InsideBusiness Connect Client - Installation Guide (Windows)

Table of Contents

Introduction

This document describes the installation of the InsideBusiness Connect Client (IBCC) on a Windows system. It follows a step-by-step approach with screenshots.

What does it do?

IBCC offers you an easy and safe solution for the automated processing of large transaction files. It gives you direct access to ING's European network for sending payment orders and receiving reports.

What is it?

IBCC is the new ING Wholesale Banking application that allows the customer to easily connect with ING InsideBusiness Connect. This is a Java program that runs as a service and establishes a safe, host-to-host connectivity between your ERP system and ING and ensures safe, fast and automated processing of transaction and report files.

The application provides folders (incoming and outgoing) for the customers to drop their payments files which will automatically be uploaded to ING. Reporting files are generated and are automatically downloaded. They can be picked up for reconciliation purposes by the ERP system of the customer.

Files can be delivered to and collected from IBCC 24 Hours a day, 7 days a week (24x7).

Foundation and Generic modules

- Easy installation via Wizard
- Configuration via GUI
- Application heartbeat monitoring
- Secure connection via SFTP
- Automated upload every second
- Automated download every 15 minutes
- Regular updates via Wizard

Version

If a version of IBCC is already installed, you can verify it via the standard windows tools: Control Panel / Programs & Features. Search for the name **InsideBusiness Connect Client**.

Installation Requirements

Account Requirements

The user needs to have an FTP account as well as customer certificates that obtain during the ING onboarding process.

Installer Rights

The installer and GUI need to be executed by a user with administrator rights.

Technical environment

The IBCC software needs to be installed on the customer's server. The installation is done via an installation wizard and configuration GUI where the customer is prompted for SFTP configuration information, namely a Logon ID (provided by ING) and a DS certificate (obtained via ING PKI or a third party). The IBCC software is supported on the following operating systems:

- Windows 11
- Windows server 2016, 2019, 2022, 2025

Verifying the executable

Checking the signature

The IBC client software installer (.exe file) is digitally signed. It is important before it is installed in your environment that you verify its signature, in order to make sure that the executable hasn't been tampered with.

The process of verifying the signature described below using standard Windows features. In the directory where the files from the zip archive are extracted, do a right-click on the `InsideBusinessConnectClient_windows_1_1x_x-x.exe` and click `properties`. In the properties pop-up click on the tab 'Digital Signature'. It should show in the 'Signature list';

```
Name of Signer:     ING Groep N.V.
Digest algorithm:   sha256
Timestamp:          <date>
```

Click on 'Details', the same information as above in the 'Signer information' frame. Here you can also click 'View Certificate' which should show;

```
Subject:
    CN = ING Groep N.V.
    O = ING Groep N.V.
    L = Amsterdam
    S = Noord-Holland
    C = NL

Issued by:
    CN = Entrust Code Signing CA - OVCS2
    O = Entrust, Inc.
    C = US

Valid from:   <date from> to <date to> *
```

Note: * this 'to' date can be in the past, the date the executable was signed should fall within this timeframe.

More detailed information on the certificate can be viewed under 'Details' and 'Certification Path'. Check whether all the certificates in the tree above the ING Groep N.V. certificate are mentioning 'Entrust code signing..' or 'Entrust Root…'. Click 'OK' to return to previous screen.

In the 'Countersignatures' frame you should see;

```
Name of Signer:    Sectigo Public Time Stamping Signer R36
E-mail address:    Not available
Timestamp:         <date> but should match previous value.
```

Again you can click on ‘Details’, the same information as above in the ‘Signer information’ frame. You can also click ‘View Certificate’ here, which should show;

```
Subject:
    CN = Sectigo Public Time Stamping Signer R36
    O = Sectigo Limited
    S = West Yorkshire
    C = GB

Issued by:
    CN = Sectigo Public Time Stamping CA R36
    O = Sectigo Limited
    C = GB

Valid from:   <date from> to <date to> *
```

More detailed information on the certificate can be viewed under ‘Details’ and ‘Certification Path’. Check whether all the certificates in the tree above the ‘Entrust Code Signing CA - OVCS2’ certificate are mentioning ‘Entrust Code Signing Root Certification Authority - CSBR1’ or ‘Entrust.net’. Click ‘OK’ to return to previous screen.

This confirms the authenticity and validity of the executable file, you can then proceed with the SHA-256 hash value check if you want.

Checking the SHA-256 hash value.

Please contact ING support to receive the link to the site where the SHA-256 hash is published.

Then open a DOS Command prompt and navigate to the location of the `InsideBusinessConnectClient_windows_1_1x_x-x.exe`.

Run the following command `certutil -hashfile InsideBusinessConnectClient_windows_1_1x_x-x.exe sha256`

You should see output matching the *example* below, but with different values.

```
SHA256 hash of InsideBusinessConnectClient_windows_1_17_1-0.exe:
a081ec1c6aeccd7d72b5811ba908aba5d32f4da7f0890d3323c84a4ad9af4928
CertUtil: -hashfile command completed successfully.
```

Check if this value ‘**a081ec1c6aeccd7d72b5811ba908aba5d32f4da7f0890d3323c84a4ad9af4928**’ matches the one you have received from the ING site. If there is a match his confirms the authenticity and validity of the executable and you can then proceed with the installation.

Installation and transfer directory

Secure the transfer and configuration directories from unauthorized access before you start using IBCC. Untrusted parties must not be able to *read or write* the data directories or the properties file.

The minimal required space for the installation of the software is 200 MB. File size for the created directories depends on the customer usage. The following directories are created inside the *Transfer* directory specified in the configuration GUI *Welcome* screen:

- **upload**: Payment files dropped here will be encrypted and sent to ING for processing.

- **download**: Decrypted Reporting files are placed here for reconciliation by the customers ERP system
- **archive**: Successful sent Payment files are archived here

The required space on disk depends on the size of the payment files. For a single transfer a minimum amount of twice the size of a payment file is needed.

As transferred payment files are kept in the **archive** directory, this directory must have enough free space to hold the payment files.

For example: For a yearly archive of monthly payments the required disk space is at least 12x the maximum payment file size.

By default, the **archive** directory will never be purged and all succeeded transfer will be kept in the folder. A purge mechanism is in place and can be configured via the IBCC configuration GUI. Please see the configuration GUI documentation for more details.

Upload folders

You will need one or more upload folders. Manage these in the *Folders* tab.

Specify as many upload folders as you like. IBCC will upload files as they appear in any of them. To avoid confusion, the GUI will not accept the same folder being listed more than once.

Each upload folder is associated with a particular *product type.* The default is PAYMENT, but if your contract includes Virtual Ledger Accounts, you can also set up separate folders for VLA uploads and you can use FACTCLT to send files to FactorLink.

Save (Ctrl+s) your GUI changes before using the new folders. This will automatically restart the service and create the designated subfolders in each upload folder.

IBCC works with upload folders you provide; it *does not create the upload folders.* Nor does it remove them from the file system when you deactivate them. It only creates the subfolders.

Atomic writes

When you (or your ERP software) writes a file into an upload folder, this must happen *atomically.* Otherwise, IBCC would have no reliable way to know whether the file is complete. Your ERP package may still be writing to it, or something may have gone wrong.

Therefore, ensure that the file is first written to a temporary location on the same physical drive as the target location, and then once it has been written completely, it should be moved or renamed to its definite location.

The IBCC service will ignore temporary files in the **upload** folders, so one way of doing this would be to start by writing the file under a name which marks it as temporary, and finally, changing its name.

Temporary files are defined as follows:

- They are hidden
- They end with the **.tmp** extension

Here is an example, in pseudocode, of how a file should correctly end up in the **upload** folder:

```
copy input_file into upload/input_file.{uuid}.tmp
move (or rename) upload/input_file.{uuid}.tmp to upload/input_file (this operation is ato
```

We recommend including some random characters (e.g. a UUID or GUID) in the temporary file name, to avoid accidental overwrites in the case where you may write multiple files into the upload folder simultaneously.

Logon User

The Logon User is the Windows user running the IBCC service. By default, the Logon User is the standard Windows user **Local Service**. It has the minimal privileges to be able to start a Windows service.

Important: For that reason, it might happen that the Logon User **Local Service** does not have access to the desired transfer folders. This will prevent the IBCC service from starting until permissions are given to **Local Service** to access the transfer folders, or until a new Logon User is configured to run the IBCC service.

Even though the default Logon User **Local Service** will work in most scenarios, it is advised to change it to a user with specific privileges.

In a case requiring the transfer folders to be on a network share, the default Logon User **Local Service** will most likely not have access to it. A new Logon User with access to the network share has to be configured to run the IBCC service.

In any case, it is very **important** for the Logon User to have access to both Installation and Transfer directories, otherwise the service might not start.

Changing the Logon User under which the IBCC service is running

This is a default Windows administration procedure. It can be done easily from the service panel, as follows:

1. Navigate to the service: **Control Panel** -> **Administrative Tools** -> **Services**.
2. Locate the **'InsideBusinessConnectSvc'** service, right-click and view the **'Properties'**.
3. Go to the **'Log On'** tab and change the user as desired.

Heartbeat monitoring

The IBCC service is sending heartbeats to the ING server every 1 hour.

Installing

The installation process of the IBCC is quite simple. It consists of:

- IBCC Setup Wizard
- IBCC Configuration GUI

The step-by-step explanation and images will guide you through the process of setting up the software on your computer.

Starting the installer

To start the installer in a Windows environment, run *IBCC_windows_{version}.exe* as an administrator.

Before the setup process begins, you might be prompted with a *User Account Control* window for confirmation.

Press **Yes** in order to continue.

Installation process - Setup Wizard

The first screen shown is the *Welcome Screen*.

Press **Next** in order to continue.

The following screen displays the *License Agreement* to the user, either in plain text or in HTML. The license agreement must be accepted to continue the installation.

Press **Next** in order to continue.

The next screen is to *Select Destination Directory* where you would like the IBCC to be installed. Here you can change the default installation directory.

Press **Next** in order to continue.

Important: Since IBCC runs as a Windows service, it is required for the IBCC installation folder to be available when the machine starts up and for the Logon User to have access to it. In other words, it is recommended to use the default installation location. Using a network share for that purpose will most likely not work.

In the next screen it is possible to *Select Start Menu Folder* in which you would like to create the program's shortcuts, or to disable their creation.

Press **Next** in order to continue.

From there, the program will begin copying application files and *Installing* IBCC on your computer.

Once that is done a screen appears confirming the installation of IBCC is finished.

Press **Finish** in order to exit.

Important: The latest Java 1.8.0 Runtime Environment is bundled with the application. BellSoft's build was used during development and testing. Use of any other JRE implementation may lead to unwanted behaviors.

Configuration process - GUI

Introduction

The purpose of the GUI application is to help the customer set up the configuration of IBCC service.

Once the *Setup Wizard* is completed, the GUI will automatically start. To start the GUI manually, run it as an administrator from the IBCC *Start Menu* group.

Namely: *InsideBusiness Connect Client > Configure InsideBusiness Connect Client*

Before the GUI begins, you might be prompted with a *User Account Control* window for confirmation.

Press **Yes** in order to continue.

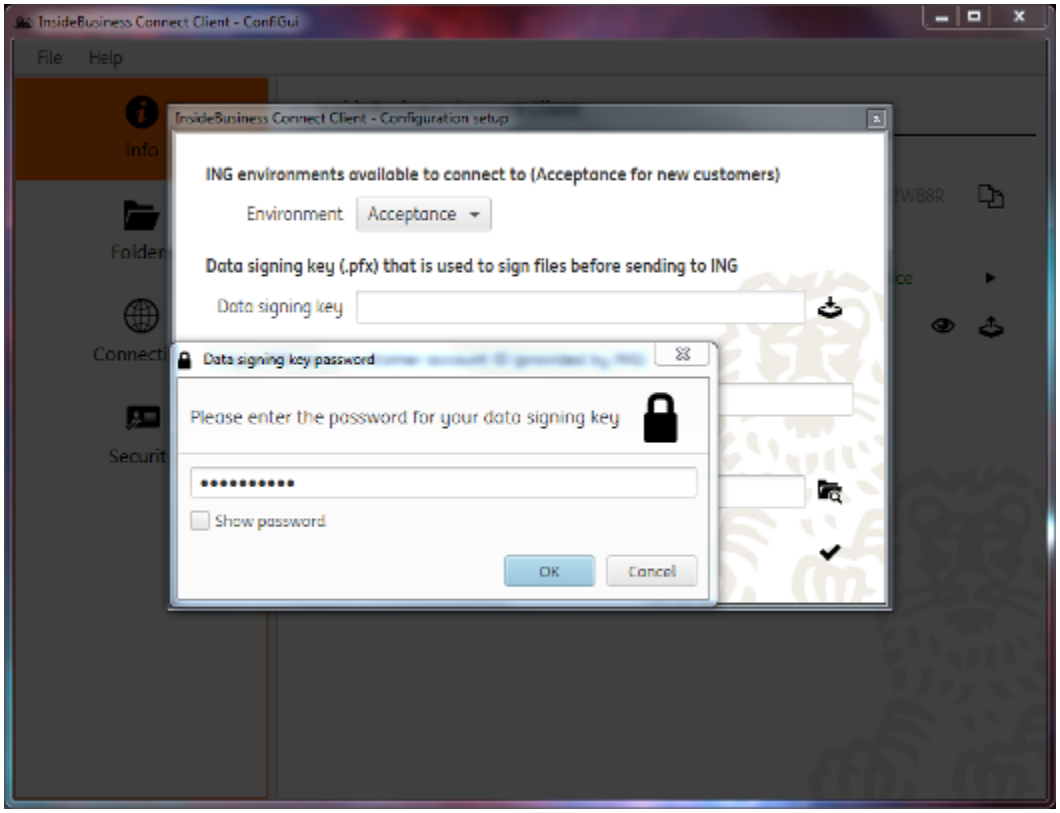
Configuration Setup screen

Upon start the *Configuration Setup* screen is shown, containing mandatory elements for initial setup:

- **Environment**
- **Data signing key**
- **Logon ID**
- **Transfer folder**

The first important configuration element is the ING **Environment**. *Acceptance* is selected by default.

The customer **Data signing key** (.pfx or .p12 extension) for the chosen environment has to be imported. After selecting the file a prompt window appears requesting customer password input. This key will be used to add digital signature to the files that will be sent to ING. The password is obfuscated before saving it.



The next field is the **Logon ID**, which is communicated beforehand by ING.

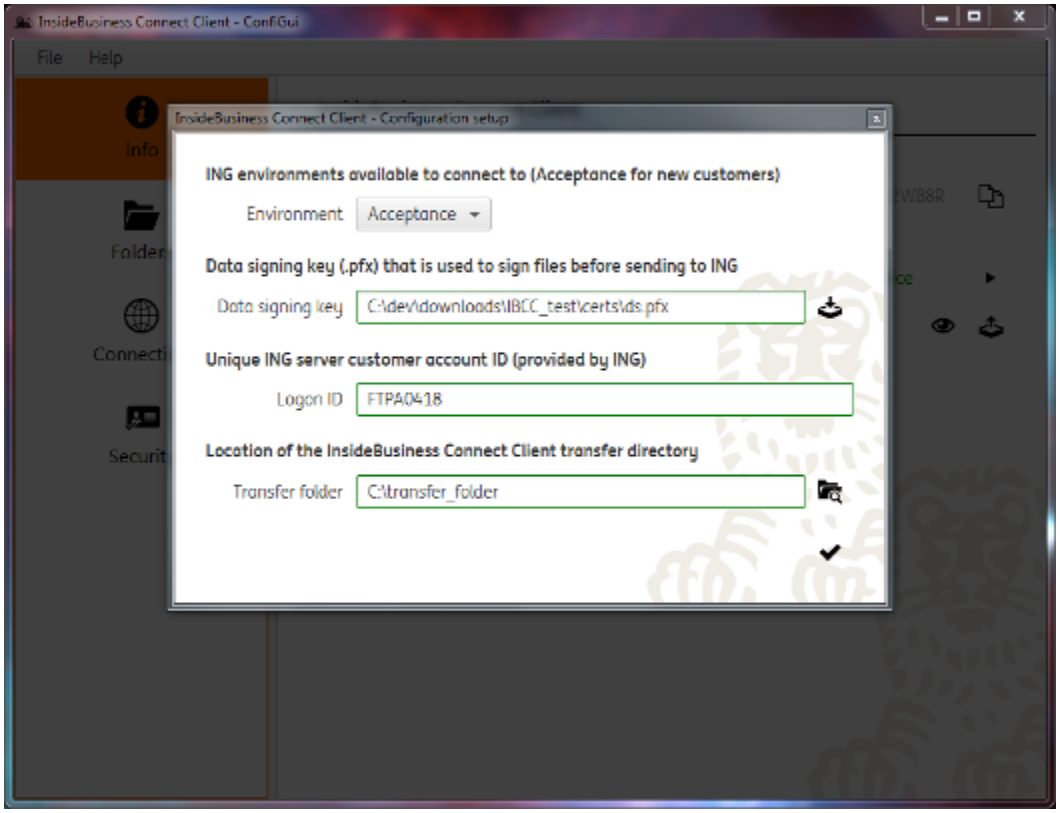
Finally, the user has to select the IBCC **Transfer folder**.

Once all fields are set accordingly and **valid** the configuration can be confirmed.

Press the *Confirm new configuration* button to continue.

Notes:

- Text fields that contain paths to mapped drives are converted to UNC paths when applicable.
- However, it is possible to paste UNC paths directly (e.g. in a case of a transfer folder pointing to a network share). In that case, no check will be performed.
- A new SSH key pair required for authentication against ING IBCC server will be generated in the background. This might take a few seconds. Actions on this SSH key are available in the *Connection* tab.
- The SSH public key and SSH fingerprint have to be known to ING. They can be exported in the *Connection* tab.

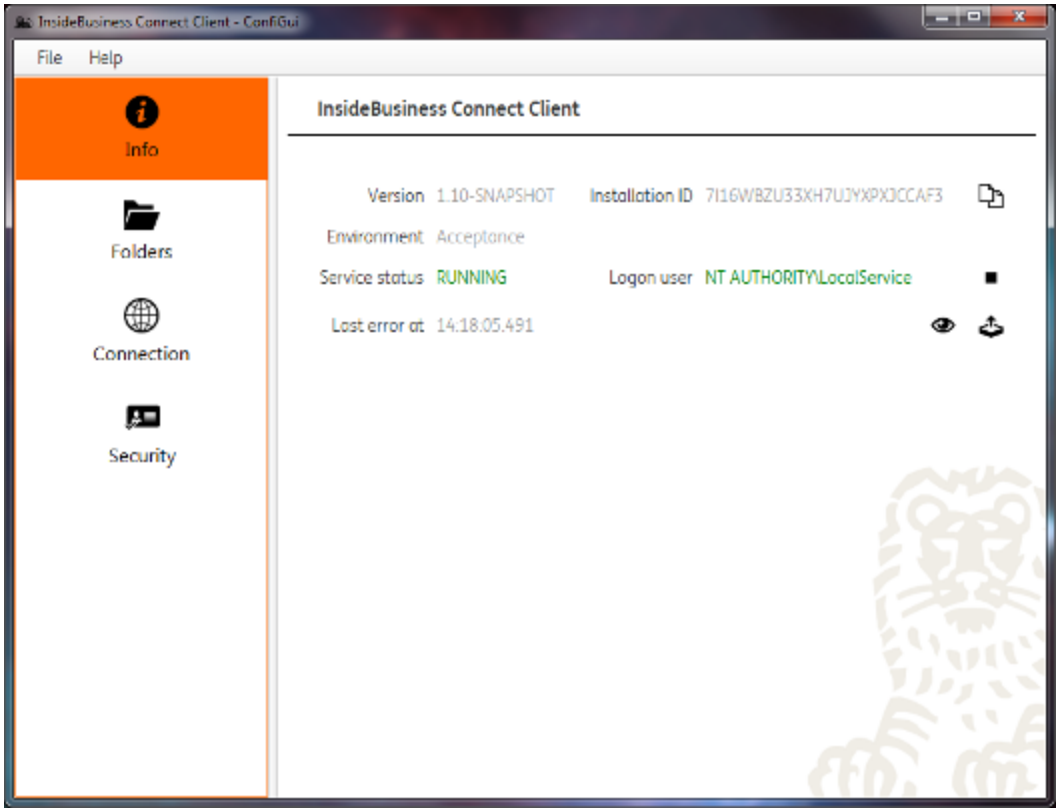


Main screen

The *Main screen* is divided into the following tabs:

- **Info**
- **Folders**
- **Connection**
- **Security**

Info



The *Info* tab displays the following information:

- **Version** - current running version of IBCC
- **Installation ID** - unique customer installation ID
- **Environment** - ING SFTP server endpoint
- **Service status** - running/stopping/stopped/starting
- **Logon user** - Windows user running the IBCC service
- **Last error log** - timestamp of the most recent IBCC service daily error

Notes:

- The *Save* prompt window pops up when starting the service if there are pending configuration changes. Press **OK** in order to accept.
- Once the IBCC service is started and running 3 folders are created (if not already existing) under the transfer directory: *upload*, *download* and *archive*.
- By default, the IBCC service will run under the default Windows *Local Service* user. This can be changed.
- IBCC service logs are archived daily.

Folders

The *Folders* tab displays the following elements:

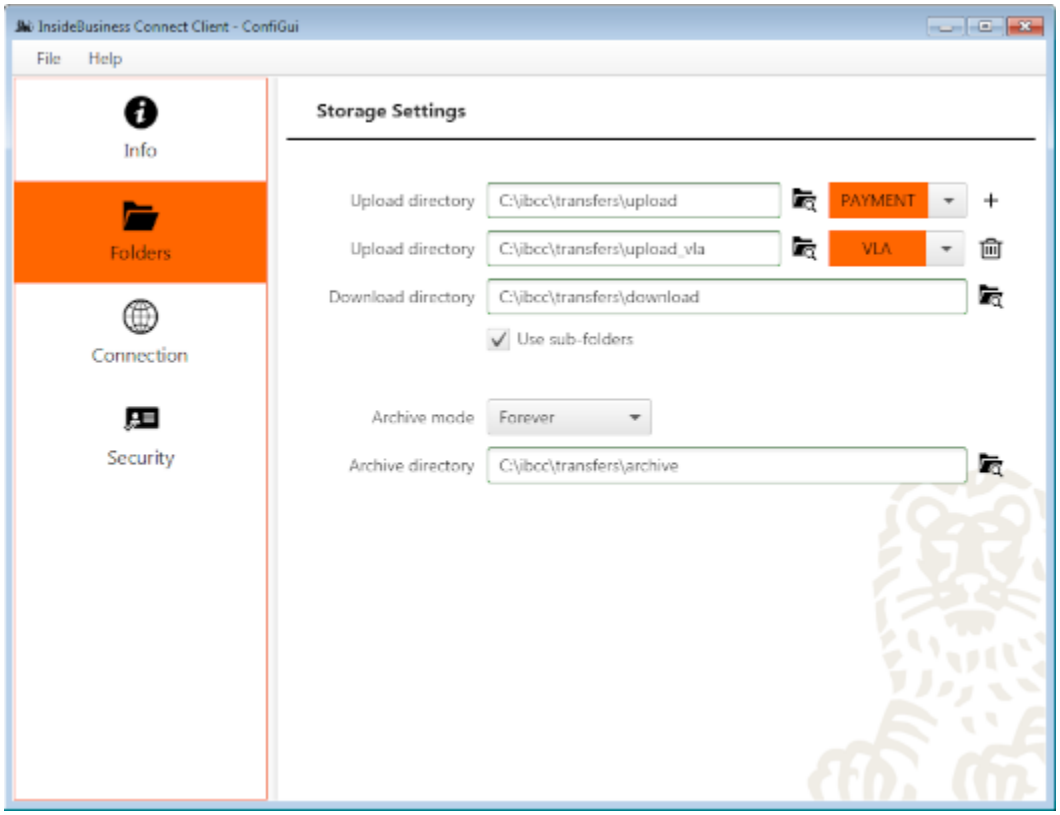
- **Upload directory** (editable text field)
- **Download directory** (editable text field)
- **Use subdirectories** - use same reporting folder structure as ING SFTP server (Default: **off**)
- **Archive mode** - data archiving behaviours:
    - **Forever**(Default) - files remain indefinitely in the archiving directory.

- **With retention time** - files will be deleted from the archiving directory if older than the given retention time (default: 168 hours). When selected, a text field shows on the right for the user to enter a retention time in hours.
- **Never** - files are deleted after successful upload and therefore never archived. *Archive directory* text field is hidden.

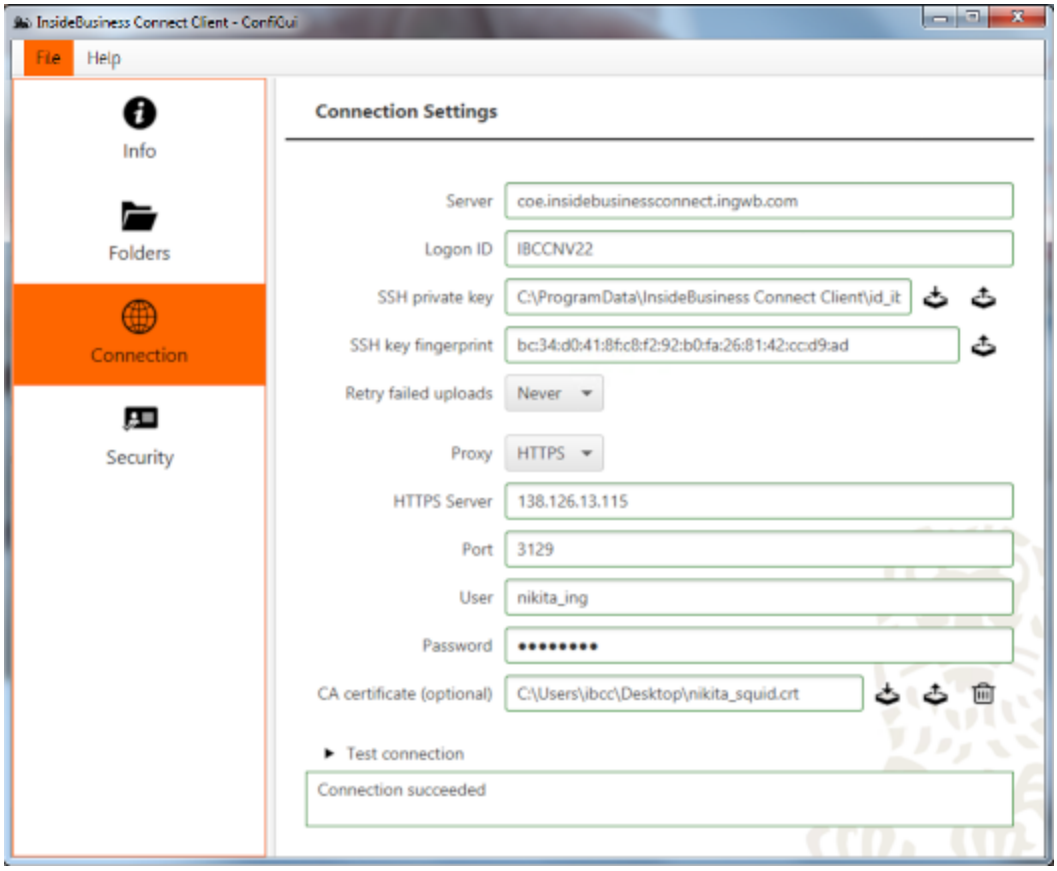
- **Archive directory** (editable text field)

Notes:

- Transfer folder text fields will be highlighted in red if the path is invalid or does not exist.
- If transfer folders are located on a network share, it is possible that the user running the Configuration GUI application (the currently logged on user) does not have access to the network share and cannot browse to it.



Connection



The *Connection* tab displays the following elements:

- **Server** - ING SFTP server endpoint
- **Logon ID** (editable text field)
- **SSH private key** - SSH authentication private key location
- **SSH key fingerprint** - SSH authentication public key fingerprint
- **Retry failed uploads** - retry mechanism behaviours:
  - **Never**(Default) - failed upload will not be retried and will remain in the **upload/error/** folder
  - **For delay** - failed uploads will be retried for a certain delay after which they will end up in the **upload/error/** folder
  - **Forever** - failed uploads will be retried forever and will never end up in the **upload/error/** folder
- **Proxy** - connection mode (HTTP | HTTPS | NO_PROXY)
  - **Server** - HTTP/S proxy endpoint
  - **Port** - HTTP/S proxy port
  - **User** - HTTP/S proxy username
  - **Password** - HTTP/S proxy password. **WARNING**: HTTP proxy accepts password unencrypted, exposing it to man-in-the-middle attacks. Use HTTPS for secure communication.
  - **CA certificate** - optional HTTPS proxy CA certificate. If left blank, the Windows system trust store is used.
- **Test connection** (Test connection result)

Important: The SFTP test connection process is ran by the currently logged on user (user running the GUI). This may be important when, e.g. running behind a proxy the user running the GUI needs to be able to access the proxy server (as well as the user running the service - *Logon user*). If the proxy is not reachable in that scenario, the test connection might time out or return an error. Solutions are described in the **Common Problems** section.

The *Connection* tab allows for the following configuration actions:

- **SFTP connection configuration:**
    - Import an SSH private key by pressing the *Import PRIVATE key* button. Select a private key in the file dialog. A matching *.pub* key should be present in the same directory.
    - Export the current SSH private key to the *Desktop* by pressing the *Export PRIVATE key* button. This file should NOT be sent to ING. It can be useful when migrating the IBCC installation to a different machine for instance.
    - Export the current SSH public key and fingerprint as a zip archive to the *Desktop* by pressing the *Export PUBLIC key and fingerprint* button. This file should be sent to ING after the initial setup as well as upon generation of a new SSH private key.
- **HTTP/S Proxy configuration:** if the customer machine is running behind a proxy, an appropriate configuration is needed.
    - To enable proxy management for the IBCC application, choose HTTP or HTTPS protocol in the *proxy* choice box.
    - When enabled, you can then configure the following:
        - HTTP/S proxy server (default: localhost).
        - HTTP/S proxy port (default for HTTP: 8080, for HTTPS: 443).
        - HTTP/S proxy user (Note: leave blank if the proxy does not require authentication, same for the below password).
        - HTTP/S proxy password (Note: the password will be obfuscated before saving it). **WARNING**: HTTP proxy accepts password unencrypted, exposing it to man-in-the-middle attacks. Use HTTPS for secure communication.
        - HTTPS proxy CA certificate (Note: Optionally import the proxy CA certificate file; otherwise only the Windows system trust store is used; the application does not perform certificate revocation checks).
        - Import proxy CA certificate by pressing the *Import HTTPS proxy CA certificate* button. Select a certificate in the file dialog.
        - Export the current proxy CA certificate to the *Desktop* by pressing the *Export HTTPS proxy CA certificate* button. It can be useful when migrating the IBCC installation to a different machine for instance.
        - Discard the current proxy CA certificate by pressing the *Discard HTTPS proxy CA certificate* button. Make sure to export and save the certificate for backup in advance. Without the CA certificate file, IBCC will use the Windows system trust store.

Notes:

- If the SSH private key is generated by **PuTTY Key Generator**, it has to be exported as PKCS#1 PEM (Namely: *Conversions* > *Export OpenSSH key*).
- A notice window pops up when importing an SSH private key before overriding the existing one. Press **OK** in order to continue.
- A prompt window pops up when importing a protected SSH private key, requesting customer password input. The password is obfuscated before saving it.
- A notice window pops up when exporting the current SSH private key to the users *Desktop* (*id_ibcc*).
- A notice window pops up when exporting the current SSH public key and fingerprint to the users *Desktop* (*IBCCPubExport_<logon id>_<environment>_<date>.zip*).

- When configuring the HTTPS proxy, first attempt to connect without providing any certificate. If the connection succeeds, no certificate is required. If you encounter SSL/certificate errors, provide the proxy's CA certificate. This is typically one of:
  - Corporate root CA certificate (most common in enterprise environments)
  - Proxy server's own certificate (if the proxy uses a self-signed certificate)
  - Intermediate CA certificate (if missing from the proxy's certificate chain)

  If the HTTPS proxy's certificate has a restricted Key Usage, it must include: digitalSignature, keyEncipherment or keyAgreement. If the Extended Key Usage specified, it must include: serverAuth. You can generate a suitable certificate and private key using the following OpenSSL command:

  ```
  $ openssl req -x509 -newkey rsa:2048 -days 730 \
  -keyout proxy.key -out proxy.crt \
  -subj "/CN=your-proxy-server-domain.com" \
  -addext "keyUsage=digitalSignature,keyEncipherment" \
  -addext "extendedKeyUsage=serverAuth"
  ```

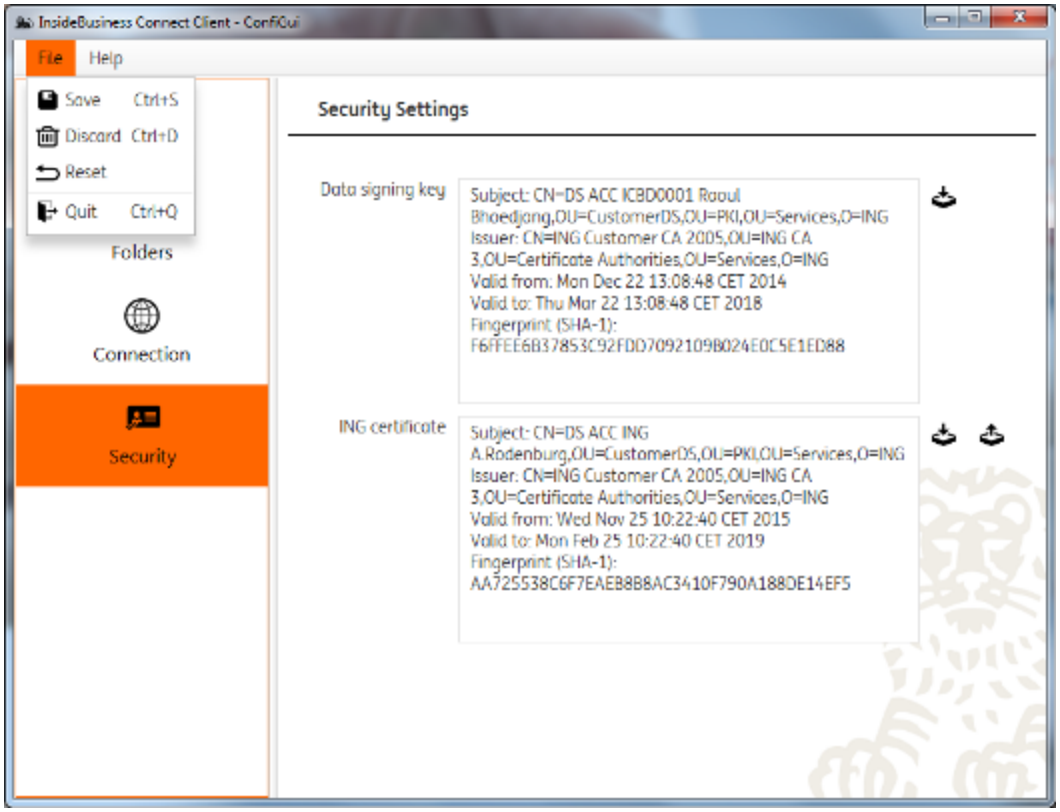
Security

The *Security* tab displays the following elements:

- **Data signing key** - used to sign content before uploading to ING SFTP Server.
  - Import a data signing key by pressing the *Import data signing key* button.
- **ING certificate**
  - Import an ING certificate by pressing the *Import ING certificate for current environment* button.
  - Export the current ING certificate by pressing the *Export ING certificate for current environment* button.

Notes:

- A prompt window pops up when importing a data signing key, requesting customer password input. The password is obfuscated before saving it.
- A notice window pops up when importing an ING certificate before overriding the existing one.
- A notice window pops up when exporting the current ING certificate to the users *Desktop* (*ING_cert_<Environment>.cer*).

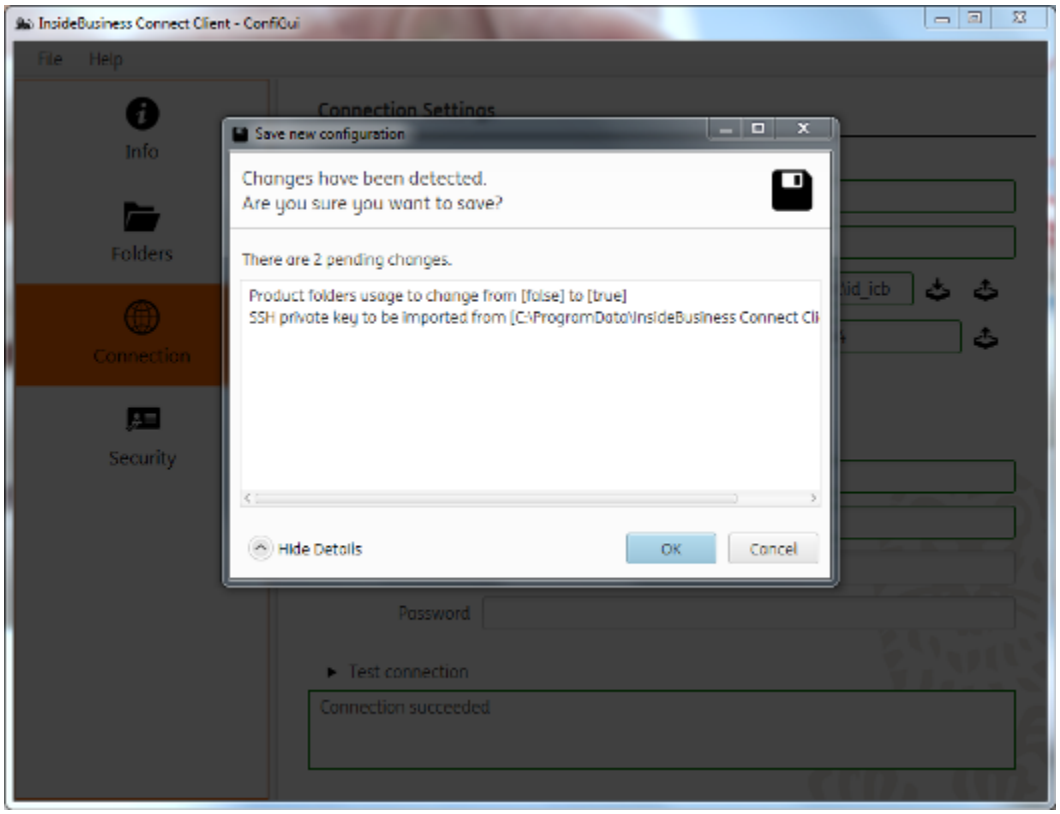


Menu bar

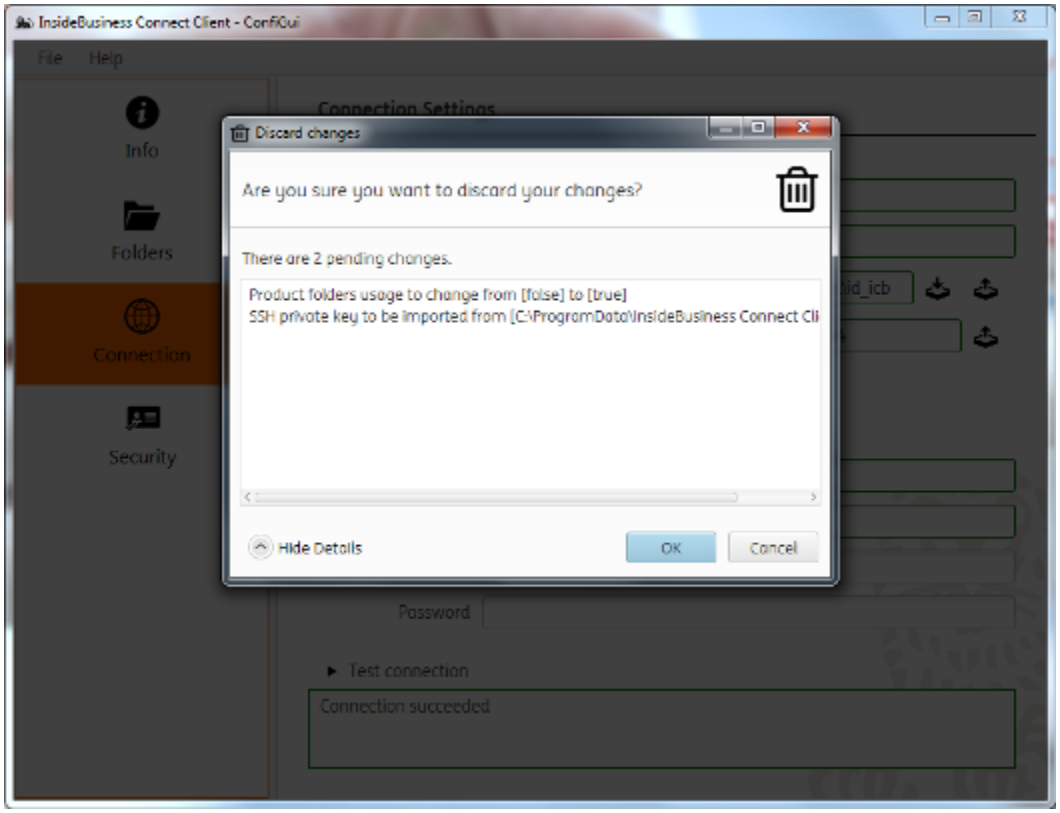
File

The *File* menu contains the following items:

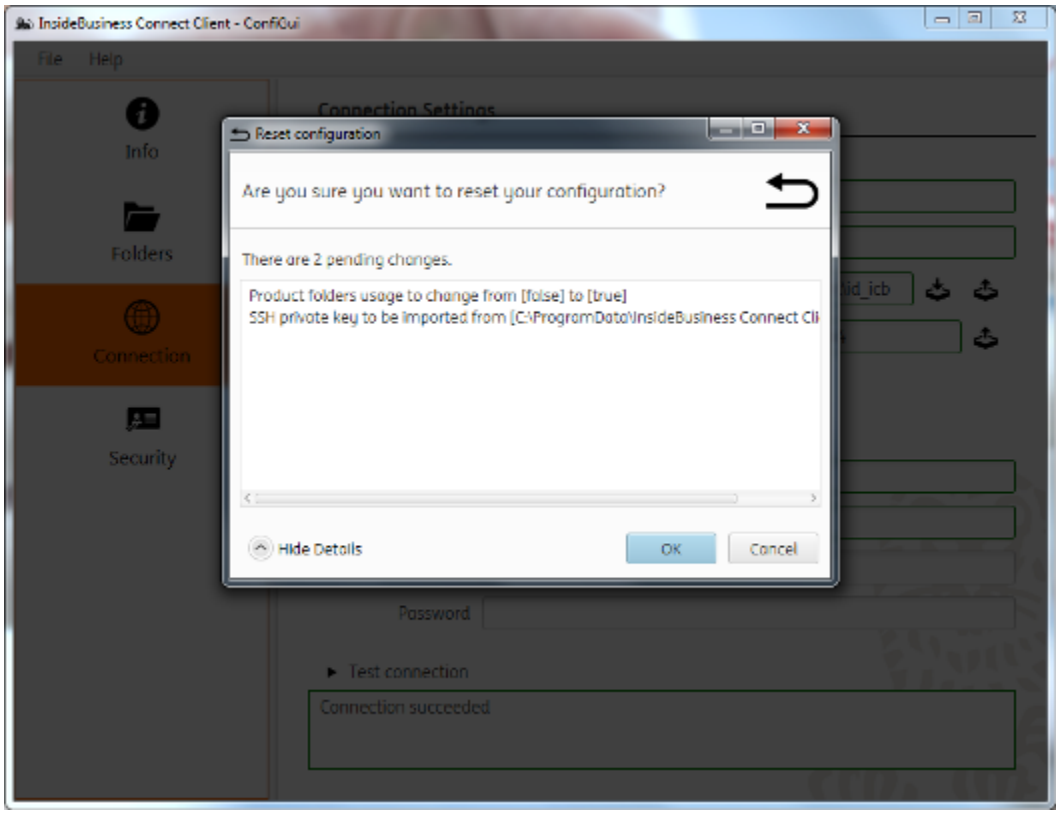
- **Save** - a prompt window pops up before saving all pending configuration changes to the properties file. Press **OK** in order to accept.



- **Discard** - a prompt window pops up before discarding all pending configuration changes. Press **OK** in order to accept.

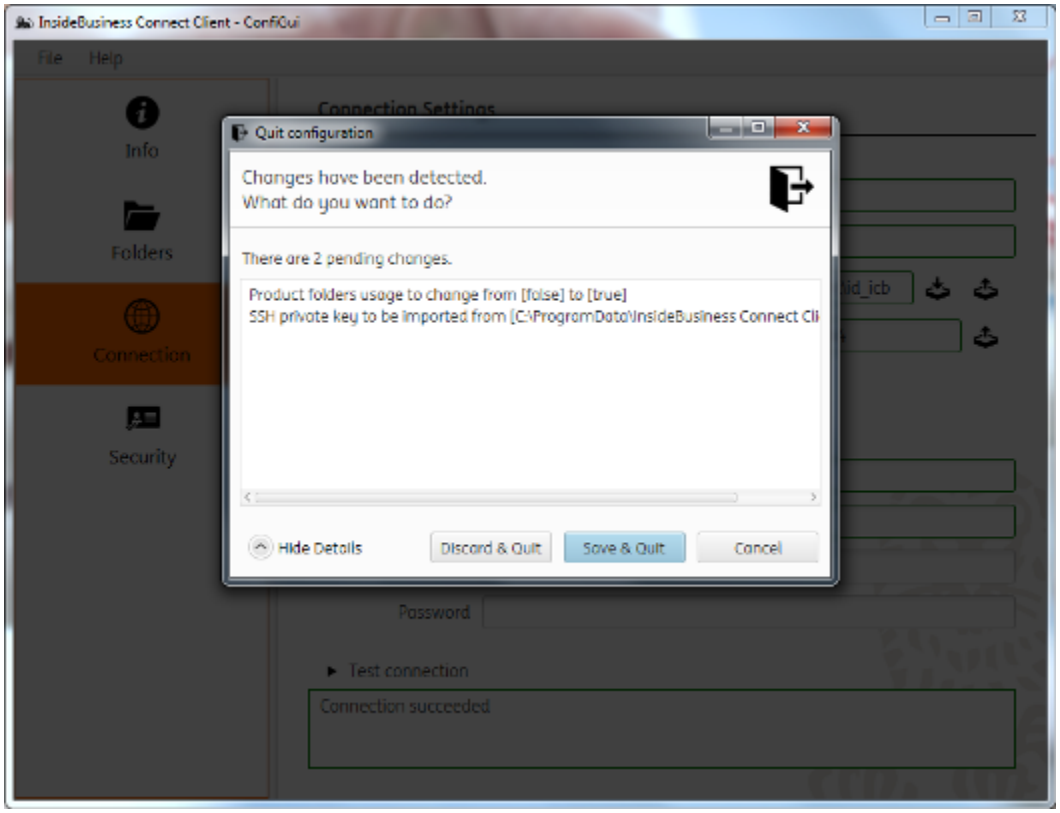


- **Reset** - a prompt window pops up before discarding all pending configuration changes and resetting the configuration to default. Press **OK** in order to accept.



- **Quit** - a prompt window pops up offering the following actions:

- **Discard and Quit** - discard all pending configuration changes and quit application.
- **Save and Quit** - save all pending configuration changes and quit application.



Note: the IBCC service will be restarted upon saving the configuration changes to the properties file.

Help

The *Help* menu contains the *IBCC Installation Guide* in the form of a web page. You can also open it using the shortcut F1.

Uninstalling

The IBCC provides the user with an *Uninstaller Wizard*.

Starting the uninstaller

The Uninstaller Wizard can be found in the *Programs and Features* entry in the *Control Panel*, or simply in the IBCC group *Start Menu* shortcut.

Namely: *InsideBusiness Connect Client > Uninstall InsideBusiness Connect Client*

The *User Access Control* window might pop up requesting confirmation.

Press **Yes** in order to continue.

Uninstallation process

The installation process of the IBCC is straightforward and is explained step by step below. The first screen is simply a confirmation of uninstallation.

Press **Next** in order to continue.

During the uninstallation a prompt window will appear inquiring whether to delete existing log files. Once that is decided upon a screen appears confirming the IBCC is successfully removed from your computer.

Press **Finish** in order to exit.

Note: In case the user wants to completely re-install the IBCC, he needs to have it successfully uninstalled first, otherwise the installer will start in update mode.

Updating

When a new release is available, launching its installation wizard will trigger an update of the already installed version. While running the update, several steps from the installation explained above are skipped.

Starting the updater

To start the installer for an update, run the new *IBCC_windows_{version}.exe* as an administrator.

Before the setup process begins, you might be prompted with a *User Account Control* window for confirmation.

Press **Yes** in order to continue.

Updating process

The first screen shown is the *Welcome Screen*.

Press **Next** in order to continue.

If a previous installation is detected, the user will be prompted with a confirmation screen in order to proceed with the update.

Press **Next** in order to continue.

By doing an update, the previous version is first uninstalled behind the scenes (but the configuration is kept as is), and the new one is installed. Once that is done a screen appears confirming the IBCC is updated and ready. The service is restarted automatically.

Press **Finish** in order to exit.

Troubleshooting

The IBCC service and configuration GUI will log data in the following directory:

%ProgramData%\InsideBusiness Connect Client\log

This is the first place to look in case of problems.

Common problems

The service does not start (either from the Configuration GUI or the Service Panel)

Most likely it is a permission issue. The Logon User does not have access to the transfer folders. If this is the case, inspecting the service logs (*daemon.log*), will reveal error messages such as **AccessDeniedException** or **FileAlreadyExistsException**. If no logging is available at that moment, refer to the next common problem *No logging is available*.

Solution: Either change the Logon User for a user that has access to the transfer folders, or explicitly give permissions to the current Logon User to have *Full Control* on the transfer folders.

No logging is available

When no logging data is available in the folder **%ProgramData%\InsideBusiness Connect Client\log** several causes can be possible.

- The logging config file points to a location that does not exist. **Solution:** edit the file **%ProgramData%\InsideBusiness Connect Client\log4j2.xml** and change the *file* value.
- The logging config file points to a location that the Logon User cannot access. **Solution:** give full control to the logging target location to the Logon User.

The above will likely occur when IBCC was updated from a version prior to **1.4**. Before version **1.4**, the logging location was in the transfer folder as well. After an update to version **1.4** or above, the Logon User was set to the default **Local Service** and this user might not have access to the target logging location set formerly in the transfer folder.

The IBCC service can connect to ING SFTP server but not the Configuration GUI

Sometimes the Configuration GUI *Test Connection* feature will return an error message, however the IBCC service runs fine and can connect to ING. This will most likely happen when using a proxy. The reason is that the current user that started the Configuration GUI cannot access the proxy server, but the Logon User can so the IBCC service runs fine.

Solution: Either start the Configuration GUI as the Logon User, or give the current user access to the proxy server.

Log messages

All the messages below are identified by a unique ID.

IBCC service

ID	Message

685b3162	An error occurred while loading the property file. The property file (*icb.properties*) from configuration directory is not present or not accessible.
930dd5b0	An error occurred while setting up the security context. Possible problems with ING or customer certificate (.pfx). Please see log file for detailed error.
059b657c	An error occurred while uploading IBCC service heartbeat. Possible problems with generating heartbeat content.
f233eec7	An error occurred while purging archive directory. Possible problems with service user access rights to transfer directory. Please check the IBCC service user.
d8092f56	An error occurred while signing the file. Possible problems with data-signing key (.pfx). Please see log file for detailed error.
51d9e0f0	An error occurred while encrypting the file. Possible problems with incompatible encryption algorithm or encoding. Please see log file for detailed error.
374f5b1f	Failed to decrypt file. The received file was not properly encrypted or encrypted with unexpected parameters. Please see log file for detailed error.
016c771a	Failed to verify file. The received file might have been signed by an untrusted source, or its signature is invalid. Please see log file for detailed error.
2159d07e	General upload error. Please investigate the logs for more detailed messages.
0787ae47	Failed SFTP connection while uploading file. Please investigate the logs for more detailed messages.
4cbcff29	Failed SFTP remote operation while attempting to upload a file. The requested remote directory might not exist or its access might be forbidden.
63468fca	Transfer was interrupted when uploading a file. It can be due to network or connectivity issues. Please see log file for detailed error.
4466f4db	General download error. Please investigate the logs for more detailed messages.
fcaab123	Failed SFTP connection while attempting to download file(s). Please investigate the logs for more detailed messages.
dea1ea2c	Failed SFTP remote operation while attempting to download file(s). The requested path might not exist or its access might be forbidden.
523c1d2c	Transfer was interrupted when downloading a file. It can be due to network or connectivity issues. Please see log file for detailed error.

Fallback scenario

Please contact ING for information regarding the fallback procedure.