Sterling Integrator®

SFTP

Version 5.0

Sterling Commerce
An IBM Company

Contents

SSH/SFTP Support in Application

Application includes adapters and services that enable you to work with trading partners using the SSH/SFTP protocol. SSH/SFTP is a widely used standard file transfer protocol. It is a de facto standard as implemented by SSH, OpenSSH, and others. You use the SSH/SFTP protocol to communicate between SFTP servers and SFTP clients.

SSH/SFTP has the following characteristics:

- Tunneled through SSH
- Widely deployed
- Used by modern scp (secure copy program) commands
- Firewall friendly (only one connection)

SSH/SCP is another protocol used to copy files between hosts on a network. It uses secsh for data transfer, and uses the same authentication and provides the same security as secsh. It requests passwords or passphrases if need for authentication.

The Application SFTP Server adapter and the SFTP Client adapter support:

- Version 2 SSH
- Version 3 SFTP protocol, as supported by OpenSSH
- Inbound scp commands using SSH/SCP protocol, as supported by OpenSSH
- Transfers of files 150 Gigabytes or more in size
- More than 150 concurrent inbound connections from trading partners to the SFTP Server adapter
- More than 50 concurrent outbound connections from the SFTP Client adapter to trading partners
- Ability to limit total concurrent sessions and sessions per user
- Failed login attempt tracking and user account locking
- Adapter access can be restricted to a selected user or group of users
- Four methods of required remote user authentication - password, public key, password or public key, or password and public key
- Importation of Host keys from OpenSSH format
- Known host verification that requires adding hosts administratively
- Resumption of transfers to and from the server
- Random file access, to allow transfer resumption

Application is compatible with most SFTP clients and SCP clients. The following clients have been tested and approved for interoperability with the SFTP Server adapter:

- Connect:Enterprise Secure Client (version 1.3.00)
- Connect:Enterprise Command Line Client (SFTP protocol version 3)
- OpenSSH (version sftp)
- GlobalSCAPE CuteFTP (professional version 7.0)
- Filezilla (version 2.2.10)

Note: To use Filezilla versions 2.2.11 through 2.2.26a, add the following phrase to the install/bin/tmp.sh file, in the JAVA_FLAGS parameter:

```
-Dfilezilla.bug.workaround=true
```

To correct a common misconception, SSH/SFTP is not:

- FTP over SSH
- Particularly like FTP at the protocol level

Licensing for SFTP

You must activate your license for the SFTP Server adapter prior to implementing SFTP or SCP.

Business Purpose for SSH/SFTP

SSH/SFTP provides an alternative means to exchange information with trading partners. The SSH/SFTP communications protocol has greater security than FTP. During an FTP session, your user name and password are transmitted in clear text. An eavesdropper can easily log your FTP user name and password. When using SSH/SFTP instead of FTP, the entire login session, including transmission of password, is encrypted, making it much more difficult for an outsider to observe and collect passwords.

By encrypting all traffic, SSH/SFTP effectively eliminates eavesdropping, connection hijacking, and other network-level attacks.

The SFTP Client adapter enables you to exchange files with trading partners who have SFTP servers. You can:

- Establish and terminate sessions
- Identify, navigate, and list the contents of directories
- Move files to, from, and within directories
- Delete files

The SFTP Server adapter enables trading partners with SFTP clients or SCP clients to exchange files with Application Mailboxes. To the external users, the Mailbox is a directory on which the user has privileges.

Using SFTP with Application Mailboxes

A *Mailbox* is a storage area for *messages*. Each message associates a name with some data (the data itself is stored in Application as a *document*.) Mailboxes are usually arranged in a hierarchy with the mailbox named “/” serving as the root.

Mailboxes in Application are analogous to the familiar directory structure offered by operating systems' file systems. A Mailbox is a directory and messages correspond to files in the directory.

Mailboxes are more feature rich than the normal file system. A mailbox can be configured to invoke a business process when a message is sent to it. Messages have well defined extractability policies that govern the conditions under which messages can be successfully extracted (retrieved).

The SFTP Server adapter uses Application Mailboxes as the repository. The prerequisites to using SSH/SFTP in Application are:

- One or more Mailboxes set up as the repository for SFTP
- Users with appropriate permissions to SFTP mailboxes
- A virtual root

Security for SSH/SFTP

Application provides features to enhance the security of file transfers using SSH/SFTP. For improved security, use the following:

- Limit login attempts (users are locked out if they exceed the limit)
- Limit concurrent logins for each user
- Limit total concurrent logins for server
- Require authentication with password and public key
- Restrict access to a certain user or group of users

Application limits the amount of information returned in response to most failed logins to prevent unauthorized users from obtaining information about the server that could be used to circumvent security. For example, if a user is not in the list of allowed users, the error is “access denied.” This avoids confirming the validity of the user to someone who may be attempting to use someone else’s credentials.

Authentication Using SSH/SFTP Keys

Authentication for SSH/SFTP connections is performed by the exchange of session keys for the server and the client. This assures that both parties know who they are exchanging data with.

Application uses passive key exchange. That is, whenever there is an action from the client side, the system checks to see if key exchange is needed. This works securely with a firewall configured to abort idle connections at a specified length of time.

There are two options for authentication, user ID and password or user ID and user key.

Sequence of events:

1. Client issues a request for connection.
2. Server responds with host signature. This must match the host key provided separately when establishing the trading partner relationship.
3. Client sends user ID and password and/or user ID and user signature, depending on the server requirements. If a user signature is required, it must match the key provided separately when establishing the trading partner relationship.
4. Server grants connection rights and a session key is generated.

Session keys are recreated after every one Gigabyte of transfer or every one hour, whichever comes first. This protects the security of SSH/SFTP transfers for large file transfers or long-lived sessions.

The following keys are used for the SFTP Client adapter to connect with a remote SFTP server:

- User Identity Key - Private/Public key pair used to identify Application as a user on a remote server. Generate this key within Application and provide the public part of the key to your trading partner.
- Known Host Key - Public key used to authenticate remote SFTP servers to the Application SFTP Client adapter. Request this key from your trading partner.

Note: You cannot create a user identity key and a host identity key with the same name.

The following keys are used for the SFTP Server adapter to allow connections from remote clients:

- Authorized User Key - Public key used to authenticate remote users to Application SFTP Server adapters. Request this key from your trading partner and include it in their user account in Application.
- Host Identity Key - Private/Public key pair used to identify the Application SFTP Server adapter to remote clients. Generate this key within Application.

SSH/SCP Support in Application

Application includes an adapter that enables you to work with trading partners using the SSH/SCP protocol. Secure copy program (SSH/SCP) copies files between hosts on a network. It uses secure shell encryption (secsh) for data transfer, and uses the same authentication and provides the same security as secsh. It requests passwords or passphrases if needed for authentication. Application can accept inbound scp commands from SCP clients when the SFTP Server adapter is configured to enable the SSH/SCP protocol.

The Application SFTP Server adapter supports:

- Version 2 SSH
- Version 3 SFTP protocol, as supported by OpenSSH
- Inbound scp commands using SSH/SCP protocol, as supported by OpenSSH
- Transfers of files 150 Gigabytes or more in size
- More than 150 concurrent inbound connections from trading partners to the SFTP Server adapter
- Ability to limit concurrent sessions in total and per user
- Failed login attempt tracking and user account locking
- Adapter access can be restricted to a selected user or group of users
- Four methods of required remote user authentication - password, public key, password or public key, or password and public key
- Importation of Host keys from OpenSSH format
- Known host verification that requires adding hosts administratively
- Resumption of transfers to and from the server
- Random file access, to allow transfer resumption

The SSH/SCP protocol has the following limitations:

- Does not support resumption
- Supports only copy operations
- Does not support list, rename, or delete

Application is compatible with most SCP clients. The following clients have been tested and approved for interoperability with the SFTP Server adapter:

- Connect:Enterprise Secure Client (version 1.3.00)
- Connect:Enterprise Command Line Client (SFTP protocol version 3)
- OpenSSH (version sftp)
- GlobalSCAPE CuteFTP (professional version 7.0)
- Filezilla (version 2.2.10)

Note: To use Filezilla versions 2.2.11 through 2.2.26a, add the following phrase to the install/bin/tmp.sh file, in the JAVA_FLAGS parameter:

```
-Dfilezilla.bug.workaround=true
```

Licensing for SFTP

You must activate your license for the SFTP Server adapter prior to implementing SFTP or SCP.

Business Purpose for SSH/SCP

SSH/SCP provides an alternative means to exchange information with trading partners who do not have SFTP clients. The SFTP Server adapter enables trading partners with SCP clients to exchange files with Application Mailboxes. To the external users, the Mailbox is a directory on which the user has privileges.

Using SCP with Application Mailboxes

A *Mailbox* is a storage area for *messages*. Each message associates a name with some data (the data itself is stored in Application as a *document*.) Mailboxes are usually arranged in a hierarchy with the mailbox named "/" serving as the root.

Mailboxes in Application are analogous to the familiar directory structure offered by operating systems' file systems. A Mailbox is a directory and messages correspond to files in the directory.

Mailboxes are more feature rich than the normal file system. A mailbox can be configured to invoke a business process when a message is sent to it. Messages have well defined extractability policies that govern the conditions under which messages can be successfully extracted (retrieved).

The SFTP Server adapter uses Application Mailboxes as the repository. The prerequisites to using SSH/SCP in Application are:

- One or more Mailboxes set up as the repository for SCP
- Users with appropriate permissions to SCP mailboxes
- Create a virtual root

Security for SSH/SCP

Application provides features to enhance the security of file transfers using SSH/SCP. For improved security, use the following:

- Limit login attempts (users are locked out if they exceed the limit)
- Limit concurrent logins for each user
- Limit total concurrent logins for server
- Require authentication with password and public key
- Control which users can access each server

Application limits the amount of information returned in response to most failed logins to prevent unauthorized users from obtaining information about the server that could be used to circumvent security. For example, if a user is not on the list of allowed users, the error is "access denied." This avoids confirming the validity of the user to someone who may be attempting to use someone else's credentials.

Authentication Using SSH Keys

Authentication for SSH/SCP connections is performed by the exchange of session keys for the server and the client. This assures that both parties know who they are exchanging data with.

Application uses passive key exchange. That is, whenever there is an action from the client side, the system checks to see if key exchange is needed. This works securely with a firewall configured to abort idle connections at a specified length of time.

There are two options for authentication, user ID and password or user ID and user key.

Sequence of events:

1. Client issues a request for connection.
2. Server responds with host signature. This must match the host key provided separately when establishing the trading partner relationship.
3. Client sends user ID and password or user ID and user signature, depending on the server requirements. If a user signature is required, it must match the key provided separately when establishing the trading partner relationship.
4. Server grants connection rights and a session key is generated.

Session keys are recreated after every one Gigabyte of transfer or every one hour, whichever comes first. This protects the security of SSH/SCP transfers for large file transfers or long-lived sessions.

The following keys are used for the SFTP Server adapter to allow connections from remote clients:

- Authorized User Key - Public key used to authenticate remote users to Application SFTP Server adapters. Optionally, request this key from your trading partner and include it in their user account in Application.
- Host Identity Key - Private/Public key pair used to identify the Application SFTP Server adapter to remote clients. Generate this key within Application.

Setting Up the SFTP Client Adapter

Use the SFTP Client adapter to connect to a trading partner's SFTP server. The major features of the SFTP Client adapter are:

- Uses perimeter services
- Commands are scriptable through BPML
- Works easily with most SFTP servers
- Accessed in a business process through the following services:
  - SFTP Client Begin Session service
  - SFTP Client CD service
  - SFTP Client DELETE service
  - SFTP Client End Session service
  - SFTP Client GET service
  - SFTP Client LIST service
  - SFTP Client MOVE service
  - SFTP Client PUT service
  - SFTP Client PWD service

How the SFTP Client Adapter Works

The SFTP Client adapter establishes a session with an external trading partner's SFTP server in the following sequence:

1. The SFTP Client adapter initiates an SSH2 connection.
2. The SFTP server accepts the connection.
3. The SFTP Client adapter negotiates user authentication with the trading partner SFTP server. A user ID and either a password or user signature, depending on the server requirements, are supplied in the business process. If a user signature is required, it is encoded by the private key and can only be decoded by the public key provided when establishing the relationship with the trading partner.
4. The SFTP server logs the user into the home directory associated with the specified user ID.
5. Data can now be exchanged between Application and the external SFTP server.
6. Use the SFTP Client adapter to send SFTP requests to perform activities such as to *put* or *get* files into a directory on the trading partner's SFTP server through perimeter services.

To use the SFTP Client adapter:

- *Generate a New SSH User Identity Key* on page 13 or *Check In an SSH User Identity Key* on page 14
- *Check In Known Host Key* on page 14
- *Exchange Information With the SFTP Trading Partner* on page 14

- *Configure a Perimeter Server for Use with the SFTP Client Adapter* on page 15
- *Configure an SFTP Client Adapter* on page 15
- *Set Up Trading Partner Profiles for SSH/SFTP* on page 15
- *Use SFTP Client Services in Business Processes* on page 16

Generate a New SSH User Identity Key

To generate a new SSH User Identity Key:

1. Select **Trading Partners > SSH > User Identity Key**.
2. Next to **Create new User Identity Key**, click **Go!**
3. Type a **Key Name**, using no spaces or special characters.

   You cannot create a user identity key and a host identity key with the same name.
4. Select the **Key Type** from the following options:
   - rsa1
   - ssh-rsa
   - ssh-dsa
5. Select the **Key Length** from the following options:
   - 768
   - 1024
   - 1536
   - 2048

   The longer the key length, the more secure the key is.
6. Type any **Comments** associated with this key. Comments are not required.
7. Click **Next**.
8. Confirm your entries and click **Finish**.

Check Out an SSH User Identity Key

To check out the key and save it to a file, suitable for sending to a trading partner:

1. Select **Trading Partners > SSH > User Identity Key.**
2. Locate the key by searching or listing.
3. Select **check out** next the key.
4. From the popup window, select the check out format from the following options:
   - SECSH
   - OpenSSH

5. Click **Go!**
6. Download the file and save it to your computer.
7. Provide it to your trading partner. See *Exchange Information With the SFTP Trading Partner* on page 14.

Check In an SSH User Identity Key

Note: You do not need to check in keys generated from within Application.

To check in an existing SSH User Identity Key from a file:

1. Select **Trading Partners > SSH > User Identity Key**.
2. Next to **Check in User Identity Key**, click **Go!**
3. Type the **Key Name** and **Passphrase**. Do not use spaces or special characters. To check in a key that is not passphrase protected, type any few characters in the passphrase field so it is not blank.
4. Browse for the file containing the key.
5. Click **Next**.
6. Confirm your entries and click **Finish**.

Check In Known Host Key

Obtain the public part of an SSH Known Host Key from the trading partner for the SFTP server you will connect to.

To check in an SSH Known Host Key from a file:

1. Select **Trading Partners > SSH > Known Host Key**.
2. Next to **Check in SSH Host Identity Key**, click **Go!**
3. Type the **Key Name**. Do not use spaces or special characters.
4. Browse for the **Public Key Filename** for the file containing the key.
5. Ensure **Enabled** is selected.
6. Click **Next**.
7. Confirm your entries and click **Finish**.

Exchange Information With the SFTP Trading Partner

To prepare to connect to an external trading partner’s SFTP server, you must obtain certain information about the server from the trading partner. You must also provide them the public part of your User Identity Key, if using public key authentication.

Use the following worksheet to record the configuration information. After you collect this information, refer to *Set Up Trading Partner Profiles for SSH/SFTP* on page 15.

Worksheet for a Trading Partner's SFTP Server
Host/IP address of server:
Port number of server:
Location and name of the Known Host Key:
User name on the trading partner's server:
Preferred Authentication Type - Password or Public Key:
SSH Password
Directory
Compression
Connection Retry Count
Retry Delay (secs)
Response Timeout (secs)
Local Port Range
Provide the location or file for the public part of your User Identity Key to the trading partner.

Configure a Perimeter Server for Use with the SFTP Client Adapter

A perimeter server is communications management software that is installed in a DMZ of a company network. A perimeter server and its client manage communication flow between the perimeter network and the Application adapters. To use SFTP to send and receive data from external trading partners, you must set up perimeter services.

Configure an SFTP Client Adapter

See *Configuring the SFTP Client Adapter*.

Set Up Trading Partner Profiles for SSH/SFTP

To set up a Trading Partner profile:

1. Select **Trading Partners** > **SSH** > **Remote Profiles**.
2. Next to **Create**, click **Go!**
3. Complete the fields using the information collected using the worksheet from *Exchange Information With the SFTP Trading Partner* on page 14.
4. Check in the **Known Host Key** using the file identified on the worksheet.

5. Click **Next**.
6. Confirm your information and click **Finish**.

Use SFTP Client Services in Business Processes

After you configure and set up the SFTP Client adapter to exchange files with a trading partner's SFTP server, build business processes that include the services provided by the SFTP Client adapter. The available services offer the following functionality:

SFTP Client Service	Functionality
SFTP Client Begin Session service	Starts an SFTP session with an external trading partner for the purpose of exchanging business documents
SFTP Client CD service	Changes directories on the trading partner's SFTP server
SFTP Client DELETE service	Deletes a document in a specified directory on the trading partner's SFTP server
SFTP Client End Session service	Ends an SFTP session with an external trading partner **Note:** Ensure business processes using the SFTP Client Begin Session service always call SFTP Client End Session service, even in error situations. If the End Session service is not called, the session will remain visible in the Service Activity Monitor until Application is restarted.
SFTP Client GET service	Retrieves a document in a specified directory on the trading partner's SFTP server
SFTP Client LIST service	Retrieves a list of files on a specified directory on the trading partner's SFTP server
SFTP Client MOVE service	Moves or renames a document in a specified directory on the trading partner's SFTP server
SFTP Client PUT service	Places a document in a specified directory on the trading partner's SFTP server
SFTP Client PWD service	Retrieves the present working directory on the trading partner's SFTP server

SSH User Identity Keys

Listing SSH User Identity Keys

To list the SSH User Identity Keys:

1. Select **Trading Partners > SSH > User Identity Key.**
2. Next to **List**, Select **ALL** or a letter from the list. Click **Go!**

Deleting SSH User Identity Keys

To delete a key so it can no longer be used:

1. Select **Trading Partners** > **SSH** > **User Identity Key.**
2. Locate the key by searching or listing.
3. Clear the **Enable** box.
4. Click **Delete**.
5. Confirm the key to delete, and click **Delete**.

SSH Known Host Keys

Listing SSH Known Host Keys

To list the SSH Known Host Keys:

1. Select **Trading Partners** > **SSH** > **Known Host Key**.
2. Next to **List**, Select **ALL** or a letter from the list. Click **Go!**

Checking Out an SSH Known Host Key

To check out a key and save it to a file, suitable for sending to a trading partner:

1. Select **Trading Partners** > **SSH** > **Known Host Key**.
2. Locate the key by searching or listing.
3. Select **check out** next the key.
4. From the popup window, select the check out format from the following options:
   - SECSH
   - OpenSSH
5. Click **Go!**
6. Download the file and save it to your computer.

Deleting SSH Known Host Keys

To delete an SSH Known Host key so it can no longer be used:

1. Select **Trading Partners** > **SSH** > **Known Host Key**.
2. Locate the key by searching or listing.
3. Clear the **Enable** box.
4. Click **Delete**.
5. Confirm the key to delete, and click **Delete**.

Setting Up the SFTP Server Adapter

Use the SFTP Server adapter to enable external SFTP clients to *put* files into a Mailbox or *get* files from a Mailbox. The client must have a Application user account with an Authorized User Key or password and an associated Mailbox with read and write privileges. If the server requires an Authorized User Key, the trading partner must provide you with the public part of their Authorized User Key in advance.

How the SFTP Server Adapter Works

The SFTP Server adapter establishes a session in the following sequence:

1. An external trading partner's SFTP client initiates an SSH2 connection.
2. The external SFTP client negotiates user authentication by providing their user ID and password and/or user ID and user signature, depending on server requirements. If a user signature is used, it must match the key registered to the user.
3. The SFTP Server adapter compares the current number of logins to the maximum number of allowed logins. If an additional login is available, the SFTP Server adapter accepts the connection and responds with the host signature.
4. The SFTP Server adapter compares the user ID to the list of users enabled to access this server. If the user is not on the list, the connection is rejected and no additional information about the failure is provided. This prevents unauthorized users from obtaining information that could be used to access the server illegitimately.
5. The SFTP Server adapter compares the number of logins of the requesting user to the maximum allowed logins per user. If an additional login is available, the SFTP Server adapter logs the user into the Mailbox associated with the specified user ID.
6. Files are exchanged between Application and the external SFTP client using standard SFTP commands.

To use the SFTP Server adapter:

- *Generate a New SSH Host Identity Key* on page 18 or *Check In an SSH Host Identity Key* on page 19
- *Check In an SSH Authorized User Key* on page 19
- *Set up a Mailbox in Application* on page 20
- *Set up a User Account* on page 20
- *Set the Mailbox Properties File* on page 20
- *Configure a Perimeter Server for Use with the SFTP Server Adapter* on page 20
- *Provide Information About the SFTP Server to Trading Partners* on page 21
- *Accept Requests From Trading Partner's SFTP Clients* on page 21

Generate a New SSH Host Identity Key

To generate a new SSH Host Identity Key:

1. Select **Deployment > SSH Host Identity Key**.
2. Next to **Create new SSH Host Identity Key**, click **Go!**
3. Type a **Host Name**, using no spaces or special characters.
4. Select the **Key Type** from the following options:
   - rsa1
   - ssh-dsa
   - ssh-rsa
5. Select the **Key Length** from the following options:
   - 768
   - 1024
   - 1536
   - 2048

   The longer the key length, the more secure the key is.
6. Type any **Key Comments** associated with this key. Comments are not required.
7. Click **Next**.
8. Confirm your entries and click **Finish**.

Note: You do not need to check in keys generated from within Application.

Check In an SSH Host Identity Key

To check in an existing SSH Host Identity Key from a file:

1. Select **Deployment > SSH Host Identity Key**.
2. Next to **Check in New Host Identity Key**, click **Go!**
3. Type the **Name** and **Passphrase**. Do not use spaces or special characters.
4. Browse for the file containing the key.
5. Click **Next**.
6. Confirm your entries and click **Finish**.

Check In an SSH Authorized User Key

Obtain the public portion of an SSH Authorized User Key from the trading partner for the SFTP clients you are enabling to connect to the SFTP Server adapter.

To check in an SSH Authorized User Key from a file:

1. Select **Trading Partner > SSH > Authorized User Key**.
2. Next to **Check in Authorized User Key**, click **Go!**
3. Type the **Key Name**. Do not use spaces or special characters.

4. Browse for the file containing the key.
5. Click **Next**.
6. Confirm your entries and click **Finish**.

You will use this key to *Set up a User Account* on page 20.

Set up a Mailbox in Application

The SFTP Server adapter uses Application Mailboxes as the repository. To use SSH/SFTP in Application:

- Set up one or more Mailboxes as the repository for SFTP
- Assign users appropriate permissions to SFTP mailboxes
- Create a virtual root

Set up a User Account

Before your trading partners can access your Application from an SFTP client, your administrator must add user accounts for them with the right permissions. For an SFTP client, these permissions include access to one or more Application Mailboxes set up exclusively for them. A user account includes a user ID and password or user ID and user key. If public key authentication is required, the user account must include the authorized user key.

Set the Mailbox Properties File

Set the following value in your mailbox.properties file:

```
disallowDuplicateMessages=true
```

This ensures that every message in a single mailbox has a unique name. It also ensures that a message and a mailbox do not have the same name. If you write a message to a mailbox and the name matches the name of a message in the mailbox, the service deletes the old message before adding the new message.

Configure a Perimeter Server for Use with the SFTP Server Adapter

A perimeter server is communications management software that is installed in a DMZ of a company network. A perimeter server and its client manage communication flow between the perimeter network and the Application adapters. To use SFTP to receive data from external trading partners, you must set up perimeter services. Refer to setting up perimeter services in the Application online library for complete details and procedures.

Configure an SFTP Server Adapter

See *Configuring the SFTP Server Adapter*.

Provide Information About the SFTP Server to Trading Partners

To prepare to accept connections from an external trading partner's SFTP client, you must provide certain information about the server (the SFTP Server adapter) to the trading partner. Use the following worksheet to record the configuration information. Provide this information to your trading partner.

Worksheet for an SFTP Server Adapter
Host/IP address of server:
Port number of server:
Location and name of the public part of your Host Identity Key:
Trading partner's Application User ID:
SSH Password
Compression

Accept Requests From Trading Partner's SFTP Clients

Now that you have set up and configured the SFTP Server adapter and provided information to your trading partners, you can accept requests to exchange data from your trading partners. When an external trading partner's SFTP client initiates an SSH2 connection, the SFTP Server adapter verifies the authentication presented against the server requirements. If the user is on the list of users authorized to access the server, the Server adapter verifies that there is an available concurrent session for the user and grants access.

Duplicate Message Names

If Application receives a request to add a message, and the request specifies that the message must not already exist (write-create-exclude), and the message already exists, Application returns an error to the SFTP client indicating that the file already exists.

Note: This applies whether Application is configured to allow or disallow duplicate messages.

Transfer Resumption

By default, transfer resumption is off. You can edit the sftp.properties file to change the default behavior. To enable listing documents that are in the staging area, set listStagedDocuments=True (default is False). See *Configuring the sftp.properties File* on page 25.

If transfer resumption is enabled and a transfer is interrupted, resulting in an incomplete document, transfer resumption allows completion of the transfer. To support transfer resumption, the SFTP Server adapter keeps partial documents in a temporary document staging area. This allows SFTP clients to resume a transfer within a specified amount of time. If the transfer is not resumed within the specified time, the partial document is removed from the staging area (by the Partial Document Clean Up service) and is no longer available for resumption.

A common behavior among SFTP clients before resuming a transfer is to request a list of the directory contents. In response to list requests, the default behavior is for the SFTP Server adapter to return a listing that includes:

- Complete documents in the target mailbox
- Partial documents in the staging area

Note: Partial documents are owned by a particular user. Application only displays partial documents to the user by whom they are owned. If two documents with the same name exist in both the mailbox and the document staging area, only the partial document in the staging area is displayed.

If the SFTP Server adapter is configured to use extractability count, aborted message retrievals decrement the extractability count. If the count has gone to zero prematurely, you can modify the count number by editing the extractable count parameter of the message.

The SFTP Server adapter does not support moving partially uploaded messages. You must complete the upload to move a message.

Mailbox Document Storage

Application Mailbox is an access controlled, hierarchical, content management, delivery, and distribution facility. Communications protocols such as SSH/SFTP traditionally interface to the native file system. In Application, these protocols interface with the Mailbox system. The benefits to this are the following:

- Scalability
- Same syntax and semantics on every operating system
- Users do not have operating system privileges, only Mailbox privileges, which simplifies security
- Eliminates the need for polling, improving performance
- Guarantees never routing incomplete or corrupt files or documents

Wildcards are not supported for mailboxes, but are supported for message names.

For SFTP, Application can use File system or Database for Mailbox document storage.

SSH Host Identity Keys

Listing SSH Host Identity Keys

To list the SSH Host Identity Keys:

1. Select **Deployment** > **SSH Host Identity Key**.
2. Next to **List**, Select **ALL** or a letter from the list. Click **Go!**

Checking Out an SSH Host Identity Key

To check out a key and save it to a file, suitable for sending to a trading partner:

1. Select **Deployment** > **SSH Host Identity Key**.
2. Locate the key by searching or listing.

3. Select **check out** next to the key.
4. From the popup window, select the check out format from the following options:
   - SECSH
   - OpenSSH
5. Click **Go!**
6. Download the file and save it to your computer.

Deleting SSH Host Identity Keys

To delete a key so it can no longer be used:

1. Select **Deployment** > **SSH Host Identity Key**.
2. Locate the key by searching or listing.
3. Clear the **Enable** box.
4. Click **Delete**.
5. Confirm the key to delete, and click **Delete**.

SSH Authorized User Keys

Obtain an SSH Authorized User Key from the trading partner for the SFTP server you will connect to.

Checking In an SSH Authorized User Key

To check in an SSH Authorized User Key from a file:

1. Select **Trading Partner** > **SSH** > **Authorized User Key**.
2. Next to **Check in Authorized User Key**, click **Go!**
3. Type the **Key Name**. Do not use spaces or special characters.
4. Browse for the file containing the key.
5. Click **Next**.
6. Confirm your entries and click **Finish**.

Listing SSH Authorized User Keys

To list the SSH Host Identity Keys:

1. Select **Trading Partner** > **SSH** > **Authorized User Key**.
2. Next to **List**, Select **ALL** or a letter from the list. Click **Go!**

Checking Out an SSH Authorized User Key

To check out a key and save it to a file, suitable for sending to a trading partner:

1. Select **Trading Partner** > **SSH** > **Authorized User Key**.

2. Locate the key by searching or listing.
3. Select **check out** next to the key.
4. From the popup window, select the check out format from the following options:
   - SECSH
   - OpenSSH
5. Click **Go!**
6. Download the file and save it to your computer.

Deleting SSH Authorized User Keys

To delete a key so it can no longer be used:

1. Select **Trading Partner > SSH > Authorized User Key**.
2. Locate the key by searching or listing.
3. Clear the **Enable** box.
4. Click **Delete**.
5. Confirm the key to delete, and click **Delete**.

Managing SSH/SFTP

Configuring the sftp.properties File

The sftp.properties file in the properties directory provides settings for the SFTP Client adapter and the SFTP Server adapter. Change the default settings when you want to:

- Provide a company-specific banner message when an SFTP client logs in to your SFTP Server adapter
- Enable transfer resumption by listing documents that are in the temporary document staging area as part of list requests
- Change the interval for forced key exchange

To configure the sftp.properties file, perform the following steps:

1. Locate the sftp.properties.in file in the properties directory where you installed Application.
2. Open the sftp.properties.in file in a text editor.
3. Configure the properties according to the following table:

Property	Description
BannerMessage	Indicates the message displayed when an SFTP Client logs in. Supports messages with multiple lines if desired. Example: BannerMessage=Application SFTP Server \n \ line 2 \n\ line 3 \n\ end of banner
listStagedDocuments	Indicates whether or not partial documents held in a temporary document staging area on the server should be included in list requests. Valid values: True - Partial documents are listed and transfer can be resumed False (default) - Transfer resumption is disabled
defaultKeyUpdateDataSize	Specifies a data unit for forced key exchange from client to server. Works in conjunction with defaultKeyUpdatePeriod. Valid values are any integer with: G = gigabyte M = megabyte K = kilobyte Default is 1G. With the default settings, if new activity occurs, the client performs another key exchange with the server to refresh the session key each hour or each gigabyte transferred, whichever occurs first.
defaultKeyUpdatePeriod	Specifies an interval in milliseconds for forced key exchange from client to server. Works in conjunction with defaultKeyUpdateDataSize. Default is 3,200,000 ms (one hour). With the default settings, if new activity occurs, the client performs another key exchange with the server to refresh the session key each hour or each gigabyte transferred, whichever occurs first.

Enabling Failed Login Tracking and Account Locking

You can track and limit the number of failed login attempts by a user, and lock the user account to prevent further attempt. To enable failed login tracking:

1. Edit the ui.properties.in file.
2. Set a numeric value for the ConsecFailedAttempts property.
3. If a user exceeds the specified number of failed login attempts, the user account is locked and must be reset before access is granted in a subsequent successful login.

SFTP Adapter Activity Monitoring (Current Activities Page)

The Current Activities page (**Business Process > Current Activities**) enables you to monitor activity of the SFTP Server and SFTP Client adapters. When you select an adapter to monitor, Application displays activity detail occurring on the adapter. The following types of activities are reported about the SFTP adapters:

- Put - Adds a file to a Application mailbox or to a trading partner directory
- Get - Retrieves a file from a Application mailbox or from a trading partner directory
- Session - Displays the presence of a session

SFTP Correlation Search

The SFTP Server adapter and the SFTP Client adapter and its related services write Application correlation records to enable searches for documents containing the following correlation identifiers:

Identifier	Valid Values
ACTION	Put, Get
Direction	outbound, inbound
Protocol	SFTP
RemoteHostAddress	remoteAddress
RemoteHostName	remoteHost
Username	username

SFTP Logs

To view logs of SFTP activity:

1. From the Administration menu, select Operations > System > Logs.
2. Under Application Logs, select from the following:
   - SFTP Client Adapter and Services

- SFTP Common Log
- SFTP Server Adapter

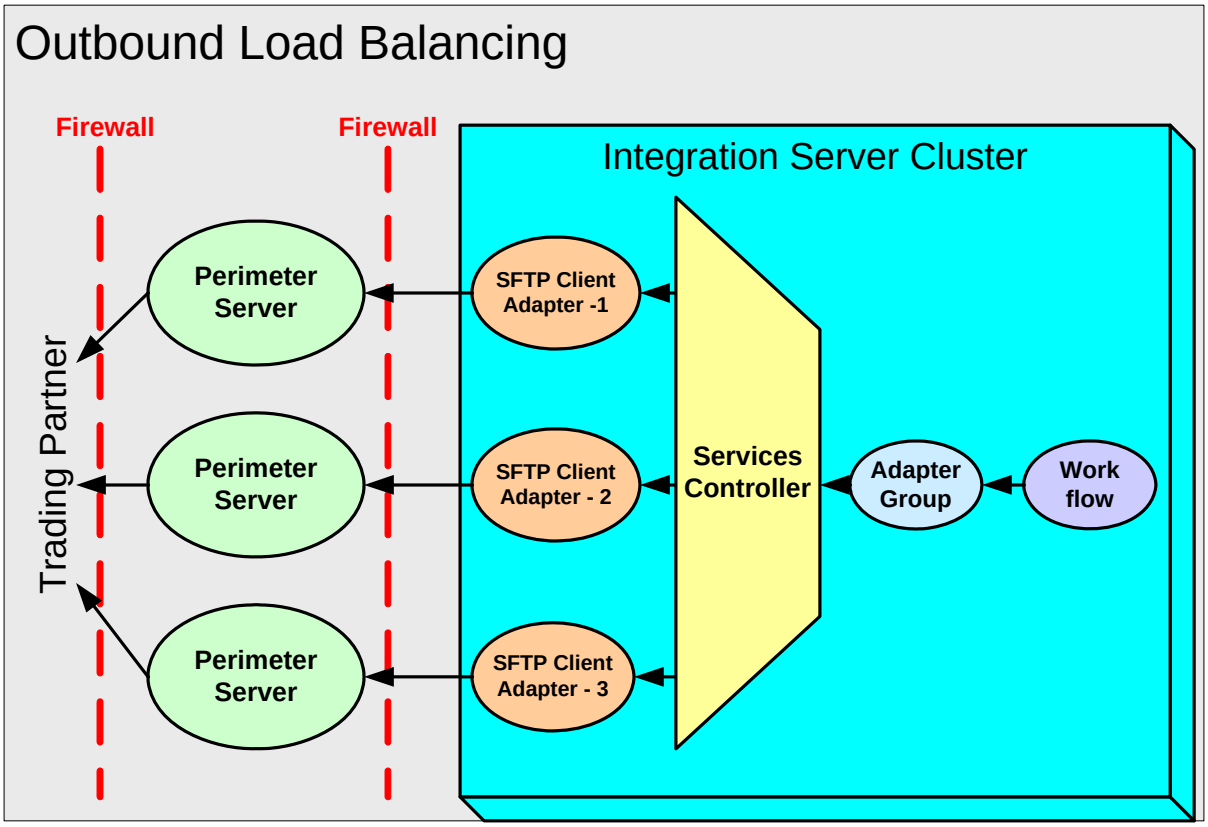
3. Click on the edit icon to adjust the settings. On provides complete logging of all activities. Off provides only error logging.

   For the SFTP Server Adapter, select Logging Level from the following:

   - Error - only errors
   - Communication Trace - errors, requests from clients, and responses from the Server adapter. This includes ACL violations.
   - All - for debugging, all activities

Load Balancing Across Adapter Groups

To accommodate large volumes of traffic, you can put multiple SFTP Client adapters into an adapter group. The following graphic depicts how outbound load balancing works:



Run SFTPClientDemoAllServices

To help you get started using the SFTP Client adapter and SFTP Server adapter, Application includes a demo that provides an example of all the services. The demo transfers a file from the SFTP Client adapter to the SFTP Server adapter.

Note: SFTPClientDemoAllServices uses a fully preconfigured SFTP Server adapter named DemoAllSFTPServerAdapter. This adapter is enabled when you complete the following procedure. A partially preconfigured adapter named SFTP Server Adapter is also included in the Application installation. Because both adapter specify the same port, you can use only one at a time. To use the SFTP Server Adapter, you must first disable the DemoAllSFTPServerAdapter, complete the configuration of SFTP Server Adapter, and enable it.

Import File

To prepare to run SFTPClientDemoAllServices:

1. Transfer the SFTPClientDemoAllConf.xml file from *INSTALL_DIR*/installed_data/sftpclient/ to your local computer.
2. Import the SFTPClientDemoAllConf.xml file through the Import wizard. Select **Deployment** > **Resource Manager** > **Import/Export**.
3. Next to Import Resources, click **Go!**
4. Browse to the SFTPClientDemoAllConf.xml file transferred in step 1. Type password for passphrase and click **Next**.
5. On the Create Resource Tag page, click **Next**.
6. On the Update Objects page, click **Next**.
7. On the Service Configuration page, select all (click the double arrow pointing right) to be imported, then click **Next**.
8. On the Mailbox Virtual Root page, select all to be imported, then click **Next**.
9. On the Mailbox Metadata page, select all to be imported, then click **Next**.
10. On the SSH Host Identity Keys or User Identity Keys page, select all to be imported, then click **Next**.
11. On the SSH Known Host Keys page, select all to be imported, then click **Next**.
12. On the SSH Authorized User Keys page, select all to be imported, then click **Next**.
13. On the Confirm page, click **Finish**.

Run Demo

To run SFTPClientDemoAllServices:

1. Select **Business Process** > **Manager**.
2. Search for **SFTPClientDemoAllServices**.

3. Click **Execution Manager**, then **Execute**.
4. Click **Go!**
5. Review the log to see the progress of the business process execution.

Note: The SFTPClientDemoAllServices process only works on servers that are running on JDK 1.5 or later. If the import returns a message indicating it cannot find the SFTP Server adapter, then your Application environment is not compatible.

Use Authentication

As part of the import in step 1, you imported a set of keys that can be used for authentication. Now you can attach the admin user to the authorized key, so that any business process that wants to authenticate itself as admin can use the matching user identity key. You can see the user identity key in the Begin Session service following. This key matches the authorized user key to assign to the admin user.

To prepare Authorized User Key

1. Go to **Accounts > User Accounts**.
2. Search for the admin user and click **Edit**.
3. For **SSH Authorized User Key** select the key named DemoAllAuthorizedUserKey.
4. Click **Save**.
5. On the confirm screen, click **Finish**.

To prepare the SFTPClientDemoAllServices business process:

1. Go to **Business Process > Manager**.
2. Search for: **SFTPClientDemoAllServices**.
3. Click **Source Manager**, then click **Edit**.
4. Under the **SFTP Client Begin Session service**, find the line that reads:

   <assign to="PreferredAuthenticationMethod">password</assign>

   Change the word password to publickey:

   <assign to="PreferredAuthenticationMethod">publickey</assign>
5. Type a description, then click **Save**.
6. On the confirm screen, click **Finish**, then click **Return**.

To run the business process to test your changes:

1. Select **Business Process > Manager**.
2. Search for **SFTPClientDemoAllServices**.
3. Click **Execution Manager**, then **Execute** the newly created version.
4. Click **Go!**
5. Click on Info, under the **Status Report** column on the **SFTP Client Begin Session Service** row.

6. Verify the following line:

   PreferredAuthenticationMethod=[public key]

   If it reads [password] instead of [public key], then public key authentication failed.

   The most likely problem is executing the wrong version. Ensure that you have enabled the new version.

Disable Demo Server Adapter

When you have completed the demo, disable the DemoAllSFTPServerAdapter so you can use SFTP Server Adapter.

1. Select **Deployment** > **Services** > **Configuration**.
2. List by type SFTP Server Adapter.
3. Clear Enable for DemoAllSFTPServerAdapter.

Index