BEA AquaLogic® Service Bus

SFTP Transport User Guide

Version: 2.6 RP1
Revised: November 2007

Contents

Introduction to SFTP Transport

Using the SFTP Transport

Introduction to SFTP Transport

The SFTP transport allows you to transfer files over SSH File Transfer Protocol (SFTP) using SSH version 2. After authentication, a connection is established between ALSB services and the SFTP server and file transfer occurs. The SFTP transport is a poll-based transport that periodically polls a specified directory based on a polling interval specified during service configuration. One-way inbound and outbound connectivity is supported for this transport.

Service Types

The SFTP transport is available only for the following service types:

- Message Service with only request message type specified during message type configuration.

Note: For a SFTP transport-based proxy service, when you select the service type as Message Service, you must specify Binary, Text, MFL, or XML as the Request Message Type. Response Message Type must be `None`.

- Any XML Service

While configuring proxy or business services, ensure that you select Message Service or XML Service as the service type. For more information about configuring proxy and business services, see Business Services and Proxy Services in *Using the AquaLogic Service Bus Console*.

Quality of Service

For inbound message transfer, the Quality of Service (QoS) is set as `exactly-once.` This ensures that a message is processed at least once.

For outbound message processing, the QoS is `best-effort`.

Note: To take care of messages that are not transferred, you must create the error handling logic (including any retry logic) in the pipeline error handler. For information about configuring error handling, see Proxy Services: Error Handlers in *Using the AquaLogic Service Bus Console*.

For more information about QoS in ALSB messaging, see Quality of Service in Modeling Message Flow in AquaLogic Service Bus in *Using the AquaLogic Service Bus Console*.

Environment Values

Environment values are certain predefined fields in the configuration data whose values are very likely to change when you move your configuration from one domain to another (for example, from test to production). For information about updating environment values, see Finding and Replacing Environment Values in *Using the AquaLogic Service Bus Console*. The environment values associated with the SFTP transport are listed in Table 1-1:

Table 1-1 Environment Values

Environment Value	Description
Archive-directory	The directory to which the files are moved from either the download directory or the remote location.
Download-directory	The directory on your local machine where files are downloaded during the file transfer.
Error-directory	The location where messages are posted if there is a problem.
Managed Server for Polling	In a cluster scenario, this value specifies the Managed Server that is used for polling.

Note: For more information about the directory values, see Configuring Proxy Services to Use the SFTP Transport and Configuring Business Services to Use the SFTP Transport.

Using the SFTP Transport

You can use the SFTP transport to transfer files using the SFTP protocol. When you configure your proxy and business services, you can choose any of the 3 authentication methods for server authentication. For more information, see Authentication Methods, Configuring Proxy Services to Use the SFTP Transport, and Configuring Business Services to Use the SFTP Transport.

When you configure a proxy service, you can use a Transport Header action to set the header values in messages. For more information, see Transport Headers and Metadata.

In addition, you can also import and export resources using ALSB Console. For more information, see Importing and Exporting Resources and UDDI Registries: Importing and Publishing Services.

SFTP Authentication Process

The following general principles apply to the SFTP authentication process for both a proxy service and business service.

- **Connection:** The ALSB service (proxy and business) always acts as the SFTP client and connects to the SFTP server.
- **Authentication by the SFTP Server:** For Public Key and Host Based authentication, the SFTP server authenticates the connection with the public key of the ALSB service. For Username Password authentication, the SFTP server authenticates the connection with the username and password. For more information, see Authentication Methods.

- **Authentication by the SFTP Client:** The ALSB service always authenticates the SFTP server with the public-key/host/IP combination present in the `known_hosts` file. For more information, see Known_hosts File.
- **Connection established:** Connection is established only when both the server and client authentications are successful. File (message) transfer can now be done.
- **Transfer:** When a proxy service is the client to the SFTP server, the file (message) is downloaded from the SFTP server and when a business service is the client to the SFTP server, the file (message) is uploaded to the SFTP server.

Authentication Methods

The following authentication methods are supported for the SFTP transport:

- Username-Password Authentication
- Host-based Authentication
- Public Key Authentication

For server authentication, you must have a `known-hosts` file on the client machine. For more information, see Known_hosts File.

Known_hosts File

ALSB services authenticate the SFTP server based on the server details in a `known_hosts` file. This file must be available on the server on which the ALSB proxy services (inbound requests) or business services (outbound requests) run and must have the host name, IP address, and public key of the remote SFTP servers to which the proxy service or business service can connect.

To use the `known_hosts` file:

1. Create a `known_hosts` file and enter these details in the following format:

   ```
   Hostname, IP algorithm publickey
   ```

   where,

   – host name specifies the host name of the SFTP server

   – IP specifies the IP address of the SFTP server

   – algorithm can be either DSA or RSA, based on the SFTP server configuration. Enter `ssh-rsa` or `ssh-dss` depending on the supported algorithm.

- – format of the public key in this file is “Open SSH public key format”. This is the public key of the SFTP server.

Multiple entries are supported in this file and it should be one entry per line.

Example:

```
getafix,172.22.52.130 ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAtR+M3Z9HFxnKZTx66fZdnQqAHQcF1vQe1+EjJ/HWYtg
Anqsn0hMJzqWMatb/u9yFwUpZBirjm3g2I9Qd8VocmeHwoGPhDGfQ5LQ/PPo3esE+CGwdnC
OyRCktNHeuKxo4kiCCJ/bph5dRpghCQIvsQvRE3sks+XwQ7Wuswz8pv58=
```

2. Move the `known_hosts` file to the `<ALSB installation directory>\user_projects\domains\alsb_domain\sbconfig\sftp` directory.

Additional tasks that need to be done for a specific authentication method are listed in the following sections.

Username-Password Authentication

Username and password authentication is done using the credentials of the user.

To enable username and password authentication for a service:

1. Create a static service account using the user credentials on the SFTP server. For more information, see Service Accounts in *Using the AquaLogic Service Bus Console*.
2. Create a `known_hosts` file. For more information, see Known_hosts File.

Host-based Authentication

Host-based authentication is done using a private host key.

To enable host-based authentication for a service:

1. Configure a service key provider with an SSL client authentication key. For information about using service key providers, see Service Key Providers in *Using the AquaLogic Service Bus Console*.
2. Create a `known_hosts` file. For more information, see Known_hosts File.
3. Configure the SFTP server to accept the requests from ALSB, which is a client to the SFTP server.

   For example, with an SFTP server on Linux, you must:

- Edit the `/etc/ssh/shosts.equiv` file and add the host name or IP address of the machine on which ALSB domain is running.
- Edit the `/etc/ssh/ssh_known_hosts` file and add the host name or IP address of the machine on which ALSB domain is running, followed by space and the public key.

  Note: Extract the public key from the key store used while creating the service key provider. The format of this public key should be Open SSH public key format.

Public Key Authentication

Public key authentication is done using your own private key.

To enable public key authentication:

1. Configure a service key provider with SSL client authentication key. For information about using service key providers, see Service Key Providers in *Using the AquaLogic Service Bus Console.*
2. Configure the SFTP server to accept the requests from ALSB (SFTP client).

   For example, with an SFTP server on Linux, you must extract the public key from the key store and put the key in the `$HOME/.ssh/authorized_keys` file on the SFTP server. Ensure the path and file are available.
3. Create a `known_hosts` file. For more information, see Known_hosts File.

Configuring Proxy Services to Use the SFTP Transport

When you create a proxy service in ALSB Console Transport Configuration page, select the transport protocol as `sftp` and specify the endpoint configuration in `sftp://hostname:port/directory` format.

where,

- hostname is the host name or IP address of the SFTP server.
- port is the port on which SFTP server is listening. Default port for SFTP is 22.
- directory is the location that is periodically polled for files. This directory is relative to the home directory of the user.

Note: Because the only service types that are supported for the SFTP transport are Message and XML, you must select either Message service or XML service when you select the service type in the General Configuration page. For more information, see Proxy Services in *Using the AquaLogic Service Bus Console*.

Configure the SFTP transport for a proxy service with values as described in Table 2-1.

Table 2-1 Configuring SFTP Proxy Service

Field	Description
User Authentication	The proxy service is authenticated by the SFTP server based on the specified user authentication method. Select one of the following: • **Username Password Authentication** - Specifies that a static service account is associated with this authentication method and the client is authenticated using the credentials provided in the service account. • **Host Based Authentication** - Specifies that a user name and service key provider are required to use this authentication method. Any user connecting from a known host is authenticated using the private key of the host. • **Public Key Authentication** - Specifies that a user name and service key provider are required to use this authentication method. All users have their own private key. For more information, see Authentication Methods.
Service Account	Enter the service account for the user, or click **Browse** to select a service account. For information about using service accounts, see Service Accounts in *Using the AquaLogic Service Bus Console*.
Service Key Provider	Enter a service key provider or click **Browse** to select a service key provider. For more information, see Service Key Providers in *Using the AquaLogic Service Bus Console.* **Note:** This option is available only when Host Based or Public Key Authentication is selected as the user authentication method.
Username	Enter the user name. This name is required only when you select either the Host Based or the Public Key authentication method. In host-based user authentication, the user name is used for polling the home directory of the user on the SFTP server. For public key user authentication, the user name is used for polling the home directory of the user and for identifying the location of the public key on the SFTP server.

Table 2-1 Configuring SFTP Proxy Service

Field	Description
Pass By Reference	Select this option to stage the file in the archive directory and pass it as a reference in the headers. **Note:** This option is available only when remote streaming is disabled.
Remote Streaming	Select this option to stream the SFTP files directly from the remote server at the time of processing. When you select this option, the archive directory is the remote directory on the SFTP server machine. Therefore, you should specify the archive directory relative to the SFTP user directory.
File Mask	Enter a regular expression to select the files that you want to pick from the directory. Default is `*.*`.
Polling Interval	Enter the interval in seconds at which the file is polled from the specified location. Default is `60`.
Read Limit	Specify the maximum number of messages to read per polling sweep. Enter `0` to specify no limit. Default is `10`.
Post Read Action	Select what happens to a message after it has been read. • **Archive** - The message is archived in the specified archived directory after file transfer. • **Delete** - The message is deleted after file transfer.
Archive Directory	Specify the path to the archive location if the **Post Read Action** option is set to **Archive**. You must specify a archive directory if the **Pass By Reference** option is selected. If remote streaming is enabled, this directory location is with respect to the SFTP server. If remote streaming disabled, the archive directory is available on the ALSB machine. When the Archive option is selected, the files are moved from either the download directory or the remote location to this directory. **Note:** Specify the directory as an absolute path. If the directory does not exist, it is automatically created. If you specify the directory as a relative path, the directory is created relative to the Java process that starts the WebLogic Server.

Table 2-1 Configuring SFTP Proxy Service

Field	Description
Download Directory	Enter the directory on your local machine where files are downloaded during the file transfer. If remote streaming is enabled, this option is disabled. **Note:** Specify the directory as an absolute path. If the directory does not exist, it is automatically created. If you specify the directory as a relative path, the directory is created relative to the Java process that starts the WebLogic Server.
Error Directory	Enter the location where messages are posted if there is a problem. If remote streaming is enabled, this directory is with respect to the SFTP server. If disabled, it is available on the ALSB machine. **Note:** Specify the directory as an absolute path. If the directory does not exist, it is automatically created. If you specify the directory as a relative path, the directory is created relative to the Java process that starts the WebLogic Server.
Request encoding	Accept the default `UTF-8` as the character set encoding for requests in SFTP transports.
Advanced Settings	
Scan Subdirectories	Select this option to recursively scan all directories within the directory that is specified in the endpoint URI.
Sort By Arrival	Select this option to deliver events in the order of arrival. This ensure that the message delivery is not random, but based on the time at which the file is downloaded into the destination directory.
Timeout	Enter the socket timeout interval, in seconds, before the connection is dropped. If you enter `0`, there is no timeout. Default is 60.
Retry Count	Specify the number of retries for SFTP connection failures. Default is 3.

For more information about configuring proxy services using SFTP transport, see SFTP Transport Configuration Page in Proxy Services in *Using the AquaLogic Service Bus Console*.

Transport Headers and Metadata

The transport header and metadata related to the SFTP transport are listed in Table 2-2.

Table 2-2 Transport Headers and Metadata

Header / Metadata	Description
FileName	The value of this transport header is used as the file name at the destination directory.
isFilePath	Metadata field. A true or false value. If True, the value specified in the FileName header is interpreted as the absolute path of the file. If False, the specified filename is interpreted as the actual name of the file.
filePath	Response metadata field. The absolute path at which the file specified in the FileName header has been written.

Configuring Transport Headers in the ALSB Message Flow

You can configure the transport headers only for outbound requests in the message flow. For information about the transport headers related to the SFTP transport, see Transport Headers and Metadata.

In the pipeline, use a Transport Header action to set the header values in messages. For information about adding transport header actions, see “Transport Headers” in Proxy Services: Actions in *Using the AquaLogic Service Bus Console*.

Configuring the Transports Headers and Metadata in Test Console

You can also configure the **filename** transport header and the **isFilePath** metadata values in the ALSB Test Console when you test SFTP transport based services during development.

For information about using Test Console, see Test Console in *Using the AquaLogic Service Bus Console* and Using the Test Console in *AquaLogic Service Bus User Guide*.

Configuring Business Services to Use the SFTP Transport

When you create a business service in ALSB Console, in the Transport Configuration page, select the transport protocol as `sftp` and specify the endpoint URI (location of the service) in `sftp://hostname:port/directory` format.

where,

- hostname is the host name or IP address of the SFTP server.
- port is the port on which SFTP server is listening. Default port for SFTP is `22`.
- directory is the location where the outbound message is stored or written. This directory is relative to the home directory of the user.

Note: Because the only service types that are supported for the SFTP transport are Message and XML, ensure that you select either Message service or XML service when you select the service type in the General Configuration page. For more information, see in Business Services in *Using the AquaLogic Service Bus Console*.

To configure the SFTP transport for a business service, specify the values as described in Table 2-3.

Table 2-3 Configuring SFTP Business Service

Field	Description
User Authentication	Select one of the following: • **Username Password Authentication** - Specifies that a static service account is associated with this authentication method and the client is authenticated using the credentials provided in the service account. • **Host Based Authentication** - Specifies that a user name and service key provider are required to use this authentication method. Any user connecting from a known host is authenticated using the private key of the host. • **Public Key Authentication** - Specifies that a user name and service key provider are required to use this authentication method. All users have their own private key. For more information, see Authentication Methods.
Service Account	Enter the service account for the user, or click **Browse** to select a service account. For information about using service accounts, see Service Accounts in *Using the AquaLogic Service Bus Console*.
Service Key Provider	Enter a service key provider or click **Browse** to select a service key provider. For more information, see Service Key Providers in *Using the AquaLogic Service Bus Console.* **Note:** This option is available only when Host Based or Public Key Authentication is selected as the user authentication method.
Username	Enter the user name. This name is required only when you select either the Host Based or the Public Key authentication method. In host-based user authentication, the user name is used for polling the home directory of the user on the SFTP server. For public key user authentication, the user name is used for polling the home directory of the user and for identifying the location of the public key on the SFTP server.
Timeout	Enter the socket timeout interval, in seconds, before the connection is dropped. If you enter 0, there is no timeout. Default is 60.
Prefix for destination File Name	Enter the prefix for the file name under which the file is stored on the remote server.

Table 2-3 Configuring SFTP Business Service

Field	Description
Suffix for destination File Name	Enter the suffix for the file name under which the file is stored on the remote server.
Request encoding	Accept the default UTF-8 as the character set encoding for requests in SFTP transports.

For more information about configuring business services using SFTP transport, see SFTP Transport Configuration Page in Business Services in *Using the AquaLogic Service Bus Console*.

Importing and Exporting Resources

When a resource exists in an ALSB domain, you can preserve the security and policy configuration details while importing that resource to ALSB by selecting the Preserve Security and Policy Configuration option. When you select this option, even if the security and policy configuration details have been updated in the resource that you want to import, the values in the existing resource are preserved. For information about importing resources from ALSB Console, see “Importing Resources” in System Administration in *Using the AquaLogic Service Bus Console*.

For SFTP services, the following details are preserved:

- client authentication method.
- reference to the service account, for services associated with username password authentication.
- reference to service key provider, for services associated with either host based or public key based authentication.
- user name, for services associated with either host based or public key based authentication.

UDDI Registries: Importing and Publishing Services

While publishing SFTP services to the UDDI registry, the authentication mode (auth-mode) is published to the registry along with other properties like endpoint URI, request-encoding, and scheme.

The protocol, load balancing algorithm, and endpoint URI values are imported from the registry while importing any service from the UDDI registry. After import, `round-robin` is the default value assigned to the load balancing algorithm. In addition, while importing SFTP services from the UDDI registry, the properties listed in Table 2-4 are imported from the registry:

Table 2-4 Properties imported from UDDI

Property	Description
Prefix for destination File Name	The prefix for the file name under which the file is stored on the remote server. The default value is set to “ ” (Null value).
Suffix for destination File Name	The suffix for the file name under which the file is stored on the remote server. The default value is set to “ ” (Null value).
Auth-mode	The authentication method that is imported from the registry. **Note:** When a SFTP business service with user authentication is imported from an UDDI registry into ALSB, a conflict is generated. You need to create a service account when the user authentication is username-password and associate it with the service. If the authorization method is host-based or public key, create a service key provider and associate it with the service.

For more information, see “Importing a Business Service From a UDDI Registry” and “Publishing a Proxy Service to a UDDI Registry” in System Administration in *Using the AquaLogic Service Bus Console.*