

Configure the File System Adapter to invoke the EBClientOrderPreProcess business process.

To create a File System adapter configuration, specify field settings in Sterling B2B Integrator and in the Graphical Process Modeler (GPM).

The following table describes the fields used to configure the File System adapter in the Sterling B2B Integrator.

Note: The field names in parentheses represent the corresponding field names in the GPM. This information is provided for your reference.

Field	Description
Name	Required. Unique and meaningful name for the service configuration.
Description	Required. Meaningful description for the service configuration, for reference.
Select a group	Group to associate with the adapter. Valid values: • None: No group is selected. • Create New Group: Allows the creation of a new group. • Select Group: Select from a list of available groups.

Field	Description
Collection folder (collectionFolder)	Required. The name of the folder or subfolder on the same computer where Sterling B2B Integrator is installed and where it collects (or picks up) files as part of a business process. If the path for the folder is not included as part of the name, the folder is assumed to be in the Sterling B2B Integrator working directory. **Note:** • The deleteAfterCollect parameter in the GPM defaults to Yes. If you do not change the default value to No, files that are collected are deleted from the Collection Folder. The File System adapter does not copy the files it collects for processing. See *Graphical Process Modeler Configuration* for information about the deleteAfterCollect parameter. • The collectionFolder parameter is read-only in the GPM. However, you can override this parameter using Business Process Modeling Language (BPML).
Filename filter (filter)	Optional. Collect only files that match a specified filter within the collection folder. Examples include: • *.txt (collects only .txt files). • *.dat (collects only .dat files). • EDI.* (collects only files named EDI with any file extension). • EDI.txt (collect only files named EDI with a file extension of .txt). **Note:** If there are multiple files in the collection folder and you leave this field blank, one of the following occurs: • If the adapter is configured to start a business process, it processes all files placed in the collection folder. • If the adapter is within a business process, it collects only the first file in the collection folder. **Note:** If you specify this option using the File System adapter configuration, you cannot override the value using the GPM filter parameter. However, you can override this parameter using BPML.
Collect files from subfolders within and including the collection folder? (useSubFolders)	Required. Whether to scan for files in subfolders of the collection folder. Valid values: • Yes: Collects files in the specified folder and all subfolders. • No: Collects files in the specified folder only. **Note:** This parameter is read-only in the GPM.

Field	Description
Use the absolute file path name for the document name? (keepPath)	Required. Whether to keep the absolute path name of the files collected when assigning the document name. Valid values: • Yes: The absolute file path name is kept with the document in the business process. Choose this value if your business process requires the path information to precede the file name. • No: Only the file name is kept with the document in the business process. **Note:** An absolute path is a path that points to the same location regardless of the working directory or combined paths. It is written in reference to a root directory. For example, `c:\dir1\subdir1\somefile.txt` (Windows) and `/home/dir1/subdir1/somefile.txt` (UNIX) are examples of absolute paths to the file somefile.txt. **Note:** This parameter is read-only in the GPM.
Start a business process once files are collected? (bootstrap)	Required. Whether to start a business process using the File System adapter after files are collected. Valid values: • Yes: Starts the business process specified from the business process drop-down list for every file that matches the filtering criteria. An instance of the business process is started for every file that matches the filtering criteria specified for file collection until the number of threads specified on the maxThreads parameter is reached. • No: No business process is started. This parameter is read-only in the GPM.
Business Process (initialWorkFlowId)	Required when **Start a business process** is set to Yes. The business process to start after files are collected. Select `EBClientOrderPreProcess` from the Business Process drop-down list. **Note:** This field displays as an option only if **Start a business process once files are collected** is set to Yes. If you specify a business process using the configuration, you cannot override this value using the GPM initialWorkFlowId option. If you select Not Applicable, a business process can be selected in the GPM. In either case, you can override this parameter using BPML.

Field	Description
Document storage type (docStorageType)	Required. Defines how the document is stored in the system. Valid values: • System Default. • Database. • File System. **Note:** This field only displays as an option only if **Start a business process once files are collected** is set to Yes. If you specify this parameter using the configuration, you cannot override this value using the GPM DocStorageType option. However, you can override this parameter using BPML.
Obscure File Contents? (obscure)	Specifies whether to obscure the file contents when collecting. Does not work with *attachFile* or *importFile*. • Yes: File contents are obscured. • No: File contents are not obscured. **Note:** This field only displays as an option only if **Start a business process once files are collected** is set to Yes. If you specify this parameter using the configuration, you cannot override this value using the GPM Obscure option. However, you can override this parameter using BPML.
User Parameter 1 (userParm1)	A user parameter that is passed to the bootstrapped workflow and placed in process data as UserParm1. **Note:** This field displays as an option only if **Start a business process once files are collected** is set to Yes. If you specify this parameter using the configuration, you cannot override this value using the GPM userParm1 option. However, you can override this parameter using BPML.
User Parameter 2 (userParm2)	A user parameter that is passed to the bootstrapped workflow and placed in process data as UserParm2. **Note:** This field displays as an option only if **Start a business process once files are collected** is set to Yes. If you specify this parameter using the configuration, you cannot override this value using the GPM userParm2 option. However, you can override this parameter using BPML.
User Parameter 3 (userParm3)	A user parameter that is passed to the bootstrapped workflow and placed in process data as UserParm3. **Note:** This field displays as an option only if **Start a business process once files are collected** is set to Yes. If you specify this parameter using the configuration, you cannot override this value using the GPM userParm3 option. However, you can override this parameter using BPML.

Field	Description
User Parameter 4 (userParm4)	A user parameter that is passed to the bootstrapped workflow and placed in process data as UserParm4. **Note:** This field displays as an option only if **Start a business process once files are collected** is set to Yes. If you specify this parameter using the configuration, you cannot override this value using the GPM userParm4 option. However, you can override this parameter using BPML.
User Parameter 5 (userParm5)	A user parameter that is passed to the bootstrapped workflow and placed in process data as UserParm5. **Note:** This field displays as an option only if **Start a business process once files are collected** is set to Yes. If you specify this parameter using the configuration, you cannot override this value using the GPM userParm5 option. However, you can override this parameter using BPML.
Run As User	Applies to the scheduling of the business process. The Run As User field displays as an option only if **Start a business process once files are collected** is set to Yes. Type the user ID to associate with the schedule, or click the list icon and select a user ID from the list. Valid value is any authentic Sterling B2B Integrator user ID. **Note:** This parameter allows someone who does not have rights to a specific business process to run it. If you select **Admin** as the user ID, you inherit administrative rights (for this run of the business process only), and can enable the scheduled run.
Use 24 Hour Clock Display	If selected, the adapter uses the 24-hour clock instead of the default 12-hour clock.

Field	Description
Schedule	Information about scheduling the business process after the File System adapter collects files. The Schedule field displays as an option only if **Start a business process once files are collected** is set to Yes. Valid values: • Do not use schedule. If you select this field, the adapter does not start a business process and does not run on a schedule. • Run based on timer. Valid values are the hour and minutes that specify when to run the adapter. If you choose to select a time interval, the valid values are the hour and minutes for the intervals. Add or delete selections as necessary. Specify any date exclusions. Indicate whether you want the adapter to run at startup. • Run daily. Valid values are the hour and minutes that specify when to run the adapter daily. If you choose to select a time interval, the valid values are the hour and minutes for the interval. Add or delete selections as necessary. Specify any date exclusions. Indicate whether you want the adapter to run at startup. • Run based on days of the week. Valid values are the day of the week, the hour, and minutes that specify when to run the adapter. If you choose to select a time interval, the valid values are the hour and minutes for the intervals. Add or delete selections as necessary. Specify any date exclusions. • Run based on days of the month. Valid values are the day of the month, hour, and minutes that specify when to run the adapter. If you choose to select a time interval, the valid values are the hour and minutes for the intervals. Add or delete selections as necessary. Specify any date exclusions.
Extraction folder (extractionFolder)	Required. The name of the folder or subfolder on the same computer where Sterling B2B Integrator is installed and where it extracts (or writes) data from the primary document as part of a business process. If you do not include the file path for the folder as part of the name, the folder is assumed to be the Sterling B2B Integrator working directory. **Note:** This parameter is read-only in the GPM.

Field	Description
Unobscure File Contents? (unobscure)	Whether to unobscure the file contents when extracting. Does not work with *exportFile*. Valid values: • Yes: File contents are unobscured. • No: File contents are not unobscured. **Note:** This parameter is read-only in the GPM.
Filenaming convention (assignFilename)	Required. Whether to override the document file name and use the assigned file name or not. Valid values: • Use the original file name as the extracted file name: Keeps the names of the files. **Note:** If the primary document has no document name, the adapter uses a default filename in the form of *nodename*_yyyyMMddHHmmssSSS.dat. • Assign a specific name: Gives you the option to navigate to a screen and specify a different filename for the file extracted to the file system. **Note:** This parameter is read-only in the GPM.
Filename (assignedFilename)	Required. File name you want to assign, including the file name extension. The Filename field displays onlyif the *Filenaming convention* is set to assign a specific name. This field cannot be left blank. You can use "%^" to assign a unique file name in the format *nodename*_yyyyMMddHHmmssSSS. For example, specifying %^.dat as the Filename assigns the name *nodename*_20040203114020982.dat to the file. **Note:** This field can also be assigned in the GPM. If you select a filename using the File System adapter configuration, you cannot override it using the GPM assignedFilename parameter. However, you can override it using BPML.
Enable Service for Business Processes	Whether to enable the service for use by business processes. If not selected, the service is disabled. For more information about enabling a service, see *Managing Services and Adapters.*

Create a Mailbox and Assign Permissions

You must associate each EBICS Client user with the preconfigured EBClientOrderMetadata mailbox.

About this task

You must create a Download (Inbox) and an Upload (Outbox) mailbox and associate each user with the mailboxes.

For more information about configuring mailboxes and assigning permissions to groups and users, see the *Sterling B2B Integrator Mailbox Help* documentation.

To create a mailbox and assign permissions to groups and users to operate on this mailbox:

Procedure

1. Log in to Sterling B2B Integrator.
2. From the **Administration Menu** , select **Deployment** > **Mailboxes** > **Configuration**.
3. Next to **Create a new Mailbox**, click **Go!**
4. In the Mailbox: Name page, select the parent mailbox in which the mailbox you are creating is embedded. You can type a partial name in the **Filter by Name** field and click the filter button for a filtered list. The root mailbox is denoted by a slash (/).
5. In the **Name** field, type a name for the mailbox you want to create. This name is used to identify the mailbox in the Application, for example, EBClientOrderMetadata.
6. Required. In the **Description** field, type a short description for the mailbox and click **Next**. Use this field to describe the mailbox. This field is not used by any other resource in the system.
7. In the Assign Groups page, use the arrows to add the groups to the **Selected Groups** list and click **Next**. All groups in the **Selected Groups** list will have permissions on this mailbox. Click the first double arrow to add all available groups to the **Selected Groups** list.
8. In the **Filter by Name** field, type a partial group name in the field and click the filter button for a filtered list.
9. In the **Accounts** menu, multiple groups can be added. No groups are required.
10. Use the arrows to add users to the **Selected Users** list and click **Next**. All users in the **Selected Users** list will have permissions on this mailbox. Click the double arrow to add all available users to the Selected Users list.
11. In the **Filter by ID** field, type a partial name in the field and click the filter button for a filtered list.

Enable the Schedule

About this task

Enabling a schedule makes the schedule active and causes the associated activity to run according to the schedule settings. A schedule must be enabled in order to run. For more information about setting up schedules to automate manual activities, see the *Sterling B2B Integrator Scheduling* documentation.

The MailboxEvaluateAllAutomaticRulesSubMin schedule is automatically enabled.

Use the following procedure to enable a schedule:

Procedure

1. Log in to Sterling B2B Integrator.
2. From the **Administration Menu**, select **Deployment** > **Schedules**.
3. Use **Search** or **List** to locate the MailboxEvaluateAllAutomaticRulesSubMin schedule and click **Go!**

4. On the Schedules page, locate the MailboxEvaluateAllAutomaticRulesSubMin schedule and ensure that the check box in the Enabled column is selected.

Create a Self-Signed Certificate

About this task

Check in the public part of the self-signed certificate into the Trusted store of Sterling B2B Integrator. To create a self-signed certificate:

Procedure

1. Choose one of the following options:
   - If you use Sterling B2B Integrator, from the **Administration Menu**, select **Trading Partner** > **Digital Certificates** > **System**.
   - If you use the AS2 Edition, from the **AS2 Administration** menu, select **Certificates.**
2. Next to **Create Self-signed Certificate,** click **Go!**
3. Enter the **Name** of the self-signed certificate.
4. Enter the name of the **Organization**.
5. Select the **Country** or origin of the self-signed certificate.
6. Enter a contact **e-mail** address for the person responsible for certificates in the organization and then click **Next**.
7. Enter the **Serial Number** for the certificate. The serial number is the number you want to assign to the self-signed certificate.
8. Enter the **Duration** (number of days) that the self-signed certificate is valid.
9. Enter the **IP addresses** of the network interfaces you want to associate with the certificate as the SubjectAltName field.
10. Enter the **DNS Names** of the network interfaces you want to associate with the certificate as the SubjectAltName field.
11. Select the **Key Length**. Select one of the following key lengths:
    - 512
    - 1024
    - 2048

    Note: The key length 1024 provides a good balance between security, interoperability, and efficiency. The key length 2048 is the most secure, but also the slowest, and may not work with some applications. For information about defining EBICS-specific key lengths for electronic signature, encryption, and authentication, see *EBICS Specification, version 2.5*.

    Note: If you select the key length 512, you must check for JDK restrictions on the key length in the `java.security` file in the JDK.
12. Select the **Signing Algorithm**.

    Note: You must use the SHA256withRSA signing algorithm for certificates used with EBICS transactions.
13. Select the **Validate When Used** option. Validation options are:
    - Validity – Verifies dates in the validity period of the certificate are still in effect. If the dates are not in effect, the certificate is not used.

      Note: Before you set a value to the validity period of the certificate, you must read and apply the best practice recommendations from the Microsoft

PKI Quick Guide. For information about the best practice recommendations for using certificates, see http://www.windowsecurity.com/articles/Microsoft-PKI-Quick-Guide-Part3.html.

- Auth Chain – Constructs a chain of trust for certificates that are not self-signed. If a chain of trust cannot be constructed using valid certificates, the certificate is not used. If the certificate is self-signed, this option verifies only the certificate signature.

14. Set the **Certificate Signing Bit** by selecting the check box.
15. Click **Next**.
16. Review the information about the self-signed certificate.
17. Click **Finish**.

Check in a CA Certificate

Based on security policies at your site, Certificate Authority (CA) certificates in the Java Key Store (JKS) can also be checked in through the console.

About this task

Before you begin, save any CA certificates that you obtained externally to a local file.

Check in all the certificates (identification and authentication, signing, and encryption) the EBICS Client user requires to transact with the bank. If a CA-signed certificate is used for configuring a user, then check in the Root CA certificate. If 3SKey is used for signing, then check in the Root 3SKey certificate. Check in the public part of the HTTPS certificate of the server into the CA store of Sterling B2B Integrator. For more information about managing digital certificates, see the *Sterling B2B Integrator Security* documentation.

To check in a CA certificate:

Procedure

1. Log in to Sterling B2B Integrator.
2. From the **Administration Menu**, select **Trading Partner** > **Digital Certificates** > **CA**.
3. Next to **New Certificate**, click **Go!**
4. Select a method to import certificates:

Import method	Next Steps
Import from JVM – Imports from the JKS keystore	1. Click **Import from JVM**. 2. Accept the default password that appears in the password field and click **Next**. If the password field is empty, the system still uses the default password.
Import from File – Imports certificates saved as a file on a local drive	1. Click **Import** from **File**. 2. Enter the file name or click **Browse** to select a CA certificate file. Click **Next**. You may ignore the password that is displayed in the password field. There is no need to erase the entry.

Available certificates are listed with a summary of identifying information. All certificates are selected by default.

5. Select the check boxes to the left of each entry to import the certificates.
6. For each certificate selected, accept the suggested Certificate Name or edit it based on your file naming conventions.
7. Select the **Validate When Used** option and click **Next**. Validation options are:
   - Validity – Verifies dates in the validity period of the certificate are still in effect. If the dates are not in effect, the certificate is not used.
   - Auth Chain – Attempts to construct a chain of trust for certificates that are not self-signed. If a chain of trust cannot be constructed using valid certificates, the certificate is not used. If the certificate is self-signed, this option verifies only the certificate signature.
8. If you receive a message stating that the certificate duplicates a certificate already in the database, enter Y or N to indicate whether to import the duplicate or not.

   This check is done on single certificates only. It does not take place when checking in one or more certificates from a file.

   Certificates are identified by SHA1 or SHA256 hash for purposes of determining duplicates. More than one copy of a certificate can be present in the database, since each certificate populates a different row and has a distinct object ID. The existing certificate is not overwritten.
9. Review the CA certificate information.
10. Click **Finish**.

Check in Trusted System Certificates

About this task

Check in the public part of the user's certificate into the Trusted store of Sterling B2B Integrator.

Before you begin, save the trusted system certificate to a file on your local computer.

To check in a trusted system certificate:

Procedure

1. Choose one of the following options:
   - If you use Sterling B2B Integrator, from the **Administration Menu**, select **Trading Partner** > **Digital Certificates** > **Trusted**.
   - If you use the AS2 Edition, from the **AS2 Administration Menu**, select **Certificates**.
2. Next to **New Certificate**, click **Go!**
3. Enter the **Filename** or click **Browse** to select the file name of the trusted certificate and then click **Next**.
4. Enter the **Certificate Name**.
5. Verify the name of the trusted certificate you are checking in. For each certificate you selected, the Certificate Name field shows a suggested name, followed by a summary of the identifying information in the certificate. You can change the name based on your file naming conventions.
6. If you have more than one trusted certificate contained in the file you selected, select the check box to the left of each certificate to check in the certificate.

7. Select the **Validate When Used** option and click **Next**. Validation options are:
   - Validity – Verifies dates in the validity period of the certificate are still in effect. If the dates are not in effect, the certificate is not used.
   - Auth Chain – Attempts to construct a chain of trust for certificates that are not self-signed. If a chain of trust cannot be constructed using valid certificates, the certificate is not used. If the certificate is self-signed, this option verifies only the certificate signature.
   - CRL cache – Controls whether the Certificate Revocation List is consulted each time the system certificate is used.
8. Review the trusted certificate information.
9. Click **Finish**.

Check in Key System Certificates

About this task

Before you begin, save the key system certificate to a file on your local computer. Check in the private part of the CA-signed certificates into the Key system certificates of Sterling B2B Integrator.

To check in a key system certificate:

Procedure

1. Choose one of the following options:
   - If you use Sterling B2B Integrator, from the **Administration Menu**, select **Trading Partner** > **Digital Certificates** > **System**.
   - If you use the AS2 Edition, from the **AS2 Administration** menu, select **Certificates**.
2. Next to **Key Certificate**, click **Go!**
3. Enter the **Certificate Name**.
4. Enter the **Private Key Password.** This password is used to encrypt the private key.
5. Enter the **Filename** or click **Browse** to select the file name of the key certificate and click **Next**.
6. Select the **Validate When Used** option and click **Next**. Validation options are:
   - Validity – Verifies dates in the validity period of the certificate are still in effect. If the dates are not in effect, the certificate is not used.
   - Auth Chain – Constructs a chain of trust for certificates that are not self-signed. If a chain of trust cannot be constructed using valid certificates, the certificate is not used. If the certificate is self-signed, this option verifies only the certificate signature.
7. Review the key certificate information.
8. Click **Finish**.

Configuring EBICS Client

You must configure EBICS Client in Sterling B2B Integrator.

Before you begin

Complete the configuration of trading partner, user account, mailboxes, and certificates in Sterling B2B Integrator listed in the *Configuration Prerequisites* topic.

About this task

You can configure EBICS Client in the following sequence:

Procedure

1. Configure existing Sterling B2B Integrator user as EBICS Client user.
2. Create a bank profile to include the EBICS host information.
3. Create an offer and associate it with a bank.
4. Associate file formats with the offer.
5. Assign user permission to users to sign and submit the orders.
6. Initialize users using one of the following methods:
   - Submit an H3K order.
   - Use INI and HIA together.

     Submit INI and HIA orders.

     Generate and sign initialization letters of INI and HIA. Mail the signed letters to the bank.

   For more information, see "Initializing a User" on page 41.
7. Use the HPB system order type to download the public certificates of the bank.
8. Validate the hash value of the certificates received from the bank.
9. Submit an order.
10. View status of events, orders, and pending tasks.

Managing Profiles in EBICS Client

Profile Management in EBICS Client enables you to configure the following profiles. A Super admin or an EBICS Client admin can configure the profiles.

- Bank
- User
- Offer
- File format

Note: A Super admin is the default admin role created when EBICS Client is installed. An authorized user can log in to the EBICS Client dashboard interface using the super admin login credentials and configure an EBICS Client admin, EBICS Client operator, and EBICS Client user and other profiles. An EBICS Client admin can also configure an EBICS Client admin, EBICS Client operator, EBICS Client user, and other profiles.

Configure an Existing User as EBICS Client User

Before you begin

Configure the following in Sterling B2B Integrator:

- Create trading partner entities.
- Create user accounts using the trading partner entities, define permissions and password policies.
- Configure upload and download mailboxes for each user.

About this task

A user can be under either one partner or multiple partners. A user is always associated with a partner to enable exchange of EBICS messages. To configure an existing Sterling B2B Integrator user as an EBICS Client user, complete the following steps:

Procedure

1. Log in to Sterling B2B Integrator EBICS Client.
2. From the **Profile management** menu, select **User**.
3. In the User Configuration page, next to **Configure existing user as EBICS user** click **GO**.
4. In the User Configuration page, specify the values for the fields according to the instructions in the following table and click **Next**:

Field	Description
User ID	Required. Unique ID of the user in the bank's system, which corresponds to the user created in the EBICS Client dashboard. From the **User ID** drop-down list, select the user ID.
User type	Required. From the **User type** drop-down list, select the role of the user. Valid values are EBICS client admin, EBICS client operator, and EBICS client user.
Timezone	Optional. Specify the time zone of the user.
Technical user	Optional. A technical user is a system configured to submit orders on behalf of a non-technical or human user. This option is valid if you selected EBICS Client User as the user type. Select this check box to configure a Technical user.
Certificate type	Required if you selected EBICS client user as the user type. Select X509 if you are using X.509 public key certificate to authorize the certificates. Select Keys if you are using RSA keys to authorize the certificates. **Note:** EBICS Client supports non-encrypted keys only.

5. *If* you selected X509 as the certificate type, specify the values for the fields according to the instructions in the following table in the Technical Information page and click **Next**:

Field	Description
Authentication private certificate	Required. Select the private key the EBICS Client uses to create a digital signature for the user in the request sent to the bank. The bank must have the public part of the key to validate the authorization. The drop-down contains a list of certificates configured in the Sterling B2B Integrator system certificate store.

Field	Description
Authentication public certificate	Required. Select the public key the user provides to the bank to validate the authorization of the user in the request from the EBICS Client. The trading partner or user shares the key with the bank. The key must be a public part of the Sterling B2B Integrator system certificate that is selected as the authentication private certificate.
Authentication key version	The key version of the authentication certificate is displayed. Valid value is X002.
Encryption private certificate	Required. Select the private key the EBICS Client uses to decrypt the response received from the EBICS Banking Server. The drop-down contains a list of certificates configured in the Sterling B2B Integrator system certificate store.
Encryption public certificate	Required. Select the public part of the Sterling B2B Integrator system certificate that is selected as the encryption private certificate. The trading partner or user shares the key with the bank.
Encryption key version	The key version of the encryption certificate is displayed. Valid value is E002.
Use hardware key-store for Electronic signature	Optional. Select this option if you have an activated 3S Key token.
Hardware key type	3S Key is displayed as the Hardware key type. 3SKey is a SWIFT secure signature key used for digital identity. You must activate the 3SKey token and register the key with the bank to enable you to sign and send messages to the bank.
Electronic signature private key	Optional. Select the private key of the Electronic Signature (ES) certificate if you are not using a hardware key for Electronic Signature.
Electronic signature public key	Required. Select the public key of the Electronic Signature (ES) certificate that is used to verify the signature of order data. The public key value of an electronic signature certificate should not be the same as an authentication or encryption certificate.
Electronic signature key version	Required if you are not using a hardware key store for electronic signature. Select the key version of the electronic signature certificate. Valid values are A005 and A006. If you are using a hardware key store for electronic signature, then the key version is set to A005 and it cannot be changed.

6. *If* you selected Keys as the certificate type, specify the values for the fields according to the instructions in the following table in the Technical Information page and click **Next**:

Field	Description
Authentication private key	Required. Click **Browse** to select the file with the private part of the authentication key from your computer.
Authentication public key	Required. Click **Browse** to select the file with the public part of the authentication key from your computer.
Authentication key version	Required. Select the key version of the authentication certificate. Valid value is X002.
Encryption private key	Required. Click **Browse** to select the file with the private part of the encryption key from your computer.
Encryption public key	Required. Click **Browse** to select the file with the public part of the encryption key from your computer.
Encryption key version	Required. Select the key version of the encryption certificate. Valid value is E002.
Electronic signature private key	Required. Click **Browse** to select the file with the private part of the Electronic signature key from your computer.
Electronic signature public key	Required. Click **Browse** to select the file with the public part of the Electronic signature key from your computer.
Electronic signature key version	Required. Select the key version of the Electronic signature certificate. Valid values are A005 and A006.

7. In the Associated Partners page, perform any of the following actions and click **Next**.
   - Click the add icon to associate a new partner with user.
   - Click the update icon next to the partner you want to edit.
   - Click the delete icon to disassociate a partner from the user.
8. This step is applicable only if you opted to add a new partner or edit an existing partner. The bank assigns a set of permissions, order types, and file formats to a user based on the offer. In the Associated partner: User settings page, specify the values for the fields according to the instructions in the following table, and click **Add partner**.

Field	Description
Partner name	Required. From the **Partner name** drop-down list, select the partner to which a user is associated. A user can be associated with many partners. **Note:** Use the Sterling B2B Integrator dashboard to create trading partner entities.

Field	Description
Upload mailbox path	Required. Configure the upload mailbox and assign users to operate the mailbox in Sterling B2B Integrator. Specify the mailbox path for the uploaded messages. You must assign a mailbox path to store the unpacked messages from an EBICS request. If the mailbox (User ID, Partner name, Inbox), already exists in Sterling B2B Integrator and if you leave this field blank, an error message asking you to specify the default mailbox path is displayed. **Note:** Ensure that the mailbox path starts with a forward slash (/).
Download mailbox path	Required. Configure the download mailbox and assign users to operate the mailbox in Sterling B2B Integrator. Specify the mailbox path for the downloaded messages. You must assign a mailbox path to store the messages that are packaged as part of an EBICS response. If the mailbox (User ID, Partner name, Outbox) already exists in Sterling B2B Integrator, and if you leave this field blank, an error message asking you to specify the default mailbox path is displayed. **Note:** Ensure that the mailbox path starts with a forward slash (/).

9. This step is applicable if you selected to configure the user delegation settings for a Technical user. In the Associated Partners page, perform any of the following actions and click **Next**.
   - Click the add icon to associate a new partner with the Technical user.
   - Click the update icon next to the partner you want to edit.
   - Click the delete icon to disassociate a partner from the Technical user.
10. This step is applicable if you are configuring user delegation settings for a Technical user. In the Associated partner: User settings page, specify the values for the fields according to the instructions in the following table, and click **Add partner**.

Field	Description
Partner name	Required. From the **Partner name** drop-down list, select the partner to which a user is associated. A user can be associated with many partners. **Note:** Use the Sterling B2B Integrator dashboard to create trading partner entities.
Delegate of	Required. Select the user who will be delegating their tasks to the technical user.

11. In the Associated Partners page, click **Next**.
12. In the Confirm page, verify the user configuration settings, and click **Finish**. You can also click the **Show All** link next to **Associate Partners** to view the list of partners associated with the user.

Search for a User Profile

About this task

To search for a user profile, complete the following steps:

Procedure

1. Log in to Sterling B2B Integrator EBICS Client.
2. From the **Profile management** menu, select **User**.
3. In the User Configuration page, perform one of the following actions, and click **GO**.
   - In the **User ID** field under **Search**, enter either a part of the user ID or the entire user ID of the user profile you are searching for.
   - From the **Alphabetically** drop-down list, select the first letter with which the ID of the user you are searching for, begins.

Edit a User Profile

About this task

You must be logged in to the EBICS Client dashboard interface as an administrator to update a user profile, delete a user profile, or view the summary of a user. To edit a user profile, complete the following steps:

Procedure

1. Log in to Sterling B2B Integrator EBICS Client.
2. From the **Profile management** menu, select **User**.
3. In the User Configuration page, using either **Search** or **List**, locate and select the user ID you want to edit, and click **GO**. You can click the user ID to view the user profile settings.
4. Click the update icon next to the user ID you want to edit.
5. In the Update: User Configuration page, specify the values for the fields according to the instructions in the following table and click **Next**:

Field	Description
Timezone	Optional. Select the time zone of the user.
Technical user	Optional. A technical user is a system configured to submit orders on behalf of a non-technical or human user. This option is valid if you selected EBICS Client User as the user type. Select this check box to configure a Technical user.
Certificate type	Required if you selected EBICS client user as the user type. Select X509 if you are using X.509 public key certificate to authorize the certificates. Select Keys if you are using RSA keys to authorize the certificates. **Note:** EBICS Client supports non-encrypted keys only.

6. *If* you selected X509 as the certificate type, specify the values for the fields according to the instructions in the following table in the Technical Information page and click **Next**:

Field	Description
Authentication private certificate	Required. Select the private key the EBICS Client uses to create a digital signature for the user in the request sent to the bank. The bank must have the public part of the key to validate the authorization. The drop-down contains a list of certificates configured in the Sterling B2B Integrator system certificate store.
Authentication public certificate	Required. Select the public key the user provides to the bank to validate the authorization of the user in the request received from the EBICS Client. The trading partner or user shares the key with the bank. The key must be a public part of the Sterling B2B Integrator system certificate that is selected as the authentication private certificate.
Authentication key version	The key version of the authentication certificate is displayed. Valid value is X002.
Encryption private certificate	Required. Select the private key the EBICS Client uses to decrypt the response received from the EBICS Banking Server. The drop-down contains a list of certificates configured in the Sterling B2B Integrator system certificate store.
Encryption public certificate	Required. Select the public part of the Sterling B2B Integrator system certificate that is selected as the encryption private certificate. The trading partner or user shares the key with the bank.
Encryption key version	The key version of the encryption certificate is displayed. Valid value is E002.
Use hardware key-store for Electronic signature	Optional. Select this option if you have an activated 3S Key token registered with the bank.
Hardware key type	3S Key is displayed as the Hardware key type. 3SKey is a SWIFT secure signature key used for digital identity. You must activate the 3SKey token and register the key with the bank to enable you to sign and send messages to the bank.
Electronic signature private key	Optional. Select the private key of the Electronic Signature (ES) certificate if you are not using a hardware key for Electronic Signature.
Electronic signature public key	Required. Select the public key of the Electronic Signature (ES) certificate that is used to verify the signature of order data. The public key value of an Electronic Signature certificate should not be the same as an authentication or encryption certificate.

Field	Description
Electronic signature key version	Required if you are not using a hardware key store for electronic signature. Select the key version of the electronic signature certificate. Valid values are A005 and A006. If you are using a hardware key store for electronic signature, then the key version is set to A005 and it cannot be changed.

7. *If* you selected Keys as the certificate type, specify the values for the fields according to the instructions in the following table in the Technical Information page and click **Next**:

Field	Description
Authentication private key	Required. Click **Browse** to select the file with the private part of the authentication key from your computer.
Authentication public key	Required. Click **Browse** to select the file with the public part of the authentication key from your computer.
Authentication key version	Required. Select the key version of the authentication certificate. Valid value is X002.
Encryption private key	Required. Click **Browse** to select the file with the private part of the encryption key from your computer.
Encryption public key	Required. Click **Browse** to select the file with the public part of the encryption key from your computer.
Encryption key version	Required. Select the key version of the encryption certificate. Valid value is E002.
Electronic signature private key	Required. Click **Browse** to select the file with the private part of the Electronic signature key from your computer.
Electronic signature public key	Required. Click **Browse** to select the file with the public part of the Electronic signature key from your computer.
Electronic signature key version	Required. Select the key version of the Electronic signature certificate. Valid values are A005 and A006.

8. In the Associated Partners page, perform any of the following actions and click **Next**.
   - Click the add icon to associate a new partner with user.
   - Click the update icon next to the partner you want to edit.
   - Click the delete icon to disassociate a partner from the user.
9. This step is applicable only if you opted to add a new partner or edit an existing partner. The bank assigns a set of permissions, order types, and file formats to a user based on the offer. In the Associated partners: User settings page, specify the values for the fields according to the instructions in the following table, and click **Add partner**.

Field	Description
Partner name	Required. From the **Partner name** drop-down list, select the partner to which a user is associated. A user can be associated with many partners. **Note:** Use the Sterling B2B Integrator dashboard to create trading partner entities.
Upload mailbox path	Required. Configure the upload mailbox and assign users to operate the mailbox in Sterling B2B Integrator. Specify the mailbox path for the uploaded messages. You must assign a mailbox path to store the unpacked messages from an EBICS request. If the mailbox (User ID, Partner name, Inbox), already exists in Sterling B2B Integrator and if you leave this field blank, an error message asking you to specify the default mailbox path is displayed. **Note:** Ensure that the mailbox path starts with a forward slash (/).
Download mailbox path	Required. Configure the download mailbox and assign users to operate the mailbox in Sterling B2B Integrator. Specify the mailbox path for the downloaded messages. You must assign a mailbox path to store the messages that are packaged as part of an EBICS response. If the mailbox (User ID, Partner name, Outbox) already exists in Sterling B2B Integrator, and if you leave this field blank, an error message asking you to specify the default mailbox path is displayed. **Note:** Ensure that the mailbox path starts with a forward slash (/).

10. This step is applicable if you selected to configure the user delegation settings for a Technical user. In the Associated Partners page, perform any of the following actions and click **Next**.
    - Click the add icon to associate a new partner with the Technical user.
    - Click the update icon next to the partner you want to edit.
    - Click the delete icon to disassociate a partner from the Technical user.
11. This step is applicable if you are configuring user delegation settings for a Technical user. In the Associated partner: User settings page, specify the values for the fields according to the instructions in the following table, and click **Add partner**.

Field	Description
Partner name	Required. From the **Partner name** drop-down list, select the partner to which a user is associated. A user can be associated with many partners. **Note:** Use the Sterling B2B Integrator dashboard to create trading partner entities.

Field	Description
Delegate of	Required. Select the user who will be delegating their tasks to the technical user.

12. In the Associated Partners page, click **Next**.
13. In the Confirm page, verify the user configuration settings, and click **Finish**. You can also click the **Show All** link next to **Associate Partners** to view the list of partners associated with the user.

Delete User Profile

About this task

You must be logged in to the EBICS Client dashboard interface as an administrator to update a user profile, delete a user profile, or view the summary of a user. To delete a user profile, complete the following steps:

Procedure

1. Log in to Sterling B2B Integrator EBICS Client.
2. From the **Profile management** menu, select **User**.
3. Using either **Search** or **List**, locate the user ID you want to delete and click **GO**.
4. Click the delete icon adjacent to the user ID you want to delete.

   Note: Deleting a user profile does not delete the corresponding mailboxes that have already been created.

Create a Bank Profile

You can create a bank profile to provide EBICS host information for a bank.

About this task

To create a bank profile:

Procedure

1. Log in to Sterling B2B Integrator EBICS Client.
2. From the **Profile Management** menu, select **Bank** > **Profile**.
3. In the Bank Configuration page, next to **Create Bank**, click **GO**.
4. In the Bank Information page, specify the values for the fields according to the instructions in the following table and click **Next**.

Field	Description
Bank ID(Host ID)	Required. Enter the bank ID or the host ID provided by the bank. It is a unique ID for the bank in the bank's system.
Bank name	Required. Specify the name of the bank.
Status	Status of the bank is set to New before validating the bank keys. After successful validation, the status changes to Activated. The status cannot be edited.

Field	Description
Is RSA preferred	Optional. If you want EBICS Client to use RSA key values for electronic signature, authentication, and encryption, select the check box. EBICS Client uses only RSA-related values for electronic signature, authentication, and encryption irrespective of the upload key type.
Use ESIG Namespace	Optional. If you want EBICS Client to use an ESIG namespace, select the check box.
Insert optional elements in KeyManagement request xml	Optional. If you want EBICS Client to use optional elements in the `KeyManagement request xml` file, select the check box.
Address Line 1	Optional. Specify the address of the bank.
Address Line 2	Optional. Specify the address of the bank.
City	Optional. Specify the name of the city where the bank is located.
State or Province	Optional. Specify the name of the state or province.
Country/Region	Optional. Select the country or region.
Zip or postal code	Optional. Specify the zip code or postal code.
E-mail Address	Optional. Specify the e-mail address of the bank.
Telephone Number	Optional. Specify the phone number with country code.

5. In the Associate URL page, click the add icon next to Associate Url, specify the values for the fields according to the instructions in the following table and click **Add Url**.

URL Alias	Required. Specify a short name for the bank URL. You can navigate to the website of the bank by typing the short name or the alias in the address field of the browser. For example, if you specified *bs* as the URL alias for the URL http://www.banksystem.com, then type *bs* in the address field of the browser to go to the website.
Is Default	Optional. Select this check box to indicate that the URL specified in the URL field is the default URL. If no URL is specified in the **Bank URL** field on the Order Information page when submitting an order, EBICS Client populates the default URL in the **Bank URL** field. If a bank URL alias is not specified, then the default URL is used for order submission when an order is submitted by a technical user.

Bank URL	Required. Specify the HTTP URL the bank hosts. A bank can have multiple URLs with a minimum of one. The Uniform Resource Locator (URL) is configured in the HTTP Server adapter to listen at the port, and receive EBICS requests, if any. **Note:** Each bank ID should have a unique port number or URL.
Bank https certificate	Optional. Select the appropriate HTTPS certificate of the bank from the drop-down list. The HTTPS certificate ensures that all transactions with the bank are encrypted and secure.

After successful addition, the bank URL details are displayed in a tabular format in the Associate URL page.

6. Click **Next**.
7. In the Select Protocol Version page, click **Retrieve supported protocol versions from bank**. Select the appropriate Protocol version from the drop-down list and click **Next**.
8. In the Confirm page, verify the bank configuration settings and click **Finish**.

Search for a Bank Profile

About this task

To search for a bank profile, complete the following steps:

Procedure

1. Log in to Sterling B2B Integrator EBICS Client.
2. From the **Profile management** menu, select **Bank** > **Profile**.
3. In the Bank Configuration page, perform one of the following actions, and click **GO**:
   - In the **Bank ID(HostID)** field under **Search**, enter either a part of the bank ID or the entire bank ID of the bank profile you are searching for.
   - From the **Alphabetically** drop-down list under **List**, select the letter with which the ID of the bank you are searching for, begins.

Edit a Bank Profile

You can edit a bank profile to revise EBICS host information for a bank.

About this task

To edit a bank profile, complete the following steps:

Procedure

1. Log in to Sterling B2B Integrator EBICS Client.
2. From the **Profile management** menu, select **Bank** > **Profile**.
3. In the Bank Configuration page, using either **Search** or **List**, locate and select the bank ID you want to edit, and click **GO**.
4. Click the update icon next to the bank ID you want to edit.
5. In the Bank Information page, specify the values for the fields according to the instructions in the following table and click **Next**.

Field	Description
Bank ID(Host ID)	Required. Enter the bank ID or the host ID provided by the bank. It is a unique ID for the bank in the bank's system.
Bank name	Required. Specify the name of the bank.
Status	Status of the bank is set to New before validating the bank keys. After successful validation, the status changes to Activated. The status cannot be edited.
Is RSA preferred	Optional. If you want EBICS Client to use RSA key values for electronic signature, authentication, and encryption, select the check box. EBICS Client uses only RSA-related values for electronic signature, authentication, and encryption irrespective of the upload key type.
Use ESIG Namespace	Optional. If you want EBICS Client to use an ESIG namespace, select the check box.
Insert optional elements in KeyManagement request xml	Optional. If you want EBICS Client to use optional elements in the `KeyManagement request xml` file, select the check box.
Address Line 1	Optional. Specify the address of the bank.
Address Line 2	Optional. Specify the address of the bank.
City	Optional. Specify the name of the city where the bank is located.
State or Province	Optional. Specify the name of the state or province.
Country/Region	Optional. Select the country or region.
Zip or postal code	Optional. Specify the zip code or postal code.
E-mail Address	Optional. Specify the e-mail address of the bank.
Telephone Number	Optional. Specify the phone number with country code.

6. In the Associate URL page, click the update icon next to the bank ID that you want to edit, specify the values for the fields according to the instructions in the following table and click **Add Url**.

URL Alias	Required. Specify a short name for the bank URL. You can navigate to the website of the bank by typing the short name or the alias in the address field of the browser. For example, if you specified *bs* as the URL alias for the URL http://www.banksystem.com, then type *bs* in the address field of the browser to go to the website.

Is Default	Optional. Select this check box to indicate that the URL specified in the URL field is the default URL. If no URL is specified in the **Bank URL** field on the Order Information page when submitting an order, EBICS Client populates the default URL in the **Bank URL** field. If a bank URL alias is not specified, then the default URL is used for order submission when an order is submitted by a technical user.
Bank URL	Required. Specify the HTTP URL the bank hosts. A bank can have multiple URLs with a minimum of one. The Uniform Resource Locator (URL) is configured in the HTTP Server adapter to listen at the port, and receive EBICS requests, if any. **Note:** Each bank ID should have a unique port number or URL.
Bank https certificate	Optional. Select the appropriate HTTPS certificate of the bank from the drop-down list. The HTTPS certificate ensures that all transactions with the bank are encrypted and secure.

After successful addition, the bank URL details are displayed in a tabular format in the Associate URL page.

7. Click **Next**.
8. In the Select Protocol Version page, click **Next**. The protocol version cannot be updated because of dependencies on the offer configuration and signatories.
9. In the Confirm page, verify the bank configuration settings and click **Finish**.

Delete a Bank Profile

About this task

To delete a bank profile, complete the following steps:

Procedure

1. Log in to Sterling B2B Integrator EBICS Client.
2. From the **Profile management** menu, select **Bank** > **Profile**.
3. In the Bank Configuration page, using either **Search** or **List**, locate and select the Bank ID (Host ID) you want to delete, and click **GO**.
4. Click the delete icon next to the bank ID you want to delete.

Validate a Bank Key

Before you begin

Submit the HPB order before validating the bank keys.

About this task

To ascertain the authenticity of the bank's identification and authentication, and encryption keys, EBICS Client allows you to validate the hash value of the certificates received from the bank. After successful validation of the bank keys, the

status of the bank changes to Activated. To validate a bank key, complete the following steps:

Procedure

1. Log in to Sterling B2B Integrator EBICS Client.
2. From the **Profile management** menu, select **Bank** > **Bank key validation**.
3. In the Bank Key Validation page, specify the values for the fields according to the instructions in the following table:

Field	Description
BankID(Host ID)	Required. Select the Bank ID from the drop-down list.
Identification and authentication key hash value(In hex format)	Required. Specify the identification and authentication key hash value provided by the bank.
Hash Algorithm	Required. Select the hash algorithm of the identification and authentication key hash value. Valid values are: • SHA1 (default) • SHA256
Encryption key hash value(In hex format)	Required. Specify the encryption key hash value provided by the bank.
Hash Algorithm	Required. Select the hash algorithm of the encryption key hash value. Valid values are: • SHA1 (default) • SHA256

4. Click **Reset** if you want to clear the existing values and enter new values.
5. Click **Validate**.

Create an Offer

About this task

Offers enable a partner to group a set of order types and file formats and process them together. An offer must be associated with a particular bank ID. Only one offer is allowed per bank. To create an offer, complete the following steps:

Procedure

1. Log in to Sterling B2B Integrator EBICS Client.
2. From the **Profile management** menu, select **Bank** > **Offer configurations**.
3. In the Offer Configuration page, next to **Create new offer**, click **GO**.
4. In the Create: Offer page, specify the values for the fields according to the instructions in the following table and click **Finish**.

Field	Description
Offer Name	Required. Specify a name for the offer.
Bank ID(Host ID)	Required. Select a bank ID from the drop-down list.

Field	Description
Associate/Disassociate order type to file formats configuration	Optional. Select the check box next to the order type. The selected order types and corresponding file formats are grouped to form an offer.

Search for an Offer

About this task

To search for an offer, complete the following steps:

Procedure

1. Log in to Sterling B2B Integrator EBICS Client.
2. From the **Profile management** menu, select **Bank** > **Offer configurations**.
3. In the Offer Configuration page, perform one of the following actions, and click **GO**.
   - In the **Bank ID(HostID)** field under **Search**, enter either a part of the bank ID or the entire bank ID with which the offer you are searching for is associated.
   - From the **Alphabetically** drop-down list under **List**, select the letter with which the offer name you are searching for, begins.

Edit an Offer

About this task

To edit an offer, complete the following steps:

Procedure

1. Log in to Sterling B2B Integrator EBICS Client.
2. From the **Profile management** menu, select **Bank** > **Offer configurations**.
3. In the Offer Configuration page, using either **Search** or **List**, locate and select the offer you want to edit, and click **GO**.
4. Click the update icon next to the offer you want to edit.
5. In the Update: Offer page, specify the values for the fields according to the instructions in the following table and click **Finish**.

Field	Description
Associate/Disassociate order type to file formats configuration	Optional. Select the check box next to the order type. The selected order types and the corresponding file formats are grouped to form the offer.

Delete an Offer

About this task

To delete an offer, complete the following steps:

Procedure

1. Log in to Sterling B2B Integrator EBICS Client.
2. From the **Profile management** menu, select **Bank** > **Offer configurations**.
3. In the Offer Configuration page, using either **Search** or **List**, locate and select the offer you want to delete, and click **GO**.
4. Click the delete icon next to the offer you want to delete.

Create a File Format

About this task

EBICS Client enables you to add file formats and associate them with the bank-technical upload (FUL) and download (FDL) order types. An order type can have zero or more file formats. The file formats for FUL and FDL order types are based on the SWIFTNet request type. For more information about SWIFTNet, see http://www.swift.com/. To create a file format, complete the following steps:

Procedure

1. Log in to Sterling B2B Integrator EBICS Client.
2. From the **Profile management** menu, select **File formats**.
3. In the File Format Configuration page, next to **Create File Format**, click **GO**.
4. In the Create: File Format page, enter the values for the fields listed in the following table and click **Next**.

Field	Description
File format	Required. Specify the name of the file format. The first part of the file format name should be one of the following elements. For example, pain.xxx.vcom.dda. The elements indicate the type of transaction. • pain. - Payment Initiation • camt. - Cash Management • tsrv. - Trade Services • tsmt. - Trade Services Management
Country/Region	Required. Select a country or region from the drop-down list.
Supported order types	Required. Select the order type for which the file format is supported. For example, FUL, FDL.

5. In the Confirm page, verify the file format settings, and click **Finish**.

Search for a File Format

About this task

To search for a file format, complete the following steps:

Procedure

1. Log in to Sterling B2B Integrator EBICS Client.
2. From the **Profile management** menu, select **File formats**.
3. In the File Format Configuration page, perform one of the following actions, and click **GO**.

- In the **File format** field under **Search**, enter either a part of the file format name or the entire file format name you are searching for.
- From the **Alphabetically** drop-down list under **List**, select the letter with which the file format that you are searching for, begins.

4. Click the file format link to view the file format settings.

Edit a File Format

About this task

To edit a file format, complete the following steps:

Procedure

1. Log in to Sterling B2B Integrator EBICS Client.
2. From the **Profile management** menu, select **File formats**.
3. In the File Format Configuration page, using either **Search** or **List**, locate and select the file format you want to edit, and click **GO**.
4. Click the update icon next to the file format you want to edit.
5. In the Update: File Format page, specify the values for the fields according to the instructions in the following table and click **Next**.

Field	Description
Country/Region	Required. Select a country or region from the drop-down list.
Supported order types	Required. Select the order type for which the file format is supported.

6. In the Confirm page, verify the values and click **Finish**.

Delete a File Format

About this task

To delete a file format, complete the following steps:

Procedure

1. Log in to Sterling B2B Integrator EBICS Client.
2. From the **Profile management** menu, select **File formats**.
3. In the File Format Configuration page, using either **Search** or **List**, locate and select the offer you want to delete, and click **GO**.
4. Click the delete icon next to the file format you want to delete.

Configure User Permission

User permissions define the offers, order types, and file formats, an EBICS Client user can process on EBICS Client. User permissions are derived from the offer created for the bank. You can assign one of the following permission types to a user:

- Signer: A signer or signatory signs or rejects an order. A submitter can submit the order only after the required signatures are obtained. A signer cannot submit the order for which the signer is the signatory.
- Submitter: A submitter can submit an order after the designated signer signs the order.

Table 2. Authorization levels

Authorization level	Permission type	Description
E	Signer	Single signature. E is the strongest authorization level.
A	Signer	Primary signature
B	Signer	Secondary signature
T	Submitter	Transport signature. Transport signatures are not used for authorization of bank-technical orders, but for authorized submission to the bank's system.

If the Electronic Signature (ES) value is set to 1, then a single signature of E or A authorization level is sufficient to process an order. If the ES value is set to 2, then a combination of E or A and B is required to process the order. However, only authorization levels T and E are supported in French banks. ES value is set to 0 in case of key management order.

Note: EBICS specification does not permit a combination of two secondary ES authorization levels (that is, authorization level B) for processing an order.

Create User Permission

About this task

To create a user permission, complete the following steps:

Procedure

1. Log in to Sterling B2B Integrator EBICS Client.
2. From the **Permissions** menu, select **User permissions**.
3. In the User Permission Configurations page, next to **Create new permission**, click **GO**.
4. In the Create: Permission Information page, from the **Offer name** drop-down list, select the name of the offer for which you want to configure user permissions. The bank ID associated with the offer is displayed. The add icon to add permission is also displayed.
5. Click the add icon. The Add permission page is displayed.
6. In the Add permission page, specify the values for the fields according to the instructions in the following table and click the add icon next to Add signatories:

Field	Description
Order type and File format	Required. The order types and file format associated with the offer are selected by default. To restrict a user from processing some order types and file formats, clear the check box next to the order type and the associated file format.
Minimum number of signatures required	Required. Specify the number of signatures required to process the order.

7. In the Add signatory page, specify the values for the fields according to the instructions in the following table and click **Add signatory**:

Field	Description
User ID	Required. From the drop-down list, select the ID of the user to whom you want to assign the permission.
Partner name	Required. From the drop-down list, select the name of the partner associated with the user.
Permission type	Required. Select one of the following permission types: • Signer • Submitter
Authorization level	Required. If you selected Submitter as the permission type, Authorization level T is assigned to the user. You do not have to select any authorization level from the drop-down list. If you selected Signer as the permission type, select one of the following authorization levels from the drop-down list: • E: Single signature • A: Primary signature • B: Secondary signature

8. Click **Save** and click **Finish**.

Search User Permission

About this task

To search for a user permission, complete the following steps:

Procedure

1. Log in to Sterling B2B Integrator EBICS Client.
2. From the **Permissions** menu, select **User permissions**.
3. In the User Permission Configuration page, perform one of the following actions and click **GO**:
   - In the **Offer name** field or **Bank(Host ID)** field, under **Search**, enter either a part of or the entire offer name or bank ID for which the user permission is configured.
   - From the **Alphabetically** drop-down list, under **List**, select the letter with which the offer name or bank ID for which the user permission is configured begins.

Edit User Permission

About this task

To edit a user permission, complete the following steps:

Procedure

1. Log in to Sterling B2B Integrator EBICS Client.
2. From the **Permissions** menu, select **User permissions**.

3. In the User Permission Configuration page, using either **Search** or **List**, locate and select the offer for which you want to edit the user permission, and click **GO**.
4. Click the update icon adjacent to the user permission you want to edit.
5. In the Update: Permission Information page, perform one of the following:
   - Click the add icon adjacent to **Add permission** to add a file format to the user permission.
   - Click the update icon adjacent to the file format.
   - Click the delete icon adjacent to the file format.
6. This step is applicable if you opted to add a permission. In the Add permission page, specify the values for the fields according to the instructions in the following table and click the add icon adjacent to Add signatories:

Field	Description
Order type and File format	Required. The order types and file format associated with the offer are selected by default. To restrict a user from processing some order types and file formats, clear the check box adjacent to the order type and the associated file format.
Minimum number of signatures required	Required. Specify the number of signatures required to process the order.

   In the Add signatory page, specify the values for the fields according to the instructions in the following table and click **Add signatory**:

Field	Description
User ID	Required. From the drop-down list, select the ID of the user to whom you want to assign the permission.
Partner name	Required. From the drop-down list, select the name of the partner associated with the user.
Permission type	Required. Select one of the following permission types: • Signer • Submitter
Authorization level	Required. If you selected Submitter as the permission type, Authorization level T is assigned to the user. You do not have to select any authorization level from the drop-down list. If you selected Signer as the permission type, select one of the following authorization levels from the drop-down list: • E - Single signature • A - Primary signature • B - Secondary signature

7. This step is applicable if you opted to edit a permission. In the Edit permission page, specify the values for the fields according to the instructions in the following table and click **Save**:

Field	Description
Minimum number of signatures required	Optional. Specify the number of signatures required to process the order.
Add icon adjacent to Add signatories	Optional. Click the add icon adjacent to Add signatories to add a signatory to the user permission.
Update icon	Optional. Click the update icon adjacent to a signatory to change the signatory settings.
Delete icon	Optional. Click the delete icon adjacent to a signatory to delete the signatory.

8. Click **Finish**.

Delete User Permission

About this task

To delete a user permission, complete the following steps:

Procedure

1. Log in to Sterling B2B Integrator EBICS Client.
2. From the **Permissions** menu, select **User permissions**.
3. In the User Permission Configuration page, using either **Search** or **List**, locate and select the offer for which you want to delete the user permission, and click **GO**.
4. Click the delete icon next to the user permission you want to delete.

Initializing a User

A bank enters into a contract with its trading partners. The contract defines the terms and conditions of business transactions agreed upon between the bank and the trading partner.

The bank does not yet have the user's public certificates. Transmission of the user's public certificates to the bank's system is required to initialize the user.

There are three order types used for subscriber initialization: H3K, INI, and HIA. H3K is the simplest and transmits all three public certificates at the same time. However, H3K cannot be used in all cases, such as if trusted keys are used or with protocol version H003. If you cannot, or prefer not to, use H3K, you can use INI and HIA together to transmit the public certificates.

Table 3. Order types for subscriber initialization

Order types	Protocol	Keys/certificates
H3K	H004	• Bank Technical Key certificate for Electronic Signature (ES) • Identification and Authentication certificate • Encryption certificate
INI	H003, H004	Bank-technical key

Table 3. Order types for subscriber initialization (continued)

Order types	Protocol	Keys/certificates
HIA	H003, H004	• Identification and Authentication key • Encryption key

H3K

With protocol version H004, you can use order type H3K, which simplifies and automates the procedure, essentially combining INI and HIA into a single step. Trusted keys are not supported for H3K, and at least the bank technical key used for the ES must be a certificate issued by a Certification Authority (CA). The remaining two certificates for identification and authorization and for encryption can be self-signed certificates. H3K requires no initialization letters.

Use INI and HIA for initialization with non-CA issued certificates or trusted keys, or with protocol version H003.

INI and HIA

The supported versions for the Electronic Signature (ES), encryption, and identification and authentication signature are components of the bank parameters. The user's bank-technical key must be newly-generated if the user does not have a suitable bank-technical key or does not want to use an existing bank-technical key for the new bank connection. The same applies for the encryption key and the identification and authentication key.

The user transmits the public certificates to the financial institution through two independent communication paths:

- INI - Sends the public bank-technical key
- HIA - Sends the public identification and authentication key and the public encryption key

When the user is first assigned to a partner, the status of the user is New. If the user sends only the INI request to the bank, the status is changed to Partly Initialized (INI). If the user sends only the HIA request to the bank, the status is changed to Partly Initialized (HIA). After the user sends both the INI and HIA requests to the bank, the status is changed to Initialized in the bank's system.

The user generates the INI and HIA letters with the hash value of the keys using the Sterling B2B Integrator EBICS Client dashboard interface, manually signs them and mails the letters to the bank. When the bank receives the initialization letters of INI and HIA, it verifies the hash values in the letters against its database. After successful verification, the status of the user is set to Ready in the bank's system, indicating that the user can now transact with the bank. The user then downloads the bank's public certificates by using the HPB system order type and validates them using the Sterling B2B Integrator EBICS Client dashboard interface. After successful validation, the bank status is set to Activated, indicating that transaction with the bank is now possible.

The subscribers can retrieve information stored by the bank using the HKD and HTD order types after the user status is set to 'Ready'.

Submitting Orders

Sterling B2B Integrator EBICS Client Users can submit orders using the **Order submission** function in the **User Menu**.

About this task

If the order that is submitted requires signatories to sign the order, then a pending task is created for the signatory. After the required number of signatures are obtained for the order, the order is submitted to the bank. The Order Submission page helps you to configure order settings and submit an order.

Procedure

1. Log in to Sterling B2B Integrator EBICS Client.
2. From the **User Menu**, select **Order submission**. Specify the values for the fields according to the instructions in the following table and click **Next**.

Field	Description
Partner name	Required. Select a partner name from the drop-down list.
Bank ID(Host ID)	Required. Select a bank ID associated with the partner from the drop-down list.
Bank URL	Required. Select the required bank URL from the drop-down list. The selected URL is used to establish an HTTP or HTTPS session with the EBICS Banking Server.
Order type filter	Required. From the drop-down list, select the appropriate order type: • Key management orders. • Bank technical orders. • VEU management orders. • Other order types.
Order type	Required. From the drop-down list, select the required order type. Order types are assigned to the offer and are represented by a 3-digit alphanumeric code that identifies the type of the order.

   Order types are displayed based on the user permission configured for the EBICS Client user.

   Note: The fields that you see in the Order Type Configuration page varies based on the order type you selected from the **Order type** drop-down. Therefore, it is important that you select an appropriate order type. For example, if you select the order type as INI, then the fields specific to INI are displayed for configuring the order.
3. *If* you selected Key management order type, then specify the values for the fields according to the instructions in the following table and click **Send**.

Field	Description
Order ID prefix	Optional. From the drop-down list, select the order ID prefix. EBICS Client allocates a unique order ID to each order based on the bank, user ID, and the order type. The client generates the order ID as per EBICS specifications. The order ID is a 4-digit alphanumeric ID. You can specify the first character of the order ID. The second, third, and fourth characters of the order ID are alphanumeric in an ascending order (A-Z or 0-9). This field is applicable to all the key management order types.
Security medium	A 4-digit security number is displayed by default. The value cannot be changed for INI, HIA, and HPB order types.
Product ID	Enter the product ID for the EBICS Client application.
Product language	Enter the language setting of the EBICS Client application that you are using. For example, enter EN if the language is set to English.
Authentication private certificate	Required. From the drop-down list, select the appropriate authentication private certificate.
Authentication public certificate	Required. From the drop-down list, select the appropriate authentication public certificate.
Authentication key version	The key version of the authentication certificate is displayed. Valid value is X002.
Encryption private certificate	Required. From the drop-down list, select the appropriate encryption private certificate.
Encryption public certificate	Required. From the drop-down list, select the appropriate encryption public certificate.
Encryption key version	The key version of the encryption certificate is displayed. Valid value is E002.
Electronic signature private key	Required. From the drop-down list, select the appropriate electronic signature private key.
Electronic signature public key	Required. From the drop-down list, select the appropriate electronic signature public key.
Electronic signature key version	Required. From the drop-down list, select the appropriate electronic signature key version.

4. *If* you selected Bank-technical order type filter, then specify the values for the fields according to the instructions in the following table and click **Send**.

Order ID prefix	Optional. From the drop-down list, select the order ID prefix. EBICS Client allocates a unique order ID to each order based on the bank, user ID, and the order type. The client generates the order ID as per EBICS specifications. The order ID is a 4-digit alphanumeric ID. You can specify the first character of the order ID. The second, third, and fourth characters of the order ID are alphanumeric in an ascending order (A-Z or 0-9).
Security medium	Required. Type a 4-digit security number in 0100 to 0499 range.
Product ID	Enter the product ID for the EBICS Client application.
Product language	Enter the language setting of the EBICS Client application that you are using. For example, enter EN if the language is set to English.

Autosubmit	Optional. This check box is applicable only for FUL order type and is selected by default. If the autosubmit option is selected, then an order is automatically submitted after the required number of signatures are obtained. If the autosubmit option is not selected, then an EBICS Client user has to log in to the EBICS Client dashboard interface, navigate to the pending tasks screen, and submit the order after the required number of signatures are obtained.
Read file from mailbox	Required. This option is applicable only for FUL order type. To upload the payload file from the mailbox, select **Yes**. Click **Select file** next to Upload file. From the Select file to upload to mailbox list, select the required file and click **Finish**. To upload the payload file from a file location, select **No**. Click **Browse** next to Upload file, navigate to the file location and select the required file.
File format	Required only for the FUL and FDL order types. From the drop-down list, select the appropriate file format.
Start date	Optional. Click the field and select the start date from the calender. This option is applicable only for FDL order type.
End date	Optional. Click the field and select the end date from the calender. This option is applicable only for FDL order type.
Order parameter list	Optional. Click **Add parameter** to define variables for an order. Complete the information pertaining to the following order parameter fields and click **Add parameter**. This option is applicable only for FDL order type. • Name: Required. Type a unique name of the parameter. Do not use any spaces or special characters in the parameter name. • Value: Required. Type a value of the parameter. • Type: Optional. Select the parameter type. The available choices are: – String – Number – Boolean

5. *If* you selected VEU management orders order type filter, then specify the values for the fields according to the instructions in the following table and click **Send**.

Order ID prefix	Optional. From the drop-down list, select the order ID prefix. EBICS Client allocates a unique order ID to each order based on the bank, user ID, and the order type. The client generates the order ID as per EBICS specifications. The order ID is a 4-digit alphanumeric ID. You can specify the first character of the order ID. The second, third and fourth characters of the order ID are alphanumeric in an ascending order (A-Z or 0-9).
Security medium	Required. Type a 4-digit security number in 0100 to 0499 range.
Product ID	Enter the product ID for the EBICS Client application.
Product language	Enter the language setting of the EBICS Client application that you are using. For example, enter EN if the language is set to English.
VEU order types	Required. Select the appropriate VEU order type from the VEU order types list.

OrderID	Required. Specify the ID of the order for which you are submitting the HVE or HVS order type.
PartnerID	Required. Specify the ID of the partner associated with the user who submitted the order for which you are submitting the HVE or HVS order type.
Order type	Required. Select the order type of the order for which you are submitting the HVE or HVS order type.
MessageDigest	Optional. Select MessageDigest to submit the hash value of the order data. **Note:** You can request for the hash value by calling or mailing the bank. The bank sends the hash value of the order data through an alternate mode of communication. For example, email.
PayloadMsgID	Optional. Select PayloadMsgID to submit the complete payload from your mailbox. Perform the following actions: 1. Click **Select**. 2. Select the required payload from the list. 3. Click **Finish**. **Note:** You can request for the payload by calling or mailing the bank. The bank sends the payload to your EBICS Client mailbox.

6. *If* you selected Other order types order type filter, then specify the values for the fields according to the instructions in the following table and click **Send**.

Order ID prefix	Optional. From the drop-down list, select the order ID prefix. EBICS Client allocates a unique order ID to each order based on the bank, user ID, and the order type. The client generates the order ID as per EBICS specifications. The order ID is a 4-digit alphanumeric ID. You can specify the first character of the order ID. The second, third, and fourth characters of the order ID are alphanumeric in an ascending order (A-Z or 0-9).
Security medium	Required. Type a 4-digit security number in 0100 to 0499 range.
Product ID	Enter the product ID for the EBICS Client application.
Product language	Enter the language setting of the EBICS Client application that you are using. For example, enter EN if the language is set to English.

Submit an order as a technical user

A technical user is a machine configured to submit orders on behalf of a non-technical (human user) EBICS Client user using a back-end file system. The technical user is associated with a non-technical user.

To submit an order using a technical user, you must configure:

- User as a technical subscriber
- File system adapter or a similar technical adapter

The scenario illustrates using a file system adapter configured on Sterling B2B Integrator.

A technical user submits the orders by placing a compressed file that contains an XML file, ordermetadata.xml and optionally the payload data in a collection folder specified when configuring a file system adapter.

The following diagram illustrates the process flow when a technical user submits orders. The backend process generates the ordermetadata.xml, packages the payload metadata in a compressed format and places it in a directory so that a technical adapter, such as the file system adapter can pick up the file and send it to EBICS Client for processing the data. The EBICS Client Runtime components include the User Mailbox, OrderPreProcessor, EBICS Client Mailbox, and EBICS Runtime. The OrderPreProcessor extracts the contents of the compressed file and transfers the XML metadata to the EBICS Client Mailbox that in turn sends it to the EBICS Runtime component for processing the metadata. The OrderPreProcessor component sends the payload data to the mailbox of the EBICS Client user. Based on the values specified in the XML, EBICS Client sends the order request to the banking server.

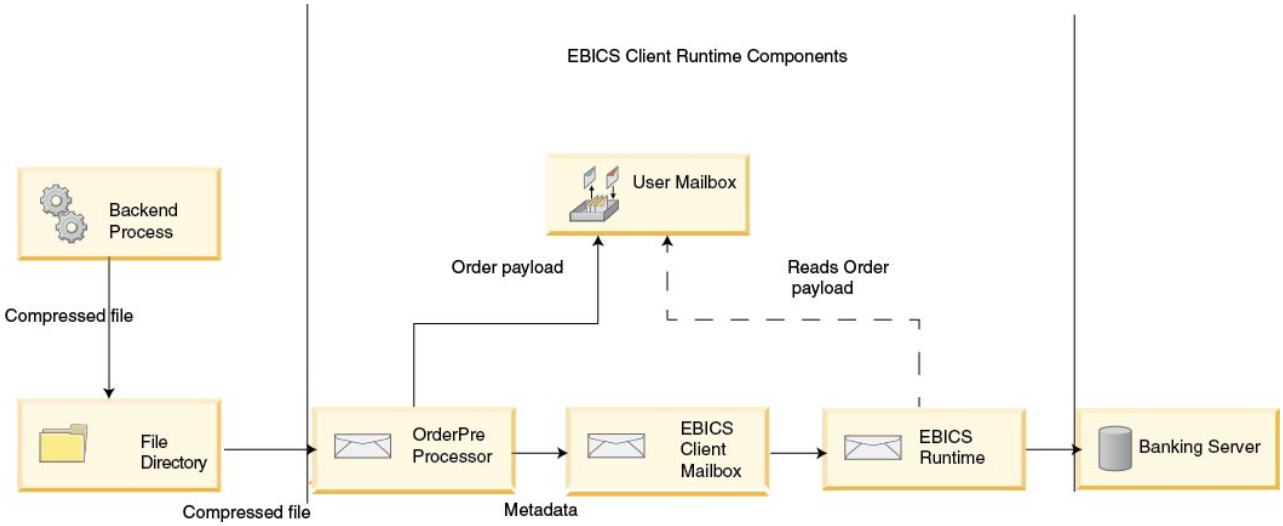

Figure 1. Process flow of order submission by a technical user

If the order type is FUL, the ordermetadata.xml contains the following details:

HostID
details of the bank involved in the transaction

UserID
non-technical user who wants to submit the FUL order

SystemID
technical user who is a delegate of the non-technical user

PartnerID
details of the partner associated with the user

OrderType
details of the order type and file format

Custom attributes
In Sterling B2B Integrator V5.2.6.1_2 and later, users can add custom attributes before submitting an EBICS order. These attributes are saved in the `ordermetadata.xml` file and then displayed in the UI of the order. To define custom attributes, use the `<ebicsUserAttribute>` tag in the `ordermetadata.xml` file.

The following example details the format of an XML if you are submitting an FUL order as a technical user.

```
<?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>
```

If the order type is INI or HIA, the system ID and the user ID have the same value in the ordermetadata.xml file.

The following example illustrates the format of an XML if you are submitting an INI order as a technical user:

```
<?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>
```

If the file name of the payload has non-ASCII characters, then use the jar utility that comes with the Java Development Kit (JDK) installed with Sterling B2B Integrator to create a compressed file. You have to execute the jar utility from the command prompt in Windows or the terminal in UNIX with the following parameters: `jar cFM <zip_fileName> ordermetadata.xml <payload_fileName with non-ASCII characters>`.

Note: Java Home must be set to the JDK.

If the file name of the payload has only ASCII characters, then either the jar utility or any application such as WinZip or WinRAR can be used to create a compressed file.

Configure a technical user

About this task

You must configure a non-technical user before configuring a technical user to associate a technical user with a non-technical user. To configure a non-technical user, complete the following steps:

Procedure

1. Log in to Sterling B2B Integrator EBICS Client.
2. From the **Profile management** menu, select **User**.

3. In the User Configuration page, next to **Configure existing user as EBICS user** click **GO**.
4. In the User Configuration page, specify the values for the fields according to the instructions in the following table and click **Next**:

Field	Description
User ID	Required. Unique ID of the user in the bank's system, which corresponds to the user created in the EBICS Client dashboard. From the **User ID** drop-down list, select the user ID.
User type	Required. From the **User type** drop-down list, select `EBICS client user` as the role of the user.
Timezone	Optional. Specify the time zone of the user.
Technical user	Select this check box to configure a Technical user. A technical user is a file system configured to submit orders.
Certificate type	Required if you selected EBICS client user as the user type. Select X509 if you are using X.509 public key certificate to authorize the certificates. Select Keys if you are using RSA keys to authorize the certificates. **Note:** EBICS Client supports non-encrypted keys only.

5. *If* you selected X509 as the certificate type, specify the values for the fields according to the instructions in the following table in the Technical Information page and click **Next**:

Field	Description
Authentication private certificate	Required. Select the private key the EBICS Client uses to create a digital signature for the user in the request sent to the bank. The bank must have the public part of the key to validate the authorization. The drop-down contains a list of certificates configured in the Sterling B2B Integrator system certificate store.
Authentication public certificate	Required. Select the public key the user provides to the bank to validate the authorization of the user in the request from the EBICS Client. The trading partner or user shares the key with the bank. The key must be a public part of the Sterling B2B Integrator system certificate that is selected as the authentication private certificate.
Authentication key version	The key version of the authentication certificate is displayed. Valid value is X002.
Encryption private certificate	Required. Select the private key the EBICS Client uses to decrypt the response received from the EBICS Banking Server. The drop-down contains a list of certificates configured in the Sterling B2B Integrator system certificate store.

Field	Description
Encryption public certificate	Required. Select the public part of the Sterling B2B Integrator system certificate that is selected as the encryption private certificate. The trading partner or user shares the key with the bank.
Encryption key version	The key version of the encryption certificate is displayed. Valid value is E002.
Use hardware key-store for Electronic signature	Optional. Select this option if you have an activated 3S Key token.
Hardware key type	3S Key is displayed as the Hardware key type. 3SKey is a SWIFT secure signature key used for digital identity. You must activate the 3SKey token and register the key with the bank to enable you to sign and send messages to the bank.
Electronic signature private key	Optional. Select the private key of the Electronic Signature (ES) certificate if you are not using a hardware key for Electronic Signature.
Electronic signature public key	Required. Select the public key of the Electronic Signature (ES) certificate that is used to verify the signature of order data. The public key value of an electronic signature certificate should not be the same as an authentication or encryption certificate.
Electronic signature key version	Required if you are not using a hardware key store for electronic signature. Select the key version of the electronic signature certificate. Valid values are A005 and A006. If you are using a hardware key store for electronic signature, then the key version is set to A005 and it cannot be changed.

6. *If* you selected Keys as the certificate type, specify the values for the fields according to the instructions in the following table in the Technical Information page and click **Next**:

Field	Description
Authentication private key	Required. Click **Browse** to select the file with the private part of the authentication key from your computer.
Authentication public key	Required. Click **Browse** to select the file with the public part of the authentication key from your computer.
Authentication key version	Required. Select the key version of the authentication certificate. Valid value is X002.
Encryption private key	Required. Click **Browse** to select the file with the private part of the encryption key from your computer.
Encryption public key	Required. Click **Browse** to select the file with the public part of the encryption key from your computer.

Field	Description
Encryption key version	Required. Select the key version of the encryption certificate. Valid value is E002.
Electronic signature private key	Required. Click **Browse** to select the file with the private part of the Electronic signature key from your computer.
Electronic signature public key	Required. Click **Browse** to select the file with the public part of the Electronic signature key from your computer.
Electronic signature key version	Required. Select the key version of the Electronic signature certificate. Valid values are A005 and A006.

7. This step is applicable only if you opted to add a new partner or edit an existing partner for a non-technical or human user. In the Associated Partners: User Settings page, specify the values for the fields according to the instructions in the following table, and click **Add partner**.

Field	Description
Partner name	Required. From the **Partner name** drop-down list, select the partner to which a user is associated. A user can be associated with many partners. **Note:** Use the Sterling B2B Integrator dashboard to create trading partner entities.
Upload mailbox path	Required. Configure the upload mailbox and assign users to operate the mailbox in Sterling B2B Integrator. Specify the mailbox path for the uploaded messages. You must assign a mailbox path to store the unpacked messages from an EBICS request. If the mailbox (User ID, Partner name, Inbox), already exists in Sterling B2B Integrator and if you leave this field blank, an error message asking you to specify the default mailbox path is displayed. **Note:** Ensure that the mailbox path starts with a forward slash (/).
Download mailbox path	Required. Configure the download mailbox and assign users to operate the mailbox in Sterling B2B Integrator. Specify the mailbox path for the downloaded messages. You must assign a mailbox path to store the messages that are packaged as part of an EBICS response. If the mailbox (User ID, Partner name, Outbox) already exists in Sterling B2B Integrator, and if you leave this field blank, an error message asking you to specify the default mailbox path is displayed. **Note:** Ensure that the mailbox path starts with a forward slash (/).

8. In the Associated Partners page, perform any of the following actions and click **Next**.

- Click the add icon to associate a new partner with the Technical user.
- Click the update icon next to the partner you want to edit.
- Click the delete icon to disassociate a partner from the Technical user.

9. A non-technical user delegates a technical user to perform the transactions. In the Associated Partners: User Settings page, specify the values for the fields according to the instructions in the following table, and click **Add partner**.

Field	Description
Partner name	Required. From the **Partner name** drop-down list, select the partner to which a user is associated. A user can be associated with many partners. A technical user and a non-technical user must belong to the same partner. The technical user inherits all the permissions of the associated non-technical user. **Note:** Use the Sterling B2B Integrator dashboard to create trading partner entities.
Delegate of	Required. Select the user who will be delegating their tasks to the technical user.

10. In the Associated Partners page, click **Next**.
11. In the Confirm page, verify the user configuration settings, and click **Finish**. You can also click the **Show All** link next to **Associate Partners** to view the following details:
    - the list of partners associated with the user.
    - the corresponding configuration details, such as upload or download mailbox path for non-technical user.
    - the technical user that is a delegate of the non-technical user.

Viewers

The following topic describes how you can view and search events (transactions), search orders, and complete your pending tasks.

Note: In EBICS Client application, the transaction time for Events and Orders is stored in GMT. For example, if the EBICS Client user is configured in Central European Standard Time (GMT+1) timezone, and an order is submitted on 3rd February 2011, 9:00 am GMT, then to search the order, specify 3rd February 2011, 10:00 am as the start date and start time in the Order search screen.

Searching for Events

Using the Event Viewer, a user can search for events or transactions and obtain event summary details through the simple and advanced search options.

About this task

You can perform either a simple search or an advanced search by using multiple parameters to refine your search. Depending on the requirement of your search, you can do the following:

- Indicate whether you want to search the event records in the live tables or in the history (archived) tables.
- Select date ranges and time ranges.

- Specify additional parameters to refine the search results.

The following procedure helps you search the event records and obtain an event summary that meets your search criteria:

Procedure

1. Log in to Sterling B2B Integrator EBICS Client.
2. From the **Viewers** menu, select **Event viewer**.
3. Complete the information pertaining to searching for events in the following table:

Field	Description
Search location	Required. Select the appropriate search location. The options are: • **Live tables**: This option is selected by default. When this option is selected, events are searched in the live tables (current) database. • **Restore tables**: When this option is selected, events are searched in the restore database.
Start date	Required. The current date by default is populated in this field based on the timezone specified while configuring the user. Click the **Start Date** field to view the calendar and select the start date from the calendar.
End date	Required. The current date by default is populated in this field based on the timezone specified while configuring the user. Click the **End Date** field to view the calendar and select the end date from the calendar.
Event type	Optional. Select an appropriate event type from the drop-down list. The available event types are: • All (default) • Info • Warning • Error • Critical
User ID	Optional. From the drop-down list, select the user ID of the EBICS Client user who initiated the order related to the event you are searching for. This option is not available for a user with the role and permissions of EBICS Client user.
Start time	Required. The default system time is displayed in the field based on the timezone specified while configuring the user. Click the **Start time** field to select the start time.
End time	Required. The default system time is displayed in the field based on the timezone specified while configuring the user. Click the **End time** field to select the end time.

Field	Description
Sort by	Optional. You can sort the search results based on the following options: • Datetime (default) • Event type • Event code • Order type • Order ID You can also sort the search results in an ascending or descending order. Select the **ASC** or **DSC** option from the drop-down list. DSC is the default option.
Refresh rate	Optional. Using the up or down arrow, specify the frequency at which you want the search results to refresh.
Refresh icon	Optional. By default, refreshing of the search results is disabled (Off). Click the refresh icon to enable the refreshing of the search results (On).

4. Click **Search**. The events summary is displayed in a tabular format, which is as follows:

Field	Description
Event Code	Click the event code link to view the event details.
Event type	The type of event that is generated is displayed. The available event types are: • All • Info • Warning • Error • Critical
Event Name	The event name is displayed.
Timestamp	The date and the time when the event was generated is displayed.
Order type	The order type for which the event was generated is displayed.
Order Seq ID	The order sequence ID of the order for which the event was generated is displayed. Click the order sequence ID link to view the order details. **Note:** An EBICS Client admin and EBICS Client operator cannot view the order document link in the Order Details page. The document link is displayed only for an EBICS Client user.
Order ID	The order ID of the order for which the event was generated is displayed. Click the order ID link to view the order details. **Note:** An EBICS Client admin and EBICS Client operator cannot view the order document link in the Order Details page. The document link is displayed only for an EBICS Client user.
User ID	When an EBICS Client admin initiates an event search, the user ID of the EBICS Client user responsible for triggering the event, such as, submitting an order, changing order configuration, is displayed. When an EBICS Client user initiates an event search, the user ID of the user who initiated the search is displayed.

5. Click **Reset** to clear the event search parameters. Resetting the search parameters does not clear the previous search results.

Searching for Orders

With the Sterling B2B Integrator EBICS Client, you can search for orders and obtain an order summary using simple or advanced search options.

About this task

You can perform either a simple search or an advanced search by using multiple parameters to refine your search. Depending on the requirement of your search, you can:

- Indicate whether you want to search the order records in the live tables or in the restore (archived) tables.
- Select date ranges and time ranges.
- Specify additional parameters to refine the search results.

To search the order records and obtain an order summary that meets your search criteria:

Procedure

1. Log in to Sterling B2B Integrator EBICS Client.
2. From the **Viewers** menu, select **Order search**.
3. Enter your search criteria according to the following table:

Table 4. Searching for orders

Field	Description
Search location	Required. Select the appropriate search location. The options are: • **Live tables**: This option is selected by default. When this option is selected, orders are searched in the live tables (current) database. • **Restore tables**: When this option is selected, orders are searched in the restore database.
Start date	Required. The current date by default is populated in this field based on the timezone specified while configuring the user. Click the **Start Date** field to view the calendar and select the start date from the calendar.
End date	Required. The current date by default is populated in this field based on the timezone specified while configuring the user. Click the **End Date** field to view the calendar and select the end date from the calendar.
Bank ID(Host ID)	Optional. Select the required bank ID.
Order ID	Optional. Type the order ID in the **Order ID** field.
Order type	Optional. Select an appropriate order type from the **Order Type** drop-down list.

Table 4. Searching for orders (continued)

Field	Description
Status	Optional. Select the appropriate status of the order from the **Status** drop-down list: • All (default) • All completed • All incompleted • Success • Failed • In progress • Pending at Client • Pending at Server
User ID	Optional. From the drop-down list, select the user ID of the EBICS Client user who initiated the order you are searching for. This option is not available for an EBICS Client user.
Permission type	Optional. Select the appropriate permission type. The options are: • Submitter: This option is selected by default. Orders are searched based on the submitter of the order. • Signer: Select this option to search for orders based on the signer of the order. Click the order ID link to view the order details. Order events, Activities, and Pending signatures tabs are not displayed when orders are searched by signer.
Start time	Required. The default system time is displayed in the field based on the timezone specified while configuring the user. Click the **Start time** field to select the start time.
End time	Required. The default system time is displayed in the field based on the timezone specified while configuring the user. Click the **End time** field to select the end time.
Partner name	Optional. Select the required partner name.
Order Seq ID	Optional. Type the order sequence ID in the **Order Seq ID** field.
File format	Optional. Select an appropriate file format from the **File format** drop-down list.
FUL Ack status	Optional. Type the FUL acknowledgment status in the **FUL Ack status** field.
Sort by	Optional. You can sort the search results based on one of the following options: • Datetime (default) • Last activity datetime • Order ID • Order type • Partner name • Bank ID(Host ID) • User ID You can also sort the search results in an ascending or descending order. Select the **ASC** or **DSC** option from the drop-down list. DSC is the default option.
Refresh rate	Optional. Using the up or down arrow, specify the frequency at which you want the search results to refresh.

Table 4. Searching for orders (continued)

Field	Description
Refresh icon	Optional. By default, refreshing of the search results is disabled (Off). Click the refresh icon to enable the refreshing of the search results (On).

4. Click **Search**. The order summary displays the following information in a tabular format:

Table 5. Order information fields

Field	Description
Order Seq ID Order ID	Click the Order ID or Order Seq ID link to view the order details. The Order summary details page is divided into two sections: **Order data** and **Order details**. The Order data section provides the following information about the selected order: • Order Seq ID • Order type • File format • Number of signatures (Signatures required to submit the order) • Start date and time • Last activity date and time • Order ID • Partner name • User ID • Bank ID(Host ID) • Status of the order • Completion date and time • Workflow ID • Document (The order payload). The order document link is displayed only for the EBICS Client user. Click the link to view the payload (for upload and download technical orders) or the order request XML (for other order types). The Order details section has three tabs: **Order events** Provides information about events pertaining to an order, such as, data compressed, data encoded, and EBICS packaging passed. **Activities** Provides information about the activities pertaining to an order, such as, Pending at client for signature and Submit action by submitter. The activities can be in one of the following states: • In progress • Completed • Failed Activities are not generated for INI, HIA, and HPB order types. **Pending tasks** Lists the users whose signatures are pending for the selected order. **HAC States** Provides processing status and details for all submitted orders
User ID	The user ID of the EBICS Client user who submitted the order.
Partner name	Name of the partner to which a user is associated, is displayed.
Bank ID(Host ID)	The bank ID or the host ID of the bank to which the EBICS Client user submitted the order. It is a unique ID for the bank in the banks system.
Order type	The order type is displayed.

Table 5. Order information fields (continued)

Field	Description
Status	The status of the order is displayed. For example: Success, Failed, In progress, and Pending at Client.
FUL Ack status	The FUL acknowledgment status of the order is displayed.
HAC Action	The HAC action is displayed. For information, see "HAC Processing" on page 114.
HAC Reason	The HAC Reason code is displayed. For information, see "HAC Processing" on page 114.
Start DateTime	The start date and time are displayed.
Completion DateTime	The completion date and time are displayed.

5. Click **Reset** to clear the order search parameters. Resetting the search parameters does not clear the previous search results.

Pending Tasks

Based on the configuration settings defined in an offer, multiple signatories may have to sign the order to process the order data. If an order is submitted for processing without obtaining the required signatures, EBICS Client does not process the order. Notifications for pending signatures are sent to the mailboxes of the concerned signatories requesting them to sign to the order. If the order is pending and needs to be signed, the user who is a signatory, sees the **Sign** link. If all the required signatures are obtained and the order is ready to be submitted, the user who is a submitter, sees the **Submit** link.

The Pending Tasks page is the landing page for Sterling B2B Integrator EBICS Client users. Use this page to view and sign or submit pending orders. To sign or submit a pending order, complete the following steps:

1. Log in to Sterling B2B Integrator EBICS Client.
2. From the **Viewers** menu, select **Pending tasks**. The pending tasks are displayed in a tabular format.

Column names	Description
Order ID	Displays the order ID. Click the order ID to view the order summary and sign the order. Click the order document link in the order details page to view the payload.
Submitter ID	Displays the submitter ID.
Bank ID(Host ID)	Displays the bank ID.
Order type	Displays the type of the order.
Datetime	Displays the timestamp in date and time format.
Status	Displays the status of the order. For example, Success, Pending at Client, Pending at Server, and so on. Depending on the required action, **Sign** or **Submit** links are displayed next to the status.

3. To sign a pending order, click **Sign**. To submit a pending order, click **Submit**.
4. *If* hardware security for electronic signature is configured for an EBICS Client user, then the Electronics Signatures page is displayed after you click **Sign**. Enter the values for the fields listed in the following table and click **Sign**:

Field	Description
Provider name	The name of the PKCS11 hardware signature module (HSM) provider is displayed.
Select DLL	Click **Browse**, navigate to the appropriate location, and select the DLL file of the HSM.
Select PKCS11 provider	Click **Load providers**, navigate to the appropriate location, and select the PKCS11 service provider file. After loading the provider files, select the appropriate file from the drop-down list.
Enter pin	Specify the security pin in the **Enter pin** field.
Select private key	Click **Load keys**, navigate to the appropriate location, and select the keys. After loading the keys, select the appropriate key from the drop-down list.

Search Pending VEU Tasks

Distributed Electronic Signature (VEU) enables you to transmit data remotely to multiple subscribers. Multiple subscribers can authorize orders remotely, independent of time and space.

Before you begin

To search the pending VEU tasks, an EBICS Client user must submit an HVU (download VEU overview) or an HVZ (download VEU overview with additional information, for example, hash value) order type.

About this task

Complete the following steps to search the pending VEU tasks:

Procedure

1. Log in to Sterling B2B Integrator EBICS Client.
2. From the **User Menu**, select **Viewers** > **Pending VEU Tasks**.
3. In the Pending VEU tasks page, specify the values for the fields listed in the following table and click **Search**.

Field	Description
Partner name	Required. Select a partner name from the drop-down list.
Bank ID(Host ID)	Required. Select a bank ID associated with the partner from the drop-down list.
Bank URL	Required. Select the required bank URL from the drop-down list. The selected URL is used to establish an HTTP or HTTPS session with the EBICS Banking Server.

A request is sent to the bank to retrieve the details of the pending VEU orders.

4. Click **Advanced Search** to specify additional search criteria for VEU management orders in the Order Submission page.
5. If the response from the bank is delayed, click **Cancel**.
6. Click **Reset** to re-enter the search criteria.

View Pending VEU Tasks

About this task

Complete the following steps to view the pending VEU tasks:

Procedure

1. Log in to Sterling B2B Integrator EBICS Client.
2. From the **User Menu**, select **Viewers** > **Pending VEU Tasks**.
3. In the Pending VEU tasks page, specify the values for the fields listed in the following table and click **Search**.

Field	Description
Partner name	Required. Select a partner name from the drop-down list.
Bank ID(Host ID)	Required. Select a bank ID associated with the partner from the drop-down list.
Bank URL	Required. Select the required bank URL from the drop-down list. The selected URL is used to establish an HTTP or HTTPS session with the EBICS Banking Server.

A request is sent to the bank to retrieve the details of the pending VEU orders.

4. In the Search Results section of the Pending VEU tasks page, you can view the following information in the search results:

Field	Description
Order type	The order type of the pending VEU order. For example, FUL.
Order ID	The order ID of the pending VEU order. Click the Order ID link to view information about the order data.
Order data size	The size of the uncompressed order data in kilobytes.
Signatures required	Total number of electronic signatures required for activation in the server.
Signatures done	The number of signatures already provided for the validation of the order.
Status	The status of the order is displayed. Valid values are pending and complete. For example, if a user has signed an order but if the order requires additional signatures to validate the order, the status of the order is pending in the VEU store. The user who has already signed the order cannot sign or cancel the order in the pending status. However, this user can submit HVT or HVD order types.

Field	Description
Datetime	The timestamp is displayed in date and time format.

Retrieve Details of a Pending VEU Order

About this task

Complete the following steps to retrieve details of a pending VEU order:

Procedure

1. Log in to Sterling B2B Integrator EBICS Client.
2. From the **User Menu**, select **Viewers** > **Pending VEU Tasks**.
3. In the Pending VEU tasks page, specify the values for the fields listed in the following table and click **Search**.

Field	Description
Partner name	Required. Select a partner name from the drop-down list.
Bank ID(Host ID)	Required. Select a bank ID associated with the partner from the drop-down list.
Bank URL	Required. Select the required bank URL from the drop-down list. The selected URL is used to establish an HTTP or HTTPS session with the EBICS Banking Server.

   A request is sent to the bank to retrieve the details of the pending VEU orders.
4. In the Search Results section of the Pending VEU tasks page, click the Order ID link. The details of the order data are displayed.

Field	Description
Order ID	The order ID of the pending VEU order. Click the Order ID link to view information about the order data.
Order type	The order type of the pending VEU order. For example, FUL.
Originator Partner ID	The Partner ID associated with the user who submitted the upload order type.
Originator user ID	Subscriber ID of the user who submitted the upload order type.
Order data available	After submitting an HVZ order type, indicates whether the order data can be downloaded in the original format or not.
Order details available	The order information for HVU order type.
Order data size	The size of the uncompressed order data in kilobytes.
Datetime	The timestamp is displayed in date and time format.

Field	Description
Ready to be signed	Indicates whether the order is already signed by the user or not. False indicates that the order is already signed by the user. True indicates that the order is ready to be signed by the user.
Signatures required	Displays the minimum number of signatures required to authorize the order.
Signatures done	The number of signatures that completed the validation of the order. Indicates the number of electronic signatures already provided and the information about previous signatories. Click the Signer info link to view the details of the signer: • Partner name: name of the trading partner • User ID • Name: name of the signatory • Time stamp • Authorization level: the authorization level of the signatory
Order info link	Click the order info link to view details about the order: • Account: Click the account info link to view the name of the account holder, currency code, account description, the role of the account holder, account number, and the bank code. • Amount: view the amount of the order transaction. • Currency code: view the currency code of the order transaction. • Debit • Execution date: view the date of the execution of the order. • Description: Click the description link to view the description and description type of the signatory.

5. In the Order data window, select one of the following options to retrieve the details for a pending VEU order:
   - From the **Submit** drop-down list, select HVT – order details to retrieve the transaction details of the order data
   - From the **Submit** drop-down list, select HVT – complete order data to retrieve the complete order data
   - From the **Submit** drop-down list, select HVD to retrieve the state of an order that is currently in VEU processing and for which the subscriber is authorized as a signatory. The subscriber receives information about the order in the form of an electronic accompanying note (DisplayFile), the order hash value (DataDigest), and the previous signatories (SignerInfo).
6. In the VEU order details window, specify the values for the following parameters:

Field	Description
Order id prefix	Select an alphabet from the drop-down list.
Security medium	Security medium for the user's bank-technical key. Type a four-digit security number in the 0100 – 0499 range.
Bank URL	Select the bank URL from the drop-down list.
Fetch limit	Valid if you selected HVT-order details. Maximum number of order details to be transmitted if the completeOrderData attribute is set to false. The default value is 100. Valid value is any non-negative integer. Specify 0 to fetch unlimited number of details. While it is possible to retrieve more than 100 details at a time, it is not ideal.
Fetch offset	Valid if you selected HVT-order details. The offset position in the original order file that marks the starting point of the transaction details to be transmitted. If the completeOrderData attribute is set to false, then the offset position applies to the sequential number of a particular order. The default value is 0. Valid value is any non-negative integer. To retrieve more than 100 records, set **fetch offset** as 0 to retrieve the first 100 records, then set **fetch offset** as 101 to retrieve the next 100 records. Continue as needed.

7. Click **Submit**.

Sign a Pending VEU order

Before you begin

To sign a pending VEU order, ensure that the following prerequisites are met:

- Ready to be Signed parameter displays True
- One of the following VEU orders are submitted:
  - HVZ
  - HVU and HVD
  - HVU and HVT - complete order data

About this task

Complete the following steps to sign a pending VEU order:

Procedure

1. Log in to Sterling B2B Integrator EBICS Client.
2. From the **User Menu**, select **Viewers** > **Pending VEU Tasks**.
3. In the Pending VEU tasks page, specify the values for the fields listed in the following table and click **Search**.

Field	Description
Partner name	Required. Select a partner name from the drop-down list.
Bank ID(Host ID)	Required. Select a bank ID associated with the partner from the drop-down list.
Bank URL	Required. Select the required bank URL from the drop-down list. The selected URL is used to establish an HTTP or HTTPS session with the EBICS Banking Server.

A request is sent to the bank to retrieve the details of the pending VEU orders.

4. In the Pending VEU tasks page, click the Order ID link. The details of the order data are displayed.

Field	Description
Order ID	The order ID of the pending VEU order. Click the Order ID link to view information about the order data.
Order type	The order type of the pending VEU order. For example, FUL.
Originator Partner ID	The Partner ID associated with the user who submitted the upload order type.
Originator user ID	Subscriber ID of the user who submitted the upload order type.
Order data available	After submitting an HVZ order type, indicates whether the order data can be downloaded in the original format or not.
Order details available	The order information for HVU order type.
Order data size	The size of the uncompressed order data in kilobytes.
Datetime	The timestamp is displayed in date and time format.
Ready to be signed	Indicates whether the order is already signed by the user or not. False indicates that the order is already signed by the user. True indicates that the order is ready to be signed by the user.
Signatures required	Displays the minimum number of signatures required to authorize the order.
Signatures done	The number of signatures that completed the validation of the order. Indicates the number of electronic signatures already provided and the information about previous signatories. Click the Signer info link to view the details of the signer: • Partner name: name of the trading partner • User ID • Name: name of the signatory • Time stamp • Authorization level: the authorization level of the signatory

Field	Description
Order info link	Click the order info link to view details about the order: • Account: Click the account info link to view the name of the account holder, currency code, account description, the role of the account holder, account number, and the bank code. • Amount: view the amount of the order transaction. • Currency code: view the currency code of the order transaction. • Debit • Execution date: view the date of the execution of the order. • Description: Click the description link to view the description and description type of the signatory.

5. Click **Sign order**.
6. In the VEU order details window, specify the values for the following parameters:

Field	Description
Order id prefix	Select an alphabet from the drop-down list.
Security medium	Security medium for the user's bank-technical key. Type a four-digit security number in the 0100 – 0499 range.
Bank URL	Select the bank URL from the drop-down list.

7. Click **Submit**.

Cancel a Pending VEU order

Before you begin

To cancel a pending VEU order, ensure that the following prerequisites are met:

- Ready to be Signed parameter displays True
- One of the following VEU orders are submitted:
  - HVZ
  - HVU and HVD
  - HVU and HVT - complete order data

About this task

Complete the following steps to cancel a pending VEU order:

Procedure

1. Log in to Sterling B2B Integrator EBICS Client.
2. From the **User Menu**, select **Viewers** > **Pending VEU Tasks**.
3. In the Pending VEU tasks page, specify the values for the fields listed in the following table and click **Search**.

Field	Description
Partner name	Required. Select a partner name from the drop-down list.
Bank ID(Host ID)	Required. Select a bank ID associated with the partner from the drop-down list.
Bank URL	Required. Select the required bank URL from the drop-down list. The selected URL is used to establish an HTTP or HTTPS session with the EBICS Banking Server.

A request is sent to the bank to retrieve the details of the pending VEU orders.

4. In the Search Results section of the Pending VEU tasks page, click the Order ID link. The details of the order data are displayed.

Field	Description
Order ID	The order ID of the pending VEU order. Click the Order ID link to view information about the order data.
Order type	The order type of the pending VEU order. For example, FUL.
Originator Partner ID	The Partner ID associated with the user who submitted the upload order type.
Originator user ID	Subscriber ID of the user who submitted the upload order type.
Order data available	After submitting an HVZ order type, indicates whether the order data can be downloaded in the original format or not.
Order details available	The order information for HVU order type.
Order data size	The size of the uncompressed order data in kilobytes.
Datetime	The timestamp is displayed in date and time format.
Ready to be signed	Indicates whether the order is already signed by the user or not. False indicates that the order is already signed by the user. True indicates that the order is ready to be signed by the user.
Signatures required	Displays the minimum number of signatures required to authorize the order.
Signatures done	The number of signatures that completed the validation of the order. Indicates the number of electronic signatures already provided and the information about previous signatories. Click the Signer info link to view the details of the signer: • Partner name: name of the trading partner • User ID • Name: name of the signatory • Time stamp • Authorization level: the authorization level of the signatory

Field	Description
Order info link	Click the order info link to view details about the order: • Account: Click the account info link to view the name of the account holder, currency code, account description, the role of the account holder, account number, and the bank code. • Amount: view the amount of the order transaction. • Currency code: view the currency code of the order transaction. • Debit • Execution date: view the date of the execution of the order. • Description: Click the description link to view the description and description type of the signatory.

5. Click **Cancel order**.
6. In the VEU order details window, specify the values for the following parameters:

Field	Description
Order id prefix	Select an alphabet from the drop-down list.
Security medium	Security medium for the user's bank-technical key. Type a four-digit security number in the 0100 – 0499 range.
Bank URL	Select the bank URL from the drop-down list.

7. Click **Submit**.

Updating System Property Values

After configuring EBICS Client, an EBICS Client admin can update the system property values.

About this task

To update system property values:

Procedure

1. Log in to Sterling B2B Integrator EBICS Client.
2. From the **Administration Menu**, select **System Property**.
3. Click **Update** to update the system property values listed in the following table:

Field	Description
Show response code	Every client service returns a response code from the server. If this code is an error code, then the business process returns a fault. If the error code is expected, use an OnFault service to continue interacting with the trading partner.

Field	Description
Connection retries	Specify the number of times the HTTP Client adapter tries to connect to the server. Valid value is any integer 0 - 50. The default value is 3.
Retry delay	Specify the number of seconds the HTTP Client adapter waits between retry attempts. The default value is 60. Valid value is any integer 1 - 7200.
Delay waiting on I/O	Specify the number of seconds to wait for the data transfer to complete before going into WAITING_ON_IO state. If -1 is specified, the service operates in blocking mode. Valid value is any numerical value.
Initialize new HTTP session for each request	If you want to initiate a new HTTP session for each request sent by the EBICS Client to the server, set this parameter to `true`. The default value is `false`. If you upload a large number of large payload (e.g. 200 MB) data to the EBICS Server using the FUL order type, this parameter should be set to `true`.
Persistence segment count	A count of the number of segments after which the run time logs an event. This parameter is valid only for Upload and Download order types. For example, if you set the Persistence segment count to five, after ten segments are uploaded to the server, two transaction data points (fifth and tenth) are persisted in the client database. If the client instance goes down after the twelfth segment is uploaded to the server, the client re-sends the tenth segment of the transaction data. If the server has already received twelve segments of the transaction data, the server notifies the client to re-send from the thirteenth segment.
OrderID generation cache size	Specify the size of the in-memory cache for order ID generation. The default value is 30.
OrderID cache miss thread wait time (in ms)	Specify the duration the thread must wait if the thread experiences a cache miss. The default value is 1000 milliseconds.
OrderID cache miss retry count	Specify the number of times the thread must wait for the cache miss interval. The default value is 5.
Product ID	Enter the product ID for the EBICS Client application.
Product language	Enter the language setting of the EBICS Client application that you are using. For example, enter EN if the language is set to English.
Orders with pending tasks retention period (in days)	Specify the number of days the orders with pending tasks have to be retained in the system without being purged. The default value is 1000.
Check KeyUsage of certificate	Specify whether to check for key usage in certificates. Valid values are: • `true` - Check for key usage. • `false` - Do not check for key usage.
Use modulus and exponent with space for Hash input in Initialization Letter	Specify `true` if the hash for initialization letter has to be calculated using hash input as modulus and exponent with space. Specify `false` if the hash for initialization letter has to be calculated using the entire certificate or public key. The default value is false.

Field	Description
Use modulus and exponent with space for Hash input in Bank key validation	Specify `true` if the hash for bank key validation has to be calculated using hash input as modulus and exponent with space. Specify `false` if the hash bank key validation has to be calculated using the entire certificate or public key. The default value is false.
Mailbox metadata path	Specify the mailbox that stores the OrderMetadata message.
HAC purge interval (in minutes)	Specify the number of minutes between auto-purge operations where EBICS scans the database for expired HAC records and purges them. The default value is `720`. For information about HAC record expiration, see the **Purge expiry** setting in "Creating an HAC Schedule" on page 118.
Cipher strength	Specify the Cipher Strength. Valid values are `Strong`, `All`, and `Weak`.
Client adapter	Specify a client adapter to send requests to trading partners. For example, configure an HTTP Client adapter to send HTTP requests to trading partners.
Raw request	Specify `true` to indicate whether a raw request message is presented to a business process. If not, specify `false`.
Raw response	Specify `true` to indicate whether a raw response is returned by a business process. If not, specify `false`.
Reset connection on error	Specify `Enable` to reset the connection to the server if the client encounters an error when attempting to connect to the server.
Response time out	Specify the number of seconds for the server to respond. The default value is 300. Valid value is any integer 1 - 999999.
Use 'esig' namespace in KeyOrderData xml	Specify `true` if you want to use 'esig' as an additional namespace instead of using 'esig' as the default namespace in KeyOrderData xml. The default value is true.
Insert optional elements in KeyManagement request xml	Specify `true` if you want to insert optional elements specified in the EBICS Key management request schema in the KeyManagement request xml. The default value is true.

4. Click **Finish** to save the changes that you updated.

My Profile

About this task

The My Profile page helps you view the user settings. The settings differ based on the user type.

Procedure

1. Log in to Sterling B2B Integrator EBICS Client.
2. From the **Administration Menu**, **Operator Menu**, or **User Menu**, select **My profile**. The following tables list the settings displayed for different user types.

Table 6. EBICS Client User

User settings	Description
User ID	The user ID is displayed.
User name	The user name is displayed.
User type	The user type is displayed.

Table 6. EBICS Client User (continued)

User settings	Description
Timezone	Timezone for the user is displayed.
Technical user	Indicates whether the user is a technical user or not. The values are: • True • False
Certificate type	The certificate type used by the user to authorize identification and authentication, encryption, and electronic signature certificates is displayed.
Authentication private certificate	The authentication private certificate for the user is displayed.
Authentication public certificate	The authentication public certificate for the user is displayed.
Authentication key version	The authentication key version is displayed.
Encryption private certificate	The encryption private certificate for the user is displayed.
Encryption public certificate	The encryption public certificate for the user is displayed.
Encryption key version	The encryption key version is displayed.
Use hardware key-store for ES	Indicates whether a hardware keystore is used for electronic signature (ES). The values are: • Yes • No
Electronic signature private key	The electronic signature private certificate for the user is displayed.
Electronic signature public key	The electronic signature public certificate for the user is displayed.
Electronic signature key version	The electronic signature key version is displayed.
Associated partner(s)	When you click the **Show all** link, the associated partners information in a tabular format is displayed. You can view the partner name, upload mailbox path, and download mailbox path.
Associated partner(s) with Banks	When you click the **Show all** link, the partners associated with the bank, the partner name, bank ID, and status are displayed. If an EBICS Client user is in Initialized or Ready state, then an INI or HIA letter can also be generated. If the EBICS Client user has permission to submit the SPR order type, then an icon to submit the SPR order type is displayed. Click the icon to suspend the current user at the bank.

Table 7. EBICS Client Super Admin, EBICS Client Admin, or EBICS Client Operator

User settings	Description
User ID	The user ID is displayed.
User name	The user name is displayed.
User type	The user type is displayed.

Table 7. EBICS Client Super Admin, EBICS Client Admin, or EBICS Client Operator (continued)

User settings	Description
Timezone	Timezone for the user is displayed.

Importing and Exporting EBICS Client Resources

You can import resources and export configuration data for resources pertaining to EBICS Client using Sterling B2B Integrator.

For example, you can export configuration data for bank profile, user profile, file formats, offer, and user permission in an XML format and store it on the system. You can import configuration data for bank profile, user profile, file formats, offer, and user permission in an XML format. For more information about managing resources, see *Resource Management* in the Sterling B2B Integrator information center.

When you select to export user permission or offer, all the dependant resource types (for example, the bank and the user profiles) are also exported. During import, ensure that you select each dependant resource type that is displayed in a separate page. For example, if you selected to import user permission, ensure that you select the associated user profiles.

Note: If you are exporting a bank profile with a default URL and the bank profile exists in the target system, but is associated with a different default URL, then the bank profile will have multiple default URLs after the import. To retain a single default URL, log in to EBICS Client application dashboard and edit the bank configuration settings. Else, the EBICS Client run time uses the first default URL fetched from the database to perform transactions.

Note: In EBICS Client, a bank can have only one offer. If a target system has an offer with a primary key same as the one in the export XML, and if the **Resources to be updated** option is set to `Yes`, then the offer in the target system is updated with the order types associated with the offer in the export XML. However, if the primary key of the offer in the target system is different from the one in the export XML, then the offer and associated order types in the target system are replaced with the offer and associated order types in the export XML.

Export EBICS Client Resources

You can use the Resource Manager in Sterling B2B Integrator to export EBICS Client resources.

About this task

To export EBICS Client resources:

Procedure

1. Log in to Sterling B2B Integrator.
2. From the **Administration Menu**, select **Deployment** > **Resource Manager** > **Import/Export**.
3. Next to **Export Resources**, click **Go**.
4. In the Output Format Type page,

a. Select the format type your data will be exported to:
   - **XML Document** (.xml)
   - **Installation Bundle** (.jar)

b. Click **Next**.

5. In the Resource Group page, choose whether to export resources based on a tag name.
   - Select **No** to indicate that you do not want to export resources based on a tag name.
   - Select **Yes** to export an entire resource group based on a tag name. Choose the tag name from the dropdown list.

   Click**Next**.
6. In the Export Type page, select **Standard - exports default version** and click **Next**.
7. In the Select Resources page, select **EBICS Client Resource(s)** and click **Next**.
8. In the Select EBICS Client Resource(s) page, select the resources you want to export:

Option	Description
File Format	Information about the file formats.
Bank Offer	Information about the offer that includes details of the bank profile and file formats associated with the offer.
User Permission	Information about the user, the trading partner (identity record), the details of the bank profile, the offer, the order types, and file formats associated with the offer.
Bank Profile	Information about the bank and the trusted certificates associated with the bank.
User Profile	Information about the user, the partner, associated data such as, mailbox permissions, identity records, trusted, and system certificates.

   Click **Next**.
9. In the page for each resource type selected, move the items to be exported from the **Available** list to the **To Be Exported** list.
   a. Optional. Filter the data using **Filter Data**.
   b. In the **Export Dependent Records** field, select **Yes** to export information configured for EBICS Client in Sterling B2B Integrator. For example, details of mailbox configuration, digital certificates, identity records, etc. Otherwise, select **No**.
   c. Click **Next**.

   Repeat as needed for each additional resource types page.
10. In the Security page, enter and confirm the system passphrase and click **Next**.
11. In the Confirm page, review the information for the resources to be exported and click **Finish**. The export file is created.
12. In the Finish page, select one of the following:
    - Click the icon next to **View Export Report** to review the export report.
    - Click the **Download** icon next to **Export data (.xml)** or **Export data (.jar)** to download the export file and save it to a hard disk.

13. Click **Return**.

Import EBICS Client Resources

You can use the Resource Manager in Sterling B2B Integrator to import EBICS Client resources.

About this task

To import EBICS Client resources:

Procedure

1. Log in to Sterling B2B Integrator.
2. From the **Administration Menu**, select **Deployment** > **Resource Manager** > **Import/Export**.
3. Next to **Import Resources**, click **Go**.
4. In the Import File page, specify the values for the fields listed in the following table and click **Next**.

Field	Description
File Name	Required. Click **Browse** to locate and select the file to import. The file must be an XML document (.xml) or an installation bundle (.jar).
Passphrase	Optional. Specify a passphrase for the file when prompted.
Skip Backup Generation	Optional. Under **Tuning Options**, if you do *not* want to generate a backup of the updated entities, select the check box.
Import All Resources	Optional. Under **Tuning Options**, if you want to import all the resources, select the check box. For example, permissions associated with the mailbox, identity records, private key certificates are automatically imported. If you do not select this option, you are prompted to select entries to import for each resource type.

5. In the Create Resource Tag page,
   a. This step is optional. If you want to associate the imported data with a resource group, then enter a **Tag Name** and a **Tag Description**.
   b. Click **Next**.
6. In the Update Objects page,
   - Select **Yes** to update the objects that exist in the system.
   - Select **No** to import objects that do not exist on the system.

   Click **Next**.
7. This step may not be applicable for all imports. For each resource type selected, move the items to be imported from the **Available** list to the **To Be Imported** list. Click **Next**.
8. In the Confirm page, review the information for the resources to be imported and click **Finish**. The data is imported.
9. In the Finish page, you can perform the following actions:
   - Click **View Import Report** to review the import report.

- Click **View Performance Report** to review the summary data in the performance report.
- Click **Download** next to **Data in Sterling B2B Integrator before Import (xml)** to get a backed up copy of the data.

  Note: If you selected the Skip Backup Generation option, the Download link is *not* displayed.

10. Click **Return**.

Permissions to Access EBICS Client User Interface

To access Sterling B2B Integrator EBICS Client Graphical User Interface (GUI) and its functions, you must be assigned to one of the following permissions groups:

- EBICSClient Admin
- EBICSClient Operator
- EBICSClient Users

The following table lists the Sterling B2B Integrator EBICS Client menu items and the permissions required to access the pages associated with each group:

Note:
Access to a menu item allows access to the full functionality of the associated page, with the delete function limited to users with administrator permissions.

Table 8. Sterling B2B Integrator EBICS Client menu items and permissions

Menu items	Permissions	EBICSClient		
		Admin	Operator	Users
Profile management > User	**CREATE**	Yes	No	No
	EDIT	Yes	No	No
	VIEW	Yes	Yes	No
	DELETE	Yes	No	No
Profile management > Bank > Profile	**CREATE**	Yes	No	No
	EDIT	Yes	No	No
	VIEW	Yes	Yes	No
	DELETE	Yes	No	No
Profile management > Bank > Offer configurations	**CREATE**	Yes	No	No
	EDIT	Yes	No	No
	VIEW	Yes	Yes	No
	DELETE	Yes	No	No
Profile management > Bank > Bank key validations	**VALIDATE**	Yes	No	No

Table 8. Sterling B2B Integrator EBICS Client menu items and permissions (continued)

Menu items	Permissions	EBICSClient		
		Admin	Operator	Users
Profile management > File formats	**CREATE**	Yes	No	No
	EDIT	Yes	No	No
	VIEW	Yes	Yes	No
	DELETE	Yes	No	No
Profile management > Keys	**CREATE**	Yes	No	No
	EDIT	Yes	No	No
	VIEW	Yes	Yes	No
	DELETE	Yes	No	No
Permissions > User permissions	**CREATE**	Yes	No	No
	EDIT	Yes	No	No
	VIEW	Yes	Yes	No
	DELETE	Yes	No	No
Order submission	**SUBMISSION**	No	No	Yes
Viewers > Event Viewer	**SEARCH**	Yes	Yes	Yes
Viewers > Order search	**SEARCH**	Yes	Yes	Yes
Viewers > Pending tasks	**VIEW**	No	No	Yes
	SIGN	No	No	Yes
Viewers > Pending VEU tasks	**VIEW**	No	No	Yes
	SIGN	No	No	Yes
	SUBMIT	No	No	Yes
Note: The Pending VEU tasks page is displayed only after submitting HVU and HVZ order types from the Order submission menu.				
System Property	**VIEW**	Yes	No	No
	UPDATE	Yes	No	No
My profile	**VIEW**	Yes	Yes	Yes

Recover upload and download transactions

When sending or receiving transaction data, if the client is down, there is a risk of losing the transaction data. To prevent loss of and to restore transaction data, EBICS Client supports transaction recovery for upload and download transactions.

Transaction recovery for upload transactions

The following example scenario illustrates transaction recovery mechanism for an upload transaction using the FUL order type:

1. Twenty segments of transaction data are uploaded to the server.
2. After ten segments are successfully uploaded, the client instance goes down.
3. Once the client instance is restored, the client re-sends the transaction data from the point it was down. In this example, the client re-sends the eleventh segment of the transaction data.

If the segment received from the client after recovery is not synchronized with the existing segment at the server, the server returns the EBICS_TX_RECOVERY_SYNC event name. The event name EBICS_TX_RECOVERY_SYNC indicates that the server is synchronizing the segments in the transaction with the client. In the Timestamp column of the Event Viewer, you can view the difference in the timestamps of the segments that are uploaded before and after the transactions are recovered.

Persisting segment count

You can update the Persistence segment count system property value from the Administration menu of EBICS Client to persist the transaction data points in the client database. For example, if you set the Persistence segment count to five, after ten segments are uploaded to the server, two transaction data points (fifth and tenth) are persisted in the client database.

If the client instance goes down after the twelfth segment is uploaded to the server, the client re-sends the tenth segment of the transaction data. If the server has already received twelve segments of the transaction data, the server notifies the client to re-send from the thirteenth segment.

Transaction recovery for download transactions

The following example scenario illustrates transaction recovery for a download transaction using the FDL order type:

1. Ten segments of transaction data are downloaded from the server.
2. The client instance goes down after the sixth segment is downloaded and persisted in the database.
3. Once the client instance is restored, the client sends a request to the server for the seventh segment.

The following example scenario illustrates transaction recovery for a download transaction using the FDL order type, when the client instance goes down during downloading of a segment:

1. Ten segments of transaction data are downloaded from the server.
2. The client instance goes down when the sixth segment is in the process of downloading from the server.

3. Once the client instance is restored, the client re-sends a request to the server for the sixth segment.

Submit and sign an FUL order type

The following example scenario demonstrates submitting and signing, or rejecting, an FUL order type where the submitter and signer are two separate entities. If the Electronic Signature (ES) value is set to 1, then a single signature of E or A authorization level is sufficient to process an order.

Before you begin

In this example scenario, the following entities are used:

- Submitter is EBICS user USERSUBMIT
- Signatory is EBICS user USERSIGN
- Bank name is BANK
- Offer name is OFFER
- Partner name is PARTNER

Attention: If you upload a large number of large payload (e.g. 200 MB) data to the EBICS Server using the FUL order type, the **`Initialize new HTTP session for each request`** parameter in the EBICS Client system properties should be set to `true`. To modify system properties, see "Updating System Property Values" on page 68.

About this task

To submit an FUL order type, when ES=1, complete the following steps using the Sterling B2B Integrator EBICS Client user interface:

Procedure

1. Configure USERSUBMIT and USERSIGN as EBICS Client users. For information about configuring an existing user as an EBICS client user, see *Configure an Existing User as EBICS Client User*.
2. Configure a bank profile for BANK. For information about configuring a bank profile, see *Create a Bank Profile*.
3. Configure an offer for OFFER. For information about configuring an offer, see *Create an Offer*.
4. Configure user permission for OFFER. For information about user permission, see *Create User Permission*.
5. Log in to Sterling B2B Integrator EBICS Client as an admin.
6. From the **Permissions** menu, select **User permissions**.
7. In the User Permission Configuration page, in the **Offer name** field, under **Search**, enter the offer name, OFFER, for which the user permission is configured.
8. Click **GO**.
9. Click the update icon adjacent to the user permission you want to edit. The offer name of the user permission is OFFER and the associated bank ID is BANK.
10. In the Update: Permission Information page, click the update icon adjacent to any FUL file format, for example, pain.001.001.02.ict.
11. In the Add permission page, specify 1 in the **No of signatures required** field.

12. Click **Add Signatories**.
13. In the Add signatory page, select USERSIGN from the **User ID** drop-down list. Select Signer as the **Permission type**.
14. Click **Save**.
15. Log in to Sterling B2B Integrator EBICS Client as an USERSUBMIT.
16. Generate the INI and HIA letters using the EBICS Client dashboard user interface, or use the H3K order type. For information about sending public keys to the bank through INI and HIA, or H3K, see *Initializing a User*.
17. Manually sign and mail the INI and HIA letters to BANK. Not applicable for H3K.
18. Initialize users using one of the following methods:
    - Submit an H3K order.
    - Use INI and HIA together.

      Submit INI and HIA orders.

      Generate and sign initialization letters of INI and HIA. Mail the signed letters to the bank.

    For more information, see "Initializing a User" on page 41.
19. After successful verification, BANK changes the status of the user, USERSUBMIT, from New to Ready, indicating that USERSUBMIT can now transact with the bank.
20. Using the HPB order type, download the public certificates of BANK.
21. Repeat steps 15 to 19 for USERSIGN.
22. Log in to Sterling B2B Integrator EBICS Client as an admin.
23. Validate the hash value of the certificates received from the bank. For information about validating bank certificates, see *Validate a Bank Key*. After successful validation of the bank keys, the status of the bank changes to Activated.
24. Log in to Sterling B2B Integrator EBICS Client as an USERSUBMIT.
25. From the **User Menu**, select **Order submission**.
26. In the Order Information page, specify the following values and click **Next**.
    - Select PARTNER as the Partner ID
    - Select BANK as the Bank ID(Host ID)
    - Select Bank technical orders as the Order type filter
    - Select FUL as the Order type
27. Specify the values for the fields according to the instructions in the following table and click **Send**:

Field	Description
Order ID prefix	Optional. From the drop-down list, select the order ID prefix, for example F. EBICS Client allocates a unique order ID to each order based on the bank, user ID, and the order type. The client generates the order ID as per EBICS specifications. The order ID is a 4-digit alphanumeric ID. You can specify the first character of the order ID. The second, third, and fourth characters of the order ID are alphanumeric in an ascending order (A-Z or 0-9).

Field	Description
Security medium	Required. Type a 4-digit security number in 0100 to 0499 range. For example, 0200.
Autosubmit	Optional. Applicable for FUL order type only. Select the check box. If the autosubmit option is selected, then an order is automatically submitted after the required number of signatures are obtained. If the autosubmit option is not selected, then an EBICS Client user has to log in to the EBICS Client dashboard interface, navigate to the pending tasks screen, and submit the order after the required number of signatures are obtained.
Read file from mailbox	To upload the payload file from the mailbox, select **Yes**. To upload the payload file from a file location, select **No**.
Upload file	Click **Browse** next to Upload file, navigate to the file location and select the file that is to be uploaded to the EBICS server.
File format	Select pain.001.001.02.ict from the drop-down list.

An order submission confirmation message is displayed.

28. To sign the order, log in to Sterling B2B Integrator EBICS Client as an USERSIGN.
29. From the **Viewers** menu, select **Pending tasks**. The FUL order submitted by USERSUBMIT is listed as a pending task. For information about pending tasks, see *Pending Tasks*. If the order contains any custom attributes, they will be visible on this screen. For information about custom attributes, see *Submit an order as a technical user*.
30. Click **Sign** to sign the pending FUL order, or click **Reject** to reject the order. If any signatory rejects the order before the required number of signatories is met, the order is no longer listed as a pending task to any of the signatories, and it should not be processed further.
31. When submitting the FUL order, if you had not enabled the autosubmit option, then log in to EBICS Client as USERSUBMIT, navigate to the pending tasks screen, and submit the FUL order that is signed by USERSIGN.

What to do next

To view the status (Success, Failed, In Progress, or Pending at Client) of the submitted order in the EBICS Client user interface, from the **Viewers** menu, select **Order Search** and provide the appropriate search criteria to locate the order.

Order types

A brief description of the order type, definition of the parameters defined for the order type, and the sample XML schema are provided for the following order types.

FUL order type

FUL is a standard order type for submitting the files to the bank. Using this order type ensures a transparent transfer of files of any format.

Access

Mailbox

Description

A user initiates a upload transaction with the bank by submitting a upload (FUL) order request. FUL order type is a bank-technical download order type.

Attention: If you upload a large number of large payload (e.g. 200 MB) data to the EBICS Server using the FUL order type, the **`Initialize new HTTP session for each request`** parameter in the EBICS Client system properties should be set to `true`. To modify system properties, see "Updating System Property Values" on page 68.

Parameters

Table 9. FUL parameters

Parameter	Description and value
HostID	The bank ID or the host ID of the bank to which the EBICS Client user submitted the order. It is a unique ID for the bank in the bank's system.
HostUrlAlias	When configuring a bank profile, you can specify multiple host URLs and set one host URL as the default. If you want to send a request to a host URL that is not the default URL, then, specify a value for this parameter.
PartnerID	The partner ID associated with the user ID.
UserID	Unique ID of the user in the bank's system, which corresponds to the user created in the EBICS Client dashboard.
SystemID	User ID of the technical user. A technical user is a delegate of the non-technical or human user.
orderIdPrefix	EBICS Client allocates a unique order ID to each order based on the bank, user ID, and the order type. The client generates the order ID according to EBICS specifications. The order ID is a 4-digit alphanumeric ID. You can specify the first character of the order ID. The second, third, and fourth characters of the order ID are alphanumeric in an ascending order (A-Z or 0-9). This parameter is used with EBICS protocol version H003 only.
SecurityMedium	A 4-digit security number in the 0000 to 0499 range.

Table 9. FUL parameters (continued)

Parameter	Description and value
OrderType	The order type of the order you are submitting. In this case, FUL is the order type.
FileFormat	The file format associated with the order type. An order type can have zero or more file formats. The file formats for FUL and FDL order types are based on the SWIFTNet request type.
autoSubmit	This parameter is applicable only for FUL order type. If this parameter is set to true, then an order is automatically submitted after the required number of signatures are obtained. If this parameter is set to false, then an EBICS Client user has to log in to the EBICS Client dashboard interface, navigate to the pending tasks screen, and submit the order after the required number of signatures are obtained.

XML schema

```
<?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>
```

Parameter List

The *EBICS - Implementation Guide in France* recommends that a test of the file transfer is necessary before transferring the actual files to the bank. Therefore, the customer workstation must have a set-up that allows transfer of files in a test as well as a production environment. To distinguish the test files from the production files, the parameter name TEST is included in the OrderParams tag for FUL and FDL order types. The OrderParams tag can be set in the orderMetaData XML. Similarly, the bank and the EBICS client can share a list of parameters and corresponding values based on a mutual understanding of the parameters defined in the contractual agreement.

The following example illustrates a scenario wherein test files are transferred and therefore the value of TEST is set to 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>
```

FDL order type

FDL is a standard order type for file downloads. Using this order type ensures a transparent transfer of files of any format.

Access

Mailbox

Description

FDL order type is a bank-technical download order type. A user initiates a download transaction with the bank by submitting a download (FDL) order request.

Parameters

Table 10. FDL parameters

Parameter	Description and value
HostID	The bank ID or the host ID of the bank to which the EBICS Client user submitted the order. It is a unique ID for the bank in the bank's system.
HostUrlAlias	When configuring a bank profile, you can specify multiple host URLs and set one host URL as the default. If you want to send a request to a host URL that is not the default URL, then, specify a value for this parameter.
PartnerID	The partner ID associated with the user ID.
UserID	Unique ID of the user in the bank's system, which corresponds to the user created in the EBICS Client dashboard.
SystemID	User ID of the technical user. A technical user is a delegate of the non-technical or human user.
orderIdPrefix	EBICS Client allocates a unique order ID to each order based on the bank, user ID, and the order type. The client generates the order ID as per EBICS specifications. The order ID is a 4-digit alphanumeric ID. You can specify the first character of the order ID. The second, third, and fourth characters of the order ID are alphanumeric in an ascending order (A-Z or 0-9). This parameter is used with EBICS protocol version H003 only.

Table 10. FDL parameters (continued)

Parameter	Description and value
SecurityMedium	A 4-digit security number in the 0000 to 0499 range.
OrderType	The order type of the order you are submitting. In this case, FDL is the order type.
FileFormat	The file format associated with the order type. An order type can have zero or more file formats. The file formats for FUL and FDL order types are based on the SWIFTNet request type.
DownloadDateRangeStart	The start date of the download of order data. This parameter is applicable only for FDL order type.
DownloadDateRangeEnd	The end date of the download of order data. This parameter is applicable only for FDL order type.

XML schema

```
<?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>
```

Parameter List

The *EBICS - Implementation Guide in France* recommends that a test of the file transfer is necessary before transferring the actual files to the bank. Therefore, the customer workstation must have a set-up that allows transfer of files in a test as well as a production environment. To distinguish the test files from the production files, the parameter name TEST is included in the OrderParams tag for FUL and FDL order types. The OrderParams tag can be set in the orderMetaData XML. Similarly, the bank and the EBICS client can share a list of parameters and corresponding values based on a mutual understanding of the parameters defined in the contractual agreement.

The following example illustrates a scenario wherein test files are transferred and therefore the value of TEST is set to 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>
```

INI order type

EBICS Client user shares the public keys for Electronic Signature with the bank through the INI (Initialization) order type.

Access

Mailbox

Description

INI is an upload key management order type. INI is used in subscriber initialization. Use INI to send the bank-technical public certificate of a customer to the bank. The order data is compressed and base64-encoded.

Self-signed certificates cannot be used for electronic signatures and consequently for user initialization (INI order type). An EBICS Client user using self-signed certificates for identification and authentication and encryption, has to use CA certificates for electronic signatures.

Parameters

Table 11. INI parameters

Parameter	Description and value
HostID	The bank ID or the host ID of the bank to which the EBICS Client user submitted the order. It is a unique ID for the bank in the bank's system.
HostUrlAlias	When configuring a bank profile, you can specify multiple host URLs and set one host URL as the default. If you want to send a request to a host URL that is not the default URL, then, specify a value for this parameter.
PartnerID	The partner ID associated with the user ID.
UserID	Unique ID of the user in the bank's system, which corresponds to the user created in the EBICS Client dashboard.
SystemID	User ID of the technical user. The INI order type can be submitted by a technical user who is a delegate of the non-techncial or human user. Hence, the value of the UserID is the same as the value of the systemID.

Table 11. INI parameters (continued)

Parameter	Description and value
orderIdPrefix	EBICS Client allocates a unique order ID to each order based on the bank, user ID, and the order type. The client generates the order ID as per EBICS specifications. The order ID is a 4-digit alphanumeric ID. You can specify the first character of the order ID. The second, third, and fourth characters of the order ID are alphanumeric in an ascending order (A-Z or 0-9). This parameter is used with EBICS protocol version H003 only.
SecurityMedium	A 4-digit security number in the 0100 to 0499 range. The value cannot be changed for INI, HIA, and HPB order types.
OrderType	The order type of the order you are submitting. In this case, INI is the order type.

XML schema

```
<?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>S</orderIdPrefix>
  <SecurityMedium>0200</SecurityMedium>
  <OrderType>INI</OrderType>
</orderMetaData>
```

HIA order type

EBICS Client user shares the public keys for identification and authentication and encryption with the bank through the HIA order type.

Access

Mailbox

Description

HIA is an upload key management order type. HIA is used to transmit user public certificates for identification and authentication, and encryption to enable the user to initiate transactions with the bank. The order data is compressed and base64-encoded.

Parameters

Table 12. HIA parameters

Parameter	Description and value
HostID	The bank ID or the host ID of the bank to which the EBICS Client user submitted the order. It is a unique ID for the bank in the bank's system.
HostUrlAlias	When configuring a bank profile, you can specify multiple host URLs and set one host URL as the default. If you want to send a request to a host URL that is not the default URL, then, specify a value for this parameter.
PartnerID	The partner ID associated with the user ID.
UserID	Unique ID of the user in the bank's system, which corresponds to the user created in the EBICS Client dashboard.
SystemID	User ID of the technical user. The HIA order type can be submitted by a technical user who is a delegate of the non-techncial or human user. Hence, the value of the UserID is the same as the value of the systemID.
orderIdPrefix	EBICS Client allocates a unique order ID to each order based on the bank, user ID, and the order type. The client generates the order ID as per EBICS specifications. The order ID is a 4-digit alphanumeric ID. You can specify the first character of the order ID. The second, third, and fourth characters of the order ID are alphanumeric in an ascending order (A-Z or 0-9). This parameter is used with EBICS protocol version H003 only.
SecurityMedium	A 4-digit security number in the 0100 to 0499 range. The value cannot be changed for INI, HIA, and HPB order types.
OrderType	The order type of the order you are submitting. In this case, HIA is the order type.

XML schema

```
<?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>
```

H3K order type

You can use the H3K order type to share the public certificates for Electronic Signature, identification and authentication, and encryption with the bank.

Access

Mailbox

Description

H3K is an upload key management order type. H3K is used to transmit user public certificates for Electronic Signature, identification and authentication, and encryption to enable the user to initiate transactions with the bank.

Parameters

Table 13. H3K parameters

Parameter	Description and value
HostID	The bank ID or the host ID of the bank to which the EBICS Client user submitted the order. It is a unique ID for the bank in the bank's system.
HostUrlAlias	When configuring a bank profile, you can specify multiple host URLs and set one host URL as the default. If you want to send a request to a host URL that is not the default URL, then, specify a value for this parameter.
PartnerID	The partner ID associated with the user ID.
UserID	Unique ID of the user in the bank's system, which corresponds to the user created in the EBICS Client dashboard.
SystemID	User ID of the technical user. The H3K order type can be submitted by a technical user who is a delegate of the non-techncial or human user. Hence, the value of the UserID is the same as the value of the SystemID.
SecurityMedium	A 4-digit security number in the 0000 to 0499 range.
OrderType	The order type of the order you are submitting. In this case, H3K is the order type.

XML schema

```
<?xml version="1.0" encoding="UTF-8"?>
<orderMetaData xmlns:ns2="partnerInfo">
  <HostID>SUBNKPK12</HostID>
  <HostUrlAlias>SUBNKPK12_URL_ALIAS</HostUrlAlias>
  <PartnerID>SUPKID</PartnerID>
  <UserID>TECHUSER</UserID>
  <SystemID>TECHUSER</SystemID>
  <SecurityMedium>0200</SecurityMedium>
  <OrderType>H3K</OrderType>
</orderMetaData>
```

HPB order type

Using the HPB order type, the EBICS Client user downloads the public certificates of the bank.

Access

Mailbox

Description

HPB is a download key management order type. The user submits an HPB order request to download the public certificates of the bank. After successful validation of the user's authentication and identification keys, the bank sends an HPB response. The HPB response contains the public bank keys. The user validates the bank keys against the internally generated hash values. After successful validation, the status of the bank changes to Activated, indicating that the partner and its associated users can now transact with the bank.

The order data is compressed, encrypted, and base64-encoded. The response message and the order data are not signed.

Parameters

Table 14. HPB parameters

Parameter	Description and value
HostID	The bank ID or the host ID of the bank to which the EBICS Client user submitted the order. It is a unique ID for the bank in the bank's system.
HostUrlAlias	When configuring a bank profile, you can specify multiple host URLs and set one host URL as the default. If you want to send a request to a host URL that is not the default URL, then, specify a value for this parameter.
PartnerID	The partner ID associated with the user ID.
UserID	Unique ID of the user in the bank's system, which corresponds to the user created in the EBICS Client dashboard.
SystemID	User ID of the technical user. A technical user is a delegate of the non-technical or human user.
orderIdPrefix	EBICS Client allocates a unique order ID to each order based on the bank, user ID, and the order type. The client generates the order ID as per EBICS specifications. The order ID is a 4-digit alphanumeric ID. You can specify the first character of the order ID. The second, third, and fourth characters of the order ID are alphanumeric in an ascending order (A-Z or 0-9). This parameter is used with EBICS protocol version H003 only.

Table 14. HPB parameters (continued)

Parameter	Description and value
SecurityMedium	A 4-digit security number in the 0100 to 0499 range. The value cannot be changed for INI, HIA, and HPB order types. The security medium for the subscriber's bank-technical key is set to 0000 since HPB orders neither require electronic signatures nor transmit bank-technical subscriber keys.
OrderType	The order type of the order you are submitting. In this case, HPB is the order type.

XML schema

```
<?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>
```

HKD order type

Using the HKD order type, the user can download customer data and subscriber data.

Access

Mailbox

Description

HKD is a download key management order type. Use the HKD order type to download information about a partner and associated subscribers stored by the bank, including information about your own company. The order data is compressed and base64-encoded.

Parameters

Table 15. HKD parameters

Parameter	Description and value
HostID	The bank ID or the host ID of the bank to which the EBICS Client user submitted the order. It is a unique ID for the bank in the bank's system.
HostUrlAlias	When configuring a bank profile, you can specify multiple host URLs and set one host URL as the default. If you want to send a request to a host URL that is not the default URL, then, specify a value for this parameter.

Table 15. HKD parameters (continued)

Parameter	Description and value
PartnerID	The partner ID associated with the user ID.
UserID	Unique ID of the user in the bank's system, which corresponds to the user created in the EBICS Client dashboard.
SystemID	User ID of the technical user. A technical user is a delegate of the non-technical or human user.
orderIdPrefix	EBICS Client allocates a unique order ID to each order based on the bank, user ID, and the order type. The client generates the order ID as per EBICS specifications. The order ID is a 4-digit alphanumeric ID. You can specify the first character of the order ID. The second, third, and fourth characters of the order ID are alphanumeric in an ascending order (A-Z or 0-9). This parameter is used with EBICS protocol version H003 only.
SecurityMedium	A 4-digit security number in the 0000 to 0499 range.
OrderType	The order type of the order you are submitting. In this case, HKD is the order type.

XML schema

```
<?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>
```

HTD order type

Using the HTD order type, the user can download customer data and subscriber data.

Access

Mailbox

Description

HTD is a download key management order type. Using HTD, the subscriber can retrieve information stored by the bank relating to their company or themselves. However, unlike HKD, the subscriber cannot retrieve information about the company’s other subscribers. The order data is compressed and base64-encoded.

Parameters

Table 16. HTD parameters

Parameter	Description and value
HostID	The bank ID or the host ID of the bank to which the EBICS Client user submitted the order. It is a unique ID for the bank in the bank's system.
HostUrlAlias	When configuring a bank profile, you can specify multiple host URLs and set one host URL as the default. If you want to send a request to a host URL that is not the default URL, then, specify a value for this parameter.
PartnerID	The partner ID associated with the user ID.
UserID	Unique ID of the user in the bank's system, which corresponds to the user created in the EBICS Client dashboard.
SystemID	User ID of the technical user. A technical user is a delegate of the non-technical or human user.
orderIdPrefix	EBICS Client allocates a unique order ID to each order based on the bank, user ID, and the order type. The client generates the order ID as per EBICS specifications. The order ID is a 4-digit alphanumeric ID. You can specify the first character of the order ID. The second, third, and fourth characters of the order ID are alphanumeric in an ascending order (A-Z or 0-9). This parameter is used with EBICS protocol version H003 only.
SecurityMedium	A 4-digit security number in the 0000 to 0499 range.
OrderType	The order type of the order you are submitting. In this case, HTD is the order type.

XML schema

```
<?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>
```

HEV order type

Using the HEV order type, the user can download the EBICS versions supported by the bank.

Access

Mailbox

Description

HEV is a download key management order type. By submitting an HEV request, the user requests the bank to provide a list of EBICS versions supported by the bank. The bank provides a response that contains a list of supported EBICS versions and the version of the relevant schema.

Parameters

Table 17. HEV parameters

Parameter	Description and value
HostID	The bank ID or the host ID of the bank to which the EBICS Client user submitted the order. It is a unique ID for the bank in the bank's system.
HostUrlAlias	When configuring a bank profile, you can specify multiple host URLs and set one host URL as the default. If you want to send a request to a host URL that is not the default URL, then, specify a value for this parameter.
PartnerID	The partner ID associated with the user ID.
UserID	Unique ID of the user in the bank's system, which corresponds to the user created in the EBICS Client dashboard.
SystemID	User ID of the technical user. A technical user is a delegate of the non-technical or human user.
OrderType	The order type of the order you are submitting. In this case, HEV is the order type.

XML schema

```
<?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>
```

PUB order type

Use PUB order type to send public key for signature verification.

Access

Mailbox

Description

PUB is an upload key management order type used to update customer's certificate and send the bank-technical public certificate to the bank. The order data is signed, compressed, encrypted, and base64-encoded.

Parameters

Table 18. PUB parameters

Parameter	Description and value
HostID	The bank ID or the host ID of the bank to which the EBICS Client user submitted the order. It is a unique ID for the bank in the bank's system.
HostUrlAlias	When configuring a bank profile, you can specify multiple host URLs and set one host URL as the default. If you want to send a request to a host URL that is not the default URL, then, specify a value for this parameter.
PartnerID	The partner ID associated with the user ID.
UserID	Unique ID of the user in the bank's system, which corresponds to the user created in the EBICS Client dashboard.
SystemID	User ID of the technical user. The PUB order type can be submitted by a technical user who is a delegate of the non-techncial or human user. Hence, the value of the UserID is the same as the value of the systemID.
orderIdPrefix	EBICS Client allocates a unique order ID to each order based on the bank, user ID, and the order type. The client generates the order ID as per EBICS specifications. The order ID is a 4-digit alphanumeric ID. You can specify the first character of the order ID. The second, third, and fourth characters of the order ID are alphanumeric in an ascending order (A-Z or 0-9). This parameter is used with EBICS protocol version H003 only.
SecurityMedium	A 4-digit security number in the 0000 to 0499 range. The value cannot be changed for INI, HIA, and HPB order types. The security medium for the subscriber’s bank-technical key is set to 0000 since HPB orders neither require electronic signatures nor transmit bank-technical subscriber keys.
OrderType	The order type of the order you are submitting. In this case, PUB is the order type.
UserSignNewPubKeyAlias	The alias of the public key of the new Electronic Signature (ES) certificate to be updated for the user.

Table 18. PUB parameters (continued)

Parameter	Description and value
UserSignNewPubKeyID	The ID of the new Electronic Signature (ES) public certificate to be updated for the user.
UserSignNewPriKeyAlias	The alias of the private key of the new Electronic Signature (ES) certificate to be updated for the user. Set this parameter if you are not using a hardware key for Electronic Signature. The bank must have the public part of the key to validate the authorization.
UserSignNewPriKeyID	The ID of the new Electronic Signature (ES) private certificate to be updated for the user. Set this parameter if you are not using a hardware key for Electronic Signature.
UserNewSignatureVersion	The key version of the new electronic signature to be updated for the user. The valid values are A005 or A006. If you are using a hardware key store for electronic signature, then the key version is set to A005 and cannot be changed.

XML schema

```
<?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>
```

HCS order type

Use HCS order type to amend of the subscriber keys for Electronic Signature, identification and authentication, and encryption.

Access

Mailbox

Description

HCS is an upload key management order type. HCS is introduced to allow modification of all the three keys in a single transaction. The three keys include bank-technical electronic signature (PUB), identification and authentication signature and encryption (HCA). Therefore, order type HCS comprises PUB and HCA. The order types PUB and HCA can be used as alternatives to HCS.

Parameters

Table 19. HCS parameters

Parameter	Description and value
HostID	The bank ID or the host ID of the bank to which the EBICS Client user submitted the order. It is a unique ID for the bank in the bank's system.
HostUrlAlias	When configuring a bank profile, you can specify multiple host URLs and set one host URL as the default. If you want to send a request to a host URL that is not the default URL, then, specify a value for this parameter.
PartnerID	The partner ID associated with the user ID.
UserID	Unique ID of the user in the bank's system, which corresponds to the user created in the EBICS Client dashboard.
SystemID	User ID of the technical user. The HCS order type can be submitted by a technical user who is a delegate of the non-techncial or human user. Hence, the value of the UserID is the same as the value of the systemID.
orderIdPrefix	EBICS Client allocates a unique order ID to each order based on the bank, user ID, and the order type. The client generates the order ID as per EBICS specifications. The order ID is a 4-digit alphanumeric ID. You can specify the first character of the order ID. The second, third, and fourth characters of the order ID are alphanumeric in an ascending order (A-Z or 0-9). This parameter is used with EBICS protocol version H003 only.
SecurityMedium	A 4-digit security number in the 0000 to 0499 range. The value cannot be changed for INI, HIA, and HPB order types. The security medium for the subscriber's bank-technical key is set to 0000 since HPB orders neither require electronic signatures nor transmit bank-technical subscriber keys.
OrderType	The order type of the order you are submitting. In this case, HCS is the order type.
UserSignNewPubKeyAlias	The alias of the public key of the new Electronic Signature (ES) certificate to be updated for the user.
UserSignNewPubKeyID	The ID of the new Electronic Signature (ES) public certificate to be updated for the user.

Table 19. HCS parameters (continued)

Parameter	Description and value
UserSignNewPriKeyAlias	The alias of the private key of the new Electronic Signature (ES) certificate to be updated for the user. Set this parameter if you are not using a hardware key for Electronic Signature. The bank must have the public part of the key to validate the authorization.
UserSignNewPriKeyID	The ID of the new Electronic Signature (ES) private certificate to be updated for the user. Set this parameter if you are not using a hardware key for Electronic Signature.
UserAuthNewPubKeyAlias	The alias of the new authentication public certificate to be updated for the user. The public key provided by the user to the bank to validate the authorization of the user in the request from the EBICS Client. The trading partner or user shares the key with the bank.
UserAuthNewPubKeyID	The ID of the new authentication public certificate to be updated for the user.
UserAuthNewPriKeyAlias	The alias of the new authentication private certificate to be updated for the user. The private key used by EBICS Client to create a digital signature for the user in the request sent to the bank. The bank must have the public part of the key to validate the authorization.
UserAuthNewPriKeyID	The ID of the new authentication private certificate to be updated for the user.
UserEncrNewPubKeyAlias	The alias of the new encryption public certificate to be updated for the user. The public part of the system certificate that is selected as the encryption private certificate. The trading partner or user shares the key with the bank.
UserEncrNewPubKeyID	The ID of the new encryption public certificate to be updated for the user.
UserEncrNewPriKeyAlias	The alias of the new encryption private certificate to be updated for the user. The private key used by EBICS Client to decrypt the response received from the bank.
UserEncrNewPriKeyID	The ID of the new encryption private certificate to be updated for the user.
UserNewSignatureVersion	The key version of the new electronic signature to be updated for the user. The valid values are A005 or A006. If you are using a hardware key store for electronic signature, then the key version is set to A005 and cannot be changed.
UserNewAuthVersion	The key version of the authentication certificate is X002.

Table 19. HCS parameters (continued)

Parameter	Description and value
UserNewEncVersion	The key version of the encryption certificate is E002.

XML schema

```
<?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>J</orderIdPrefix>
  <SecurityMedium>0200</SecurityMedium>
  <OrderType>HCS</OrderType>
  <UserSignNewPubKeyAlias>CAEBSignASaiPub</UserSignNewPubKeyAlias>
  <UserSignNewPubKeyID>blrgislin32:node1:12e961909b2:10416964</UserSignNewPubKeyID>
  <UserSignNewPriKeyAlias>CAEBSignASaiPriv</UserSignNewPriKeyAlias>
  <UserSignNewPriKeyID>blrgislin32:node1:12e961909b2:10414702</UserSignNewPriKeyID>
  <UserAuthNewPubKeyAlias>CAEBAuthSaiPub</UserAuthNewPubKeyAlias>
  <UserAuthNewPubKeyID>blrgislin32:node1:12e961909b2:10416444</UserAuthNewPubKeyID>
  <UserAuthNewPriKeyAlias>CAEBAuthSaiPriv</UserAuthNewPriKeyAlias>
  <UserAuthNewPriKeyID>blrgislin32:node1:12e961909b2:10413399</UserAuthNewPriKeyID>
  <UserEncrNewPubKeyAlias>CAEBEncrSaiPub</UserEncrNewPubKeyAlias>
  <UserEncrNewPubKeyID>blrgislin32:node1:12e961909b2:10416577</UserEncrNewPubKeyID>
  <UserEncrNewPriKeyAlias>CAEBEncrSaiPriv</UserEncrNewPriKeyAlias>
  <UserEncrNewPriKeyID>blrgislin32:node1:12e961909b2:10414316</UserEncrNewPriKeyID>
  <UserNewSignatureVersion>A005</UserNewSignatureVersion>
  <UserNewAuthVersion>X002</UserNewAuthVersion>
  <UserNewEncVersion>E002</UserNewEncVersion>
</orderMetaData>
```

HCA order type

Use HCA order type to send amendment of the subscriber key for identification and authentication and encryption.

Access

Mailbox

Description

HCA is an upload key management order type used to update customer's certificate for identification and authentication and encryption. The order data is signed, compressed, encrypted, and base64-encoded.

Parameters

Table 20. HCA parameters

Parameter	Description and value
HostID	The bank ID or the host ID of the bank to which the EBICS Client user submitted the order. It is a unique ID for the bank in the bank's system.

Table 20. HCA parameters (continued)

Parameter	Description and value
HostUrlAlias	When configuring a bank profile, you can specify multiple host URLs and set one host URL as the default. If you want to send a request to a host URL that is not the default URL, then, specify a value for this parameter.
PartnerID	The partner ID associated with the user ID.
UserID	Unique ID of the user in the bank's system, which corresponds to the user created in the EBICS Client dashboard.
SystemID	User ID of the technical user. The HCA order type can be submitted by a technical user who is a delegate of the non-techncial or human user. Hence, the value of the UserID is the same as the value of the systemID.
orderIdPrefix	EBICS Client allocates a unique order ID to each order based on the bank, user ID, and the order type. The client generates the order ID as per EBICS specifications. The order ID is a 4-digit alphanumeric ID. You can specify the first character of the order ID. The second, third, and fourth characters of the order ID are alphanumeric in an ascending order (A-Z or 0-9). This parameter is used with EBICS protocol version H003 only.
SecurityMedium	A 4-digit security number in the 0000 to 0499 range. The value cannot be changed for INI, HIA, and HPB order types. The security medium for the subscriber’s bank-technical key is set to 0000 since HPB orders neither require electronic signatures nor transmit bank-technical subscriber keys.
OrderType	The order type of the order you are submitting. In this case, HCA is the order type.
UserAuthNewPubKeyAlias	The alias of the new authentication public certificate to be updated for the user. The public key provided by the user to the bank to validate the authorization of the user in the request from the EBICS Client. The trading partner or user shares the key with the bank.
UserAuthNewPubKeyID	The ID of the new authentication public certificate to be updated for the user.
UserAuthNewPriKeyAlias	The alias of the new authentication private certificate to be updated for the user. The private key used by EBICS Client to create a digital signature for the user in the request sent to the bank. The bank must have the public part of the key to validate the authorization.

Table 20. HCA parameters (continued)

Parameter	Description and value
UserAuthNewPriKeyID	The ID of the new authentication private certificate to be updated for the user.
UserEncrNewPubKeyAlias	The alias of the new encryption public certificate to be updated for the user. The public part of the system certificate that is selected as the encryption private certificate. The trading partner or user shares the key with the bank.
UserEncrNewPubKeyID	The ID of the new encryption public certificate to be updated for the user.
UserEncrNewPriKeyAlias	The alias of the new encryption private certificate to be updated for the user. The private key used by EBICS Client to decrypt the response received from the bank.
UserEncrNewPriKeyID	The ID of the new encryption private certificate to be updated for the user.
UserNewAuthVersion	The key version of the authentication certificate is X002.
UserNewEncVersion	The key version of the encryption certificate is E002.

XML schema

```
<?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>E</orderIdPrefix>
  <SecurityMedium>0200</SecurityMedium>
  <OrderType>HCA</OrderType>
  <UserAuthNewPubKeyAlias>CAEBAuthLMPub</UserAuthNewPubKeyAlias>
  <UserAuthNewPubKeyID>270:3290569:130ae100679:goldie:node1</UserAuthNewPubKeyID>
  <UserAuthNewPriKeyAlias>CAEBAuthLMPriv</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>
```

HPD order type

Using the HPD order type, the user can download bank parameters.

Access

Mailbox

Description

HPD is a download key management order type. The subscriber can receive information pertaining to the bank's specific access (for example, URL or IP address to the bank and designation of the bank) and protocol parameters (for example, support for EBICS protocol versions, recovery, prevalidation, X.509, and so on). The order data is signed, compressed, encrypted, and base64-encoded.

Parameters

Table 21. HPD parameters

Parameter	Description and value
HostID	The bank ID or the host ID of the bank to which the EBICS Client user submitted the order. It is a unique ID for the bank in the bank's system.
HostUrlAlias	When configuring a bank profile, you can specify multiple host URLs and set one host URL as the default. If you want to send a request to a host URL that is not the default URL, then, specify a value for this parameter.
PartnerID	The partner ID associated with the user ID.
UserID	Unique ID of the user in the bank's system, which corresponds to the user created in the EBICS Client dashboard.
SystemID	User ID of the technical user. A technical user is a delegate of the non-technical or human user.
orderIdPrefix	EBICS Client allocates a unique order ID to each order based on the bank, user ID, and the order type. The client generates the order ID as per EBICS specifications. The order ID is a 4-digit alphanumeric ID. You can specify the first character of the order ID. The second, third, and fourth characters of the order ID are alphanumeric in an ascending order (A-Z or 0-9). This parameter is used with EBICS protocol version H003 only.
SecurityMedium	A 4-digit security number in the 0000 to 0499 range.
OrderType	The order type of the order you are submitting. In this case, HPD is the order type.

XML schema

```
<?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>
```

SPR order type

Use the SPR order type to suspend a user's access authorization.

Access

Mailbox

Description

SPR is an upload key management order type. A subscriber can be suspended from transacting further with the bank for several reasons. One of the primary reasons for suspending a user is if the subscriber keys are compromised. If there is any suspicion that the subscriber keys are compromised, the subscriber must immediately suspend their access authorization to all the bank systems that use the keys.

The SPR order type does not compromise any additional order data and therefore does not contain any order file. The electronic signature of the EBICS Client user who is to be suspended is sent to the bank. The order data is a blank character. The signature is compressed, encrypted, and base64 encoded similar to a standard upload transaction.

Once a subscriber is suspended from transacting with the bank, the subscriber has to submit a new set of INI and HIA order types to the bank. If a subscriber is suspended by the bank, initialization through INI and HIA is not possible. Only the bank can revoke the suspension.

Parameters

Table 22. SPR parameters

Parameter	Description and value
HostID	The bank ID or the host ID of the bank to which the EBICS Client user submitted the order. It is a unique ID for the bank in the bank's system.
HostUrlAlias	When configuring a bank profile, you can specify multiple host URLs and set one host URL as the default. If you want to send a request to a host URL that is not the default URL, then, specify a value for this parameter.
PartnerID	The partner ID associated with the user ID.
UserID	Unique ID of the user in the bank's system, which corresponds to the user created in the EBICS Client dashboard.
SystemID	User ID of the technical user. The SPR order type can be submitted by a technical user who is a delegate of the non-techncial or human user. Hence, the value of the UserID is the same as the value of the systemID.

Table 22. SPR parameters (continued)

Parameter	Description and value
orderIdPrefix	EBICS Client allocates a unique order ID to each order based on the bank, user ID, and the order type. The client generates the order ID as per EBICS specifications. The order ID is a 4-digit alphanumeric ID. You can specify the first character of the order ID. The second, third, and fourth characters of the order ID are alphanumeric in an ascending order (A-Z or 0-9). This parameter is used with EBICS protocol version H003 only.
SecurityMedium	A 4-digit security number in the 0000 to 0499 range.
OrderType	The order type of the order you are submitting. In this case, SPR is the order type.

XML schema

```
<?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>
```

HVD order type

Using the HVD order type, the user can retrieve the state of a VEU order.

Access

Mailbox

Description

HVD is a download order type for distributed signature. Use the HVD order type to retrieve the state of an order that is currently in VEU processing and for which the subscriber is authorized as a signatory. With HVD, the hash value of the order is retrieved.

Parameters

Table 23. HVD parameters

Parameter	Description and value
OrderType	The order type of the order you are submitting. In this case, HVD is the order type.

Table 23. HVD parameters (continued)

Parameter	Description and value
SecurityMedium	A 4-digit security number in the 0000 to 0499 range.
VEUOrderSeqID	The sequence ID of the transaction for which you are retrieving the HVD details. EBICS Client assigns a sequence ID to a transaction.
orderIdPrefix	EBICS Client allocates a unique order ID to each order based on the bank, user ID, and the order type. The client generates the order ID as per EBICS specifications. The order ID is a 4-digit alphanumeric ID. You can specify the first character of the order ID. The second, third, and fourth characters of the order ID are alphanumeric in an ascending order (A-Z or 0-9). This parameter is used with EBICS protocol version H003 only.

XML schema

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

HVE order type

Using the HVE order type, the user can add a VEU signature.

Access

Mailbox

Description

HVE is an upload order type for distributed signature. Use the HVE order type to add a bank-technical signature for authorization to an order for VEU processing. The signature data is compressed, encrypted, and base64 encoded.

Parameters

Table 24. HVE parameters

Parameter	Description and value
PartnerID	The partner ID associated with the user ID.
HostID	The bank ID or the host ID of the bank to which the EBICS Client user submitted the order. It is a unique ID for the bank in the bank's system.

Table 24. HVE parameters (continued)

Parameter	Description and value
HostUrlAlias	When configuring a bank profile, you can specify multiple host URLs and set one host URL as the default. If you want to send a request to a host URL that is not the default URL, then, specify a value for this parameter.
OrderType	The order type of the order you are submitting. In this case, HVE is the order type.
orderIdPrefix	EBICS Client allocates a unique order ID to each order based on the bank, user ID, and the order type. The client generates the order ID as per EBICS specifications. The order ID is a 4-digit alphanumeric ID. You can specify the first character of the order ID. The second, third, and fourth characters of the order ID are alphanumeric in an ascending order (A-Z or 0-9). This parameter is used with EBICS protocol version H003 only.
Product	The product for the EBICS Client application.
productLang	The language setting of the EBICS Client application that you are using. For example, specify EN if the language is set to English.
SecurityMedium	A 4-digit security number in the 0000 to 0499 range.
UserID	Unique ID of the user in the bank's system, which corresponds to the user created in the EBICS Client dashboard.
OrigPartnerID	The Partner ID associated with the user who submitted the upload order type.
OrigOrderID	The order ID of the order for which the signature is applied.
OrigOrderType	The order type of the order for which the signature is applied.
VeuMessageDigest	Specify the Message Digest to submit the hash value of the order data. You can request for the hash value by calling or mailing the bank. The bank sends the hash value of the order data through an alternate mode of communication, for example, email.
PAYLOADMSGID	Specify a ID for the payload message to submit the complete payload from your mailbox. You can request for the payload by calling or mailing the bank. The bank sends the payload to your EBICS Client mailbox.
VEUOrderSeqID	The sequence ID of the transaction for which you are applying the signature using HVE. EBICS Client assigns a sequence ID to a transaction.

XML schema

The following XML schema illustrates the use of HVE using VEU message digest:

```
<?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>uU0nuZNNPgilLlLX2n2r+sSE7+N6U4DukIj3rOLvzek=</VeuMessageDigest>
</orderMetaData>
```

The following XML schema illustrates the use of HVE using payload message ID when the entire payload is available in the mailbox:

```
<?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>
 <PAYLOADMSGID>71</PAYLOADMSGID>
 <OrigPartnerID>PARTNERPK56</OrigPartnerID>
 <OrigOrderID>V568</OrigOrderID>
 <OrigOrderType>C2S</OrigOrderType>
</orderMetaData>
```

The following XML schema illustrates the use of HVE using VEU order sequence ID. The order details are retrieved from the bank using VEU download order types before applying HVE:

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

HVS order type

Using the HVS order type, the user can permanently cancel an existing order from VEU processing.

Access

Mailbox

Description

HVS is an upload order type for distributed signature. Use the HVS order type to permanently cancel an existing order from VEU processing. The subscriber sends an HVS request to cancel an order and delivers the bank-technical signature required for cancellation through the hash value of the order data. The HVS response does not contain any VEU-specific data.

Parameters

Table 25. HVS parameters

Parameter	Description and value
PartnerID	The partner ID associated with the user ID.
HostID	The bank ID or the host ID of the bank to which the EBICS Client user submitted the order. It is a unique ID for the bank in the bank's system.
HostUrlAlias	When configuring a bank profile, you can specify multiple host URLs and set one host URL as the default. If you want to send a request to a host URL that is not the default URL, then, specify a value for this parameter.
OrderType	The order type of the order you are submitting. In this case, HVS is the order type.
orderIdPrefix	EBICS Client allocates a unique order ID to each order based on the bank, user ID, and the order type. The client generates the order ID as per EBICS specifications. The order ID is a 4-digit alphanumeric ID. You can specify the first character of the order ID. The second, third, and fourth characters of the order ID are alphanumeric in an ascending order (A-Z or 0-9). This parameter is used with EBICS protocol version H003 only.
Product	The product for the EBICS Client application.
productLang	The language setting of the EBICS Client application that you are using. For example, specify EN if the language is set to English.
SecurityMedium	A 4-digit security number in the 0000 to 0499 range.
UserID	Unique ID of the user in the bank's system, which corresponds to the user created in the EBICS Client dashboard.
OrigPartnerID	The Partner ID associated with the user who submitted the upload order type.
OrigOrderID	The order ID of the order for which the signature is applied.
OrigOrderType	The order type of the order for which the signature is applied.

Table 25. HVS parameters (continued)

Parameter	Description and value
VeuMessageDigest	Specify the Message Digest to submit the hash value of the order data. You can request for the hash value by calling or mailing the bank. The bank sends the hash value of the order data through an alternate mode of communication, for example, email.
PAYLOADMSGID	Specify a ID for the payload message to submit the complete payload from your mailbox. You can request for the payload by calling or mailing the bank. The bank sends the payload to your EBICS Client mailbox.
VEUOrderSeqID	The sequence ID of the transaction assigned by the client for which you are applying the signature using HVS.

XML schema

The following XML schema illustrates the use of HVS using VEU message digest:

```
<?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+N6U4DukIj3rOLvzek=</VeuMessageDigest>
</orderMetaData>
```

The following XML schema illustrates the use of HVS using payload message ID when the entire payload is available in the mailbox:

```
<?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>
```

The following XML schema illustrates the use of HVS using VEU order sequence ID. The order details are retrieved from the bank using VEU download order types before applying HVS:

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

HVT order type

Using the HVT order type, the user can retrieve detailed information about an order from VEU processing for which the user is authorized as a signatory.

Access

Mailbox

Description

HVT is a download order type for distributed signature. Use the HVT order type to retrieve transaction details about an order from VEU processing.

Parameters

Table 26. HVT parameters

Parameter	Description and value
OrderType	The order type of the order you are submitting. In this case, HVT is the order type.
SecurityMedium	A 4-digit security number in the 0000 to 0499 range.
VEUOrderSeqID	The sequence ID of the transaction for which you are downloading transaction details using HVT. EBICS Client assigns a sequence ID to a transaction.
orderIdPrefix	EBICS Client allocates a unique order ID to each order based on the bank, user ID, and the order type. The client generates the order ID as per EBICS specifications. The order ID is a 4-digit alphanumeric ID. You can specify the first character of the order ID. The second, third, and fourth characters of the order ID are alphanumeric in an ascending order (A-Z or 0-9). This parameter is used with EBICS protocol version H003 only.

Table 26. HVT parameters (continued)

Parameter	Description and value
completeOrderData	If the completeOrderData attribute is set to true, the user sends a request to receive the complete order file. If the completeOrderData attribute is set to false, the user sends a request to receive specific details, such as, account details, implementation deadline, amount, and other description.
fetchLimit	Maximum number of order details to be transmitted if the completeOrderData attribute is set to false. The default value is 100. Valid value is any non-negative integer. Specify 0 to fetch unlimited number of details. While it is possible to retrieve more than 100 details at a time, it is not ideal.
fetchOffset	The offset position in the original order file that marks the starting point of the transaction details to be transmitted. If the completeOrderData attribute is set to false, then the offset position applies to the sequential number of a particular order. The default value is 0. Valid value is any non-negative integer. To retrieve more than 100 records, set **fetch offset** as 0 to retrieve the first 100 records, then set **fetch offset** as 101 to retrieve the next 100 records. Continue as needed.

XML schema

The following sample XML demonstrates the use of HVT order type when the completeOrderData attribute is set to true:

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

The following sample XML demonstrates the use of HVT order type when the completeOrderData attribute is set to false:

```
<?xml version="1.0" encoding="UTF-8"?>
<orderMetaData>
 <OrderType>HVT</OrderType>
 <SecurityMedium>0200</SecurityMedium>
 <VEUOrderSeqID>39132G7e0939003jfj34535536657</VEUOrderSeqID>
 <orderIdPrefix>V</orderIdPrefix>
 <completeOrderData>false</completeOrderData>
 <fetchLimit>5</fetchLimit>
 <fetchOffset>2</fetchOffset>
</orderMetaData>
```

HVU order type

Using the HVU order type, the user can list the orders for which the user is authorized as a signatory.

Access

Mailbox

Description

HVU is a download order type for distributed signature. Use the HVU order type to download VEU overview. In the HVU request, the subscriber optionally submits a list of order types for which the subscriber is authorized as a signatory.

Parameters

Table 27. HVU parameters

Parameter	Description and value
PartnerID	The partner ID associated with the user ID.
HostID	The bank ID or the host ID of the bank to which the EBICS Client user submitted the order. It is a unique ID for the bank in the bank's system.
HostUrlAlias	When configuring a bank profile, you can specify multiple host URLs and set one host URL as the default. If you want to send a request to a host URL that is not the default URL, then, specify a value for this parameter.
OrderType	The order type of the order you are submitting. In this case, HVU is the order type.
orderIdPrefix	EBICS Client allocates a unique order ID to each order based on the bank, user ID, and the order type. The client generates the order ID as per EBICS specifications. The order ID is a 4-digit alphanumeric ID. You can specify the first character of the order ID. The second, third, and fourth characters of the order ID are alphanumeric in an ascending order (A-Z or 0-9). This parameter is used with EBICS protocol version H003 only.
Product	The product for the EBICS Client application.
productLang	The language setting of the EBICS Client application that you are using. For example, specify EN if the language is set to English.
SecurityMedium	A 4-digit security number in the 0000 to 0499 range.
UserID	Unique ID of the user in the bank's system, which corresponds to the user created in the EBICS Client dashboard.

Table 27. HVU parameters (continued)

Parameter	Description and value
VEUOrderTypes	The order types in the form of an XML list for which HVU data is to be retrieved.

XML schema

```
<?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>
```

HVZ order type

Using the HVZ order type, the user can download VEU overview with additional information.

Access

Mailbox

Description

HVZ is a download order type for distributed signature. Use the HVZ order type to download VEU overview with additional information. In the HVZ request, the subscriber optionally submits a list of order types for which the subscriber is authorized as a signatory. HVZ response order data contains the complete information of HVU response order data and HVD response order data, except the display file element.

Parameters

Table 28. HVZ parameters

Parameter	Description and value
PartnerID	The partner ID associated with the user ID.
HostID	The bank ID or the host ID of the bank to which the EBICS Client user submitted the order. It is a unique ID for the bank in the bank's system.
HostUrlAlias	When configuring a bank profile, you can specify multiple host URLs and set one host URL as the default. If you want to send a request to a host URL that is not the default URL, then, specify a value for this parameter.

Table 28. HVZ parameters (continued)

Parameter	Description and value
OrderType	The order type of the order you are submitting. In this case, HVZ is the order type.
orderIdPrefix	EBICS Client allocates a unique order ID to each order based on the bank, user ID, and the order type. The client generates the order ID as per EBICS specifications. The order ID is a 4-digit alphanumeric ID. You can specify the first character of the order ID. The second, third, and fourth characters of the order ID are alphanumeric in an ascending order (A-Z or 0-9). This parameter is used with EBICS protocol version H003 only.
Product	The product for the EBICS Client application.
productLang	The language setting of the EBICS Client application that you are using. For example, specify EN if the language is set to English.
SecurityMedium	A 4-digit security number in the 0000 to 0499 range.
UserID	Unique ID of the user in the bank's system, which corresponds to the user created in the EBICS Client dashboard.
VEUOrderTypes	The order types in the form of an XML list for which HVZ data is to be retrieved.

XML schema

```
<?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>
```

Pending task action

Use the taskMetaData XML to sign or submit a pending order.

Access

Mailbox

Description

Based on the configuration settings defined in an offer, multiple signatories may have to sign the order to process the order data. If an order is submitted for processing without obtaining the required signatures, EBICS Client does not process the order. The user who is a signatory or who is authorized to submit an order can view the particular order in the list of pending tasks using EBICS Client dashboard interface.

The user who is a signatory must sign the pending order. After all the required signatures are obtained, the user, who is a submitter, submits the order.

Parameters

Table 29. EBICSPendingTaskAction parameters

Parameter	Description and value
UserID	Unique ID of the user in the bank's system, which corresponds to the user created in the EBICS Client dashboard.
OrderSeqId	The sequence ID of the transaction for which the signature or submission of the order is pending. EBICS Client assigns a sequence ID to a transaction.
action	You can sign or submit the pending order. If the pending order is to be submitted, set the parameter to submit. If the pending order is to be signed, set the parameter to sign.
isHSM	Valid if the action parameter is set to sign. The user must provide appropriate hardware security key information to sign the order. Currently, EBICS Client supports Hardware Signature Module (HSM) using 3SKey only. If you want to send HSM using an API for signing an order, then ensure that the CEB_ORD_TASK_PEND table is updated with the signature.

XML schema

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

HAC Processing

When an EBICS Customer Acknowledgment (order type HAC) is downloaded in Sterling B2B Integrator, data including status and reason code information is created as defined in EBICS Specification 2.5.

The HAC order type is a technical acknowledgment to the client providing processing status and details for submitted orders. This includes actions and results that occur while uploading, downloading, or signing files and may include information about the content of the file.

Users do not directly initiate HAC requests. Instead, HAC requests are automatically performed by the Sterling B2B Integrator EBICS Client according to defined schedules set up using the HAC scheduler. Each HAC response provides a full history of EBICS actions and status information since the last HAC request. Data from each HAC response is stored by Sterling B2B Integrator.

To view HAC data, use either the EBICS Client **Order search** viewer in Sterling B2B Integrator or **EBICS Search** in Sterling File Gateway.

Search results may contain HAC actions and reason codes as described in the following table:

Table 30. HAC Actions and Reason Codes

HAC Action	Type of Action	Reason Code	HAC Result
File submitted to the bank	FILE_UPLOAD	DS0C	User locked/certificate revoked
		DS08	Decompression error
		DS09	Decryption error
		TA01	Upload aborted
		TS01	Upload successful
File downloaded from the bank	FILE_DOWNLOAD	DS0C	User locked/certificate revoked
		DS08	Decompression error
		DS09	Decryption error
		TA01	Download aborted
		TD01	No data available for download
		TS01	Download successful
Electronic signature submitted to the bank	ES_UPLOAD	ID01	Original order folder has not been sent before
		DS0C	User locked/certificate revoked
		DS08	Decompression error
		DS09	Decryption error
		TA01	Upload of ES aborted
		TS01	Upload of ES successful

Table 30. HAC Actions and Reason Codes (continued)

HAC Action	Type of Action	Reason Code	HAC Result
Signature verification	ES_VERIFICATION	AM21	Amount exceeds limit
		DS01	ES(s) are correct
		DS0A	Number of ES(s) insufficient
		DS0B	ES(s) are not correct
		DS0C	Certificate is revoked/user is locked
		DS0D	Certificate is not valid/public key not activated
		DS0E	Certificate not present/public key doesn't exist
		DS0F	CA for certificate is unknown
		DS0G	Signer not allowed to sign this operation
		DS0H	Signer not allowed to sign this account
		DS08	Decompression error
		DS09	Decryption error
		DS10	Certificate revoked for first signer
		DS11	Certificate not valid for first signer
		DS12	Certificate not present for first signer
		DS13	CA unknown for first signer
		DS14	User (signer) is unknown on the server
		DS15	The same ES already has been sent to the bank
		DS16	Public key version not correct
		DS17	Order data and ES(s) don't match
		DS18	Repeat order (file not testable)
		DS19	Signer's ES rights are insufficient
		DS20	Certificate revoked for second signer
		DS21	Certificate rot valid for second signer
		DS22	Certificate not present for second signer
		DS23	CA unknown for second signer
		DS24	Waiting time expired and file deleted by bank
		DS25	File deleted by bank (multiple reasons)
		DS26	Same user signed multiple times
		DS27	User (signer) not yet activated
		TD02	File cannot be read
		TD03	The file format is invalid
		TS04	File with attributes "DZHNN" (not ES signed)

Table 30. HAC Actions and Reason Codes (continued)

HAC Action	Type of Action	Reason Code	HAC Result
Forwarding to VEU	VEU_FORWARDING	DS06	Order transferred to the VEU
VEU signature verification	VEU_VERIFICATION	AM21	Amount exceeds limit
		DS01	ES(s) are correct
		DS0B	ES(s) are not correct
		DS0C	Certificate is revoked/user is locked
		DS0D	Certificate is not valid/public key not activated
		DS0E	Certificate not present/public key doesn't exist
		DS0F	CA for certificate is unknown
		DS0G	Signer not allowed to sign this operation
		DS0H	Signer not allowed to sign this account
		DS10	Certificate revoked for first signer
		DS11	Certificate not valid for first signer
		DS12	Certificate not present for first signer
		DS13	CA unknown for first signer
		DS14	User (signer) is unknown on the server
		DS15	The same ES already has been sent to the bank
		DS16	Public key version not correct
		DS17	Order data and ES(s) don't match
		DS18	Repeat order (file not testable)
		DS19	Signer's ES rights are insufficient
		DS20	Certificate revoked for second signer
		DS21	Certificate rot valid for second signer
		DS22	Certificate not present for second signer
		DS23	CA unknown for second signer
		DS24	Waiting time expired and file deleted by bank
		DS25	File deleted by bank (multiple reasons)
		DS26	Same user signed multiple times
		DS27	User (signer) not yet activated
		TD02	File cannot be read
		TD03	The file format is invalid
End of VEU signature verification	VEU_VERIFICATION_END	DS05	Order was correct, forwarded for post-processing

Table 30. HAC Actions and Reason Codes (continued)

HAC Action	Type of Action	Reason Code	HAC Result
Cancellation of VEU order	VEU_CANCEL_ORDER	DS02	Order cancelled
		DS03	Order not cancelled
HAC end of order (positive)	ORDER_HAC_FINAL_POS	Not Provided	Final indication for successful processing of the order.
HAC end of order (negative)	ORDER_HAC_FINAL_NEG	Not Provided	Final indication for failed processing of the order.

HAC Scheduling

Users do not directly initiate HAC requests. Instead, HAC requests are automatically performed by the Sterling B2B Integrator EBICS Client according to schedules defined using HAC Scheduling in the EBICS Client Administration menu.

HAC Scheduling is only available for Sterling B2B Integrator users with administrative permissions (admin or super admin).

Each HAC schedule submits an HAC request for a specified partner ID to a specified bank ID using a specific user ID. The HAC schedule also defines how often the HAC request is processed and when the collected data is purged.

To create an HAC schedule, there must be at least one user ID per partner ID, that is in state "Ready" and has permissions to submit orders of type HAC.

When a scheduled HAC request is processed, EBICS order history data is collected and received in an HAC response. Each HAC response provides a full history of EBICS actions and status information since the last HAC request. Data from each HAC response is stored by Sterling B2B Integrator.

Creating an HAC Schedule

To create HAC schedules in Sterling B2B Integrator, use HAC Scheduling in the EBICS Client Administration menu.

About this task

Restriction: Only a Sterling B2B Integrator user with administrative permissions can create HAC schedules. To create an HAC schedule, there must be at least one user ID per partner ID, that is in state "Ready" and has permissions to submit orders of type HAC.

To create an HAC schedule:

Procedure

1. Log in to Sterling B2B Integrator EBICS Client.
2. From the **Administration** menu, select **HAC Scheduling**.
3. In the HAC Schedule Configuration page, next to **Create new schedule**, click **GO**.
4. In the Create: HAC schedule information page, specify the values for the fields according to the instructions in the following table:

Field	Description
Bank ID(Host ID)	Select a bank ID from the drop-down list.
Partner ID	Select a partner ID that is associated with the bank from the drop-down list.
User ID	From the drop-down list, select the ID of the user. **Restriction:** There must be at least one user ID per partner ID, that is in state "Ready" and has permissions to submit orders of type HAC.
Security medium	Enter the security medium.
Request interval	From the drop-down list, select the interval for submitting HAC requests: • disabled • every 5 minutes • every 15 minutes • every 30 minutes • every hour • every 3 hours • every 6 hours • every 12 hours • every day • every 2 days This determines how often a new HAC order is submitted for the partner name to the bank ID with the user ID to collect order processing history data. Each HAC report contains all new order activities since the last HAC request results were issued.

Field	Description
Purge expiry	From the drop-down list, select when the collected HAC report data should expire: • never • after a day • after 2 days • after a week • after 2 weeks • after a month Expired HAC data records are automatically purged from the database during the next execution of the auto-purge process. The frequency of auto-purge execution is controlled by the **HAC purge interval (in minutes)** setting in the EBICS Client system properties. For information about the system properties, see "Updating System Property Values" on page 68. **Important:** If you select **never**, the HAC data records will never expire, and therefore will never be automatically purged from the database. Records will accumulate in the database indefinitely unless they are manually removed from the database tables when no longer needed. This selection applies only to HAC data collected in the future. If this value is later changed, HAC data already stored in the database will retain the value that was assigned at the time it was collected and stored in the database.

5. Click **Finish**:

Searching for an HAC Schedule

To search for HAC schedules in Sterling B2B Integrator, use HAC Scheduling in the EBICS Client Administration menu.

About this task

To search for an HAC schedule:

Procedure

1. Log in to Sterling B2B Integrator EBICS Client.
2. From the **Administration** menu, select **HAC Scheduling**.
3. In the HAC Schedule Configuration page, perform one of the following:
   - Under **Search**, in the **Bank(Host ID)** field or **Partner ID** field, enter part or all of the bank ID or partner ID.
   - Under **List**, from the **Alphabetically** drop-down list, select the first letter or number of the bank ID. Select **All** to list all HAC schedules.
4. Click **GO**.

Viewing an HAC Schedule

To view HAC schedules in Sterling B2B Integrator, use HAC Scheduling in the EBICS Client Administration menu.

About this task

To view the settings for an HAC schedule:

Procedure

1. Log in to Sterling B2B Integrator EBICS Client.
2. From the **Administration** menu, select **HAC Scheduling**.
3. In the HAC Schedule Configuration page, using either **Search** or **List**, locate and select the HAC schedule you want to edit, and click **GO**.
4. Click the partner name link for the HAC schedule you want to view. The HAC schedule settings are displayed.

Editing an HAC Schedule

To edit HAC schedules in Sterling B2B Integrator, use HAC Scheduling in the EBICS Client Administration menu.

About this task

Restriction: Only a Sterling B2B Integrator user with administrative permissions can edit HAC schedules.

To edit an HAC schedule:

Procedure

1. Log in to Sterling B2B Integrator EBICS Client.
2. From the **Administration** menu, select **HAC Scheduling**.
3. In the HAC Schedule Configuration page, using either **Search** or **List**, locate and select the HAC schedule you want to edit, and click **GO**.
4. Click the update icon adjacent to the HAC schedule you want to edit.
5. In the Update: HAC schedule information page, specify the values for the fields according to the instructions in the following table:

Field	Description
Bank ID(Host ID)	Displays the Bank ID. Cannot be edited.
Partner ID	Displays the Partner ID. Cannot be edited.
User ID	From the drop-down list, select the ID of the user. **Restriction:** There must be at least one user ID per partner ID, that is in state "Ready" and has permissions to submit orders of type HAC.
Security medium	Enter the security medium.

Field	Description
Request interval	From the drop-down list, select the interval for submitting HAC requests: • disabled • every 5 minutes • every 15 minutes • every 30 minutes • every hour • every 3 hours • every 6 hours • every 12 hours • every day • every 2 days This determines how often a new HAC order is submitted for the partner name to the bank ID with the user ID to collect order processing history data. Each HAC report contains all new order activities since the last HAC request results were issued.

Field	Description
Purge expiry	From the drop-down list, select when the collected HAC report data should expire: • never • after a day • after 2 days • after a week • after 2 weeks • after a month Expired HAC data records are automatically purged from the database during the next execution of the auto-purge process. The frequency of auto-purge execution is controlled by the **HAC purge interval (in minutes)** setting in the EBICS Client system properties. For information about the system properties, see "Updating System Property Values" on page 68. **Important:** If you select **never**, the HAC data records will never expire, and therefore will never be automatically purged from the database. Records will accumulate in the database indefinitely unless they are manually removed from the database tables when no longer needed. This selection applies only to HAC data collected in the future. Changing this value does not affect HAC data records already stored in the database. The change only affects data collected and stored after the new value is assigned. Existing data records will retain the value that was assigned at the time they were collected and stored in the database.

6. Click **Finish**:

Deleting an HAC Schedule

To delete HAC schedules in Sterling B2B Integrator, use HAC Scheduling in the EBICS Client Administration menu.

About this task

To delete an HAC schedule:

Procedure

1. Log in to Sterling B2B Integrator EBICS Client.
2. From the **Administration** menu, select **HAC Scheduling**.
3. In the HAC Schedule Configuration page, using either **Search** or **List**, locate and select the HAC schedule you want to delete.
4. Click **GO**.
5. Click the delete icon next to the HAC schedule you want to delete.

Results

The HAC schedule is deleted.

Deleting the HAC schedule has no effect on already downloaded HAC status data in the database. These records remain in the table until their individual purge expiry date as set in the HAC schedule at the time the HAC request was submitted.

Return codes

When using EBICS Client, you may receive return codes and event messages.

Return codes for events

The tables here list the return code, the corresponding event message and a brief description of the return code.

Table 31. Return codes for events

Return Code	Event Message	Description
EBICSCL2302	Order Data Compressed	Indicates that the order data of the transaction is compressed. No action required.
EBICSCL2303	Order Data Encrypted	Indicates that the order data of the transaction is encrypted. No action required.
EBICSCL2304	Order Data Encoded	Indicates that the order data of the transaction is encoded. No action required.
EBICSCL2305	Order Data Signed	Indicates that the order data of the transaction is signed. No action required.
EBICSCL2306	Order Data Decompressed	Indicates that the order data of the transaction is decompressed. No action required.
EBICSCL2307	Order Data Decrypted	Indicates that the order data of the transaction is decrypted. No action required.
EBICSCL2308	Order Data Decoded	Indicates that the order data of the transaction is decoded. No action required.
EBICSCL2309	Signature Data Compressed	Indicates that the signature data of the transaction is compressed. No action required.
EBICSCL2310	Signature Data Encrypted	Indicates that the signature data of the transaction is encrypted. No action required.

Table 31. Return codes for events (continued)

Return Code	Event Message	Description
EBICSCL2311	Signature Data Encoded	Indicates that the signature data of the transaction is encoded. No action required.
EBICSCL2312	Signature Data Decompressed	Indicates that the signature data of the transaction is decompressed. No action required.
EBICSCL2313	Signature Data Decrypted	Indicates that the signature data of the transaction is decrypted. No action required.
EBICSCL2314	Signature Data Decoded	Indicates that the signature data of the transaction is decoded. No action required.
EBICSCL2300	EBICS Packaging Passed	Indicates that the packaging of the order data was successful. No action required.
EBICSCL2301	EBICS Packaging Failed	Indicates that the packaging of the order data was not successful. A few of the reasons for the failure of packaging may be a result of failure when compressing order data, or encrypting order data, or erroneous keys used in signature or encryption. Review the list of events using Event Viewer from the EBICS Client dashboard interface.
EBICSCL2500	EBICS Unpackaging Passed	Indicates that the unpackaging of the order data was successful. No action required.
EBICSCL2501	EBICS Unpackaging Failed	Indicates that the unpackaging of the order data was not successful. A few of the reasons for the failure of unpackaging may be a result of failure when decompressing order data, or decrypting order data, or erroneous keys used in signature verification. Review the list of events using Event Viewer from the EBICS Client dashboard interface.
EBICSCL2318	Valid Response Received	Indicates that you have received a valid response from the server when you submit an order type.

Table 31. Return codes for events (continued)

Return Code	Event Message	Description
EBICSCL2319	Erroneous Response Received	Indicates that the server returned an erroneous response for a particular order request. For more information about the response, view the list of events using Event Viewer from the EBICS Client dashboard interface for technical and business return codes.
EBICSCL2320	EBICS Initialisation Request Passed	Indicates that the request has been initialized.
EBICSCL2321	EBICS Data Transfer Request Passed	Indicates that the request for transfer of data has been accepted by the bank.
EBICSCL2322	No Submitter Authority	Indicates that you do not have the user permission to submit an order. Configure the user permission for the role with authorization level set to T and permission type set to Submitter.
EBICSCL2323	Unpackaged data writing to Mailbox success	Indicates that the data was unpackaged and stored in the user mailbox.
EBICSCL2324	Unpackaged data writing to Mailbox failure	The failure to write unpackaged data to a mailbox may be a result of inadequate permission to access mailbox. For more information, see the ebicsClient.log file.
EBICSCL2325	Pending Tasks created for Authorizers	Indicates that pending tasks are created for the user. View the list of pending tasks to be signed using the EBICS Client dashboard interface.
EBICSCL2326	Pending Tasks created for Submitter	Indicates that pending tasks are created for the user who is authorized to submit orders. View the list of pending tasks to be submitted using the EBICS Client dashboard interface.
EBICSCL2327	Signature generation successful for Authorizer	Indicates that the signature generation was successful when a signatory signed an order that was pending for signature.

Table 31. Return codes for events (continued)

Return Code	Event Message	Description
EBICSCL2328	Signature generation failed for Authorizer	Indicates that the signature generation was unsuccessful when a signatory signed an order that was pending for signature.
EBICSCL2329	OrderType is invalid	Indicates that the order type specified is invalid. Specify a valid order type.
EBICSCL2330	HostID is invalid	Indicates that the host ID or the bank ID specified is invalid. Specify a valid host ID.
EBICSCL2331	PartnerID and UserID combination is invalid	Indicates that the user ID and the associated partner ID combination is invalid. Specify a valid combination of user ID and associated partner ID.
EBICSCL2332	SystemID is invalid	Indicates that the system ID specified is invalid. Specify a valid system ID.
EBICSCL2333	Missing mandatory parameter in order metadata	Indicates that a mandatory parameter in the order metadata is not included. Review the ordermetadata.xml for the missing parameter and specify a valid value for the parameter.
EBICSCL2334	Security Medium is invalid	Indicates that the value specified for security medium is not valid. Enter a four-digit security number in the 0100 – 0499 range.
EBICSCL2335	Unable to parse Primary Document in Workflow	Re-check configuration and initiate transaction.
EBICSCL2336	Encryption Public Key not found for Bank	Upload a valid encryption key.
EBICSCL2337	Could not retrieve Key for usage	When signing or encrypting order data, the key to the alias could not be retrieved.
EBICSCL2338	Segment Upload to Host	The order data segment was successfully uploaded to the server.
EBICSCL2339	Segment Download from Host	The order data segment was successfully downloaded from the server.
EBICSCL2340	Calculated Total Number of segments to be Uploaded	EBICS Client calculates the total number of segments of an order data that is to be uploaded.

Table 31. Return codes for events (continued)

Return Code	Event Message	Description
EBICSCL2341	Got Total Number of segments to be Downloaded	EBICS Client receives the total number of segments of an order data that is to be downloaded.
EBICSCL2342	Auto Submit value is invalid	Indicates that the value defined for autosubmit is not valid and therefore the order cannot be automatically submitted. Enter a valid value for the autosubmit parameter. Valid values are true and false.
EBICSCL2343	Country code value is invalid	Indicates that the abbreviation for a country is not valid. Specify a valid format for country abbreviations.
EBICSCL2344	Host not yet Active	Indicates that the server at the bank is not yet active. Download the bank keys using the HPB order type and validate the bank keys.
EBICSCL2345	User not yet Ready	Indicates that the subscriber initialization for the user is not yet complete. Generate the INI and HIA letters for the user associated with the partner and send them to the bank for validation.
EBICSCL2346	Response data writing to Mailbox success	Indicates that the response received from the bank was successfully stored in the mailbox.
EBICSCL2347	Response data writing to Mailbox failure	The failure to write response data to a mailbox may be a result of inadequate permission to access mailbox. For more information, see the ebicsClient.log file.
EBICSCL2348	Error putting message into Mailbox	Indicates that the message could not be uploaded to the mailbox.
EBICSCL2349	No Response from Server	Indicates that the server did not respond when a request was sent to the server.
EBICSCL2350	Invalid response from Server	Indicates that the server returned an invalid response when a request was sent to the server.

Table 31. Return codes for events (continued)

Return Code	Event Message	Description
EBICSCL2392	Mandatory Parameter for HttpClient missing	Indicates that the name of the configured http client adapter is null, or adapter properties are missing, or if the host or port is not configured properly. If SSL is enabled, CA certificate is not configured.
EBICSCL2393	HttpClient Instance Not Found	Indicates that the http client adapter instance is missing.
EBICSCL2394	Error in Ending HTTP Session with Server	Indicates that an error occurred when ending the HTTP session with the server, which may be a result of not finding a valid session.
EBICSCL2395	Host Not Found	Indicates that the host or port is not configured properly.
EBICSCL2396	Handshake Failure	When connecting to the server using SSL. the connection may be unsuccessful, for example, because of invalid certificates.
EBICSCL2398	Could not complete connection to specified host	Indicates that the client was unable to connect to a host even when the session was successfully started.
EBICSCL2351	Invalid key length for signature	Indicates that the length of the bank-technical keys is invalid for signature. Ensure that the key length is equal to or greater than 1536 bit and equal to or lesser than 4096 bit. For information about defining EBICS-specific key lengths for electronic signature, encryption, and authentication, see *EBICS Specification, version 2.5*.

Table 31. Return codes for events (continued)

Return Code	Event Message	Description
EBICSCL2352	Invalid key length for authentication	Indicates that the length of the bank-technical keys is invalid for identification and authentication. Ensure that the key length is equal to or greater than 1024 bit and equal to or lesser than 16384 bit. For information about defining EBICS-specific key lengths for electronic signature, encryption, and authentication, see *EBICS Specification, version 2.5*.
EBICSCL2353	Invalid key length for encryption	Indicates that the length of the bank-technical keys is invalid for encryption. Ensure that the key length is equal to or greater than 1024 bit and equal to or lesser than 16384 bit. For information about defining EBICS-specific key lengths for electronic signature, encryption, and authentication, see *EBICS Specification, version 2.5*.
EBICSCL2354	Error in starting HTTP Session with Server	Indicates that an error occurred when starting an HTTP session with the server.
EBICSCL2355	Error in parsing OrderMetadata Document with Message ID	Check whether the XML is well-formed or not.
EBICSCL2356	Technical Subscriber does not have permissions to be a delegate of the User specified	Configure technical user and associate the technical user with an existing user.
EBICSCL2357	Error while trying to retrieve message from Mailbox	Indicates that an error occurred when retrieving a message from the mailbox.
EBICSCL2358	Error in parsing OrderMetadata Document	Check whether the XML is well-formed.
EBICSCL2359	Signature Application Rejected	Signature application rejected because the signature requirements were already met for the order.
EBICSCL2360	Submission Application Rejected	Submission application rejected because the order has already been submitted to the bank.

Table 31. Return codes for events (continued)

Return Code	Event Message	Description
EBICSCL2361	Ordermetadata file is not a zip file or no files present inside the zip	Ensure that the ordermetadata file is in a compressed format and that the zip file has valid content.
EBICSCL2362	Incorrect number of files present in Ordermetadata zip	Indicates that the number of files present in the ordermetadata.zip file is incorrect. For example, when submitting an FUL order type from back-end, if the zip file does not contain either the payload data or the ordermetadata.xml or both.
EBICSCL2363	Missing file with name ordermetadata.xml in Ordermetadata zip	Ensure that the zip file contains a file with the name ordermetadata.xml.
EBICSCL2364	Missing Payload file in Ordermetadata zip for OrderType FUL	Ensure that the zip file contains the payload order data for order type FUL.
EBICSCL2365	Error while trying to retrieve Transport URL or other mandatory transport parameters	Indicates that the host URL is malformed or the client is unable to retrieve HTTP configuration details from the database.
EBICSCL2366	Error while decrypting the data	An error occurred when decrypting the data. This can be caused by many things. For example, The data being encrypted with the wrong certificate or incomplete encrypted data could cause this error.
EBICSCL2367	Error while encrypting the data	An error occurred when encrypting the data. This can be caused by many things. For example, an invalid or missing key could cause this error.
EBICSCL2368	Error while creating XML authentication	The error may be a result of , for example, certificate not configured or unable to retrieve the certificate.
EBICSCL2369	Error while verifying XML authentication	The error may be a result of , for example, certificate not configured or unable to retrieve the certificate.
EBICSCL2370	Unexpected Return code from Server	The server returned an error not defined in the client database.
EBICSCL2371	EBICS Client Internal Error	An internal error occurred when processing an EBICS request.

Table 31. Return codes for events (continued)

Return Code	Event Message	Description
EBICSCL2403	NIST compliance error	NIST compliance error. Please check whether the algorithm/keystrength being used is NIST compliant in the current configured NIST compliance mode.
EBICSCL2404	Signature certificate not issued by a CA	Signature certificate not issued by a certification authority (CA). IssuerDN: ${0}.
EBICSCL2405	EBICS Protocol version mismatch, server replies with different version than order type is offered for	EBICS Protocol version mismatch, OrderType INI offered for H003 but the EBICS server sent a response for protocol version H004.

Return codes for HPB

Table 32. Return codes for HPB

Return Code	Event Message	Description
EBICSCL1701	EBICS HPB Request Creation Failed	An error occurred when creating an HPB request.
EBICSCL1702	EBICS HPB Request Creation Passed	The HPB order request was created successfully.
EBICSCL1703	EBICS HPB Response Parsing Failed	An error occurred when parsing an HPB response.
EBICSCL1704	EBICS HPB Response Parsing Passed	The HPB response was parsed successfully.
EBICSCL1705	EBICS HPB Response Un-Packing Passed	The HPB response was unpacked successfully.
EBICSCL1706	EBICS HPB Response Un-Packing Failed	An error occurred when unpacking an HPB response.
EBICSCL1707	EBICS HPB Bank Certs Save Failed	An error occurred when saving the bank keys.
EBICSCL1708	EBICS HPB Bank Certs Save Pass	The HPB bank keys were saved successfully.

Return codes for keys

Table 33. Return codes for keys

Return Code	Event Message	Description
EBICSCL2372 to EBICSCL2381	Could not retrieve Private Key for usage	The following is a list of possible reasons for failure to retrieve private keys: • SystemCertificate not found in Database • Certificate is Expired • Certificate Not Yet Valid • Certificate is Held • Certificate is Revoked • Invalid Issuer Signature for a certificate in the chain • CertPathValidation failed • Error in Certificate • Error in fetching Certificate • Error in fetching key from RSA KeyStore
EBICSCL2382 to EBICSCL2391	Could not retrieve Public Key for usage	The following is a list of possible reasons for failure to retrieve public keys: • Key not found in Database • Certificate is Expired • Certificate Not Yet Valid • Certificate is Held • Certificate is Revoked • Invalid Issuer Signature for a certificate in the chain • CertPathValidation failed • Error in Certificate • Error in fetching Certificate • Error in fetching key from RSA KeyStore

Return codes for generating order IDs

Table 34. Return codes for generating order IDs

Return Code	Event Message	Description
EBICSCL2399	OrderID generation re-initialized	Indicates that the last three alphanumeric values in the order ID, which can range from 000 to zzz, was re-initialized to 000.

Table 34. Return codes for generating order IDs (continued)

Return Code	Event Message	Description
EBICSCL2400	Order logging failed in the EBICS client system	The order ID already exists in the system for partner ID. Contact administrator for further action.
EBICSCL2401	OrderID generation failed	In a multi-node scenario, when one of the nodes fails to refresh the order ID cache and consequently fails to generate an Order ID for a particular order.
EBICSCL2402	OrderID Cache configuration error	Check the configuration for order ID cache under System Properties.

Technical return codes

Table 35. Technical return codes

Return Code	Event Message	Description
ESRVT011000	[t011000] EBICS_DOWNLOAD_ POSTPROCESS_DONE	The positive acknowledgment of the EBICS response that is sent to the client from the server.
ESRVT011001	[t011001] EBICS_DOWNLOAD_ POSTPROCESS_SKIPPED	The negative acknowledgment of the EBICS response that is sent to the client from the server.
ESRVT011101	[t011101] EBICS_TX_SEGMENT_ NUMBER_UNDERRUN	The server terminates the transaction if the client, in an upload transaction, has specified a very high (when compared to the number specified in the initialization phase) number of segments that are to be transmitted to the server.
ESRVT031001	[t031001] EBICS_ORDER_ PARAMS_IGNORED	The supplied order parameters that are not supported by the bank are ignored.
ESRVT061001	[t061001] EBICS_AUTHENTICATION _FAILED	The bank is unable to verify the identification and authentication signature of an EBICS request.
ESRVT061002	[t061002] EBICS_INVALID_REQUEST	The received EBICS XML message does not conform to the EBICS specifications.
ESRVT061099	[t061099] EBICS_INTERNAL_ERROR	An internal error occurred when processing an EBICS request.
ESRVT061101	[t061101] EBICS_TX_RECOVERY_ SYNC	If the bank supports transaction recovery, the bank verifies whether an upload transaction can be recovered. The server synchronizes with the client to recover the transaction.

Table 35. Technical return codes (continued)

Return Code	Event Message	Description
ESRVT091002	[t091002] EBICS_INVALID_USER _OR_USER_STATE	Error that results from an invalid combination of user ID or an invalid subscriber state.
ESRVT091003	[t091003] EBICS_USER_ UNKNOWN	The identification and authentication signature of the technical user is successfully verified but the non-technical subscriber is not known to the bank.
ESRVT091004	[t091004] EBICS_INVALID_ USER_STATE	The identification and authentication signature of the technical user is successfully verified and the non-technical subscriber is known to the bank, but the user is not in a 'Ready' state.
ESRVT091005	[t091005] EBICS_INVALID_ ORDER_TYPE	Upon verification, the bank finds that the order type specified in invalid.
ESRVT091006	[t091006] EBICS_UNSUPPORTED_ ORDER_TYPE	Upon verification, the bank finds that the order type specified in valid but not supported by the bank.
ESRVT091007	(H003 protocol) [t091007] EBICS_USER_ AUTHENTICATION _REQUIRED (H004 protocol) [t091007] EBICS_DISTRIBUTED_ SIGNATURE_AUTHORISATION _FAILED	Subscriber possesses no authorization of signature for the referenced order in the VEU administration.
ESRVT091008	[t091008] EBICS_BANK_PUBKEY_ UPDATE_REQUIRED	The bank verifies the hash value sent by the user. If the hash value does not match the current public keys, the bank terminates the transaction initialization.
ESRVT091009	[t091009] EBICS_SEGMENT_ SIZE_EXCEEDED	If the size of the transmitted order data segment exceeds 1 MB, the transaction is terminated.
ESRVT091010	[t091010] EBICS_INVALID_XML	The XML schema does not conform to the EBICS specifications.
ESRVT091011	[t091011] EBICS_INVALID_HOST_ID	The transmitted host ID is not known to the bank.
ESRVT091101	[t091101] EBICS_TX_UNKNOWN_ TXID	The supplied transaction ID is invalid.

Table 35. Technical return codes (continued)

Return Code	Event Message	Description
ESRVT091102	[t091102] EBICS_TX_ABORT	If the bank supports transaction recovery, the bank verifies whether an upload transaction can be recovered. If the transaction cannot be recovered, the bank terminates the transaction.
ESRVT091103	[t091103] EBICS_TX_MESSAGE_ REPLAY	To avoid replay, the bank compares the received Nonce with the list of nonce values that were received previously and stored locally. If the nonce received is greater than the tolerance period specified by the bank, the response EBICS_TX_MESSAGE_ REPLAY is returned.
ESRVT091104	[t091104] EBICS_TX_SEGMENT_ NUMBER_EXCEEDED	The serial number of the transmitted order data segment must be less than or equal to the total number of data segments that are to be transmitted. The transaction is terminated if the number of transmitted order data segments exceeds the total number of data segments.
ESRVT091112	[t091112] EBICS_INVALID_ORDER_ PARAMS	In an HVT request, the subscriber specifies the order for which they want to retrieve the VEU transaction details. The HVT request also specifies an offset position in the original order file that marks the starting point of the transaction details to be transmitted. The order details after the specified offset position are returned. If the value specified for offset is higher than the total number of order details, the error EBICS_INVALID_ORDER_ PARAMS is returned.
ESRVT091113	[t091113] EBICS_INVALID_REQUEST_ CONTENT	The EBICS request does not conform to the XML schema definition specified for individual requests.
ESRVT091117	[t091117] EBICS_MAX_ORDER_DATA_ SIZE_EXCEEDED	The bank does not support the requested order size.
ESRVT091118	[t091118] EBICS_MAX_SEGMENTS_ EXCEEDED	The submitted number of segments for upload is very high.

Table 35. Technical return codes (continued)

Return Code	Event Message	Description
ESRVT091119	[t091119] EBICS_MAX_ TRANSACTIONS _EXCEEDED	The maximum number of parallel transactions per customer is exceeded.
ESRVT091120	[t091120] EBICS_PARTNER_ID_ MISMATCH	The partner ID of the electronic signature file differs from the partner ID of the submitter.
ESRVT091121	[t091121] EBICS_INCOMPATIBLE_ ORDER_ATTRIBUTE	The specified order attribute is not compatible with the order in the bank system. If the bank has a file with the attribute DZHNN or other electronic signature files (for example, with the attribute UZHNN) for the same order, then the use of the order attributes DZHNN is not allowed. Also, if the bank already has the same order and the order was transmitted with the order attributes DZHNN, then again the use of the order attributes DZHNN is not allowed.
(H004 protocol) ESRVT091219	[t091219] EBICS_CERTIFICATES _VALIDATION_ERROR	The server is unable to match the certificate with the previously declared information automatically.

Bank-technical return codes

Table 36. Bank-technical return codes

Return Code	Event Message	Description
ESRVB011301	[b011301] EBICS_NO_ONLINE_ CHECKS	The bank does not principally support preliminary verification of orders but the EBICS request contains data for preliminary verification of the order.
ESRVB091001	[b091001] EBICS_DOWNLOAD_ SIGNED_ONLY	The bank system only supports bank-technically signed download order data for the order request. If the subscriber sets the order attributes to DZHNN and requests the download data without the electronic signature of the bank, the transaction initialization is terminated.

Table 36. Bank-technical return codes (continued)

Return Code	Event Message	Description
ESRVB091002	[b091002] EBICS_DOWNLOAD_ UNSIGNED_ONLY	The bank system only supports unsigned download order data for the order request. When it is agreed that the subscriber can download order data only without the electronic signature of the bank, if the subscriber sets the order attributes to OZHNN and requests the download data with the electronic signature of the bank, the transaction initialization is terminated.
ESRVB090003	[b090003] EBICS_AUTHORISATION_ ORDER_TYPE_FAILED	The subscriber is not entitled to submit orders of the selected order type. If the authorization is missing when the bank verifies whether the subscriber has a bank-technical authorization of signature for the order, the transaction is cancelled.
ESRVB090004	[b090004] EBICS_INVALID_ORDER_ DATA_FORMAT	The order data does not correspond with the designated format.
ESRVB090005	[b090005] EBICS_NO_DOWNLOAD_ DATA_AVAILABLE	If the requested download data is not available, the EBICS transaction is terminated.
ESRVB090006	[b090006] EBICS_UNSUPPORTED_ REQUEST_ FOR_ORDER_INSTANCE	In the case of some business transactions, it is not possible to retrieve detailed information of the order data.
ESRVB091105	[b091105] EBICS_RECOVERY_NOT_ SUPPORTED	If the bank does not support transaction recovery, the upload transaction is terminated.
ESRVB091111	[b091111] EBICS_INVALID_ SIGNATURE_ FILE_FORMAT	The submitted electronic signature file does not conform to the defined format.
ESRVB091114	[b091114] EBICS_ORDERID_ UNKNOWN	Upon verification, the bank finds that the order is not located in the VEU processing system.
ESRVB091115	[b091115] EBICS_ORDERID_ALREADY_ EXISTS	The submitted order number already exists.
ESRVB091116	[b091116] EBICS_PROCESSING_ERROR	When processing an EBICS request, other business-related errors occurred.
ESRVB091201	[b091201] EBICS_KEYMGMT_ UNSUPPORTED_ VERSION_SIGNATURE	When processing an INI request, the order data contains an inadmissible version of the bank-technical signature process.

Table 36. Bank-technical return codes (continued)

Return Code	Event Message	Description
ESRVB091202	[b091202] EBICS_KEYMGMT_ UNSUPPORTED_ VERSION_ AUTHENTICATION	When processing an HIA request, the order data contains an inadmissible version of the identification and authentication signature process.
ESRVB091203	[b091203] EBICS_KEYMGMT_ UNSUPPORTED_ VERSION_ENCRYPTION	When processing an HIA request, the order data contains an inadmissible version of the encryption process.
ESRVB091204	[b091204] EBICS_KEYMGMT_ KEYLENGTH_ ERROR_SIGNATURE	When processing an INI request, the order data contains an bank-technical key of inadmissible length.
ESRVB091205	[b091205] EBICS_KEYMGMT_ KEYLENGTH_ERROR_ AUTHENTICATION	When processing an HIA request, the order data contains an identification and authentication key of inadmissible length.
ESRVB091206	[b091206] EBICS_KEYMGMT_ KEYLENGTH_ ERROR_ENCRYPTION	When processing an HIA request, the order data contains an encryption key of inadmissible length.
ESRVB091207	[b091207] EBICS_KEYMGMT_NO_ X509_SUPPORT	A public key of type X509 is sent to the bank but the bank supports only public key value type.
ESRVB091208	[b091208] EBICS_X509_CERTIFICATE_ EXPIRED	The certificate is not valid because it has expired.
ESRVB091209	[b091209] EBICS_X509_CERTIFICATE_ NOT_VALID_YET	The certificate is not valid because it is not yet in effect.
ESRVB091210	[b091210] EBICS_X509_WRONG_ KEY_USAGE	When verifying the certificate key usage, the bank detects that the certificate is not issued for current use.
ESRVB091211	[b091211] EBICS_X509_WRONG_ ALGORITHM	When verifying the certificate algorithm, the bank detects that the certificate is not issued for current use.
ESRVB091212	[b091212] EBICS_X509_INVALID_ THUMBPRINT	The thumb print does not correspond to the certificate.
ESRVB091213	[b091213] EBICS_X509_CTL_INVALID	When verifying the certificate, the bank detects that the certificate trust list (CTL) is not valid.
ESRVB091214	[b091214] EBICS_X509_UNKNOWN_ CERTIFICATE_AUTHORITY	The chain cannot be verified because of an unknown certificate authority (CA).

Table 36. Bank-technical return codes (continued)

Return Code	Event Message	Description
ESRVB091215	[b091215] EBICS_X509_INVALID_ POLICY	The certificate has invalid policy when determining certificate verification.
ESRVB091216	[b091216] EBICS_X509_INVALID_ BASIC_CONSTRAINTS	The basic constraints are not valid when determining certificate verification.
ESRVB091217	[b091217] EBICS_ONLY_X509_ SUPPORT	The bank supports evaluation of X.509 data only.
ESRVB091218	[b091218] EBICS_KEYMGMT_ DUPLICATE_KEY	The key sent for authentication or encryption is the same as the signature key.
ESRVB091301	[b091301] EBICS_SIGNATURE_ VERIFICATION_FAILED	Verification of the electronic signature has failed.
ESRVB091302	[b091302] EBICS_ACCOUNT_ AUTHORISATION_FAILED	Preliminary verification of the account authorization has failed.
ESRVB091303	[b091303] EBICS_AMOUNT_CHECK_ FAILED	Preliminary verification of the account amount limit has failed.
ESRVB091304	[b091304] EBICS_SIGNER_UNKNOWN	The signatory of the order is not a valid subscriber.
ESRVB091305	[b091305] EBICS_INVALID_ SIGNER_STATE	The state of the signatory is not admissible.
ESRVB091306	[b091306] EBICS_DUPLICATE_ SIGNATURE	The signatory has already signed the order.

Return codes for VEU

Table 37. Return codes for VEU

Return Code	Event Message	Description
EBICSCL1050	Error while Unmarshalling the ResponseOrderData and persisting into DB	Indicates that the response order data is not well-formed.

Return codes for console events

Table 38. Return codes for console events

Return Code	Event Message	Description
EBICSCL9000	User created successfully	The user profile was created successfully.
EBICSCL9001	User updated successfully	The user profile was updated successfully.
EBICSCL9002	User deleted successfully	The user profile was deleted successfully.

Table 38. Return codes for console events (continued)

Return Code	Event Message	Description
EBICSCL9003	User creation failed	Creating of a user profile failed. This error may be the result of, for example, the user profile already exists or if the parameters in the user configuration have invalid values.
EBICSCL9004	User update failed	Verify that the parameters for user configuration have valid values or if the connection to the database is down.
EBICSCL9005	User deletion failed	Verify that the parameters for user configuration have valid values or if the connection to the database is down.

Return codes for login

Table 39. Return codes for login

Return Code	Event Message	Description
EBICSCL9020	User Login was successful	The user was successfully logged onto the system.
EBICSCL9021 and EBICSCL9022	User Login failed	An attempt to log on to the hub was unsuccessful because of invalid user name or password or insufficient privileges.
EBICSCL9023	User does not have privilege to access the URI	Verify that you have the correct permission and role to access the URI.
EBICSCL9024	The following features must be licensed as EBICS Client	Obtain the license from IBM Support.
EBICSCL9025	Account has been locked	Account has been locked as maximum number of unsuccessful login exceeded its limit.

Return codes for file format

Table 40. Return codes for file format

Return Code	Event Message	Description
EBICSCL9050	File format created successfully	The file format was created successfully.
EBICSCL9051	File format updated successfully	The file format was updated successfully.
EBICSCL9052	File format creation failed	Verify that the parameters for file format configuration have valid values or if the connection to the database is down.

Table 40. Return codes for file format (continued)

Return Code	Event Message	Description
EBICSCL9053	File format update failed	Verify that the parameters for file format configuration have valid values or if the connection to the database is down.
EBICSCL9054	File format deleted successfully	The file format was deleted successfully.
EBICSCL9055	File format deletion failed	Verify that the connection to the database is up or if the order type is associated with the appropriate file format.

Return codes for bank

Table 41. Return codes for bank

Return Code	Event Message	Description
EBICSCL9070	Bank created successfully	The bank profile was created successfully.
EBICSCL9071	Bank updated successfully	The bank profile was updated successfully.
EBICSCL9072	Bank creation failed	Verify that the parameters for bank configuration have valid values or if the connection to the database is down.
EBICSCL9073	Bank update failed	Verify that the parameters for bank configuration have valid values or if the connection to the database is down.
EBICSCL9074	Bank deleted successfully	The bank profile was deleted successfully.
EBICSCL9075	Bank deletion failed	Verify that the connection to the database is up.
EBICSCL9076	Bank key validated successfully	The bank key was validated successfully.
EBICSCL9077	Bank key validation failed	The hash value received from the bank does not match the hash value stored in EBICS Client system.

Return codes for order submission

Table 42. Return codes for order submission

Return Code	Event Message	Description
EBICSCL9090	Order submitted successfully	The order was submitted successfully.

Table 42. Return codes for order submission (continued)

Return Code	Event Message	Description
EBICSCL9095	Order submission failed	A few of the reasons for the failure of order submission are, if the submitter does not have the required permission, if the certificates are not valid, if the validation of bank keys failed, and so on.

Return codes for offer

Table 43. Return codes for offer

Return Code	Event Message	Description
EBICSCL9101	Offer created successfully	The offer was created successfully.
EBICSCL9102	Offer creation failed	Verify that the connection to the database is up.
EBICSCL9103	Offer updated successfully	The offer was updated successfully.
EBICSCL9104	Offer update failed	Verify that the connection to the database is up.
EBICSCL9105	Offer deleted successfully	The offer was deleted successfully.
EBICSCL9106	Offer deletion failed	Verify that the connection to the database is up.

Return codes for user permissions

Table 44. Return codes for user permissions

Return Code	Event Message	Description
EBICSCL9120	User Permissions created successfully	The user permission was created successfully.
EBICSCL9121	User Permissions creation failed	Verify that the connection to the database is up.
EBICSCL9122	User Permissions updated successfully	The user permission was updated successfully.
EBICSCL9123	User Permissions update failed	Verify that the connection to the database is up.
EBICSCL9124	User Permissions deleted successfully	The user permission was deleted successfully.
EBICSCL9125	User Permissions deletion failed	Verify that the connection to the database is up.

Return codes for pending signature

Table 45. Return codes for pending signature

Return Code	Event Message	Description
EBICSCL9141	Signature submitted	The signature was submitted successfully.
EBICSCL9142	Signature submission failed	Verify that the connection to the database is up or if the message was written successfully to the mailbox.
EBICSCL9143	Signature updated	The signature was updated successfully.
EBICSCL9144	Signature update failed	Verify that the connection to the database is up or if the message was written successfully to the mailbox.

Return codes for pending VEU signature

Table 46. Return codes for pending VEU signature

Return Code	Event Message	Description
EBICSCL9151	VEU Signature submitted	The VEU signature was submitted successfully.
EBICSCL9152	VEU Signature submission failed	Verify that the connection to the database is up or if the message was written successfully to the mailbox.

Index

Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

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

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

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

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those

websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

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

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBMproducts. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to

IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work must include a copyright notice as shown in the next column.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium and the Ultrium Logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

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®, and Sterling Integrator® are trademarks or registered trademarks of Sterling Commerce®, Inc., an IBM Company.

Other company, product, and service names may be trademarks or service marks of others.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Printed in USA