Sterling B2B Integrator

SFTP

Version 5.2

Sterling B2B Integrator

SFTP

Version 5.2

Note

Before using this information and the product it supports, read the information in “Notices” on page 27.

Copyright

This edition applies to Version 5 Release 2 of Sterling B2B Integrator and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

SSH/SFTP

Sterling B2B Integrator includes adapters and services that enable you to work with trading partners using the SSH/SFTP protocol.

SSH/SFTP Support

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.

Note: To correct common misconceptions, SSH/SFTP is not FTP over SSH, nor is it particularly like FTP at the protocol level.

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 needed for authentication.

The 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

Sterling B2B Integrator is compatible with most SFTP clients and SCP clients. The following clients have been tested and approved for interoperability with the SFTP Server adapter:

- Sterling Connect:Enterprise® Secure Client (version 1.3.00)
- Sterling 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
  ```

Important: If you experience a timeout when resuming a file transfer on a very large file, increase the server response timeout value in your SFTP or SCP client to 60 seconds or more.

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 Mailboxes in Sterling B2B Integrator. To an external user, the Mailbox is a directory on which the user has privileges.

Using SFTP with Mailboxes

A *Mailbox* is a storage area for *messages*. Each message associates a name with some data (the data itself is stored in Sterling B2B Integrator as a *document*.) Mailboxes are usually arranged in a hierarchy with the mailbox named "/" serving as the root.

Mailboxes in Sterling B2B Integrator 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 system Mailboxes as the repository. The prerequisites to using SSH/SFTP 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

Sterling B2B Integrator provides features to enhance the security of file transfers using SSH/SFTP. For improved security, do 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

The amount of information returned in response to most failed logins is limited 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.

The system 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 a key provided separately when establishing the trading partner relationship. 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 to allow an SFTP Client adapter to connect with a remote SFTP server.

- User Identity Key – Private/Public key pair used to identify Sterling B2B Integrator as a user on a remote server. Generate this key within Sterling B2B Integrator and provide the public part of the key to your trading partner.
- Known Host Key – Public key used to authenticate remote SFTP servers to Sterling B2B Integrator's SFTP Client adapter. Request this key from your trading partner.

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

- Authorized User Key – A public key used to authenticate remote users to Sterling B2B Integrator SFTP Server adapters. One one or more Authorized User keys can be associated with a user account. Request the key(s) from your trading partner and include the key(s) in their Sterling B2B Integrator user account.
- Host Identity Key – Private/Public key pair used to identify the Sterling B2B Integrator SFTP Server adapter to remote clients. Generate this key within Sterling B2B Integrator.

Support of SSH-DSS 2048 Keys in Sterling B2B Integrator

IBM Sterling B2B Integrator versions 5242 and higher using public and private SSH keys generated by Sterling B2B Integrator have Q values of 256 bits. This is the default behavior and impacts some communications when utilized with 2048-bit DSA keys.

When using Sterling B2B Integrator to Sterling B2B Integrator SFTP communication, there is no impact. When using Sterling B2B Integrator with Third Party communications with DSA keys, there is no impact for the keys generated externally since they have Q values of 160 bits; however, if the keys are generated through Sterling B2B Integrator, it may impact communication where the Third Party application is not able to process DSA keys with Q values of 256 bits. In this case, communication fails for the client or server at the key verification step with a failure to process 2048 DSA keys.

To resolve this issue, you can create keys with an external tool, such as PuttyGen to create 2048 DSA keys that have a Q value of 160 bits.

SSH/SCP Support

SSH/SCP Support

The system provides an adapter to enable you to work with trading partners using the SSH/SCP protocol. The 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. The system accepts inbound scp commands from SCP clients when the SFTP Server adapter is configured to enable the SSH/SCP protocol.

The Sterling B2B Integrator 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

The system is compatible with most SCP clients. The following clients have been tested and approved for interoperability with the SFTP Server adapter:
- Sterling Connect:Enterprise® Secure Client (version 1.3.00)
- Sterling 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
```

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 Sterling B2B Integrator Mailboxes. To the external users, the Mailbox is a directory on which the user has privileges.

Using SCP with Mailboxes

A *Mailbox* is a storage area for *messages*. Each message associates a name with some data (the data itself is stored in Sterling B2B Integrator as a *document*.) Mailboxes are usually arranged in a hierarchy with the mailbox named "/" serving as the root.

Mailboxes in Sterling B2B Integrator are analogous to the familiar directory structure offered by operating system 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 Sterling B2B Integrator Mailboxes as the repository. The prerequisites to using SSH/SCP in Sterling B2B Integrator 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

Sterling B2B Integrator 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

Sterling B2B Integrator 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.

Sterling B2B Integrator 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 Sterling B2B Integrator SFTP Server adapters. Optionally, request this key from your trading partner and include it in their user account in Sterling B2B Integrator.
- Host Identity Key – Private/Public key pair used to identify the Sterling B2B Integrator SFTP Server adapter to remote clients. Generate this key within Sterling B2B Integrator.

SFTP Client Adapter

SFTP Client Adapter Set Up

Use the SFTP Client adapter to connect to a trading partner's SFTP server. For a list of its major features, see *SFTP Client Adapter*.

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 Sterling B2B Integrator 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.

Use a SFTP Client Adapter

About this task

To use a SFTP Client adapter:

1. Generate a New SSH User Identity Key or Check In an SSH User Identity Key
2. Obtain an SSH Known Host Key Automatically and Check It In or Check In an SSH Known Host Key from a File
3. Exchange Information With the SFTP Trading Partner
4. Configure a Perimeter Server for Use with the SFTP Client Adapter
5. Configure an SFTP Client Adapter
6. Set Up Trading Partner Profiles for SSH/SFTP

7. Use SFTP Client Services in Business Processes

Generate a New SSH User Identity Key

About this task

To generate a new SSH User Identity Key:

Procedure

1. Select **Trading Partners** > **SSH** > **User Identity Key**.
2. Next to **Create new User Identity Key**, click **Go!**
3. Type a **Key Name**. Do not use spaces or special characters. You cannot create a user identity key and a host identity key with the same name.

   Attention: SSH Authorized User Key names should not identify an associated trading partner. Select a naming convention where trading partners remain anonymous. Anyone with access to the dashboard My Account interface can see a list of all SSH Authorized User Key names in the system, not just their own.
4. Select the **Key Type**:
   - rsa1
   - ssh-rsa
   - ssh-dsa
5. Select the **Key Length**:
   - 768
   - 1024
   - 1536
   - 2048

   The longer the key length, the more secure the key.
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

About this task

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

Procedure

1. Select **Trading Partner** > **SSH** > **User Identity Key**.
2. Locate the key by searching or listing.
3. Select **check out** next to the key.
4. From the pop-up 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 the key to your trading partner. See *Exchange Information With the SFTP Trading Partner.*

Check In an SSH User Identity Key

Before you begin

You do not need to check in keys generated from within Sterling B2B Integrator.

About this task

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

Procedure

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.

   Note: To check in a key that is not passphrase protected, type several 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**.

Obtain an SSH Known Host Key Automatically and Check It In

Before you begin

To use the SSH/SFTP protocol to connect to your trading partner's SFTP server, you must obtain the public part of a Known Host Key for that SFTP server. One method is to obtain the key automatically during the check-in process.

Before you begin:

- Obtain the host name or IP address and the port of the server you are connecting to.
- Configure the default SSHKeyGrabberAdapter service instance to use the appropriate perimeter server and (if used) proxy server. See the adapter documentation for details.

About this task

To obtain an SSH Known Host key automatically and check it in:

Procedure

1. From the Administration Menu, go to **Trading Partner** > **SSH** > **Known Host Key**.
2. In the Check in section, next to **New Known Host Key**, click **Go!**
3. Enter the **Key Name**. Do not use spaces or special characters.
4. Select **Obtain key from a Remote Host**.
5. Ensure that **Enabled** is selected and click **Next**.
6. Enter the remote host or IP address and the port and click **Next**. Sterling B2B Integrator connects to the remote host, collects the key, and displays a summary of key information for review.You can then check in the key, or save the file for later check in.

To:	Perform these steps:
Save the file to disk	1. Choose one of the following formats and click **Go!** • OpenSSH • SECSH 2. Complete the download and the save dialogs. 3. If you do not want to check in the key at this time, stop here.
Check in the key	1. Click **Next**. 2. Review the key information before check in and click **Finish**.

Check In an SSH Known Host Key from a File

Before you begin

To use the SSH/SFTP protocol to connect to your trading partner's SFTP server, you must obtain the public part of a Known Host Key for that SFTP server and check it in to Sterling B2B Integrator. Instead of obtaining it automatically during check in, you may choose to check in a key from a local file.

About this task

Before you begin, this procedure assumes that you have received the public part of an SSH Known Host key and saved it to a local file.

Procedure

1. From the Administration Menu, select **Trading Partner** > **SSH** > **Known Host Key**.
2. In the Check in section, next to **New Known Host Key**, click **Go!**
3. Enter the **Key Name**. Do not use spaces or special characters.
4. Select **Obtain key from a file**.
5. Browse to the file containing the key.
6. Ensure that **Enabled** is selected and 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*.

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:

Worksheet for a Trading Partner's SFTP Server
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.

Set Up Trading Partner Profiles for SSH/SFTP

After you have gathered and recorded your external trading partner's SFTP server configuration information, you must set up a trading partner profile for them.

About this task

To set up a Trading Partner profile:

Procedure

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*.

   Note: The Remote Host field accepts only alphanumeric and dash characters.

   Note: The Remote User field accepts only alphanumeric, dash, underscore, and "$" characters.

   Important: The maximum length for the password in the password field is 55 characters.
4. Check in the **Known Host Key** using the file identified on the worksheet.

   Note: With V5.2.5 and higher, you can check in multiple Known Host Keys and select them from the list to choose keys from the known host key ring. This allows the SFTP Begin Client Session service to connect to different SFTP servers as long as the Known Host Keys for these servers are referenced in the SSH Remote Profile. This can be useful, for example, if you need to send files using SFTP to a load-balanced DNS server with a virtual IP address.
5. Click **Next**.
6. Confirm your information and click **Finish**.

Perimeter Server Configuration 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 Sterling B2B Integrator adapters. To use SFTP to send and receive data from external trading partners, you must set up perimeter services.

SFTP Client Adapter Configuration

See *Configuring the SFTP Client Adapter*.

SFTP Client Services for Use 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 Sterling B2B Integrator 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

List SSH User Identity Keys

About this task

To list the SSH User Identity Keys:

Procedure

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

Delete SSH User Identity Keys

About this task

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

Procedure

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**.

List SSH Known Host Keys

About this task

To list the SSH Known Host Keys:

Procedure

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

Check Out an SSH Known Host Key

About this task

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

Procedure

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 pop-up 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.

Delete SSH Known Host Keys

About this task

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

Procedure

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**.

SFTP Server Adapter

SFTP Server Adapter Set Up

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 Sterling B2B Integrator 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 an 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 one of the keys 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 Sterling B2B Integrator and the external SFTP client using standard SFTP commands.

Use a SFTP Server Adapter

About this task

To use a SFTP Server adapter:

1. Generate a New SSH Host Identity Key or Check In an SSH Host Identity Key
2. Check In an SSH Authorized User KeySet up a Mailbox in Sterling B2B Integrator
3. Set up a Mailbox in Sterling B2B Integrator
4. Set up a User Account
5. Set the Mailbox Properties File
6. Configure a Perimeter Server for Use with the SFTP Server Adapter
7. Provide Information About the SFTP Server to Trading Partners
8. Accept Requests From Trading Partner's SFTP Clients

Generate a New SSH Host Identity Key

About this task

To generate a new SSH Host Identity Key:

Procedure

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 Sterling B2B Integrator.

Check In an SSH Host Identity Key

About this task

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

Procedure

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

Before you begin

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.

You can associate one or more Authorized User Keys with a user account when the account is set up or edited.

About this task

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

Procedure

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**.

SFTP Mailboxes

About this task

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

Procedure

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

User Accounts

Before your trading partners can access your system 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 Sterling B2B Integrator 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.

Edit the Mailbox Properties File

About this task

To edit the Mailbox Properties File:

Procedure

1. Locate the *mailbox.properties* file in the properties directory where you installed the system.
2. Open the *mailbox.properties* file in a text editor.
3. Set the following value in your *mailbox.properties* file:
   ```
   disallowDuplicateMessages=true
   ```
4. Save and close the file.

Perimeter Server Use with a 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 system 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 Sterling B2B Integrator online library for complete details and procedures.

Configure an SFTP Server Adapter

See *Configuring the SFTP Server Adapter*.

Provide SFTP Server Information 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 Sterling B2B Integrator 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 SFTP Server adapter verifies that there is an available concurrent session for the user and grants access.

Duplicate Message Names

If Sterling B2B Integrator 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, Sterling B2B Integrator returns an error to the SFTP client indicating that the file already exists.

Note: This applies whether Sterling B2B Integrator 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 *Configure the sftp.properties File*.

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 by SFTP clients is to request a list of the directory contents before resuming a transfer. 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. Sterling B2B Integrator 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

The mailbox document storage feature 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 the system, these protocols interface with the mailbox document storage feature. The benefits to this are:

- 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, Sterling B2B Integrator can use File system or Database for mailbox document storage.

SSH Host Identity Key Procedures

List SSH Host Identity Keys

About this task

To list the SSH Host Identity Keys:

Procedure

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

Check Out an SSH Host Identity Key

About this task

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

Procedure

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 pop-up 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.

Delete SSH Host Identity Keys

About this task

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

Procedure

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 Key Procedures

SSH Authorized User Key

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

Check In an SSH Authorized User Key

About this task

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

Procedure

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**.

List SSH Authorized User Keys

About this task

To list the SSH Host Identity Keys:

Procedure

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

Check Out an SSH Authorized User Key

About this task

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

Procedure

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 pop-up 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.

Delete SSH Authorized User Keys

About this task

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

Procedure

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

Configure the sftp.properties File

The `sftp.properties` file in the `properties` directory provides settings for the SFTP Client adapter and the SFTP Server adapter.

Before you begin

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

About this task

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

Procedure

1. Locate the `sftp.properties.in` file in the `properties` directory where you installed Sterling B2B Integrator.
2. Edit the `sftp.properties.in` file.
3. Configure the properties. The properties are listed in 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=Sterling B2B Integrator 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
checkpointInterval (V5.2.6 or later)	Controls the amount of uploaded data between checkpoints. Checkpoints save the incomplete uploaded file for later resumption. Actual checkpoint is at the end of the buffer write that exceeds the interval. The checkpoint occurs only if the server adapter is configured for resumption, and if the upload is to a Global Mailbox. If you set the property to `0`, automatic checkpoint is disabled. Default value for the property is 100M. You can also specify the value in kilobytes or gigabytes. Valid value is any integer with one of the following units: • G = gigabyte • M = megabyte • K = kilobyte Default is 100M. Setting to `0` disables automatic checkpoints.
defaultKey UpdateDataSize	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.

Property	Description
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.

Enable Failed Login Tracking and Account Locking

About this task

You can track and limit the number of failed login attempts by a user, and lock the user account to prevent further attempts. For more information, see Lockout Policies Overview.

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, Sterling B2B Integrator displays activity detail occurring on the adapter.

The following types of activities are reported about the SFTP adapters:

- Put – Adds a file to a Sterling B2B Integrator mailbox or to a trading partner directory
- Get – Retrieves a file from a Sterling B2B Integrator 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 Sterling B2B Integrator 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

View SFTP Logs and Adjust Settings

About this task

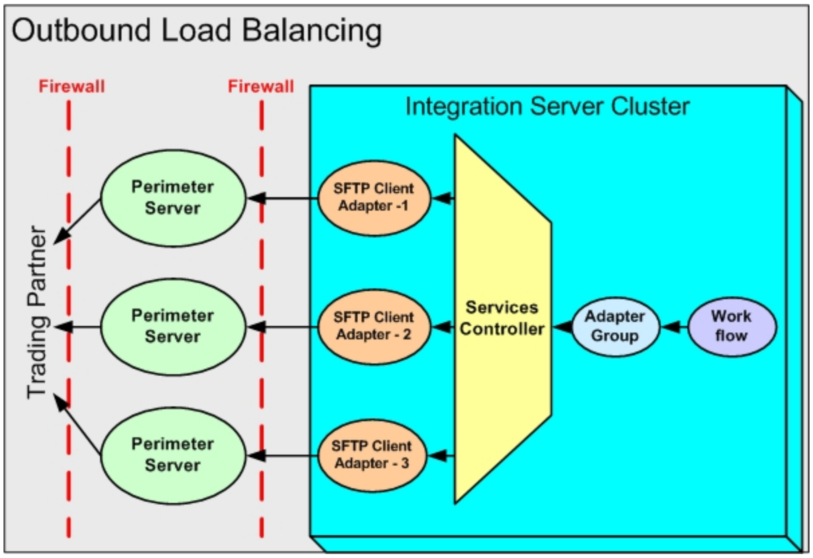
To view logs of SFTP activity:

Procedure

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 a Logging Level from the following:
   - Error – only errors
   - Communication Trace – errors, requests from clients, and responses from the SFTP 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

SFTPClientDemoAllServices Demo

To help you get started using the SFTP Client adapter and SFTP Server adapter, a demo service is provided to show how it works. 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 Sterling B2B Integrator installation. Because both adapters 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 Demo File

About this task

To import the *SFTPClientDemoAllServices* demo file:

Procedure

1. Transfer the *SFTPClientDemoAllConf.xml* file from `<INSTALL_DIR>/install/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

Before you begin

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 Sterling B2B Integrator environment is not compatible.

About this task

To run the SFTPClientDemoAllServices demo:

Procedure

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.

User Authentication

As part of the *Import Demo File* task, 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. This key matches the authorized user key to assign to the admin user.

Prepare Authorized User Key

About this task

To prepare an authorized user key:

Procedure

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**.

Prepare SFTPClientDemoAllServices Business Process

About this task

To prepare the SFTPClientDemoAllServices business process:

Procedure

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**.

Run SFTPClientDemoAllServices Business Process

About this task

To run the business process to test your changes:

Procedure

1. Select **Business Process** > **Manager**.
2. Search for **SFTPClientDemoAllServices**.
3. Click **Execution Manager**, then **Execute** the newly created version.
4. Click **Go!**
5. Click **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 that you are executing the wrong version. Verify that you have enabled the new version of the business process.

Disable Demo Server Adapter

About this task

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

Procedure

1. Select **Deployment** > **Services** > **Configuration**.
2. List by type **SFTP Server Adapter** and click **Go!**
3. Clear the **Enabled** checkbox for DemoAllSFTPServerAdapter.

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.

Product Number:

Printed in USA