Oracle® Service Bus

HTTP and Poller Transports User Guide

10*g* Release 3 (10.3)

October 2008

ORACLE

Oracle Service Bus HTTP and Poller Transports User Guide, 10*g* Release 3 (10.3)

Contents

Transports

SFTP Transport

CHAPTER 1

Transports

You can use different types of transports to configure proxy services or business services in Oracle Service Bus. The transport protocol you select depends on the service type, the type of authentication required, the service type of the invoking service, and so on.

Poll-based transports are transports with transport pollers pinned to a managed server. These transports use the JMS framework to ensure that the processing of a message is done at least once. E-mail, File, FTP, and SFTP are poll-based transports. This section describes the poll-based transports and the HTTP transport. For information on SFTP, see SFTP Transport.

This document includes the following sections:

- HTTP Transport
- E-mail Transport
- File Transport
- FTP Transport

HTTP Transport

The HTTP transport lets you send messages between clients and service providers through Oracle Service Bus using the http/s protocol. The HTTP transport also provides support for working with REST (Representational State Transfer) environments, as described in REST Support.

You can select the HTTP transport protocol when you configure any type of proxy or business service. Use the following endpoint URI formats:

- **Proxy Services**: /someService
- **Business Services**: http://host:port/someService

where `someService` is the name of proxy service or a business service

Configuring Proxy Services using the HTTP Transport

Table 1-1 describes the parameters you can specify to configure the HTTP transport for a proxy service.

Table 1-1 Parameters for Configuring HTTP Transport for Proxy Service

Parameter	Description
HTTPS Required	Select this check box for inbound HTTPS endpoints. To learn more, see Configuring Transport-Level Security in the *Oracle Service Bus Security Guide*.

Table 1-1 (Continued) Parameters for Configuring HTTP Transport for Proxy Service

Parameter	Description
Authentication	You must configure one of the following authentication methods: • **None** - Specifies that authentication is not required. • **Basic** - Specifies that basic authentication is required to access this service. Basic authentication instructs WebLogic Server to authenticate the client using a user name and password against the authentication providers configured in the security realm, such as a Lightweight Directory Access Protocol (LDAP) directory service and Windows Active Directory. The client must send its user name and password on the HTTP request header. Basic authentication is strongly discouraged over HTTP because the password is sent in clear text. However, it is safe to send passwords over HTTPS because HTTPS provides an encrypted channel. **Warning:** By default, all users (authorized and anonymous) can access a proxy service. To limit the users who can access a proxy service, create a transport-level authorization policy. See Editing Transport-Level Access Policies in Using the Oracle Service Bus Console. • **Client Certificate** - Specifies encrypted communication and strong client authentication (two-way SSL). To learn more, see Configuring Transport-Level Security in the *Oracle Service Bus Security Guide*. • **Custom Authentication** - Specifies that an authentication token is contained in an HTTP header. The client's identity is established through the use of this client-supplied token. You must configure an Identity Assertion provider that maps the token to an Oracle Service Bus user. The custom authentication token can be of any active token type supported by a configured WebLogic Server Identity Assertion provider.
Dispatch Policy	Select a dispatch policy for this endpoint. Leave blank to use the default dispatch policy. Dispatch policy refers to the instance of WLS Work Manager that you want to use for the service endpoint. For information about Work Managers, see Using Work Managers to Optimize Scheduled Work and Create Global Work Managers in the WebLogic Server *Administration Console Online Help*.

Table 1-1 (Continued) Parameters for Configuring HTTP Transport for Proxy Service

Parameter	Description
Request Encoding	• For HTTP inbound transports: If the character set encoding parameter of the `Content-Type` header is not specified in Client Request, enter a character set encoding parameter. If you do not enter a value, the field defaults to `ISO-8859-1`. • For HTTP outbound transports: If you have not configured a request encoding, the Oracle Service Bus run time decides the most appropriate encoding while it makes a request to the business service. In the case of a non-passthrough scenario, the default character encoding is `UTF-8` at run time. However if it is a passthrough scenario, the run time will pass through the encoding received with the outbound response.
Response Encoding	Accept the default `ISO-8859-1` as the character set encoding for responses in HTTP transports, or enter a different character set encoding.
Advanced Settings	
Authentication Header	Enter the HTTP header (any except Authorization) from which Oracle Service Bus is to extract the token. This field is available only if you selected the Custom Authentication check box. For example, client-xyz-token.
Authentication Token Type	Select an authentication token type. Only the active token types configured for an Identity Assertion provider are available. (See “Configuring Identity Assertion Providers” under Configuring Custom Authentication in the Oracle Service Bus Security Guide for more information.) This field is available only if you selected the Custom Authentication check box.

For more information on how to configure HTTP transport based proxy services and advanced settings, see Transport Configuration in *Using the Oracle Service Bus Console*.

Configuring Business Services using the HTTP Transport

You must select HTTP as the transport protocol when you configure any type of business service based on HTTP and the endpoint URI is of the form:

```
http://<host:port/someService>
```

where:

- `host`: is the name of the system that hosts the service.
- `port`: is the port number at which the connection is made.
- `someService`: is a target service.

Note: You must specify the following endpoint URI when you configure a business service based on HTTPS.

```
https://<host:port/someService>
```

Table 1-2 describes all the parameters you can specify to configure HTTP transport for a business service.

Table 1-2 Parameters for Configuring HTTP Transport for Business Service

Parameter	Description
Timeout	Enter the response timeout interval in seconds. If you enter 0, there is no timeout.
HTTP Request Method	This parameter lets you to use one of the following HTTP methods in a request: • **POST** – Passes all its data, of unlimited length, directly over the socket connection as part of its HTTP request body. The exchange is invisible to the client, and the URL does not change. For REST-based requests, POST tells the transport to perform a create/replace operation or perform an action with the request. • **GET** – You can include as part of the request some of its own information that better describes what to get. This information is passed as a sequence of characters appended to the request URL in a query string. You can use GET in a business service with a Service Type of "Any XML Service," or with a Service Type of "Messaging Service" when the Request Message Type is set to "None." For REST-based requests, GET retrieves a representation of a remote resource. • **PUT** – You can use PUT in a business service with a Service Type of "Any XML Service" or "Messaging Service." PUT tells the transport to perform a create/replace operation with a REST-based request, such as uploading a file to a known location. • **HEAD** – You can use HEAD in a business service with a Service Type of "Any XML Service," or with a Service Type of "Messaging Service" when the Response Message Type is set to "None." HEAD tells the transport to get header information for a remote resource rather than getting a full representation of the resource in a REST-based request. • **DELETE** – You can use PUT in a business service with a Service Type of "Any XML Service" or "Messaging Service." DELETE tells the transport to perform a delete operation with a REST-based request. **Note:** If a method is already set in the $outbound/transport/request/http:http-method variable, that value takes precedence over any method you select for HTTP Request Method.

Table 1-2 Parameters for Configuring HTTP Transport for Business Service

Parameter	Description
Authentication	Select one of the following: • **None** - Specifies that authentication is not required to access this service. • **Basic** - Specifies that basic authentication is required to access this service. Basic authentication instructs WebLogic Server to authenticate the client using a user name and password against the authentication providers configured in the security realm, such as a Lightweight Directory Access Protocol (LDAP) directory service and Windows Active Directory. The client must send its user name and password on the HTTP request header. Basic authentication is strongly discouraged over HTTP because the password is sent in clear text. However, it is safe to send passwords over HTTPS because HTTPS provides an encrypted channel. **Warning:** By default, all users (authorized and anonymous) can access a business service. To limit the users who can access a business service, create a transport-level authorization policy. See Editing Transport-Level Access Policies in Using the Oracle Service Bus Console. • **Client Certificate** - Specifies encrypted communication and strong client authentication (two-way SSL). To learn more, see Configuring Transport-Level Security in the *Oracle Service Bus Security Guide*.
Service Account	A service account is an alias resource for a user name and password. This is a required field if you selected the **Basic Authentication Required** field. For more information, see Service Accounts in Using the Oracle Service Bus Console.
Follow HTTP redirects	Select this check box to specify that HTTP redirects (which are requests with a response code `3xx`) should be automatically followed. A re-direct occurs when you send an outbound request to the URL of a business service, and that service returns a response code (for example, `302`) that says the URL is no longer valid and this request needs to be sent to another URL. If the **Follow HTTP Redirects** check box is selected, Oracle Service Bus automatically re-sends the request to the new URL without any action on your part. Deselect this check box if you do not want the HTTP redirects to be automatically followed.
Dispatch Policy	Select the instance of WebLogic Server Work Manager that you want to use for the dispatch policy for this endpoint. The default Work Manager is used if no other Work Manager exists. For information about Work Managers, see Using Work Managers to Optimize Scheduled Work and Create Work Manager in the WebLogic Server *Administration Console Online Help*.

Table 1-2 Parameters for Configuring HTTP Transport for Business Service

Parameter	Description
Request Encoding	Accept the default `iso-8859-1` as the character set encoding for requests in HTTP transports, or enter a different character set encoding.
Response Encoding	Accept the default `iso-8859-1` as the character set encoding for responses in HTTP transports, or enter a different character set encoding.
Proxy Server	Enter a proxy server resource or click Browse to choose an entry from the list of configured proxy server resources.

For more information on how to configure this transport, see Transport Configuration in *Using the Oracle Service Bus Console*.

REST Support

The HTTP transport provides support for working with REST (Representational State Transfer) environments through Oracle Service Bus, whether you have REST clients that need to interact with non-REST service providers, non-REST clients that need to interact with REST-based service providers, or REST-to-REST services you want to expose through Oracle Service Bus.

In a REST pattern, you invoke HTTP methods (such as GET, PUT, HEAD, POST, and DELETE) on resources that are located at specific URLs. For example, when a user updates his own profile information in a Web application that uses REST, a POST action updates the user information in the database through the service's REST API.

Oracle Service Bus provides the following placeholder variables for handling REST-based requests for inbound and outbound communication:

- **$inbound or $outbound/transport/request/http:http-method** – For handling HTTP methods such as GET, PUT, HEAD, POST, and DELETE.
- **$inbound or $outbound/transport/request/http:query-string** – For handling query strings in a URL. For example, in the URL http://localhost:7021/myproxy/weather?operation=temperature&pincode=80439/, the query string is operation=temperature&pincode=80439.

- **$inbound or $outbound/transport/request/http:relative-URI** – For handling relative portions of a REST resource URL (relative to the proxy service URI). For example, in the URL http://localhost:7021/myproxy/weather, /weather is a relative URL to http://localhost:7021/myproxy.

REST in Proxy Services

With an Oracle Service Bus proxy service, you have the flexibility to interact with REST patterns, whether you are receiving REST-based requests or generating REST-based actions.

For example, if your team wants to develop REST-based applications and invoke services in a non-REST service provider, you can send REST operations through a proxy service and transform those operations into a format the service provider understands; or you could transform a non-REST request into a resource URL and invoke an operation in a REST-based service provider.

XQuery Examples

Following are XQuery examples of URI parsing using HTTP variables in a proxy server.

Relative-URI

A proxy service has a URI http://localhost:7001/weather, and you want to capture the relative URI parts of a request. You create the following XQuery:

```
<relative-URI>
{
for $c in
fn:tokenize($inbound/ctx:transport/ctx:request/http:relative-URI, "/")
where fn:string-length($c) != 0
return
<part>
{$c}
</part>
}
</relative-URI>
```

If a request comes with the URI of http://localhost:7001/weather/temperature/35457, the relative-URI will be /temperature/35457, and the XQuery output will be:

```
<relative-URI>
    <part>temperature</part>
    <part>35457</part>
</relative-URI>
```

Query-String

A proxy service has a URI http://localhost:7001/weather, and you want to capture the URL query string. You create the following XQuery:

```
<query-params>
{
for $c in
fn:tokenize($inbound/ctx:transport/ctx:request/http:query-string, "&amp;")
return
<param name="{fn:substring-before($c,"=")}"
value="{fn:substring-after($c,"=")}"></param>
}
</query-params>
```

If a request comes with a URI of http://server:7001/weather?operation=temperature&pincode=35457, the query-string will be operation=temperature&pincode=35457, and the XQuery output will be:

```
<query-params>
    <param name='operation' value='temperature'/>
    <param name='pincode' value='35457'/>
</query-params>
```

Headers

If your service requires specific headers to handle HTTP/REST methods, create user-defined HTTP header variables in your proxy service message flow.

REST in Business Services

With an Oracle Service Bus business service, you can invoke REST-based services.

For REST operations, the HTTP transport uses the value in the $outbound/transport/request/http:http-method variable. If that variable does not supply an HTTP method, the HTTP transport lets you select one of the following **HTTP Request Methods** in the transport configuration: POST, PUT, HEAD, GET, AND DELETE.

Note: If the business service uses a **Service Type** of WSDL Web Service, only the POST method is available.

Using the $outbound/transport/request-http/http-method variable, you can also supply your own methods. For example, you can use COPY, MOVE, and LOCK for WebDAV environments (Web-based Distributed Authoring and Versioning).

Use the following guidelines for setting $outbound variables:

- The transport does not provide run-time validation for custom methods or for manually set supported methods that do not comply with the constraints described in this section.
- Since $outbound is only available in a Routing node, you cannot specify a method name at run time for publish and service callout actions.
- If the $outbound query-string is set, the business service passes the query string as part of the URI while invoking an external service.
- If the $outbound relative-URI is set, the business service uses that value to generate the URI, which is relative to the business service URI.

  For example, in a business service with a URI of

  http://service.com/purchaseOrder

  and the following HTTP variables

  $outbound/transport/request-http/relative-URI: “/PO12367” and
  $outbound/transport/request-http/query-string: “item=NO1&color=black”

  The final resolved URI is

  http://service.com/purchaseOrder/PO12367?item=NO1&color=black

Response Codes for HTTP Business Services

The HTTP transport provides the following response codes for HTTP methods:

Method	Response Codes
POST	200 (OK) 201 (Created) 204 (No Content)
PUT	200 (OK) 201 (Created) 204 (No Content) 301 (Moved Permanently) – The server sends the response code. The business service handles this response by resending the original request.
HEAD, GET	200 (OK)
DELETE	200 (OK) 202 (Accepted) 204 (No Content)

E-mail Transport

You can select the e-mail transport protocol when you configure a Messaging Type or Any XML Service type of proxy service or business service. The following topics describe how to configure proxy services and business service using the E-mail transport.

Note: E-mail transport supports one-way messaging for services of Messaging Services type.

When you create a messaging type proxy service or a messaging type business service using e-mail transport you must set the response type to none in the Message Type configuration page.

Configuring Proxy Services using the E-mail Transport

When you configure a proxy service using the e-mail transport, you must specify an endpoint URI in the following format:

```
mailfrom:<mailserver-host:port>
```

where `mailserver-host:` is the name of the host mail server port: is the port used by the mail server host.

Table 1-3 describes the parameters you can configure for an e-mail transport based proxy service.

Table 1-3 Parameters for Configuring E-mail Transport for Proxy Services

Parameter	Description
Service Account	This is a mandatory parameter. This is the service account resource. The service account consists of a user name/password combination required to access the e-mail account.
Polling Interval	This is a mandatory parameter. This parameter specifies the polling interval in milliseconds. The default value is `60 ms`.
E-mail Protocol	This is a mandatory parameter. There are two types of protocol from which you can select, `imap` and `pop3`. The default protocol is `pop3`.
Read Limit	This is a mandatory parameter. This specifies the number of files to be read in each poll. The default value is `10`.
Pass By Reference	If this parameter is enabled, the file is staged in the archive directory and passed as a reference in the message headers.
Post Read Action	This is a mandatory parameter. This specifies whether the files should be deleted, moved, or archived after being read by the service. By default the files are deleted after reading.
Attachments	This is a mandatory parameter. This parameter specifies if the attachments are to be archived or ignored. By default this parameter is set to ignore. **Note:** If attachments are archived, the attachment files are passed as a reference in the message headers irrespective of the settings for the Pass By Reference parameter.
IMAP Move Folder	This is the destination of the messages if the `Post Read Action` is set to move. You must configure this field only if `Post Read Action` is set to move.

Table 1-3 (Continued) Parameters for Configuring E-mail Transport for Proxy Services

Parameter	Description
Download Directory	This is a mandatory parameter. It specifies the file system directory path to download the message.
Archive Directory	This is a mandatory parameter. A file URI that points to the directory where the files are archived. This field is active only when `Post Read Action` parameter is set to archive.
Error Directory	This is an optional parameter. This parameter specifies the type of encoding to read the request message. The default encoding is `iso-8859-1`.

For more information on how to configure e-mail services, see Transport Configuration in *Using the Oracle Service Bus Console*.

Configuring Business Services using the E-mail Transport

When you configure a business service using the e-mail transport, you must specify the endpoint URI in the following format:

```
mailto:<name@domain_name.com>
```

where `<name@domain_name.com>` is the e-mail destination.

Table 1-4 describes the parameters you can configure for an e-mail transport based proxy service.

Table 1-4 Parameters for Configuring E-mail Transport for Business Services

Parameter	Description
SMTP Server	You must select an SMTP Server from the drop-down list. You must first create the SMTP Server resource.
Mail Session	This parameter is optional. It is the JNDI name of the configured mail session. You can select mail sessions from the drop-down list.
From Name	You must first configure mail sessions in the WebLogic Server Console.
From Address	Create a Mail Session in WebLogic Server Administration Console. You must set the Mail Session parameter or the SMTP Server parameter.

Table 1-4 Parameters for Configuring E-mail Transport for Business Services

Parameter	Description
Reply To Name	This is an optional parameter. This parameter specifies the name from which the reply should be sent.
Reply To Address	This is an optional parameter. This parameter specifies the e-mail address from which the e-mail message should be sent.
Connection Timeout	This is an optional parameter. You can use this parameter to specify time in milliseconds after which the connection to the SMTP server times out.
Request Encoding	This is an optional parameter. This parameter specifies the type of encoding to read the request message. The default encoding is iso-8859-1.

For more information on how to configure this transport, see Transport Configuration in *Using the Oracle Service Bus Console*.

File Transport

You can select the File transport protocol when you configure a Messaging Type or Any XML Service type of proxy service and the endpoint URI is of the form:

`file:///<root-dir/dir1>`

where `root-dir/dir1` is the absolute path to the destination directory.

Note: File transport supports one-way messaging only for services of Messaging Service type.

When you create a messaging type proxy service or a messaging type business service using file transport you must set the response type to `none` in the Message Type configuration page.

Configuring Proxy Services using the File Transport

Table 1-5 describes the parameters you can specify to configure the file transport for a proxy service.

Table 1-5 Parameters for Configuring File Transport for Proxy Services

Parameter	Description
File Mask	This is an optional parameter. This specifies the files that should be polled by the proxy service. If the URI is a directory and `*.*` is specified, then the service will poll for all the files in the directory.
Polling Interval	This is a mandatory parameter. This specifies the value for the polling interval in milliseconds. The default value is `60 ms`.
Read Limit	This is a mandatory parameter. This specifies the number of files to be read in each poll. The default value is `10`. If `0` is specified, all the files are read.
Sort By Arrival	This is an optional parameter. This parameter indicates the sequence of events raised in the order of the arrival of files. The default value for this parameter is `False`.
Scan Subdirectories	This is optional. If enabled, the sub-directories are also scanned.
Pass By Reference	If this parameter is enabled, the file is staged in the archive directory and passed as a reference in the headers.
Post Read Action	This parameter is mandatory. This specifies whether the files should be deleted or archived after being read by the service. By default the files are to be deleted after reading.
Stage Directory	This is a mandatory parameter. This file URI points to the staging directory. **Note:** You must not put the stage directory inside the polling directory.
Archive Directory	This is a mandatory parameter. This file URI points to the directory where the files are archived. This field is active only when `Post Read Action` parameter is set to archive. **Note:** You must not put the archive directory inside the polling directory

Table 1-5 Parameters for Configuring File Transport for Proxy Services

Parameter	Description
Error Directory	This is a mandatory parameter. This URI points to a directory, in which the contents of the file will be stored in case of a error. **Note:** You must not put the error directory inside the polling directory
Request Encoding	This is an optional parameter. This parameter specifies the type of encoding to read the request message. The default encoding is `utf-8`.

For more information on how to configure file transport based proxy services, see Transport Configuration in *Using the Oracle Service Bus Console*.

Configuring Business Services using the File Transport

When you configure a business service using the file transport you must specify the endpoint URI in the following format:

```
file:///<root-dir/dir1>
```

where `root-dir/dir1` is the absolute path to the destination directory.

Table 1-6 describes the parameters you can specify to configure the file transport for a proxy service.

Table 1-6 Parameters for Configuring File Transport for Business Services

Parameter	Description
Prefix	This is an optional parameter. This parameter specifies the prefix to be attached to the filename.
Suffix	This is an optional parameter. This parameter specifies the suffix to be attached to the filename.
Request Encoding	This is an optional parameter. This specifies the type of encoding to read the message. The default encoding which will be used is utf-8.

For more information on how to configure this transport, see Transport Configuration in *Using the Oracle Service Bus Console*.

FTP Transport

You can select the FTP transport protocol when you configure a Messaging Type or Any XML Service type of proxy service and the endpoint URI is of the form:

`ftp://<hostname:port/directory>`

where

- `hostname`–is the name of the host on which the destination directory is stored.
- `port`–is the port number at which the FTP connection is made.
- `directory`–is the destination directory.

Note: File transport supports one-way messaging for services of Messaging Services type.

When you create a messaging type proxy service or a messaging type business service using FTP transport you must set the response type to `none` in the Message Type configuration page.

Configuring Proxy Services using the FTP Transport

Table 1-7 describes the parameters you can specify the parameters to configure the FTP transport for a proxy service.

Table 1-7 Parameters for Configuring FTP Transport for Business Services

Parameter	Description
User Authentication	You must select one of the following types of user authentication: • anonymous–If you select anonymous, you do not require any login credentials to login to the FTP server, but you optionally supply your e-mail ID for identification. • external user–If you select external user, you have to reference a Service Account resource, which contains your user name/password for the FTP server.
Pass By Reference	This is an optional parameter. If this parameter is enabled, the file is staged in the archive directory and passed as a reference in the headers.
Remote Streaming	This is an optional parameter. Setting this parameter to `True` will poll FTP files directly from the remote server at processing time.

Table 1-7 (Continued) Parameters for Configuring FTP Transport for Business Services

Parameter	Description
File Mask	This is a mandatory parameter. This specifies the files that should be polled by the proxy service. If the URI is a directory and `*.*` is specified, then the service will poll all the files in the directory.
Polling Interval	This is a mandatory parameter. This specifies the value for the polling interval in milliseconds. The default value is `60 ms`.
Read Limit	This is a mandatory parameter. This specifies the number of files to be read in each poll. The default value is `10`.
Post Read Actions	This is a mandatory parameter. This specifies whether the files should be deleted or archived after being read by the service. By default, the files are deleted after reading.
Transfer Mode	This parameter specifies whether the mode of file transfer is binary or ASCII. By default the transfer is `binary`.
Stage Directory	This is a mandatory parameter. This file URI points to the staging directory.
Archive Directory	This is a mandatory parameter. This file URI points to the directory where the files are archived. This field is active only when `Post Read Action` parameter is set to archive.
Error Directory	This is a mandatory parameter. This URI points to a directory location, where the contents of the file will be stored in case of a error.
Request Encoding	This is an optional parameter. This parameter specifies the type of encoding to read the request message. The default encoding is `utf-8`.
Advanced Settings	Click the icon to expand the `Advanced Settings` section. Configuring parameters in this section is optional. The parameters you can set in this section are: • Scan Subdirectories–This is optional. If enabled the sub-directories are also scanned. • Sort By Arrival • Timeout • Retry

For more information on how to configure file transport based proxy services, see Transport Configuration in *Using the Oracle Service Bus Console*.

Configuring Business Services using the FTP Transport

You can select the FTP transport protocol when you configure a Messaging Type or Any XML Service type of business service and the endpoint URI is of the form:

```
ftp://<hostname:port/directory>
```

where

- `hostname`–is the name of the host on which the destination directory is stored.
- `port`–is the port number at which the FTP connection is made.
- `directory`–is the destination directory.

Table 1-8 describes the parameters you must specify to configure the FTP transport for a business service.

Table 1-8 Parameters for Configuring FTP Transport for Business Service

Parameter	Description
User Authentication	You must select one of the following types of User Authentication: • **anonymous**–If you select anonymous, you do not require any login credentials to login to the FTP server. But you optionally supply your e-mail ID for identification. • **external user**–If you select external user, you have to reference a Service Account resource, which contains your user name/password for the FTP server.
Prefix for destination filename	This is a mandatory parameter. This parameter specifies the prefix to be attached to the filename.
Suffix for destination filename	This is a mandatory parameter. This parameter specifies the suffix to be attached to the filename.
Request Encoding	This is an optional parameter. This parameter specifies the encoding for the request message.

For more information on how to configure this transport, see Transport Configuration in *Using the Oracle Service Bus Console*.

CHAPTER 2

SFTP Transport

The SFTP transport is a poll-based transport that allows you to transfer files securely over the SSH File Transfer Protocol (SFTP) using SSH version 2. It polls a specified directory at regular intervals based on a predefined polling interval. After authentication, a connection is established between Oracle Service Bus services and the SFTP server, enabling file transfer. The SFTP transport supports one-way inbound and outbound connectivity.

The following are the key features of SFTP transport:

- The SFTP transport is available for the following service types:
  - Messaging service (with request message type specified)
  - Any XML service

  For more information about configuring service types, see Business Services: Creating and Managing and Proxy Services: Creating and Managing in *Using the Oracle Service Bus Console*.
- The SFTP transport supports processing of large messages. When you configure a proxy service, you can enable content streaming and specify whether large messages must be buffered in memory or in a disk file. For more information, see Streaming Body Content in *Oracle Service Bus User Guide*.
- For inbound message transfer, the QoS is set to **`exactly-once`**, which ensures that every message is processed at least once. For outbound message processing, the QoS is **`best-effort`**.

Note: For messages that are not transferred, you must create the error-handling logic (including any retry logic) in the pipeline error handler. For more information, see Proxy Services: Error Handlers in *Using the Oracle Service Bus Console*.

For more information about QoS in Oracle Service Bus messaging, see Modeling Message Flow in Oracle Service Bus in *Oracle Service Bus User Guide*

Environment Values

Environment values are predefined fields in the configuration data and are likely to change when you move the configuration from one domain to another (for example, from test to production). The following table lists the environment values associated with the SFTP transport.

Table 2-1 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 to which files are downloaded during the file transfer.
Error Directory	The location where messages are posted if there is a problem.
Managed Server for Polling	The managed server that is used for polling (in a cluster scenario).

For more information, see:

- Customization in *Using the Oracle Service Bus Console*
- Configuring Proxy Services
- Configuring Business Services.

General Principles of SFTP Authentication

The following principles are applicable to the SFTP authentication process for both proxy and business services:

- Connection: The Oracle Service Bus 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 Oracle Service Bus service.
  - For username-password authentication, the SFTP server authenticates the connection with the username and password.
- Authentication by the SFTP client**:** The Oracle Service Bus service always authenticates the SFTP server with the public-key/host/IP combination defined in the **`known_hosts`** file. For more information, see Creating the Known Hosts File.
- Connection establishment**:** The connection is established only when both the server and client authentications are successful.
- Transfer
  - If the client is a proxy service, the file (message) is downloaded from the SFTP server.
  - If the client is a business service, the file (message) is uploaded to the SFTP server.

Run-Time Behavior

Transferring files by using the SFTP transport involves the following steps:

1. The proxy service polls the input directory at regular intervals.

   Note: A new connection is created for each poll cycle.

2. If the proxy service finds a file in the input directory, it renames the file with a **`.stage`** extension. This renaming ensures that the service does not pick up the same files during the next polling cycle.

   The **`.stage`** file exists in the input directory until it is delivered.

Note: If the file cannot be retrieved from the input directory (due to network failure, for example), the **`.stage`** file is processed during a clean-up cycle. The clean-up cycle is performed every 15 minutes or after 15 polling cycles, whichever occurs later. If a **`.stage`** file exists during two consecutive clean-up cycles, it is processed again.

3. A JMS task is created for the message and added to the domain-wide JMS queue.
4. A domain-wide MDB receives the task and processes the message.

   Note: The task uses a pooled connection for processing the message. If a connection is not available in the pool, a new connection is created.

5. The message is delivered to the pipeline and the **`.stage`** file is deleted.

   Note: If an SFTP business service is configured, the service puts the message in the outbound directory through a pooled connection.

In the message is not delivered, the transport attempts to transfer it again and repeats the process up to a predefined number of attempts. If the message cannot be delivered, it is moved to the error directory.

Using the SFTP Transport

You can use the SFTP transport to transfer files securely using SSH File Transfer Protocol (SFTP).

The following sections describe how you can use the SFTP transport to transfer files securely:

- Enabling SFTP Authentication: This section describes the authentication methods that the SFTP transport supports.
- Configuring Proxy Services and Configuring Business Services: These sections describe how you can configure proxy and business services to use the SFTP transport.
- Handling Communication Errors and Troubleshooting: These sections provide information to help you solve problems that may occur while configuring or using the SFTP transport.
- Importing Resources: This section describes the SFTP services-specific policy and configuration details that you can preserve when you import resources.
- Importing and Publishing Services: UDDI Registries: This section lists the properties that are published when SFTP services are published to UDDI registries. It also lists the properties that are imported when SFTP services are imported from UDDI registries.

Enabling SFTP Authentication

The SFTP transport supports the following authentication methods:

- Username-password authentication
- Host-based authentication
- Public key authentication

Oracle Service Bus services authenticate the SFTP server based on the server details defined in a **known_hosts** file. So to enable server authentication, you must create a **known-hosts** file on the client machine.

Creating the Known Hosts File

The **known_hosts** file must exist in the server on which the Oracle Service Bus proxy services (inbound requests) or business services (outbound requests) run. The file must contain the host name, IP address, and public key of the remote SFTP servers to which the proxy service or business service can connect.

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

   Hostname,IP algorithm publickey

   – *Hostname* is the host name of the SFTP server.

   – *IP* is 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 algorithm that is supported.

   – *publickey* is the public key of the SFTP server. It must be in the Open SSH public key format.

   Example:

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

   The **known_hosts** file can contain multiple entries, but each entry must be on a separate line.

2. Move the **known_hosts** file to the **$DOMAIN_HOME\osb\transports\sftp** directory.

   Note: The directories /transports/sftp are not created automatically. You must create the directories.

Enabling Username-Password Authentication

Username-password authentication is the simplest and quickest method of authentication. It is based on the credentials of the user.

To enable username and password authentication for a service:

1. Create a static service account by using the user credentials on the SFTP server. For more information, see Service Accounts in *Using the Oracle Service Bus Console.*
2. Create a **known_hosts** file. For more information, see Creating the Known Hosts File.

Enabling Host-Based Authentication

Host-based authentication uses a private host key. This method can be used when all the users share a private host.

To enable host-based authentication for a service:

1. Configure a service key provider with an SSL client authentication key. For more information, see Service Key Providers in *Using the Oracle Service Bus Console.*
2. Create a **known_hosts** file. For more information, see Creating the Known Hosts File.
3. Configure the SFTP server to accept requests from Oracle Service Bus, which is a client to the SFTP server.

   For example, for an SFTP server on Linux, you must do the following:

   – Edit the **/etc/ssh/shosts.equiv** file and add the host name or IP address of the machine on which the Oracle Service Bus domain runs.

   – Edit the **/etc/ssh/ssh_known_hosts** file and add the host name or IP address of the machine on which the Oracle Service Bus domain runs, followed by a space and the public key.

     Note: You can extract the public key from the key store that was used while creating the service key provider. The public key must be in the Open SSH format.

Enabling Public Key Authentication

Public key authentication is performed using your own private key. This method can be used when each user has a private key.

To enable public key authentication:

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

   For example, for an SFTP server on Linux, you must extract the public key from the key store and enter the key in the **`$HOME/.ssh/authorized_keys`** file on the SFTP server. Ensure that the path and file exist.
3. Create a **`known_hosts`** file. For more information, see Creating the Known Hosts File.

Configuring Proxy Services

When you create a proxy service in the **Transport Configuration** page of the Oracle Service Bus Console, you must select the transport protocol as **`sftp`** and specify the endpoint configuration in the following format:

`sftp://`*`hostname`*`:`*`port/directory`*

- *`hostname`* is the host name or IP address of the SFTP server.
- *`port`* is the port on which SFTP server is listening. The default port for SFTP is `22`.
- *`directory`* is the location that is polled for files at regular intervals. This path to this directory is relative to the home directory of the user.

Note: Since the SFTP transport supports only message and XML service types, you must select **Messaging Service** or **Any XML Service** as the service type in the **General Configuration** page of the Oracle Service Bus Console.

When you select **Messaging Service** as the service type,

- You must specify **Binary**, **Text**, **MFL**, or **XML** as the request message type.
- You must set the response message type to **None** because the SFTP transport supports only one-way messaging.

For more information, see Proxy Services: Creating and Managing in *Using the Oracle Service Bus Console*.

Configure the proxy service as described in the following table.

Table 2-2 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 the required authentication method. • **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. 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. Users have their own private keys.
Service Account	Enter the service account for the user, or click **Browse** and select a service account. For information about using service accounts, see Service Accounts in *Using the Oracle Service Bus Console*.
Service Key Provider	This field is available only for the public key and host-based authentication methods. Enter a service key provider, or click **Browse** and select a service key provider. For more information, see Service Key Providers in *Using the Oracle Service Bus Console.*
Username	This value is required only when you select either the host-based or public key authentication method. • In host-based authentication, the user name is required for polling the home directory of the user on the SFTP server. • In public key authentication, the user name is required for polling the home directory of the user and for identifying the location of the public key on the SFTP server. Enter the user name.
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.

Table 2-2 Configuring SFTP Proxy Service (Continued)

Field	Description
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 must specify the archive directory relative to the SFTP user directory.
File Mask	You can use the file mask for transferring files of specific types. Enter a regular expression to select the files that you want to pick from the directory. The default value is **`*.*`**.
Polling Interval	Polling interval is the frequency at which the input directory is polled. Polling involves creation of an SFTP connection. Enter the interval (in seconds) at which the file must be polled from the specified location. The default value is **`60`**. **Note:** Avoid setting a low polling interval because a low interval causes frequent polls on the directory.
Read Limit	If numerous files exist in the poll directory, you can limit the number of concurrent transfers by selecting an appropriate value in this field. If you do not want to specify a limit, enter **`0`** (zero). The default value is **`10`**. **Note:** In some cases, the SFTP server may limit the number of concurrent connections; make sure that the read limit you define is lower than the server-defined limit.
Post Read Action	Select the action that must be performed on the message after the file is transferred. • **Archive**: The message is archived in the specified archived directory. • **Delete**: The message is deleted.

Table 2-2 Configuring SFTP Proxy Service (Continued)

Field	Description
Archive Directory	If **Post Read Action** is set to **Archive**, then, after the files are transferred, they are moved (from either the download directory or the remote location) to the archive directory. If you selected the **Pass By Reference** option, you must specify the archive directory. If remote streaming is enabled, the archive directory is with respect to the SFTP server. If remote streaming is disabled, the archive directory is available on the Oracle Service Bus machine. Specify the absolute path of the archive directory. **Note:** If the directory does not exist, it is created automatically. If you specify a relative path, the directory is created at a path that is relative to the Java process that starts the WebLogic Server.
Download Directory	During file transfer, the files are downloaded to this directory. If remote streaming is enabled, this option is disabled. Specify the absolute path of the directory on your local machine to which files are downloaded during the file transfer. **Note:** If the directory does not exist, it is created automatically. If you specify a relative path, the directory is created at a path that is relative to the Java process that starts the WebLogic Server.
Error Directory	If a problem occurs during file transfer, the messages are posted to the error directory. If remote streaming is enabled, the error directory is with respect to the SFTP server. If remote streaming is disabled, the error directory is available on the Oracle Service Bus machine. Specify the absolute path of the error directory. **Note:** If the directory does not exist, it is created automatically. If you specify a relative path, the directory is created at a path that is relative to the Java process that starts the WebLogic Server.
Request encoding	Accept the default value (**UTF-8**) as the character set encoding for requests in the SFTP transports.

Table 2-2 Configuring SFTP Proxy Service (Continued)

Field	Description
Advanced Settings	
Scan Subdirectories	Select this option if you want all subdirectories within the directory that is specified in the endpoint URI to be scanned recursively. **Note:** Scanning subdirectories requires additional processing overhead; so use this option judiciously.
Sort By Arrival	Select this option to deliver events in the order of arrival. This ensures that message delivery is not random, but based on the time at which the file is downloaded to the destination directory.
Timeout	Enter the socket timeout interval, in seconds, after which the connection must be dropped. If you do not want the connection to time out, enter **`0`**. The default value is `60`.
Retry Count	You can use this setting to enable multiple attempts in case of errors such as network failure. Specify the number of retries for SFTP connection failures. The default value is `3`.

For more information about configuring proxy services to use the SFTP transport, see Proxy Services: Creating and Managing in *Using the Oracle Service Bus Console*.

Configuring Transport Headers and Metadata

When you configure a proxy service, you can use a Transport Header action to set the header values in messages. The following table lists the transport header and metadata related to the SFTP transport.

Table 2-3 Transport Headers and Metadata

Header / Metadata	Description
`FileName`	This value is used as the file name in the destination directory.
`isFilePath`	This is a metadata field. The possible values are true and false. • True: **`FileName`** is interpreted as the absolute path of the file. • False: **`FileName`** is interpreted as the name of the file.
`filePath`	This is a response metadata field that indicates the absolute path at which the file specified in the **`FileName`** header is written.

Configuring Transport Headers in the Oracle Service Bus Message Flow

You can configure the transport headers only for outbound requests in the Oracle Service Bus message flow. In the pipeline, use a transport header action to set the header values in messages. For more information, see Proxy Services: Actions in *Using the Oracle Service Bus Console*.

Configuring Transports Headers and Metadata in the Test Console

You can configure the **`FileName`** transport header and the **`isFilePath`** metadata values in the Oracle Service Bus test console when you test the SFTP transport-based services during development. For more information, see Test Console in *Using the Oracle Service Bus Console* and Using the Test Console in *Oracle Service Bus User Guide*.

Configuring Business Services

When you create a business service in the **Transport Configuration** page of the Oracle Service Bus Console, you must select the transport protocol as **`sftp`** and specify the endpoint URI (location of the service) in the following format:

`sftp``://`*`hostname`*`:`*`port`*`/`*`directory`*

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

Note: Since the SFTP transport supports only message and XML service types, you must select **Messaging Service** or **Any XML Service** as the service type in the **General Configuration** page of the Oracle Service Bus Console.

When you select **Messaging Service** as the service type,

- You must specify **Binary**, **Text**, **MFL**, or **XML** as the request message type.
- You must set the response message type to **None** because the SFTP transport supports only one-way messaging.

For more information, see Business Services: Creating and Managing in *Using the Oracle Service Bus Console*.

Configure the business service as described in the following table.

Table 2-4 Configuring SFTP Business Service

Field	Description
User Authentication	The proxy service is authenticated by the SFTP server based on the specified user authentication method. Select the required authentication method. • **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. 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. Users have their own private keys.
Service Account	Enter the service account for the user, or click **Browse** and select a service account. For information about using service accounts, see Service Accounts in *Using the Oracle Service Bus Console*.
Service Key Provider	This field is available only for the public key and host-based authentication methods. Enter a service key provider, or click **Browse** and select a service key provider. For more information, see Service Key Providers in *Using the Oracle Service Bus Console*.
Username	This value is required only when you select either the host-based or public key authentication method. • In host-based authentication, the user name is required for polling the home directory of the user on the SFTP server. • In public key authentication, the user name is required for polling the home directory of the user and for identifying the location of the public key on the SFTP server. Enter the user name.
Timeout	Enter the socket timeout interval, in seconds, after which the connection must be dropped. If you do not want the connection to time out, enter **`0`**. The default value is `60`.
Prefix for destination File Name	Enter the prefix for the name of the file that is stored on the remote server.

Table 2-4 Configuring SFTP Business Service (Continued)

Field	Description
Suffix for destination File Name	Enter the suffix for the name of the file that is stored on the remote server.
Request encoding	Accept the default value (**`UTF-8`**) as the character set encoding for requests in the SFTP transports.

For more information about configuring business services using the SFTP transport, see Business Services: Creating and Managing in *Using the Oracle Service Bus Console*.

Handling Communication Errors

You can configure the SFTP transport-based business services to handle communications errors, which can occur when a connection or user authentication fails while connecting to the remote SFTP server. When you configure the business service, you can enable the business service endpoint URIs to be taken offline after a specified retry interval.

For more information, see the following topics in Monitoring in *Using the Oracle Service Bus Console*:

- "Configuring Operational Settings for Business Services"
- "Viewing Business Services Endpoint URIs Metrics"

Troubleshooting

Most of the errors occur while configuring an SFTP proxy or business service. The following are a few tips to help you understand and solve the errors:

- Make sure that you have an appropriately configured **`known_hosts`** file in place.
- For public key authentication, you must store the public key file on the server. For more information, see the documentation accompanying your SFTP server.
- The **`Connection refused`** error message indicates that the SFTP server is not available on the configured host and port.

- The **`Authentication failed`** error message indicates that the username or password is not valid, or that the public key is not configured correctly.
- The **`Connection did not complete`** error message is displayed after the actual error that caused the connection failure (example: **`Key not found`**) is displayed.
- The **`Key not found for IP, host`** error message indicates that the **`known_hosts`** file does not contain an entry that corresponds to the specified IP-host combination. If the entry exists, then try with another algorithm key; for example, if the earlier attempt was with an RSA key, try again with a DSA key.

Importing Resources

When you import a resource that exists in an Oracle Service Bus domain, you can preserve the existing security and policy configuration details of the resource by selecting the **Preserve Security and Policy Configuration** option. The following SFTP service-specific details are preserved when you import a resource:

- Client authentication method
- Reference to the service account (for services associated with username-password authentication)
- Reference to the service key provider (for services associated with host-based or public key authentication)
- User name (for services associated with host-based or public key authentication)

For more information about importing resources from the Oracle Service Bus Console, see Importing Resources in *Using the Oracle Service Bus Console*.

Importing and Publishing Services: UDDI Registries

When an SFTP service is published to the UDDI registry, `Authentication mode`, `Request encoding`, `Sort by arrival`, and `File mask` are the properties that are published.

Table 2-5 lists the properties that are imported from the registry when an SFTP service is imported from the UDDI registry.

Table 2-5 Properties Imported from UDDI Registry

Property	Description
Prefix for destination file name	The prefix for the name of the file that is stored on the remote server. The default value is **" "** (null).
Suffix for destination file name	The suffix for the name of the file that is stored on the remote server. The default value is **" "** (null).
Authentication mode	The authentication method that is imported from the registry. When an SFTP business service with user authentication is imported from an UDDI registry to Oracle Service Bus, a conflict is generated. • For username-password authentication, you must create a service account and associate it with the service. • For host-based or public key authentication, you must create a service key provider and associate it with the service.

After the service is import imported, the default value of the load balancing algorithm is **`round-robin`**.

For more information, see UDDI in *Using the Oracle Service Bus Console*.