Oracle® Secure File Transport

User's Guide

Release 5.4

E49654-04

November 2015

ORACLE®

Oracle Secure File Transport User's Guide, Release 5.4

E49654-04

Contents

Preface v

Audience v
Documentation Accessibility v
Conventions v

1 Oracle Secure File Transport Overview and Prerequisites

1.1 Overview of Oracle SFT 1-1
1.1.1 Oracle SFT Architecture 1-2
1.1.2 Supported Data Types 1-2
1.2 Supported Versions 1-3
1.3 Prerequisites 1-3
1.3.1 Firewall Limits 1-3
1.3.2 Oracle Single Sign On Account 1-4
1.4 Downloading and Installing Oracle ASR and SFT 1-4
1.4.1 Using ASR Manager Relay with Oracle SFT (optional) 1-5
1.4.2 Oracle SFT on IPv6 1-5

2 Running and Configuring Oracle SFT

2.1 Running Secure File Transport 2-1
2.2 Configuring Secure File Transport and Components 2-1
2.2.1 Configure the HTTP Listener to Receive Files from Explorer 2-1
2.2.2 Configure the HTTPS Listener to Receive Files from Explorer 2-2
2.3 Using Command Line Options 2-2
2.3.1 Modify the Oracle Secure File Transport (SFT) Configuration 2-3
2.3.2 Manage the Oracle SFT Listener 2-3

3 Using Oracle SFT to Send Files to Oracle

3.1 Prioritize an Explorer File 3-1
3.2 Send Files from Explorer to the HTTP Listener 3-2
3.3 Send Files from Explorer to the SFT Transfer Directory 3-2
3.4 Send a File with Priority 3-2

4 Troubleshooting Oracle Secure File Transport (SFT)

4.1 Configure E-mail Notification of File Transfer Failure 4-1

4.2 Configure Failure Retry Settings 4-1
4.3 View SFT Log Files 4-2
4.4 Resolving "Unauthorized" Problems 4-2
4.5 View the Oracle SFT Configuration 4-2

Index

Preface

This user's guide describes the Oracle Secure File Transport (SFT). SFT is an automated, configurable method for sending data collected by Explorer software, or other system telemetry data, to Oracle Corporation.

Audience

It is intended for all Oracle SFT users.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at
http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit
http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit
http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1

Oracle Secure File Transport Overview and Prerequisites

This chapter provides an overview of Oracle Secure File Transport (SFT) and includes the prerequisites required for installing and running the application.

The following topics are provided:

- Overview of Oracle SFT
- Supported Versions
- Prerequisites

1.1 Overview of Oracle SFT

Oracle Secure File Transport (SFT) supports data transfer between customer environments and Oracle. The SFT tool is used to periodically deliver Explorer data collector files for proactive reporting and for sending Explorer, core, log, or other files for support services diagnostics. SFT is designed to support customer network environments in which Explorer clients do not have Internet access and to provide a central point to manage Explorer telemetry.

SFT is a daemon process that runs in the background, periodically scanning a specified directory for new files and forwarding that data to the configured destination, Oracle Corporation. A daemon process runs in the background, rather than under your direct control. The daemon process restarts automatically on system reboots and continues running until it receives a system-wide interrupt command.

SFT is intended as an aggregation and transfer point for telemetry data from other hosts. It detects and validates configured file types then invokes a transfer process to send the data to the configured destination.

SFT is part of Oracle Auto Service Request (ASR) Manager (`asrmanager`) that is installed under a standard location, `/opt/asrmanager`.

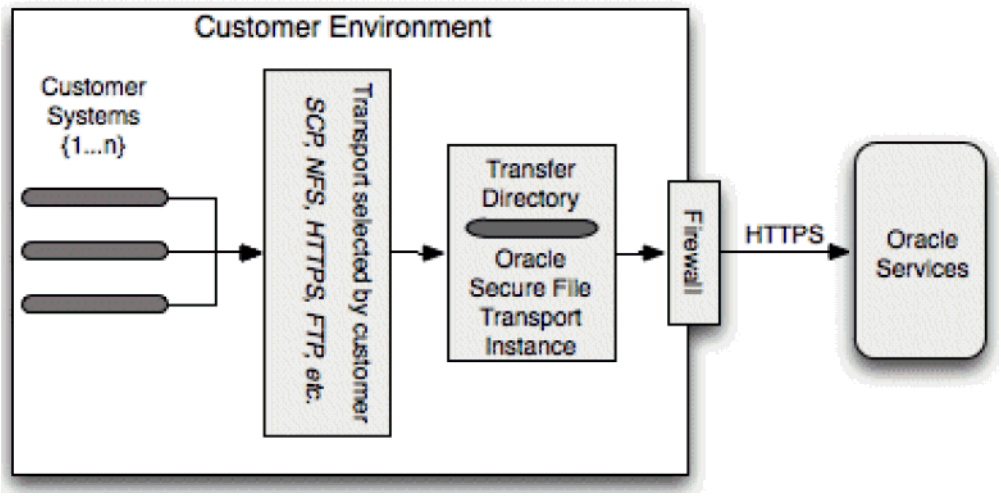
SFT is launched through a command line interface. SFT is a separate download that runs on versions 9 and 10 of the Solaris Operating System (OS) running Java 1.6.0 or higher. All transfers between your system and Oracle use industry-standard Secure Sockets Layer (SSL) encryption, which ensures the security of the transfer of your data.

The `/usr/bin/gzip` and `/usr/bin/tar` commands are required for transfer of Explorer files and should have been included with your Solaris OS. SFT runs as a software bundle within Oracle ASR. You must be a superuser to launch the ASR process or use any of the SFT or ASR command line options.

1.1.1 Oracle SFT Architecture

Figure 1–1 shows the configuration and communication routes of a typical SFT network:

Figure 1–1 Oracle SFT Architecture



SFT can support any number of Explorer clients. You may want to use multiple SFT instances for manageability and to ensure that files are sent to Oracle without unreasonable delay. A single SFT instance can support up to 32 concurrent transfers. You need to define the concurrency appropriate to your specific needs and infrastructure. The number of concurrent transfers depends on the volume of Explorer files you need to send, the average size of the files, and your network bandwidth. If a single SFT instance does not satisfy the file transfer volume, then additional Sun SFT instances should be installed on other hosts.

1.1.2 Supported Data Types

SFT supports two data types:

- **Explorer data packages.** These files should retain their filenames as created by Explorer (`explorer.<hostid>.*.tar.gz`). SFT does some checks to validate the Explorer file before attempting to send it. Any validation failures are logged and the file is moved to the directory for failed transfers.
- Any files to assist in support case resolution such as core files, log files, configuration files, and so forth. These files must be named with the service request (SR) number, optionally preceded by the word case, and followed by additional file description and an extension.

The preferred format is:

```
#-name.ext
```

Where `name` is the file name and extension is the file extension.

Sample filenames include:

```
1-234567890-core.gz
case_2-1234567_messages.Z
CASE-3-1234567890-vmcore.bz2
Case1-12345678.resolv.conf
1-12345678-core.dump
```

```
case-2-123456789.nsswitch.conf
```

If a file in the transfer directory does not match the filename pattern for any active slot, the file simply remains in the transfer directory and no information about that file is logged.

> **Note:** Only validated files that are awaiting transfer are reported with the `/opt/asrmanager/bin/sftransport info` command.

1.2 Supported Versions

Table 1–1 shows the platforms and software supported by Oracle SFT:

Table 1–1 Supported Platforms and Software

Platform	Version
Oracle Solaris	9, 10, and 11
Oracle Linux	5.3 or later
Red Hat Linux	6.3 or later
Java	1.6.0 or later

> **Note:** If you experience any `jar` errors during installation, then you will need to need to install the full Java JDK 1.6.0.

For details about software and operating system requirements, see *Verifying Operating System Requirements* and *Verifying Java Requirements* in the *Oracle® Auto Service Request (ASR) Manager User's Guide*:

`http://docs.oracle.com/cd/E37710_01/install.41/e18475/toc.htm`

1.3 Prerequisites

Review the following prerequisites before installing SFT:

- Firewall Limits
- Oracle Single Sign On Account

1.3.1 Firewall Limits

SFT communicates with Oracle's servers using HTTPS and encrypts information that it sends using 128-bit SSL encryption. The system where SFT is running requires outbound access to port 443.

If your firewall limits the hostnames that may be contacted, SFT communicates only with transport.oracle.com. Check the `/var/opt/asrmanager/sftransport/config/sftransport.xml` file to confirm which is in use for active slots.

If your firewall limits communication by target IP address, you may want to perform a lookup for the addresses of these hostnames. However, keep in mind that Oracle reserves the right to change the IP addresses of these hostnames.

1.3.2 Oracle Single Sign On Account

To run Secure File Transport, you must have a My Oracle Support account. To register for one, go to the following web site:

`https://support.oracle.com`

then follow the links to *Register for an Account*.

In addition, the account used must have Service Request Create/Update permissions on at least one Support Identifier in My Oracle Support. The permissions on the support identifier control what uploads a user can perform using SFT. For more information see:

- *How To Add A Support Identifier (SI) To Your User Account* (Oracle Support Document 1070936.1)
- *Oracle Diagnostic File Upload* (Oracle Support Document 1547088.2)

These documents are available from My Oracle Support:

`https://support.oracle.com`

1.4 Downloading and Installing Oracle ASR and SFT

Because SFT is part of Oracle Auto Service Request (ASR) Manager (`asrmanager`), it is downloaded and installed as part of an ASR installation into a standard location, `/opt/asrmanager`.

To download and install Oracle ASR:

1. Download and unzip the ASR software package from My Oracle Support:

   `https://support.oracle.com/rs?type=doc&id=1185493.1`

2. Open a terminal window and make sure you are logged in to the ASR Manager system as `root`.
3. From the directory where you unzipped the ASR package, install the ASR package using the following command:
   - For Solaris, run: `pkgadd -d <asrmanager-version_num-time_stamp>.pkg`
   - For Linux, run: `rpm -i <asrmanager-version_num-time_stamp>.rpm`
4. As the installation progresses, you are prompted to make several selections. Use the list below to determine how to respond to the installation prompts:
   - When prompted: "`. . . select all packages to process`," press **[Return]** to select all packages.
   - When prompted: "`. . . install conflicting files`," enter **Y**.
   - When prompted: "`. . . scripts will be executed with super-user permission during the process of installing this package`," enter **Y**.
5. Add the `asr` command to the `PATH` environment variable. This update would be made to the root user's `.profile`, `.cshrc`, `.kshrc`, or `.bashrc` files as needed (for both Solaris and Linux):

```
PATH=$PATH:/opt/asrmanager/bin
export PATH
```

Note: The instructions provided in this document assume that the `PATH` variable has been set.

6. Enable SFT:

```
/opt/asrmanager/bin/sftransport enable
```

7. Confirm proper network connectivity between the ASR Manager and Oracle, as described in *Test Connectivity from the ASR Manager to Oracle*. When complete, continue to *Registering the ASR Manager* in the *Oracle® Auto Service Request (ASR) Manager User's Guide*:

http://docs.oracle.com/cd/E37710_01/install.41/e18475/toc.htm

Note: Oracle SFT 5.4 does not require `SUNWsftransport` and `SUNWsasm` packages.

WARNING! However, the `/var/opt/SUNWsftransport` directory should remain and NOT be deleted. It still used by other applications (such as Explorer) to store files into that directory. Also, ASR 5.4 looks for files located in that directory.

Check for `SUNWsasm` packages and remove them if exist:

Solaris:

```
pkginfo -l SUNWsasm
pkgrm SUNWsasm
```

Linux:

```
rpm -qa SUNWsasm
rpm -e SUNWsasm
```

1.4.1 Using ASR Manager Relay with Oracle SFT (optional)

Oracle Secure File Transport (SFT) can use the ASR Manager Relay sharing a common connection to Oracle.

For details about the ASR Manager Relay, see *Enabling HTTP Receiver for ASR Manager Relay, Solaris 11, and SDP2* in the *Oracle® Auto Service Request (ASR) Manager User's Guide*:

http://docs.oracle.com/cd/E37710_01/install.41/e18475/ch2_asr_manager.htm#ASRUD134

At this time, only one layer is supported:

```
Oracle SFT --> ASR Manager Relay --> Oracle
```

1.4.2 Oracle SFT on IPv6

For IPv6, the ASR Manager server needs to be enabled for dual stack IPv6/IPv4. ASR Manager supports IPv6 to and from assets configured for ASR. The traffic outbound from the ASR Manager to `transport.oracle.com` currently only supports IPv4 traffic.

2

Running and Configuring Oracle SFT

This chapter described how to run Oracle Secure File Transport (SFT) and the configuration options supported.

The following sections are provided:

- Running Secure File Transport
- Configuring Secure File Transport and Components
- Using Command Line Options

2.1 Running Secure File Transport

To run SFT, enter the following command:

```
/opt/asrmanager/bin/sftransport start_listener
```

2.2 Configuring Secure File Transport and Components

The following configuration topics are presented:

- Configure the HTTP Listener to Receive Files from Explorer
- Configure the HTTPS Listener to Receive Files from Explorer

2.2.1 Configure the HTTP Listener to Receive Files from Explorer

The HTTP Listener is a separate daemon process from the main transfer process that receives data. It can be setup and enabled during the SFT installation procedure. If the Listener is enabled, the Listener port can be verified or changed during the SFT installation.

You can send core files and other case-data files from Explorer to the SFT transfer directory using the HTTP Listener.

1. In the `/etc/opt/SUNWexplo/default/explorer` configuration file, set the `EXP_TRANSPORT` variable to `http://server:port`.
2. Run Explorer with the `-p` command line option.
3. Configure then run Explorer with the `-T http://server:port` command line option.

You can also use the `explorer -g` option to specify the SFT transport server and port. The example below shows a sample output of this option.

Example: Using the 'explorer -g' Option

```
Automatic Submission
At the completion of Explorer, all output may be sent to Oracle or alternate
destinations.

Target: https://supportfiles.sun.com/curl
Send explorer output via HTTPS when -P is specified (y/n)?

Choose 'n' to specify an alternate target, such as your Secure File Transport
(SFT) listener
[]: n

When -P is specified, would you like Explorer output to be sent to an
alternate target destination, such as your Secure File Transport (SFT)
listener (y/n)?

If yes, then enter the http[s]://server:port
Otherwise, enter only a single '-' for your reply.
HTTPS destination or a '-'
[http://mysftransportlistener:88]:
```

2.2.2 Configure the HTTPS Listener to Receive Files from Explorer

The HTTPS Listener provides the same basic functionality as the HTTP listener, with added SSL encryption.

1. In the `/etc/opt/SUNWexplo/default/explorer` configuration file, set the `EXP_TRANSPORT` variable to `http://server:port`.
2. Run Explorer with the `-p` command line option.
3. Configure then run Explorer with the `-T http://server:port` command line option.
4. Generate the SSL certificate for the SFT host by following the SSL Certificate directions located at:

   `http://www.eclipse.org/jetty/documentation/current/configuring-ssl.html`

5. Modify the `/var/opt/asrmanager/sftransport/config/listener.xml` configuration file to enable SSL as follows:
   a. The `listener.xml` file has a section for `SslSocketConnector` that is commented out by default; un-comment this section and add the appropriate port and key/password configuration.
   b. Ensure no conflict with port 443, the default port on the SFT host. If port 443 is already being used then change the Listener port to another acceptable value.
   c. Comment out the `jetty.nio.SelectChannelConnector <Item>` element, so that `jetty.security.SslSocketConnector` is the only active connector. For more information, see the Jetty documentation.

2.3 Using Command Line Options

The following sections describe command line options for modifying the SFT configuration and for managing the HTTP Listener:

- Modify the Oracle Secure File Transport (SFT) Configuration
- Manage the Oracle SFT Listener

2.3.1 Modify the Oracle Secure File Transport (SFT) Configuration

Table 2–1 describes the command line options you can use to change the SFT configuration (`/opt/asrmanager/bin/sftransport`):

Table 2–1 Oracle SFT (sftransport) Command Line Options

Option	Description
enable	Enable Oracle Secure File Transport
disable	Disable Oracle Secure File Transport
start_listener	Start Oracle Secure File Transport listener
stop_listener	Stop Oracle Secure File Transport listener
show_listener_status	Show status of Oracle Secure File Transport listener
set_port	Set Oracle Secure File Transport listener port
set_directory	Set directory used for file transfer
show_config	Show configuration settings
info	Show current transfers
help	Display a list of commands
?	Display a list of commands

2.3.2 Manage the Oracle SFT Listener

Table shows commands and scripts you can use to manage the Oracle SFT Listener (`/opt/asrmanager/bin/sftransport`):

Table 2–2 Oracle SFT Listener Options

Option	Description
start_listener	Start Oracle Secure File Transport listener
stop_listener	Stop Oracle Secure File Transport listener
show_listener_status	Show status of Oracle Secure File Transport listener

3

Using Oracle SFT to Send Files to Oracle

This chapter describes how to send Explorer files to Oracle using Secure File Transport (SFT).

Oracle SFT has the ability to recognize two use cases for Explorer files, each of which is processed differently:

- **Proactive files** - proactive Explorer files are routed to the Risk Analysis Engine.
- **Reactive/on-demand files** - by default, SFT gives priority to the reactive/on-demand files

Reactive Explorer files are routed to Support Services personnel for analysis. When working with Support Services, you might be asked to send an Explorer file for extended diagnostics and troubleshooting. Once SFT is installed and configured, it can be used to send high-priority Explorer files.

Refer to the Services Tools Bundle documentation library for information about Explorer:

`http://docs.oracle.com/cd/E35557_01/index.htm`

The following topics are presented:

- Prioritize an Explorer File
- Send Files from Explorer to the HTTP Listener
- Send Files from Explorer to the SFT Transfer Directory
- Send a File with Priority

3.1 Prioritize an Explorer File

To send an Explorer file for customer support (that is, reactive) purposes, enter the following command:

```
explorer -sr {SR number} -options
```

where `{SR number}` is the iSupport service request (SR) number.

This causes SFT to prioritize the delivery of this Explorer file ahead of other files that might be queued, and it will deliver the file to an Oracle location where it can be readily accessed by Support Services.

3.2 Send Files from Explorer to the HTTP Listener

If a system has Explorer installed, use this command to send core files and other case-data files to the SFT transfer directory using the HTTP Listener:

```
/opt/SUNWexplo/bin/curl.{sparc or i386} -T {file}
"{Listener-URL}/?file={filename}"
```

where

- {file} includes a path to the file location on the local system
- {filename} in the target URL is the filename only, using the correct filename format that includes service request (SR) number. This file name does not have to match the filename on the local system.

For example:

```
/opt/SUNWexplo/bin/curl.sparc -T /var/core.gz
"http://my-sft-server:8080/?file=1-2345678.gz"
```

Note: Oracle recommends that you compress files to reduce the size of the data transfer, as shown by `core.gz`.

3.3 Send Files from Explorer to the SFT Transfer Directory

Explorer files placed in the SFT transfer directory will be sent to Oracle. The default location for the SFT transfer directory is:

```
/var/opt/asrmanager/sftransport/transfer
```

When running Explorer on the same server as SFT, you can run the `explorer -g` command and specify the SFT transfer directory. For example:

```
# explorer -g
Absolute path of the Explorer output top location?
# [/opt/SUNWexplo/output]: /var/opt/asrmanager/sftransport/transfer
```

For sending Explorer files on servers other than the SFT server, you have several choices:

- Use the HTTP Listener (see Send Files from Explorer to the HTTP Listener).
- Use NFS to share the SFT transfer directory to other servers on your network and configure Explorer to send output to the NFS-mounted SFT transfer directory.
- Use a file transfer method such as ftp, sftp, scp, etc., to send the Explorer file to the SFT transfer directory on the SFT server.

3.4 Send a File with Priority

When you select transferPath during the `pkgadd`, a subdirectory called `priority` is created in the `transferPath` directory. Files placed in this `priority` subdirectory are given preference over other files being transferred in the `transferPath` directory. However, since validation and file transfers occur in parallel, some non-priority items might finish transferring before a priority file. Explorer files that are generated for a specific support case (using the `explorer -C` option to provide a case number) are treated as priority files whether placed in the priority subdirectory or the main transfer directory.

4

Troubleshooting Oracle Secure File Transport (SFT)

This chapter describes how to troubleshoot Oracle SFT errors such as file transfer failure.

With SFT, you can:

- Configure file transfer failure settings, including:
  - E-mail notification of file transfer failure
  - Number of failure retries
  - Interval between retries
- View information about errors in the SFT log files.
- View the SFT man pages.

You can configure SFT to send e-mail notifications in the event of file transfer failure. SFT also provides the ability to configure the total number of retries in the event of transfer failure, and the wait time between these retries.

The following troubleshooting topics are provide:

- Configure E-mail Notification of File Transfer Failure
- Configure Failure Retry Settings
- View SFT Log Files
- Resolving "Unauthorized" Problems
- View the Oracle SFT Configuration

4.1 Configure E-mail Notification of File Transfer Failure

Follow the instructions in the `/var/opt/asrmanager/sftransport/config/logging.properties` file.

4.2 Configure Failure Retry Settings

Edit the following attributes in the `/var/opt/asrmanager/sftransport/config/sftransport.xml` file:

- `transferTries` attribute - This attribute defines the total number of attempts made to resend a file in the event of file transfer failure, including the original attempt.

If the transfer fails before completion, such as when the network connection is lost, the first retry resumes from the point at which the transfer failed.

If this attribute is set to 1, no retries are attempted.

- `secondsBetweenTries` attribute - This attribute defines the wait time, in seconds, before a transfer is retried after failure.

  The recommended value is 60 seconds, which allows time to clear up the original attempt. The value must be greater than 1 to enable the attribute.

4.3 View SFT Log Files

The SFT log files contain all information about file transfer attempts and any errors that occurred. Log files, which are in XML format, can be viewed with any text viewer.

To use an internet browser-based log viewer, see the `/opt/asrmanager/sftransport/logviewer/readme.txt` file. This file describes how to use the SFT listener process, which is included with SFT, to view the logs.

4.4 Resolving "Unauthorized" Problems

If you encounter an "Unauthorized" error messages in the SFT log file, there may be problems with the Oracle transport service. For example:

```
<transfer success="0" attemptNumber="19"
date="2013-11-10T11:38:58-0800"><file>/var/opt/SUNWsftransport/transfer/explorer.8
4004920.myhostname-2013.11.10.15.01.tar.gz</file>
<url>http://transport.oracle.com:8080/v1/queue/explorer</url>
<result status="1">Transfer failed after 0 seconds java.net.ProtocolException:
HTTP Error: 401 Unauthorized
```

If these problems continue to occur, open a Service Request using My Oracle Support:

https://support.oracle.com

4.5 View the Oracle SFT Configuration

```
run> /opt/asrmanager/bin/sftransport show_config

DESCRIPTION
The /var/opt/asrmanager/sftransport/configuration/sftransport.xml
configuration file is deployed when sftransport is enabled.

     This file can be edited directly to change Secure File Tran-
     sport  configuration.  The daemon must be restarted for con-
     figuration changes to take effect.  This file  is  used  for
     main  daemon parameter configuration as well as all transfer
     slot definitions.  Below is an example sftransport.xml file:
    ____________________________________________________________________________
    | <sftransport>                                                            |
    |   <config version="2.1">                                                 |
    |     <sleepSeconds>60</sleepSeconds>                                      |
    |     <transferTries>2</transferTries>                                     |
    |     <secondsBetweenTries>15</secondsBetweenTries>                        |
    |     <transferPath>/var/opt/SUNWsftransport/transfer</transferPath>       |
    |     <failedPath>/var/opt/SUNWsftransport/failed</failedPath>             |
    |     <diskThreshold>90</diskThreshold>                                    |
    |     <geo>AMER</geo>                                                      |
    |   </config>                                                              |
```

```
|   <slots>                                                                  |
|     <slot type="explorer" threads="2" archivePath="/archive/explorer-data">|
|       <url>/v1/queue/explorer</url>                                        |
|     </slot>                                                                |
|     <slot type="explorer" threads="0" archivePath="">                      |
|       <url>/v1/queue/inactive-example</url>                                |
|     </slot>                                                                |
|     <slot type="casedata" threads="1" archivePath="">                      |
|       <url>/v1/queue/case-data</url>                                       |
|     </slot>                                                                |
|     <slot type="srdata" threads="1" archivePath="">                        |
|       <url>/v1/queue/case-data</url>                                       |
|     </slot>                                                                |
|   </slots>                                                                 |
| </sftransport>                                                             |
|____________________________________________________________________________|
```

ELEMENTS

The following configuration elements are used by the Secure File Transport software:

<sleepSeconds>

defines the number of seconds between the times the daemon checks the main "transferPath" location for any new data that it may send. This attribute cannot be empty or less than 10. Secure File Transport recommends a minimum of 60 seconds for this attribute.

<transferTries>

defines the maximum total number of tries (attempts) to transfer any data file/package. This attribute cannot be empty or less than 1.

<secondsBetweenTries>

defines the number of seconds to wait between successive transfer attempts for any data file/package. This attribute cannot be empty or less than 0.

<transferPath>

defines the location where all data to be sent to Oracle will be placed. All transfer slots get assigned data to transfer from this location. There is a "priority" sub-directory under the "transferPath", and data placed under this sub-directory is given preference over the data under the main directory. This attribute cannot be empty and must be a valid and accessible path.

<failedPath>

defines the location where SFT places all data files/packages that were not able to be sent successfully. This attribute cannot be empty and must be a valid and accessible path.

<diskThreshold>

defines the threshold in percentage of full disk for "transferPath" and "failedPath" locations. Warning messages will start to be logged if diskspace usage in these locations goes over the threshold. This attribute may be zero to disable this check, or greater than

```
     0 and less than 100 to perform the check.

<geo>
     defines the geography of  the  SFT  installation  (e.g.
     AMER, EMEA or APAC).

<slot>
     is a member of the  <slots>  parent  element.   A  slot
     basically defines data types that are supported by SFT.
     There must be at least 1 active slot in order  for  SFT
     daemon to start successfully.

     "type" - defines a supported data type.  This attribute
     cannot  be  empty.  Oracle SFT supports three data
     types: "explorer", "casedata" and "srdata".  Only files
     matching the proper filename pattern for each slot type
     will be transferred.  See the sftransport(1m) man  page
     for filename details.

     NOTE: an SFT installation cannot  have  more  than  one
     active   slot   of   the  same  type.   In  the  sample
     sftransport.xml above, one explorer type slot is active
     (with  2  transfer threads) and the other explorer type
     slot is inactive (with 0 transfer  threads).   Both  of
     these  slots  cannot  be made active or the daemon will
     report a configuration error at startup.

     "threads" - defines the maximum  number  of  concurrent
     transfer  threads that should handle the data transfer.
     If this attribute is set to 0, then the  slot  is  con-
     sidered  "inactive".   The  number of threads should be
     chosen carefully on  a  case  by  case  basis,  and  it
     depends  on  the  volume  of  data  that  needs  to  be
     transferred  as  well  as  the  amount   of   available
     bandwidth.   The  maximum  value  allowed  by SFT is 32
     transfer threads.

     "archivePath" - is an optional attribute  that  can  be
     included for <slot>.  The value of the attribute is the
     path to a directory where files  will  be  moved  after
     successful transfer. If the attribute is omitted or has
     an  empty  value  then  files  are  deleted  from  the
     transferPath after successful transfer.  To temporarily
     disable archiving but still remember the previous  path
     used,  set  the  value  to  empty and note the previous
     value using "<!-- comment -->" syntax.

     "url" - url defines the destination path on  the  Tran-
     sport server. SFT only supports the following destinat-
     ions:
     /v1/queue/explorer for "explorer" data type,
     /v1/queue/case-data for "casedata" data type.
     /v1/queue/case-data for "srdata" data type.
     This attribute can  only  contain  either  one  of  the
     values  listed here.  The protocol and hostname portion
     of the destination URLs are defined in  the  configura-
     tion  file  for  Oracle Automated Service Manager. That
     base URL is shared among all bundles using  data  tran-
     sport.
     All regions: https://transport.oracle.com
```

Index

C

CLI options, 2-2
communication routes, 1-2
configure, 2-1
  HTTP listener, 2-1
  HTTPS listener, 2-2

D

daemon, 1-1
data types, 1-2

E

environment variables
  PATH, 1-4

F

firewall limites, 1-3

O

Oracle SFT
  architecture, 1-2
  configuration, 4-2
  overview, 1-1
  prerequisites, 1-3
  supported data types, 1-2
  supported versions, 1-3

P

platforms supported, 1-3
prerequisites, 1-3
  Oracle SSO, 1-4
priority, 3-2
Proactive files, 3-1

R

Reactive/on-demand files, 3-1
running, 2-1

S

send file, 3-2
software supported, 1-3
supported data types, 1-2
supported versions, 1-3

T

troubleshooting, 4-1