



TIBCO FTL®

Development

Version 6.10.1 | July 2023

Contents

Contents	2
About this Product	8
Product Overview	10
Package Contents	12
Directory Structure Reference	12
Sample Programs Reference	12
Brief Definitions of Key Concepts	15
Messaging Concepts	15
Infrastructure Concepts	16
Administrative Concepts	17
Information for Developers	19
API Reference Documentation	19
Sample Programs	19
C Programmer's Checklist	19
Java Programmer's Checklist	20
.NET Framework and .NET Core Programmer's Checklist	21
Go Programmer's Checklist	23
Restrictions on Names	24
Reserved Names	24
Length Limit	24
IPv4 and IPv6	25
Application Design	26
Structuring Programs	26

Structuring Programs in Go	27
Application Instance Identifier	28
Callbacks and Recursive Dispatch	29
Inline Mode	29
Request/Reply	29
Recovery of a Disabled Process Restart versus Reopen the Realm	30
Clean-Up	31
Consolidation with Loose Coupling	32
Endpoints	34
Abilities	35
Endpoints and Stores	36
Send: Blocking versus Non-Blocking	37
Messages	39
Message Objects in Program Code	39
Message Origin	39
Message Ownership	39
Message Access	41
Message Mutability	41
Copy of a Message	41
Messages and Thread-Safety	42
Field Values and Types	42
Field Data Type Reference	42
Storage of Field Values within Messages	44
DateTime	44
Formats: Managed, Built-In, and Dynamic	45
Format Names	46
Field Names	47
Flexibility in Formats and Messages	47
Field Access: Names and References	48
Reusing Message Objects	48

Built-In Formats Reference	49
Opaque Format	50
Keyed Opaque Format	50
String Encoding	50
DateTime Values Printable String Form	53
Go: Marshal Method for FTL Messages	53
Delivery	62
Inbound Message Delivery	62
Content Matchers	63
Match Semantics	65
Match String Syntax	65
Content Matcher Performance and Architecture	67
Subscriber Interest	67
Inline Mode	67
Callback Restrictions with Inline Mode	68
Transport Restrictions with Inline Mode	68
FTL Server Interactions	73
FTL Server Connect Call	73
Application Name	73
Client Label	74
Operation of the Realm Connect Call	75
Trust Properties of the Realm Connect Method	75
Trust File	76
Reconnect Properties of the Realm Connect Method	77
Update and Disable	77
Logs	78
Log Levels	78
Log Level Tuning via API	78
Log Output Targets	81

Log Content and Form	83
Advisory Messages	84
Advisory Message Common Fields Reference	84
Subscribing to Advisory Messages	85
Advisory Messages Catalog	86
DATALOSS FAILOVER_LOSS	88
DATALOSS SENDER_DISCARD	89
DATALOSS QUEUE_LIMIT_EXCEEDED	90
DATALOSS INCOMPLETE_MESSAGE	92
DATALOSS TPORT_DATALOSS	93
DATALOSS RECONNECT_LOSS	95
DATALOSS STORE_DISCARD_DATALOSS	96
DATALOSS UPSTREAM_LOSS	98
DATALOSS DIRECT_SUB_LOSS	99
ORDINAL_UPDATE	101
GROUP_STATUS	101
RESOURCE_AVAILABLE	102
RESOURCE_UNAVAILABLE	103
RETRANSMISSION RETRANSMISSION_REQUEST	105
RETRANSMISSION RETRANSMISSION_SENT	106
RETRANSMISSION RETRANSMISSION_SUPPRESSED	107
SUBSCRIBER_FORCE_CLOSE	109
LOCK_LOST	110
Notifications	111
Notifications Catalog	111
CLIENT_DISABLED	111
Groups of Applications	113
Introduction to Groups	113
Simple Fault Tolerance with Groups	113
Groups with More than Two Roles	115

Weights for Group Members	117
Groups Principles of Operation	119
Group Service	119
Group Members	119
Interactions within a Group	120
Side Effects of Groups	120
Techniques for Programming with Groups	121
Program Structure for Groups	121
Activation Interval	121
Disconnect	122
Group Status	122
Group Observer	123
Programmer's Checklist Addenda for Groups	124
Persistence: Stores and Durables	125
Purposes of Persistence	125
Basic Definitions for Persistence	127
Publisher Mode and Send Policy	129
Durable Subscribers	131
Standard Durables	132
Shared Durables	135
Last-Value Durables	138
Acknowledgment of Message Delivery	142
Message Delivery Behavior	142
Maximum Message Size	143
Delivery Count for Standard and Shared Durables	143
Programmer's Checklist Addenda for Stores and Durables	144
Key/Value Maps	146
Locks	146
Direct Publishers and Subscribers	149

Use Cases for Direct Publishers and Subscribers	151
Programming with Direct Publishers	152
Programming with Direct Subscribers	153
Multithreading with Direct Publishers and Subscribers	154
Multiple Direct Subscribers	155
Coordination Forms	156
TIBCO Documentation and Support Services	157
Legal and Third-Party Notices	160

About this Product

TIBCO® is proud to announce the latest release of TIBCO FTL® software.

The release is the latest in a long history of TIBCO products that leverage the power of Information Bus® technology to enable truly event-driven IT environments. TIBCO FTL software is part of TIBCO Messaging®. To find out more about TIBCO Messaging software and other TIBCO products, please visit us at www.tibco.com.

Product Editions

TIBCO Messaging is available in a community edition and an enterprise edition.

TIBCO Messaging - Community Edition is ideal for getting started with TIBCO Messaging, for implementing application projects (including proof of concept efforts), for testing, and for deploying applications in a production environment. Although the community license limits the number of production processes, you can easily upgrade to the enterprise edition as your use of TIBCO Messaging expands.

The community edition is available free of charge. It is a full installation of the TIBCO Messaging software, with the following limitations and exclusions:

- Users may run up to 100 application instances or 1000 web/mobile instances in a production environment.
- Users do not have access to TIBCO Support, but you can use TIBCO Community as a resource (community.tibco.com).

TIBCO FTL in the Community Edition has the following additional limitations and exclusions:

- Excludes transport bridges
- Excludes the RDMA transport protocol
- Excludes disaster recovery features
- Excludes customizable dashboards and monitoring gateway

TIBCO Messaging - Enterprise Edition is ideal for all application development projects, and for deploying and managing applications in an enterprise production environment. It

includes all features presented in this documentation set, as well as access to TIBCO Support.

Product Overview

TIBCO FTL® software is a messaging infrastructure product. It features high speed, structured data messages, and clearly defined roles for application developers and application administrators. TIBCO FTL software can achieve low message latency with consistent performance.

Components

TIBCO FTL software consists of these main components.

API Libraries

Developers use APIs in application programs.

FTL Server

The FTL server is a multi-purpose executable component that can consolidate several services into one server process: realm service, persistence service, transport bridge service, group service, authentication service, and eFTL service.

Combining services can simplify usage, especially in cloud-based installations.

FTL Services

An FTL server can provide one or more of the following services, as specified in its configuration file.

Realm Service

Applications obtain operational metadata from a realm service. The realm service funnels operational metrics from application clients to external monitoring points.

Authentication Service

The realm service can authenticate users against a separate authentication service or an internal authentication service.

Persistence Service

Persistence services store messages for durable subscribers.

Transport Bridge Service

Bridge services forward messages between two endpoints.

eFTL Service

eFTL services forward messages between eFTL clients and FTL clients. With eFTL, the messaging backbone can communicate with a variety of client devices, applications, and other things—smartphones, tablets, browsers, sensors.

Other Messaging Systems

TIBCO FTL can interoperate with the other component systems of TIBCO Messaging software, such as monitoring using [TIBCO® Messaging Monitor for TIBCO FTL®](#).

Package Contents

Directory Structure Reference

The TIBCO FTL installation directory contains the subdirectories in this table.

TIBCO FTL Directories

Directory	Description
bin	DLL files (for Windows). FTL server executable.
bin/modules	The FTL server manages the executable services of other related products, such as TIBCO eFTL. To enable this functionality, product installers for those products place their service components into the <i>FTL</i> product tree under this directory.
include	C API header files (in subdirectories).
lib	Library files (for UNIX and macOS). Java .jar files.
monitoring	Scripts to start and stop the monitoring gateway and the InfluxDB data base.
samples	Sample programs. For more detail, see Sample Programs Reference .
scripts	Post-installation scripts for Linux platforms.

Sample Programs Reference

Sample programs serve as models for your own programs. You can use sample programs to experiment with TIBCO FTL software, test for correct installation, and demonstrate

performance in your network environment.

Sample Programs

These tables describe some of the sample programs, however, the list is not exhaustive. For instructions on running the sample programs, and for descriptions of other sample programs, see the readme files in each directory.

Each sample program prints a usage summary in response to the -h command line option.

Sample Programs for One-to-Many Communication

Programs	Description
tibrecvex	tibrecvex creates a subscriber and outputs the messages it receives. Start this program first.
tibsendex	tibsendex publishes messages for tibrecvex.

Sample Programs for One-to-One Communication

Programs	Description
tibreply	tibreply creates a subscriber, and replies to request messages it receives. Start this program first.
tibrequest	tibrequest creates an inbox subscriber, sends request messages to tibreply, and receives replies at its inbox.

Files

Files in Samples Directory

File	Description
readme.txt	Instructions to compile and run sample programs.
setup	Script that defines environment variables for the samples, such as PATH, LD_LIBRARY_PATH and CLASSPATH. Start with this script.

Directories

Samples Directories

Directory	Description
bin	Executable sample programs, precompiled from C sources.
config	More sample configuration files, for use as instructional models, but not related to the sample programs.
docker	Docker resources and information.
helm	Sample to deploy FTL on a Kubernetes cluster with the default configuration.
jaas	Files that configure JAAS authentication and authorization for the sample scripts.
scripts	<p>Sample scripts to start and stop the FTL server. Before running the sample programs you <i>must</i> start the FTL server with this script.</p> <p>Sample configuration file for the FTL server.</p> <p>The readme.txt file contains instructions for using these samples.</p>
src	<p>Sample program source code in C, Java, and .NET. You may use these samples as models for your application programs.</p> <p>The readme.txt file contains instructions for compiling.</p>
yaml	FTL server samples. The readme.txt file contains instructions.

Brief Definitions of Key Concepts

These brief definitions are reminders of the key concepts of TIBCO FTL software.

For a more intuitive picture of TIBCO FTL software and its concepts, please read in TIBCO FTL [Concepts](#) as your first introduction to this product.

Messaging Concepts

Application programs (clients) use TIBCO FTL software to communicate by sending messages to one another. Programs send messages using *publisher* objects, and receive messages using *subscriber* objects.

FTL typically uses a message broker architecture. For low latency, FTL can be configured such that messages travel directly between peer application programs.

Messages and Fields

A *message* is a structured unit of data. The structure is flexible, and developers tailor the structure to the needs of the application.

Each message consists of a set of named *fields*. Each field can contain a value of a specific data type.

One-to-Many Communication

Publishers can send messages using *one-to-many* communication. These messages can reach potentially many subscribers.

A subscriber can use a *content matcher* to receive only those messages in which a particular set of fields contain specific values.

One-to-One Communication

For efficient *one-to-one* communication, publishers can also send messages that can reach one specific *inbox subscriber*. The *inbox* data structure uniquely identifies an

inbox subscriber.

Inbox subscribers cannot use content matchers. An inbox subscriber receives all messages directed to it.

Infrastructure Concepts

Applications and FTL servers communicate through an infrastructure and FTL topology.

Endpoint

An *endpoint* is the connection point for publishers and subscribers in communicating programs. Application architects and developers determine the set of endpoints that an application requires. Administrators formally define those endpoints. Programs create publisher and subscriber objects using those endpoints.

Transport

A *transport* is the underlying medium that moves message data between endpoints. For example, TCP transports and multicast transports can move messages among programs connected by a network, and a shared memory transport can move messages among separate program processes on a multi-core hardware platform.

Affiliated Servers and Sites

For larger-scope messaging systems, FTL servers at different geographic sites can cooperate to distribute services. These affiliated servers are typically arranged as a *primary* site with one or more *satellite* sites. Each primary or satellite site can consist of multiple cooperating *core* and *auxiliary* servers. A third type of site, Disaster Recovery (*DR*) site, serves as a complete backup/standby site in the system.

Persistence Stores and Durables

You can use persistence stores and durables to strengthen message delivery assurance, to apportion message streams among a set of cooperating subscribers, to provide last-value availability, to provide a key/value map, or to simply serve as a message broker. Stores can be replicated and/or written to disk within a persistence service to provide persisted messaging.

Persistence Clusters

Multiple persistence services can form a persistence cluster, where the persistence services form a quorum with an active persistence service, and backup, synchronized standby persistence services.

Administrative Concepts

A *realm* is a namespace that defines resources and configurations available to application programs. (Those resources include endpoints, transports, and formats.)

Administrators can use the following types of interfaces to define the realm:

- FTL Administrative GUI (Graphical User Interface)
- REST API (either via a command line tool like curl, or the Swagger extension on the GUI: REST API Reference)
- YAML file configuration options, which are read at FTL server startup
- FTL server command-line options (typically within a script)

The TIBCO FTL base library caches the realm definition in a *realm object* and consults the local realm object for information about endpoints, transports, and message formats. Application programs connect to the *realm service* to read the relevant parts of the realm definition. If the realm definition changes, the realm service updates its application clients.

Realm definition parameters fall into the following categories:

- Realm Properties - General and common settings for the entire realm
- Applications - Client programs that utilize publish, subscribe, monitoring, or other FTL client API features.
- Transports - Note that transports are not visible to application developers, rather, they are strictly the responsibility of the administrator. From the developer's perspective, these details are hidden behind endpoints.
- Persistence - Configuration of stores, persistence clusters, and zones.
- Bridges - A service that forwards messages among sets of transport buses.
- Formats - Definitions of message formats

Architects, administrators, and developers coordinate the detailed requirements of applications using *coordination forms* (see [Coordination Forms](#)).

When configuration changes are edited and stored, they then can be deployed, per a controlled deployment procedure.

Information for Developers

API Reference Documentation

Reference documentation for the TIBCO FTL API is available only in HTML format.

The documentation set includes API reference resources for each supported programming language.

Sample Programs

The directory `TIBCO_HOME/ftl/version/samples` includes sample programs that you can use as models for programming, compiling, linking, and running.

For more information, see [Sample Programs Reference](#).

C Programmer's Checklist

Use this checklist when developing C programs that use the TIBCO FTL API.

When using the group facility, see also [Programmer's Checklist Addenda for Groups](#).

Environment

Use the setup script in the samples directory to set environment variables.

Code

Include the header file `ftl.h` (which in turn includes other header files).

Compile

Compile programs with an ANSI-compliant C compiler.

Use the compiler flags in the Makefile in the samples/src/c directory.

Link

On UNIX platforms, use the linker flags `-ltib -ltibutil`.

On Windows platforms, link the corresponding C library files, `tib.lib` and `tibutil.lib`.

Run

On Windows platforms, the PATH variable must include the bin directory to use the TIBCO FTL DLL files.

On UNIX platforms, the LD_LIBRARY_PATH variable must include the lib directory to use the TIBCO FTL library files.

Ensure that the TIBCO FTL realm server is running, and that each client process can connect to it.

Java Programmer's Checklist

Use this checklist when developing programs that use the TIBCO FTL Java API.

When using the group facility, see also [Programmer's Checklist Addenda for Groups](#).

Environment

The CLASSPATH must include an archive file that contains the TIBCO FTL classes (`tibftl.jar` from the lib directory). Use the setup script in the samples directory to set environment variables.

Code

Java programs must import this package:

```
import com.tibco.ftl.*;
```

Compile

TIBCO FTL classes require Java 1.8 (or later) 64-bit.

The CLASSPATH must include an archive file that contains the TIBCO FTL classes (tibftl.jar from the lib directory).

Run

TIBCO FTL classes requires Java 1.8 (or later) 64-bit.

On Windows platforms, the PATH variable must include the bin directory to use the TIBCO FTL DLL files.

On Mac OS X platforms, the java.library.path property must include the lib directory to use the TIBCO FTL library files.

On other UNIX platforms, either the LD_LIBRARY_PATH variable or the java.library.path variable must include the lib directory to use the TIBCO FTL library files.

Ensure that the FTL server is running, and that each client process can connect to it.

.NET Framework and .NET Core Programmer's Checklist

Use this checklist when developing programs that use the TIBCO FTL .NET API.

When using the group facility, see also [Programmer's Checklist Addenda for Groups](#).

Environment

Set up the environment for .NET Framework 4.7.2 or later. Ensure that it is current with the latest updates.

TIBCO FTL classes require Microsoft Visual Studio 2017 for development.

TIBCO FTL software requires 64-bit support (in the operating system and .NET Framework/Core).

Use the setup script in the samples directory to set environment variables.

For .NET Framework, ensure that the PATH environment variable includes the .NET Framework SDK (%windir%\Microsoft.NET\Framework64\dotnet_version).

For .NET Core, ensure that LD_LIBRARY_PATH (UNIX), PATH (Windows) or DYLD_LIBRARY_PATH (Mac OS) points to TIBCO_HOME/ftl/<version>/lib (UNIX, Mac OS) or TIBCO_HOME\ftl\<version>\bin (Windows).

Also for .NET Core, ensure that the dotnet driver version 2.1 is installed.

Code

To simplify coding, programs can include this statement:

```
using TIBCO.FTL;
```

Compile

TIBCO FTL classes require .NET Framework 4.7.2 or later.

To use the TIBCO FTL classes, programs must reference the assembly TIBCO.FTL. If the .NET framework is properly installed, then installing TIBCO FTL registers the assembly with the Windows general assembly cache (GAC).

The assembly TIBCO.FTL is compiled with platform target x64. You must compile applications that use TIBCO.FTL accordingly.

Run

TIBCO FTL classes require .NET Framework 4.7.2 or later.

To use the TIBCO FTL classes, application processes must access the assembly TIBCO.FTL, which installs into the Windows general assembly cache (GAC).

The PATH variable must include the bin directory to use the TIBCO FTL DLL files.

You must arrange appropriate .NET security for your applications. The base library calls unmanaged code, and requires full trust.

Ensure that the FTL server is running, and that each client process can connect to it.

Go Programmer's Checklist

Use this checklist when developing programs that use the TIBCO FTL Go API.

When using the group facility, see also [Programmer's Checklist Addenda for Groups](#).

Environment

Use the setup script in the samples directory to set environment variables.

Ensure that the Go compiler is in the PATH environment variable.

Code

Include the package `tibco.com/ftl`.

If your program uses the groups API feature, include the package `tibco.com/ftl/group`.

Compile and Link

Compile programs with a Go compiler, version 1.12.1 or later.

On the compiler command line, set `CGO_CFLAGS` to `<FTL_HOME>/include`. For example:

```
CGO_CFLAGS="-I /opt/tibco/ftl/6.10/include"
```

On the compiler command line, set `CGO_LDFLAGS` to `<FTL_HOME>/lib`, and include all of the required libraries. For example:

```
CGO_LDFLAGS="-L /opt/tibco/ftl/6.10/lib -lssl -lcrypto -ltib -ltibutil -ltibgroup"
```

Run

On Windows platforms, the PATH variable must include the bin directory to use the TIBCO FTL DLL files.

On UNIX platforms, the `LD_LIBRARY_PATH` variable must include the lib directory to use the TIBCO FTL library files.

Ensure that the FTL server is running, and that each client process can connect to it.

Restrictions on Names

Names and other literal strings must conform to the restrictions in the following topics.

Reserved Names

All names that begin with an underscore character (`_`) are reserved. It is illegal for programs to define fields, endpoints, applications, transports, formats, durables, stores, clusters, or zones with these reserved names.

You may use the underscore character elsewhere, that is, where it is *not* the *first* character of a name.

Length Limit

All names are limited to a maximum length of 256 bytes.

This limit includes names of fields, endpoints, applications, transports, formats, durables, stores, clusters, or zones. It also extends to string values in content matchers.

If you use UTF-8 characters that are larger than one byte, remember that the limit restricts the number of bytes in the name, rather than the number of characters.

IPv4 and IPv6

TIBCO FTL software supports both IPv4 and IPv6.

TIBCO FTL components accept either IPv4 and IPv6 addressing in the following cases:

- FTL server GUI fields configuring these transport parameters:
 - RUDP transport: Host field
 - Static TCP transport: Host field
 - Dynamic TCP transport: Subnet Mask field
- Arguments to client API calls that specify client connections to FTL servers
- Values that specify ports, either in FTL server configuration files, or in FTL server administration utility command line arguments

All other cases accept only IPv4 addressing.

Notation

Specify IPv4 addresses in 4-part dot-decimal notation.

Specify IPv6 addresses in hexadecimal notation, with colon (:) separators, surrounded by square brackets. Square brackets *must* be present.


In situations where it is correct and meaningful to specify *star* (that is, asterisk, *) as a wildcard address, TIBCO FTL software interprets this wildcard as *both* an IPv4 wildcard *and* an IPv6 wildcard. (That is, it listens on all relevant interfaces in *both* protocols.)

You can specify the loopback address in IPv4 as either `localhost` or `127.0.0.1`, and in IPv6 as `:::1` or an equivalent notation.

Application Design

Structuring Programs

These steps outline the main structural components of most application programs that communicate using TIBCO FTL.

 **Note:** For Go program structure, see [Structuring Programs in Go](#).

Procedure

Task A Initializing TIBCO FTL Objects

1. Create a realm object by connecting to an FTL server. (C programs must first open the top-level FTL object, and then a realm object.)

Task B Defining Callbacks

2. Define callbacks to process inbound messages.
3. Define callbacks to process advisory messages, as needed.
4. Define callbacks to handle out-of-band notifications.
5. Define callbacks for timer events, timer completion, and queue completion, as needed.

Task C Sending Messages

6. Define methods to construct outbound messages.
7. Instantiate endpoints as publisher objects.
8. Arrange to call the send methods of publishers.

Programs usually call send methods in the context of a data-generation loop, or in the context of message callbacks, or both. (You can use timer callbacks to implement a data-generation loop.)

Task D Receiving Messages

9. Instantiate endpoints as subscriber objects. (With a durable, supply a name property.)

10. Create event queues, and add each subscriber to an event queue.
11. Start a loop to dispatch event queues.
Task E Recovery and Clean-Up
12. Recover from administrative disable (see [Recovery of a Disabled Process Restart versus Reopen the Realm](#)).
13. Exit cleanly (see [Clean-Up](#)).

Structuring Programs in Go

Application programs in the Go language differ in several ways from programs in other languages. These steps outline the main structural components of most Go application programs that communicate using TIBCO FTL.

Summary of Differences

- Go does not support FTL timer events.
- Queue objects do not require explicit dispatch.
- Subscribe calls are methods of event queue objects, and these methods automatically add the new subscriber objects to the queue.
- When an inbound message arrives, the queue places the message on a subscriber channel, where your message processing methods can receive it.
- FTL inline mode is not relevant to Go programs.

Procedure

Task A Initializing TIBCO FTL Objects

1. Create a realm object by connecting to an FTL server.

Task B Processing Events

2. Create channels for inbound messages, and define goroutines to process messages from those channels.
3. Create channels for advisory messages, and define goroutines to process advisories, as needed.
4. Create a channel for out-of-band notifications, and define a goroutine to process notifications.

5. Launch the goroutines that poll message channels.

Task C Sending Messages

6. Define structs for marshaling data to and from messages.
7. Define methods to construct outbound messages.
8. Instantiate endpoints as publisher objects.
9. Arrange to call the send methods of publishers.

Programs usually call send methods in the context of a data-generation loop, or during message processing, or both.

Task D Receiving Messages

10. Create an event queue object.
11. Create subscriber objects.

Supply a channel as an argument. (The goroutines that process messages on the channel are already running.)

With a durable, supply a name property.

Task E Recovery and Clean-Up

12. Recover from administrative disable (see [Recovery of a Disabled Process Restart versus Reopen the Realm](#)).
13. Exit cleanly (see [Clean-Up](#)).

Application Instance Identifier

Administrators can arrange transports to implement endpoints in different ways, and select among them at run time using an *application instance identifier*.

Application programs can obtain that identifier from the command line, a configuration file, or an environment variable, and then supply that identifier as a property value in the realm connect call.

Design this ability into all application programs from the outset, even if you do not expect to use it. Coordinate with administrators to agree upon a standard way for programs to obtain identifiers. See the "Durable Coordination Form" in the FTL [Product Guides](#) list.

Callbacks and Recursive Dispatch

When designing application callbacks, do not recursively dispatch the same event queue.

Illegal Dispatch of queue A invokes a callback that dispatches queue A.

Legal Dispatch of queue A invokes a callback that dispatches queue B.

Illegal Dispatch of queue A invokes a callback that dispatches queue B, which invokes a callback that dispatches queue A again.

Inline Mode

Programs that receive time-sensitive messages can use inline mode to favor low latency over high throughput. Inline mode reduces inbound message latency by consolidating transport I/O and message callback processing into one thread.

For a complete description of inline mode, its usage, requirements and restrictions, see [Inline Mode](#).

For background information to help you better understand inline mode, read all of [Delivery](#).

Do *not* use inline mode unless callbacks *always* return quickly (see [Callback Restrictions with Inline Mode](#)).

When specifying inline mode, programmers and administrators must coordinate to avoid illegal state exceptions. See:

- [Transport Restrictions with Inline Mode](#),
- "Application Coordination Form" in the FTL [Product Guides](#) list

Request/Reply

Request/reply is an important communication pattern. Proper use of this pattern places requirements on the runtime environment.

- The replying process must be operational before the requesting process sends requests.

- The transports that carry the requests and replies must have already established operational communications before either process sends a request or a reply.
- The replying process must reply to each message as received directly from the requesting process, using the `SendReply` call.

Design programs to ensure robust behavior in situations where these requirements are *not* satisfied.

For example, a program that sends a request and then waits indefinitely for a reply is fragile. If the replying process is not available, or the transport's communications are not operating, then the request message does not reach its intended recipient, and the requesting process does not receive any information about this failure.

A more robust program would repeat the request at intervals until it receives a reply, or until it exceeds some reasonable limit.

Recovery of a Disabled Process Restart versus Reopen the Realm

When the FTL server disables an application process, the application can recover in one of two ways: either create a new objects and resume operation, or exit and restart.

The appropriate course of action depends on business factors and program design factors:

- *Process restart cost.* The program's start sequence might be time-consuming, or use resources heavily. For example, a start sequence might load a large data set into process memory, or establish several database connections. Seek to avoid that restart cost by re-using the existing context and state.
- *Downtime cost.* Business factors might require minimal interruption of an application process.
- *Parallel activities.* An application might do some activities which do not require TIBCO FTL communication. It could be appropriate for those activities to continue non-stop operation while the program creates a new realm object. For example, a program could control machinery and also send sensor data to other applications. In this example the controller thread must not stop, even if sensor messages temporarily stop flowing.
- *Simplicity.* Unless any of the preceding factors prohibit it, in many cases the simplest

and fastest action is to exit and restart the program.

- *Fresh start.* An application's state could become stale while communications are suspended. Returning to a valid state might be more complicated or time-consuming than starting fresh.

Disabled Advisory

When the FTL server disables an application process, the process receives a `CLIENT_DISABLED` advisory. This advisory signals the need for recovery action.

Clean-Up

Design programs to behave appropriately when they exit, and when they create a new realm object and its associated objects. (For example, creating new realm objects could be a recovery path after the FTL server disables the client process.)

Proper clean-up serves two goals:

- The FTL server and administrators can distinguish application processes that exit cleanly from processes that exit abnormally. When a process cleans up, you can infer that it exited deliberately, rather than unexpectedly.
- Clean-up manages the resources within a process that closes and reopens the realm but does not exit.

Program Exit

When a program exits, it is important to close the realm object. This step closes the FTL server's connection to the program process. The FTL server stops monitoring the process.

When a program exits, it is not necessary to close or destroy other objects associated with the realm object.

Nonetheless, in C programs, you must close the top-level FTL object as well as the realm object.

Close and Reopen the Realm

In contrast, the clean-up requirements are different when a program does not completely exit, but instead creates a new realm object. In this situation, programs must do these

steps, in order:

Close or destroy objects associated with the defunct realm object: including messages, property objects, field reference objects, content matchers, subscribers, publishers, inboxes, and event queues.

Close the defunct realm object.

Open a new realm object (that is, connect to the FTL server).

Create objects associated with the new realm.

Consolidation with Loose Coupling

With process transports, program threads within a process can communicate with one another by publishing and subscribing to messages. The main use case for process transports is consolidation of several application processes into one process, to boost performance by decreasing message latency.

To understand the concept of consolidation, consider a purely administrative first step toward the goal of decreasing latency. The administrator can run cooperating application processes on a single host computer, where they can communicate using a shared memory transport.

A second step is analogous, but involves programming. The developer can consolidate the loosely-coupled modules of a distributed application into a single program, where they run in separate threads that communicate using a process transport.

When consolidating application modules, you may retain the same endpoint structure as before consolidation. That is, if two modules each used a separate endpoint name before consolidation, the consolidated program can continue to use the same two endpoint names, and the administrator can bind them both to the same process transport. (Notice that this endpoint structure reflects the loose coupling among the module threads.)

✓ **Tip: Avoid Copying Messages**

For best performance with a process transport, avoid the need to copy messages:

- Publish messages to only one subscriber, in one receiving thread. Publishing a message to two or more subscribers in two or more receiving threads requires a separate copy of the message for each receiving thread.
- Set the publisher property to release messages to send, and set the subscriber property to release messages to callback.

Endpoints

An endpoint is an abstraction that represents a set of publishers and subscribers in communicating programs.

Programming

Within an application program, an endpoint begins as a name. Program code uses the endpoint name to create endpoint instances, that is, publisher and subscriber objects. Then programs use the publishers to send messages, and the subscribers to receive messages.

Each subscriber object and each call to a publisher send method introduces an ability requirement (see [Abilities](#)). Application architects and developers record these requirements in endpoint coordination forms. See the "Endpoint Coordination Form" in the FTL [Product Guides](#) list.



Tip: For many applications or communicating application suites, a single endpoint name suffices.

Configuration

Administrators configure transport connectors to satisfy those ability requirements. Connectors bind transports to endpoints. Those transports implement the endpoints, transferring message data from publishers to subscribers.

Administrators can also view an endpoint as a complex entity, embracing four separate communication abilities. A transport connector can separately enable any subset of those four abilities.



Tip: The default application definition is a valid configuration for applications that use only one endpoint.

Abilities

An endpoint has four communication abilities. A separate aspect of the API embodies each of these abilities. The following table summarizes the four abilities.

Each of these four abilities and the API call that embodies it correspond to a distinct sub-stream of messages, called an *ability sub-stream*.

Endpoint Abilities: Definitions

Ability	API	Description
One-to-Many Receive	Subscriber object	Carries one-to-many messages inbound to the endpoint's subscribers in the application.
One-to-One Receive	Inbox subscriber object	Carries one-to-one messages inbound to the endpoint's inbox subscribers in the application.
One-to-Many Send	Send call of a publisher object	Carries one-to-many messages outbound from the endpoint's publishers in the application.
One-to-One Send	Send-to-inbox call of a publisher object	Carries one-to-one messages outbound from the endpoint's publishers in the application.

Notice that each ability combines two dimensions: *reach* and *direction*:

- *Reach*
 - *One-to-many abilities* carry messages that can reach *potentially many* subscribers.
 - *One-to-one abilities* carry messages that can reach *one* specific *inbox* subscriber.
- *Direction*
 - *Receive abilities* carry messages *inbound to* an application.
 - *Send abilities* carry messages *outbound from* an application.

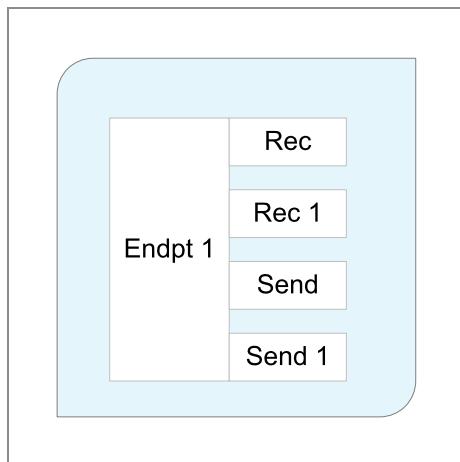
Endpoint Abilities Matrix

	Inbound	Outbound
One-to-Many	Receive	Send
One-to-One	Receive Inbox	Send Inbox

Administrators can configure these abilities in the FTL server GUI (see [Endpoint Details Panel](#)).

Endpoint and its abilities are represented with the following shape. Here, Endpoint 1 has four abilities: Receive, Receive 1, Send, and Send 1.

Figure 1: Four Endpoint Abilities



Endpoints and Stores

When an application uses persistence stores and durables, endpoints play an additional role. Administrators can associate each application endpoint with at most one persistence store.

That persistence store serves all publisher and subscriber instances of the endpoint, in all process instances of the application.

Programs can supply either a durable name or a subscriber name to the create subscriber call, connecting the new subscriber object to a specific durable within the endpoint's persistence store.

Number of Endpoints

For many applications a single endpoint name suffices.

Minimizing the number of endpoints usually simplifies design, programming, and administration. Justify each additional endpoint based on requirements, for example:

- A functional requirement (such as forwarding)
- A business requirement to separate the data streams (such as security, or data priority)
- An administrative requirement to control the endpoints in different ways (such as efficiency, or flexibility)

Notice that *endpoint* is not analogous to the concept of *destination* in the Java Messaging System (JMS). Within a program, one endpoint name can yield several subscriber objects, each selecting a different subset of inbound messages. Furthermore, one endpoint can instantiate publishers as well as subscribers.

Tactics to Reduce Endpoints

If you think an additional endpoint might be necessary, consider whether these tactics might reduce that need, and simplify the situation:

- A program can create several publishers and subscribers from a single endpoint name.
- Administrators can define connectors to carry the four abilities of an endpoint in a way that either merges their sub-streams, or keeps them separate.
- Administrators can configure all application instance definitions to implement an endpoint using a common bus as a shared communication medium, or configure disjoint subsets of instances that use totally separate buses.

Send: Blocking versus Non-Blocking

Administrators determine the behavior of send calls when a transport bus is full. Program developers may advise administrators concerning the correct behavior.

Send calls in an application program place outbound messages on a bus, which is external to the program process. A transport mediates this I/O operation. Under normal circumstances, the I/O operation completes quickly, and the send call returns.

If the bus is *full*, that is, it cannot accept any more messages, then two behaviors are possible. Administrators select one of these two behaviors, and configure it in the transport definition.

Blocking and Non-Blocking Send

Behavior	Description
Blocking Send	When the bus is full, the send call blocks, and does not return until it has placed all the outbound message data on the bus.
Non-Blocking Send (Default Behavior)	<p>When the bus is full, the transport buffers outbound messages in a backlog buffer in process memory until the bus can accept them. The send call returns.</p> <p>When the bus can accept more messages, the transport automatically moves them from its backlog buffer to the bus.</p> <p>If the backlog buffer overflows, the transport discards the oldest messages in the buffer to make room for new messages. The discarded messages do not arrive at slow receivers. The base library reports dataloss advisories to slow receivers.</p>

Use [TIBCO FTL Endpoint Coordination Form](#) to document the correct behavior.

To configure this behavior in a transport definition, see “Transport Definition Reference.”

Messages

Message Objects in Program Code

The following categories describe messages and the ways that your program code can interact with them.

Message Origin

Origin is the way in which a message object comes into existence. The origin of a message within a program is either local or inbound:

- A message that program code creates using an explicit call is a *local* message.
- A message that a program receives through a subscriber is an *inbound* message.

Message Ownership

Either your program code owns a message, or the TIBCO FTL library owns it. Ownership depends in part upon message origin, but releasing a message can change its ownership.

Release of Message Ownership

Subscribers can release ownership of inbound messages. Such *released inbound* messages belong to your program code, effective upon dispatch to your callback.



Tip: Releasing messages is appropriate when a callback delegates message processing to a separate thread.

To enable release to callback behavior, the program must supply a property to the subscriber create call.

Message Ownership, Determining Factors

Origin	Released	Ownership
Local	No	Your program code owns a local message.
Inbound	No	The library owns an inbound message.
	Release to callback	Your program code owns an inbound message that the subscriber has released to the callback.

Destruction

The responsibility to destroy a message depends entirely on the current ownership of a message.

Message, Responsibility to Destroy

Ownership	Responsibility to Destroy
Program code	Program code
Library	Library

SubMessages

When program code owns a message that contains nested submessages, destroying the outer message does not automatically destroy submessages contained within its fields or arrays. To effectively reclaim storage, the program must first destroy all the inner submessages and then the outer message.

Message Access

Message origin and current ownership determine the time frame within which your program can safely access a message object and its data.

Message Access, Determining Factors

Origin	Released (Ownership)	Access
Local	No (program code owns)	Until your program destroys the message
Inbound	No (library owns)	Until your callback returns
	Released to callback (program code owns)	Until your program destroys the message

Message Mutability

Mutability indicates whether your program may modify a message:

- A program may modify a *mutable* message by adding, deleting, or changing field values.
- A program cannot modify an *immutable* message in any way.

Mutability depends entirely on the origin of a message.

Message Mutability Depends on Origin

Origin	Mutability
Local	A local message is mutable.
Inbound	An inbound message is immutable, even if the subscriber released it to the callback.

Copy of a Message

Programs can copy any message.

- The copy is local, even if the original message is inbound.
- Your program owns the copy, even if the library owns the original.
- Your program can pass the copy to another thread.
- The copy is mutable, because it is local. Modifying the copy does not affect the original.
- The copy, along with all of its data content, is completely independent of the original inbound message. Even if the library destroys the original, the copy remains accessible. (See also, [Storage of Field Values within Messages](#).)

Messages and Thread-Safety

Messages are *not* thread-safe. Ensure that only one thread at a time accesses a message and its data.

Field Values and Types

Messages contain data values in a set of fields. Structurally, a field pairs a name of type string with a value of a specific data type.

The format of a message defines the data type of each field that the message can contain.

Field Data Type Reference

A data type describes the value of a field within a message or a message format.

Administrators use the type names in the first column of the following table to define formats.

Programs denote the data type of message fields using the type constants in the second column of the table.

Field Data Types

Type Name (in Realm)	Type Constant (in Programs)	Description	Primitive
long	TIB_FIELD_TYPE_LONG	A long integer.	Yes
long_array	TIB_FIELD_TYPE_LONG_ARRAY	An array of long integers.	No
double	TIB_FIELD_TYPE_DOUBLE	A double-length floating point number.	Yes
double_array	TIB_FIELD_TYPE_DOUBLE_ARRAY	An array of double-length floating point numbers.	No
string	TIB_FIELD_TYPE_STRING	A UTF-8 string.	No
string_array	TIB_FIELD_TYPE_STRING_ARRAY	An array of UTF-8 strings.	No
opaque	TIB_FIELD_TYPE_OPAQUE	An opaque byte-array.	No
message	TIB_FIELD_TYPE_MESSAGE	A message (that is, the field's value is a submessage).	No
message_array	TIB_FIELD_TYPE_MESSAGE_ARRAY	An array of messages.	No
inbox	TIB_FIELD_TYPE_INBOX	An inbox.	No
datetime	TIB_FIELD_TYPE_DATETIME	A DateTime value.	No
datetime_array	TIB_FIELD_TYPE_DATETIME_ARRAY	An array of DateTime values.	No

Storage of Field Values within Messages

Values stored in a message field are part of the message, that is, they reside in memory associated with the message, and allocated by the library.

When a field's type is a primitive type, calls that get the field's value copy that value from the message. In contrast, when a field's type is non-primitive, calls that get the field's value return a pointer to memory within the message. (The fourth column of the table in [Field Data Type Reference](#) indicates primitive and non-primitive types.)

Programs must *not* modify non-primitive values that reside in memory associated with a message. For example, you must not set the value of a cell in a long array extracted from a message.

Furthermore, non-primitive values remain valid only for a limited time:

- A subsequent call that sets the value of that field invalidates a pointer returned by a preceding get call.
- Destroying the message invalidates all pointers returned by preceding get calls.

DateTime

Application programs can use the TIBCO FTL data type `DateTime` to represent date and time values with large range and nanosecond precision.

`DateTime` values combine two numeric components:

- The `sec` component represents whole seconds with up to 64 bits. Zero denotes the UNIX epoch: midnight entering January 1, 1970.
- The `nsec` component represents nanoseconds after the time that the `sec` component denotes. Although the data structure stores this component in a signed 64-bit integer, this component is always non-negative, between zero and 999,999,999 (inclusive).

For example, the value -1 seconds plus 999,999,998 nanoseconds represents December 31, 1969, 2 nanoseconds before midnight (that is, 2 nanoseconds before the epoch).

Formats: Managed, Built-In, and Dynamic

A *format* defines the set of fields that a message can contain: including field names and data types.

TIBCO FTL software supports three broad categories of format: managed, built-in, and dynamic formats. These categories have differing constraints and performance characteristics.

Dynamic Format

An application can define a format dynamically, as it constructs a message. That is, the sending program implicitly determines the set of fields and their data types as it sets field values.

When a program creates a message, and specifies an unrecognized format name (that is, neither built-in nor preloaded), then TIBCO FTL software automatically treats it as a dynamic format.

While easy to use, dynamic formats are inefficient because each message must be self-describing. That is, a dynamic format message necessarily includes its own format metadata. Expect larger message sizes, slower transmission, slower processing, and longer field access times.

Dynamic formats are useful for rapid prototyping projects. To improve performance, you can switch to defining the application's formats as managed formats when the project nears the production stage.

Unnamed Dynamic Format

A program can create a message with a dynamic format, but supply null as the format name. Such *unnamed dynamic formats* are single-use. Administrators cannot ever upgrade them to managed formats.

You can use unnamed dynamic formats as a convenience when you cannot determine the structure and content of a message in advance. Unnamed formats save you the effort of naming the formats and keeping track of the names.

The performance of unnamed dynamic formats is identical to named dynamic formats.

Managed Format

Application architects and developers determine the set of formats that an application needs. Administrators then define those managed formats globally.

Administrators make managed formats available to an application by including them as *preload formats* for the application.

Programs can use these managed formats to compose new messages, or to unpack inbound messages. A message with a managed format is small and fast. It does not carry format metadata because that metadata is available to applications from the FTL server.

For efficiency and for safety, administrators can use the `Manage All Formats` and `Dynamic Message Formats` parameters to restrict the formats available to some or all of the applications in a realm. That is, administrators can require that applications use only preload formats and built-in formats, and prohibit applications from using dynamic formats.

Built-In Format

TIBCO FTL software defines a set of highly optimized built-in formats, which are defined within the base library and always available to all applications. No administrative action is required to make them available.

The performance characteristics of built-in formats are similar to managed formats. When used properly, a built-in format can outperform a managed format.

For more information, see [Built-In Formats Reference](#).

Format Names

Format names must be unique within a realm, and ideally, throughout the network.

Format names cannot be the empty string.

Format names may contain space characters.

See also [Restrictions on Names](#).

Field Names

Field names must be unique within each format. (Nonetheless, two separate formats may use the same field name.)

Field names cannot be null, nor the empty string.

Field names may contain space characters.

See also [Restrictions on Names](#).

Flexibility in Formats and Messages

An application suite needs a set of message formats that embraces the various purposes for which it sends messages. Nonetheless, the simplicity of a smaller set of formats usually yields optimal results.

When a format defines many possible fields, and a program sets only a few field values in a message, the message remains small, bearing only those fields that the program actually sets.

At one extreme, you can define a single catch-all format with all possible fields. Application programs can use as few or as many fields as is appropriate, without incurring a performance penalty.

When designing the set of formats for an application suite, balance these competing principles:

- *Specificity* Define as many formats as the application needs. If an application sends messages for different purposes, and the content structure of those messages is different, then define separate and specific formats for those messages.
- *Compactness* Defining a small number of formats is a good practice. A large set of formats is more difficult to understand, to configure, to use properly, and to maintain as your application evolves. If a subset of the formats are similar, and their usage or meanings are similar, then consider merging them into one format that contains a *union* of their fields.

Field Access: Names and References

The APIs provide two versions of each message field accessor call: one accepts a field name, while the other accepts a field reference object.

Accessing a field by name involves string comparison operations, which can increase processing latency.

Access by field reference is more efficient than access by name. Field reference objects contain a field name, along with internal information that facilitates efficient access.

Programs can repeatedly use a field reference object to efficiently access a field, even across messages of different formats. For example, if formats A and B both have a field named `foo`, then a field reference object with field name `foo` accesses the correct field in messages of either format.

Reusing Message Objects

It is faster to reuse an existing message object than to destroy it and create a new one. Programs can gain efficiency by reusing message objects, whenever possible.

- If a program repeatedly sends the *exact same message content*, then the best practice is to create that message object only once, sending it many times.
- If a program sends many messages of the same format, with the same fields, but with *varying field values*, then the best practice is to reuse one message object, clearing and modifying individual field values appropriately before each send call.
- If a program sends many messages of the same format, but the *set of fields varies*, then the best practice is to reuse one message object, clearing all of its fields and setting new values before each send call.

A program that sends a limited variety of messages can combine these tactics for reusing message objects. For each send call, it can select an appropriate message from a set of pre-constructed message objects, and modify as needed. To determine the optimum way to combine these tactics, test performance empirically.

Built-In Formats Reference

Built-in formats are optimized for efficiency, and are always available. Administrators do not need to explicitly define them, nor specify them among an application's preload formats.

The C API defines global constants as listed in the following table.

The Java API defines these constants as fields of class `Message`.

The .NET API defines these constants as fields of class `FTL`.

Built-In Formats

Format Name Constant	Description
TIB_BUILTIN_MSG_FMT_OPAQUE	<p>The message consists of a singleton field of type opaque.</p> <p>The constant TIB_BUILTIN_MSG_FMT_OPAQUE_FIELDNAME denotes the name of that singleton field. (The value of the constant is <code>_data</code>.)</p> <p>For the fastest and most efficient message transfer, limit the data payload to TIB_BUILTIN_MSG_FMT_OPAQUE_MAXSIZE (12000 bytes).</p>
TIB_BUILTIN_MSG_FMT_KEYED_OPAQUE	<p>This keyed opaque format enhances the opaque format with a key field of type string. Content matchers can match against the key field.</p> <p>The constant TIB_BUILTIN_MSG_FMT_KEY_FIELDNAME denotes the name of the string field. (The value of the constant is <code>_key</code>.)</p> <p>The constant value TIB_BUILTIN_MSG_FMT_KEY_MAXLEN is the maximum length, in bytes, of the key string field, including the null terminator character.</p> <p>The constant TIB_BUILTIN_MSG_FMT_OPAQUE_FIELDNAME denotes the name of the opaque data field. (The value of the constant is <code>_data</code>.)</p> <p>For the fastest and most efficient message transfer, limit the data payload to TIB_BUILTIN_MSG_FMT_OPAQUE_MAXSIZE (12000 bytes). Payload size includes the key, with its null terminator character, and the opaque data.</p>

Opaque Format

Applications can use the built-in opaque format to exchange messages that contain unstructured data. Opaque messages are very efficient, and can achieve very low-latency performance.

Opaque messages are an excellent choice for streaming data.

Application code can also embed structured data within opaque messages, however, application code is entirely responsible for the structure: the application must pack the data at the sender, and unpack the data at the receiver.

Content matchers *cannot* select opaque messages. (Recall that content matchers require an exact match on all specified field names and field values. Opaque values vary too much for content matchers.)

To optimize performance, built-in opaque formats limit the size of the data payload. If you need to send larger payloads, define a static format with an opaque field.

Keyed Opaque Format

When applications require efficient opaque messages, and also require content matching, you can use the keyed opaque built-in format. Keyed opaque messages are optimized: though less efficient than the opaque built-in format, they are more efficient than an equivalent managed format.

Applications can use content matchers to match against the key field.

To optimize performance, built-in opaque formats limit the combined size of the data payload and the key. If you need to send larger payloads, define a static format with an opaque field and a string key field.

String Encoding

To preserve interoperability throughout your enterprise, all strings must use UTF-8 encoding.

- When the TIBCO FTL Java and .NET libraries send messages, all strings are automatically UTF-8 encoded.

- C programs must treat strings in inbound messages as UTF-8 encoded strings.
- C programs must send only UTF-8 encoded strings.

i Note: Strings cannot include embedded null characters.

Message: Printable String Form

Programs can convert a message to a printable string. You can output the string to log files, or user output streams. The string does *not* contain sufficient information to reconstitute the original message.

Messages as Printable Strings

Element	Form	Detail
Message Nested message	<i>{field, field, field, field}</i>	Curly braces surround a list of fields, separated by commas. (For readability, you may add space characters.)
Field (with a value)	<i>data_type:field_ name=value</i>	Data type, colon, field name, equals symbol, value.
Clear field (no value)		The output omits the field entirely.
Array	<i>[val, val, val, val]</i>	Square brackets surround array elements, which are separated by commas. (For readability, you may add space characters.)
Opaque	<i><length bytes></i>	Angle brackets surround the length of the opaque data.
String	<i>"chars"</i>	Double-quotes surround the characters of the string. This representation does not use escape characters.
DateTime	<i>yyyy-mm- dd hh:mm:ss.fracZ</i>	For more information, see DateTime Values Printable String Form .

Printable String Example

This example message string has added whitespace to increase readability. (Actual printable strings do not include vertical formatting or indenting.)

```
{long:myLong=44,
 opaque:myOpaque=<128 bytes>,
 message:myInner_msg=
  {double:a_double_field=5.300000,
   string:an_inner_string_field="the inner "value""},
 long_array:an_array=[11, 12, 13, 14, 15, 16, 17, 18, 19, 20],
 message_array:a_msg_array=
  [{double:a_double_field=5.300021,
   string:an_inner_string_field="first inner string"},
   {double:a_double_field=123.4506,
   string:an_inner_string_field="second inner string"},
   {double:a_double_field=72.90927,
   string:an_inner_string_field="third inner string"},
   {double:a_double_field=17.17017,
   string:an_inner_string_field="fourth inner string"},
   {double:a_double_field=42.00000,
   string:an_inner_string_field="fifth inner string"}]}
```

Several aspects of this example are noteworthy:

- The second field, myOpaque, displays a token representing a byte-array. It does not attempt to display the actual bytes in the byte-array.
- The third field, myInner_msg, contains a nested submessage. Curly braces surround the submessage, which in turn has two fields.

The second of those two fields in the nested submessage contains a string. The string value is surrounded by double-quote character, and the string itself contains two double-quote characters (around the word "value"). Those inner double-quote characters are *not* preceded by an escape character.

- The fourth field, an_array, contains an array. The array values are surrounded by square brackets, and separated by commas.
- The fifth field, a_msg_array, contains an array of 5 messages. Each message contains two fields: a double and a string.

DateTime Values Printable String Form

The TIBCO FTL library calls print DateTime field values as strings. Double-quotes surround the characters of the string.

DateTime values print in UTC format, also known as Zulu time or GMT. The ISO-8601 standard requires appending a Z character in this notation.

For example, November 19, 2010 6:50:55 PM PST prints as:

```
2010-11-20 02:50:55.000000000Z
```

DateTime printing uses Common Era numbering for years. This system does not include a year zero. So for example, the time 1 second before 0001-01-01 00:00:00.000000000Z would print as -0001-12-31 23:59:59.000000000Z.

DateTime printing uses a proleptic Gregorian calendar. That is, when formatting dates earlier than the adoption of the Gregorian calendar, it projects the Gregorian calendar backward beyond its actual invention and adoption.

Go: Marshal Method for FTL Messages

The FTL Go language API implements the marshal and unmarshal interfaces to convert message datatype.

Methods

The `Message` type has two methods to conveniently import and export message fields:

- `Marshal` imports a Go structure or map into an FTL message.
- `Unmarshal` exports the fields of an FTL message to a Go structure or map.

FTL marshaling and unmarshaling support only those maps with key type string.

Marshaling ignores nil as the field value of a Go structure and as a slice element.

FTL Numeric Field Types

FTL messages store all Go language integral types as `TIB_FIELD_TYPE_LONG` fields, corresponding to the Go language type `int64`.

FTL messages store all Go language floating-point types as `TIB_FIELD_TYPE_DOUBLE` fields, corresponding to the Go language type `float64`.

These designations apply within the following tables.

- *IT* refers to any of the following integral types: `int`, `int8`, `int16`, `int32`, `int64`, `uint`, `uint8`, `uint16`, `uint32`, `uint64`, `uintptr`, `bool`.
- *FT* refers to any of the following floating-point types: `float32`, `float64`.

Conversion of Go Types to FTL Fields

Go Type	Marshals to FTL Message Field Type
IT	TIB_FIELD_TYPE_LONG
*IT	
FT	TIB_FIELD_TYPE_DOUBLE
*FT	
[]IT	TIB_FIELD_TYPE_LONG_ARRAY
*[]IT	
[]*IT	
*[]*IT	
[]FT	TIB_FIELD_TYPE_DOUBLE_ARRAY
*[]FT	
[]*FT	
*[]*FT	
string	TIB_FIELD_TYPE_STRING
*string	
[]string	TIB_FIELD_TYPE_STRING_ARRAY
*[]string	
[]*string	
*[]*string	

Go Type	Marshals to FTL Message Field Type
byte *byte	TIB_FIELD_TYPE_OPAQUE
Note: []*byte and []*[]byte are not allowed.	
time.Time *time.Time	TIB_FIELD_TYPE_DATETIME
[]time.Time *[]time.Time []*time.Time *[]*time.Time	TIB_FIELD_TYPE_DATETIME_ARRAY
structure pointer to structure	TIB_FIELD_TYPE_MESSAGE
embedded structure pointer to embedded structure	individual fields within the message
ftl.Message *ftl.Message	TIB_FIELD_TYPE_MESSAGE
[]ftl.Message *[]ftl.Message []*ftl.Message *[]*ftl.Message	TIB_FIELD_TYPE_MESSAGE_ARRAY

Go Type	Marshals to FTL Message Field Type
ftl.Inbox *ftl.Inbox	TIB_FIELD_TYPE_INBOX
map[string]	TIB_FIELD_TYPE_MESSAGE

Note: Each element of the map marshals into a field within the message, with the element key becoming the field name. The key type must be string.

Conversion of FTL Fields to Go Types

FTL Message Field Type	Unmarshals to Go Type
TIB_FIELD_TYPE_LONG	IT
Supports strict conversion.	*IT
TIB_FIELD_TYPE_DOUBLE	FT
Supports strict conversion.	*FT
TIB_FIELD_TYPE_LONG_ARRAY	[]IT *[]IT []*IT []*IT The target struct must be a slice, not an array.
TIB_FIELD_TYPE_DOUBLE_ARRAY	[]FT *[]FT []*FT []*FT The target struct must be a slice, not an array.
TIB_FIELD_TYPE_STRING	string *string

FTL Message Field Type	Unmarshals to Go Type
TIB_FIELD_TYPE_STRING_ARRAY	[]string *[]string []*string **string The target struct must be a slice, not an array.
TIB_FIELD_TYPE_OPAQUE	byte *byte
TIB_FIELD_TYPE_DATETIME	time.Time *time.Time
TIB_FIELD_TYPE_DATETIME_ARRAY	[]time.Time *[]time.Time []*time.Time **time.Time The target struct must be a slice, not an array.
TIB_FIELD_TYPE_MESSAGE	structure embedded structure ftl.Message *ftl.Message map[string] *map[string]
TIB_FIELD_TYPE_MESSAGE_ARRAY	Array of structures []ftl.Message *[]ftl.Message []*ftl.Message

FTL Message Field Type	Unmarshals to Go Type
	<code>[]*ftl.Message</code> <code>[]map[string]</code> <code>*[]map[string]</code> The target struct must be a slice, not an array.
TIB_FIELD_TYPE_INBOX	<code>ftl.Inbox</code> <code>*ftl.Inbox</code>

Field Tags in struct Definitions

For convenience, you can use field tags to guide marshaling and unmarshaling (similar to JSON processing). For example:

```
type myStructType struct {
    myFieldA int `json:"my_field_A" ftl:"myFieldA"`
    myFieldB int `json:"my_field_B" ftl:"myFieldB,strict"`
    myFieldC int `json:"my_field_C" ftl:"myFieldC,zeromissing,omitzero"`
}
```

FTL software recognizes tags with this general form:

```
ftl:"<fieldname>[,<options>]"
```

- `<fieldname>` is the name of a field in an FTL message, corresponding to the tagged field of the Go struct definition.
- `<options>` is a comma-separated list of options to apply marshaling and unmarshaling the field (see the following table).
- Separate the individual tags with a space character. Each line of the example illustrates this with a space between the JSON tag and FTL tag.

Option	Description
strict	When unmarshaling, enforce strict conversion for numeric fields.

Option	Description
	<p>In strict conversion, the sign of a numeric FTL field value must be compatible with the corresponding Go language field type. If it is not compatible, the unmarshal call returns an error.</p> <p>For example, consider the effect of unmarshaling an FTL message field with type <code>TIB_FIELD_TYPE_LONG</code>. The value 100 fits into any unsigned Go field, or into an <code>int8</code>. But the value -1000 does not fit, and strict conversion would reject it.</p> <p>Non-strict conversion could yield unpredictable values for values that do not fit.</p>
<code>zeromissing</code>	<p>When unmarshaling, supply zero values for missing fields.</p> <p>If the target Go struct definition specifies a field but a corresponding field does not exist in the source FTL message, then conversion sets the Go field to the zero value of its field type.</p> <p>When this option is absent, unmarshaling does not modify the target Go field unless the field is present in the FTL message.</p>
<code>omitzero</code>	<p>When marshaling, omit fields that contain the zero value.</p> <p>This option is analogous to <code>omitempty</code> in JSON marshaling. If the Go field contains the zero value for its type, then marshaling does not add a corresponding field to the FTL message.</p> <p>Zero values include <code>false</code>, <code>0</code>, <code>0.0</code>, <code>""</code>, a nil pointer or interface value, and any empty array, slice, map, structure, or string.</p> <p>When this option is absent, marshaling adds an FTL field corresponding to every Go field.</p>
<code>format=<format_name></code>	<p>Marshal a Go field value that is itself a nested structure to an FTL message with format <code><format_name></code>. (Use this option when your FTL application definition manages all formats.)</p> <p>When this option is absent, marshal a nested structure to an FTL message of unnamed dynamic format (that is, null format name).</p>

Examples

The FTL go API provides a simple mechanism for marshaling structures into an FTL message, and for unmarshaling FTL messages into a structure. The use of field tags is similar to that found in the encoding/json package. Note that structure fields must be exportable in order to be marshaled or unmarshaled. In simple terms, this means the field name must begin with an upper-case letter.

Marshal/unmarshal also supports the use of maps, in the form `map[string]interface{}`. In this case, the FTL field name corresponds to the map entry key, and the FTL field value corresponds to the map entry value.

The following example unmarshals message data into a Go structure:

```
type HelloMessage struct {
    Type string `ftl:"type"`
    Message string `ftl:"message"`
}
func main() {
    // Create an instance of the HelloMessage structure. Then unmarshal
    // the message into the structure, based on the tags attached to
    // each field in the structure.
    //
    // Note that a pointer to the structure (or map) must be passed to
    // the Unmarshal() function.
    helloMsg := HelloMessage{}
    if err = msg.Unmarshal(&helloMsg); err != nil {
        log.Fatal(ftl.ErrStack(err))
    }
    // Print the message contents, both as a formatted FTL message
    // (via the message String() function) and the as the
    // unmarshaled structure content (using go's %#v formatting directive).
    //
    log.Printf("message: %s\n", msg.String())
    log.Printf("Unmarshalled message: %#v\n", helloMsg)
}
```

The following example marshals Go structure data into a message:

```
func main() {
    msg, err := realm.NewMessage("helloworld")
    if err != nil {
        log.Fatal(ftl.ErrStack(err))
    }
}
```

```
// Defer the destruction of the message.
defer msg.Destroy()
// Construct the message content into a map[string]interface{}.
content := make(map[string]interface{})
content["type"] = "hello"
content["message"] = "hello world earth"
// Marshal the message content into the FTL message. Note that a
// pointer to the map must be passed to msg.Marshal().
if err = msg.Marshal(&content); err != nil {
    log.Fatal(ftl.ErrStack(err))
}
```

For more information about FTL message marshaling/unmarshaling, see the samples in [.../samples/src/golang/src/tibco.com/ftl-sample](#).

Delivery

Inbound Message Delivery

These six phases define the precise terminology that describes the delivery of an inbound message:

Phases of Inbound Message Delivery

	Phase	Description
1	<i>Receive</i>	A transport presents a message to a subscriber.
2	<i>Match</i>	If a subscriber has a content matcher, it filters the message. A matching message advances to the next phase. A message that does not match is discarded.
3	<i>Distribute</i>	The library adds the message to the event queue associated with the subscriber.
4	<i>Dispatch</i>	A dispatch call in your program removes messages from the event queue, and invokes the appropriate callback.
5	<i>Process</i>	Your callback gets data from the message and uses it.
6	<i>Release</i>	The callback returns, releasing the message and its resources.

Phases, Pipelines, and Threads

Consider the six delivery phases as two pipelines. Event queues serve as a stopover point between the two pipelines:

- The *receive pipeline* includes the receive, match, and distribute phases.
- The *dispatch pipeline* includes the dispatch, process, and release phases.

Specific threads do the work that moves a message through each pipeline. Each thread requires CPU resources to do that work.

- One or more *receive threads* drive the receive pipeline. Inbound data arrives on a transport's data source.
 - In the receive phase, receive threads pump messages out of those data sources.
 - In the match phase, receive threads filter messages through the content matcher.
 - In the distribute phase, receive threads place messages on the appropriate event queues.
- One or more *dispatch threads* drive the dispatch pipeline.
 - In the dispatch phase, dispatch threads pump messages out of event queues.
 - In the process phase, dispatch threads process messages using application callbacks.
 - In the release phase, dispatch threads reclaim message resources.

The functional definition of a dispatch thread is any program thread that calls an event queue's dispatch method. Your application program determines the number of dispatch threads required to dispatch and process messages from all its event queues in a timely and efficient manner. (Developers: record the number of dispatch threads on each programs' application coordination form.)

With regular event queues, receive threads are internal to the TIBCO FTL library, and the library determines the number of receive threads. In contrast, with inline event queues, the application's dispatch thread also serves the functional role of a receive thread, as it combines all six phases into a single pipeline (see [Inline Mode](#)).

Both pipelines begin by polling for available messages: the receive phase polls a transport's data source, and the dispatch phase polls an event queue. For the details of polling, see "Receive Spin Limit" in TIBCO FTL [Administration](#).

Content Matchers

A content matcher filters the inbound stream of messages for a subscriber.

Content matchers operate during the match phase of message delivery. (Also see [Subscriber Interest](#).)

A subscriber can have at most one content matcher. A subscriber without a content matcher distributes all inbound messages to its event queue: it does not filter out any messages. In contrast, a subscriber with a content matcher distributes only the messages that match it.

An inbox subscriber cannot have a content matcher. An inbox subscriber always receives all the messages sent to its inbox.

Each content matcher has a *match string*, which defines its filtering action. The match string specifies a set of field names paired with corresponding values. Fields can be matched as true (value present), false (value absent), a string value, or a long value. (see [Match Semantics](#)).

Content matchers can be constructed to match on the following which removes the need to construct multiple subscribers.

- Match on all fields (a logical AND match): The match string matches a message if and only if every field specification in the match string correctly matches the presence, absence, or value of a corresponding field in the message. For example, a subscriber with the following interest would receive messages only if the bank is ABCBank and the type is debits. The subscriber would not receive the message if the publisher were sending a message with bank ABCBank and type of credits.

```
{"bank": "ABCBank", "type": "debits"}
```

which can be read as:

```
("bank" is "ABCBank") AND ("type" is "debits")
```

- Match on one or more fields (a logical OR match): The match string matches a message if *any* field in the match string matches the presence, absence, or value of a corresponding field in the message. For example, a subscriber with the following interest would receive messages if the bank is ABCBank and the type is debits or credits.

```
[{"type": "debits"}, {"type": "credits"}]
```

or this shorter syntax:

```
{"type": ["debits", "credits"]}
```

which can be read as (any bank):

```
("type" is "debits" OR "type" is "credits")
```




Caution: A logical OR match is not permitted on the key field in the matcher used by a last-value durable subscriber. A subscriber must specify exactly one string value for the key field.

- A combination of AND and OR matching For example:
`{"bank": "ABCBank", "type": ["debits", "credits"]}`
 which can be read as:
 ("bank" is "ABCBank") AND ("type" is "debits" OR "type" is "credits")



Note: There are some restrictions on last-value durables with regard to the key field. See [Last-Value Durables](#), "Content Matchers".

Match Semantics

Content matchers interpret match strings using these simple rules.

- If the match string specifies a field with boolean token *true*, that field must be *present* in the message in order to match.
- If the match string specifies a field with boolean token *false*, that field must be *absent* from the message in order to match.
- If the match string specifies a field with either a string or long integer value, that field must be present in the message with that value.
- When comparing a field name or a value, all comparisons must be exact. Matching does not support wildcards nor regular expressions.

Match String Syntax

Construct matchers on this syntactic template in JSON format.

Logical AND Syntax

field:value pairs are in curly braces and separated by commas). Each field name can appear at most once.

```
{"fieldname1":"value1" , ... , "fieldnameN":"valueN"}
```

Logical OR Syntax

A logical OR can be expressed in one of two ways:

1. As a list of possible values for a given field.

```
{"f1": ["v1", "v2"]}
```

2. As a list of valid matchers, which need not be related to each other, and each could be a logical OR.

```
[{"f1": "v1"}, {"f1": "v2"}, ..., {"f1": "vn", "f2": "w1"}]
```

```
[{"f1": ["v1", "v2"]}, [{"f2": "w1"}, {"f2": "w2"}]]
```

Other Syntax Rules

Logical AND as well as logical OR syntax follow these rules:

- Enclose field names and string values in double-quote characters. You may precede quote characters with an escape character, as needed.
- Do *not* enclose boolean tokens in double-quote characters.
- Values can be long integers, strings, or the special boolean tokens true or false.
- When *value* is a string, its maximum length is 256 characters (see [Restrictions on Names](#)).
- Whitespace is ignored, except within double-quote characters.

Content Matcher: Match String Examples

```
{"Symbol": "TIBX"}
{"Symbol": "TIBX", "Order": "Buy", "Price": "Market"}
{"Item": "Book", "Title": "The Power of Now"}
{"Answer": 42}
{"MustHave": true, "MustNotHave": false, "MustBeZero": 0}
```

Content Matcher Performance and Architecture

For best performance, match against no more than 10 fields. (Fewer is faster.)

If your application requires regular expression matches, numeric value ranges, or more than 10 match fields, then the best practice is to narrow the field of messages with a content matcher, and then code your callback to refine the filtering even further.

Subscriber Interest

Whenever possible, publishers send messages only to interested subscribers. That is, publishers send only those messages that match at least one subscriber content matcher. This behavior can reduce bandwidth consumption, and can enhance subscriber performance in some situations.

To support this feature, subscribers send content matchers to publishers, which apply them to *outbound* messages.

Inline Mode

Programs that receive time-sensitive messages can use inline mode to favor low latency over high throughput. Inline mode reduces inbound message latency by consolidating transport I/O and message callback processing into one thread.

Before using inline mode, you must thoroughly understand the important details in this topic and the topics that follow.

Background

The term *inline mode* refers to the execution thread of the six phases of message delivery (see [Inbound Message Delivery](#)).

In regular operation the first three phases are separate from the last three phases. That is, the receive, match, and distribute phases occur in an internal receive thread, separate from program code. Meanwhile, the dispatch, process, and release phases occur in a dispatch thread, starting with a dispatch API call within application program code. The event queue is a loose coupling between these two triplets of phases: namely, the receive and dispatch pipelines.

In contrast, inline mode co-locates all six phases in the same thread. That is, the entire phase stack operates as a single I/O pipeline from the underlying transport, through the application program's dispatch call, to message processing and release. All six phases occur within one program thread, at the application's dispatch call. This tactical optimization eliminates a source of latency, namely, context-switching overhead between the distribute and dispatch phases. However, this tight coupling introduces several restrictions and potential pitfalls, which become the responsibility of the application programmer.

Callback Restrictions with Inline Mode

Inline mode requires that callbacks *always* return quickly. Otherwise, long callbacks could delay message I/O, which would defeat the purpose of inline mode.

For example, the negative consequences of long callbacks could include a large I/O backlog. As a result, the receiving program could lose inbound messages. Furthermore, message buffers at the publishing end of a transport could fill up. To prevent overflow at these buffers, the transport could block programs at the publishing end, delaying their outbound messages.

Transport Restrictions with Inline Mode

Inline mode restricts underlying transports. Conformance with the following restriction must be ensured.



Restriction: When a transport is associated with an *inline* event queue, it cannot be associated with any other event queue.

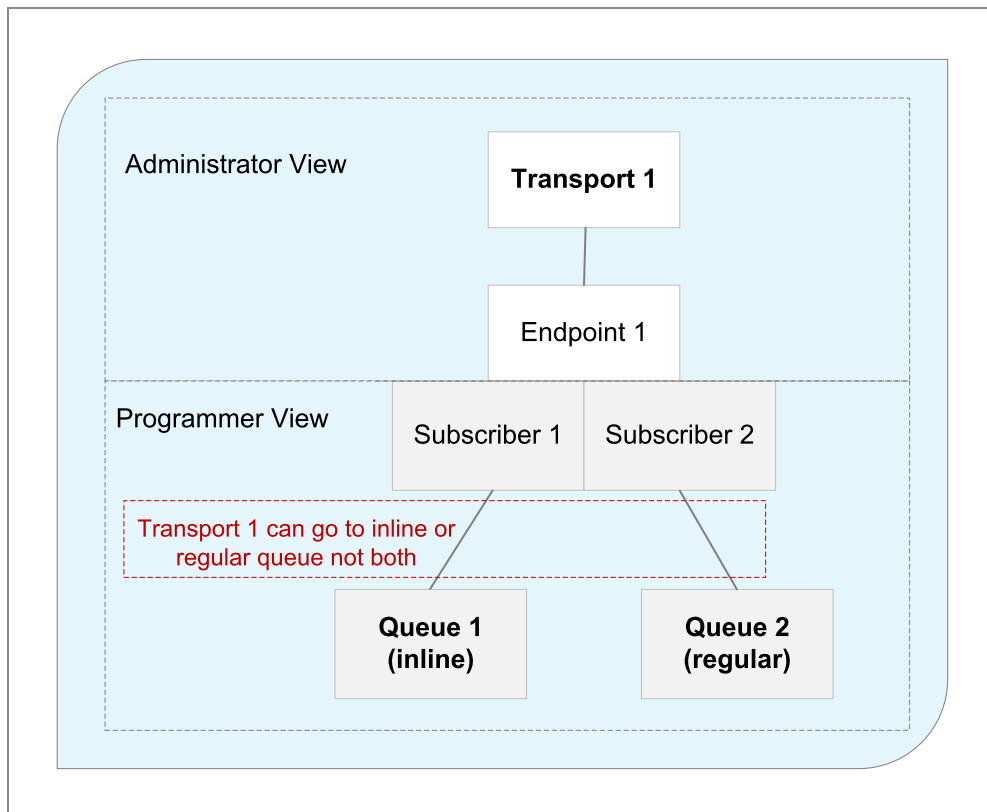
Violating the restriction results in an illegal state exception. The add subscriber API call throws the exception when the program attempts to add a subscriber that would violate the principle.

When specifying inline mode, programmers must coordinate with administrators to avoid illegal state exceptions.

Programmer Violation

The first diagram illustrates a violation attributable to programmer error. The programmer created two subscribers (S1 and S2) from a single endpoint (E1), and adds them to two event queues, at least one of which (Q1) is an inline queue. This situation would associate the underlying transport (T1) of the subscribers with two incompatible queues (Q1 and Q2), violating the restriction.

Figure 2: Illegal Inline Queue, Simple Case



To rectify the violation, either add both subscribers to a single inline event queue (Q1), or to two *ordinary* event queues, neither of which use inline mode.

Hidden Violation

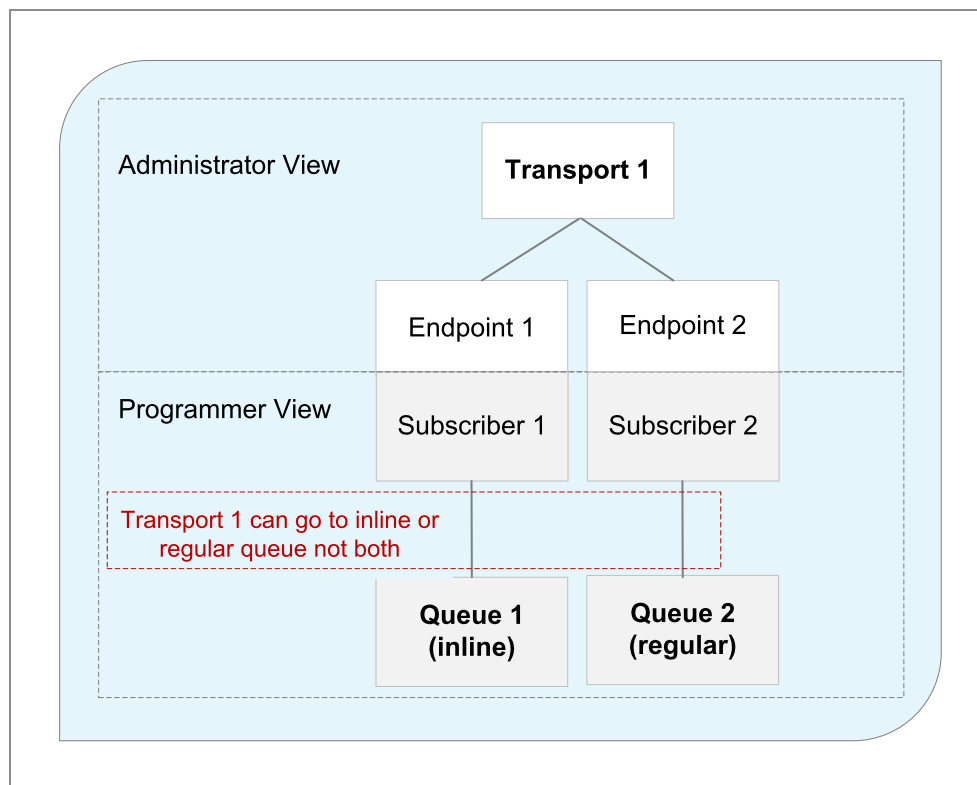
While it would appear straightforward for programmers to avoid the violation of the simple case of the first diagram, the situation is more complicated because responsibilities are divided between programmers and administrators.

From a programmer's perspective, transports are ordinarily hidden behind endpoint names. Conversely, administrators can ordinarily employ transports to implement

endpoints without understanding the specifics of subscribers and queues in application programs. However, inline mode tightly couples transport I/O to program code, which in turn blurs the usual separation of responsibilities between programmer and administrator. As a result, the restriction requires that programmers and administrators coordinate whenever a program uses inline event queues.

Consider the following example. The situation in the second diagram might appear correct from the separate perspectives of the programmer and the administrator, but combining their perspectives reveals a hidden violation.

Figure 3: Illegal Inline Queue, Hidden Violation



The programmer instantiates two subscribers (S1 and S2) on two separate endpoints (E1 and E2), and associates them with separate queues (Q1 and Q2). Q1 is an inline queue.

Meanwhile, the administrator employs a single transport (T1) to implement the two endpoints (E1 and E2).

Because T1 is associated with Q1, which is an inline queue, this arrangement violates the principle. When the program adds S2 to Q2, the add subscriber call throws an exception, whether or not Q2 uses inline mode.

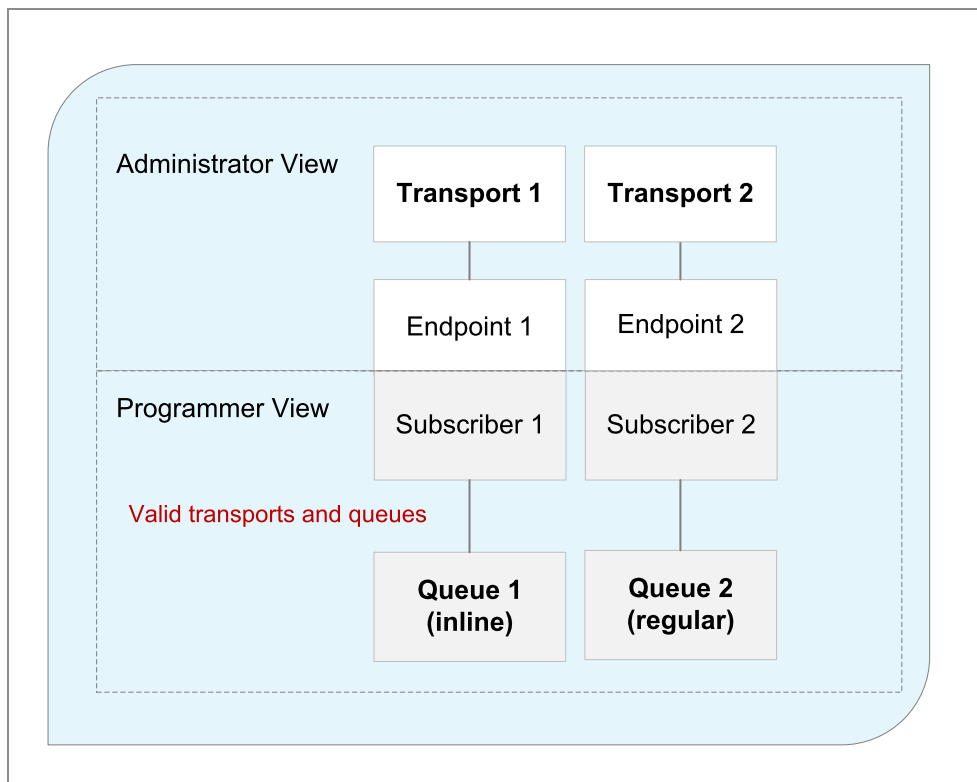
By coordinating their information, the programmer and administrator can cooperate to avoid the violation in any of three ways:

- Use ordinary queues instead of inline mode.
- Use separate transports to implement the two endpoints E1 and E2 (see [Separate Transports to Correct a Violation](#), which follows).
- Add subscribers S1 and S2 to only one inline queue (see [Single Queue to Correct a Violation](#), which follows).

Separate Transports to Correct a Violation

In the third diagram, transport T1 is associated with only one inline event queue, Q1. This arrangement does *not* violate the restriction.

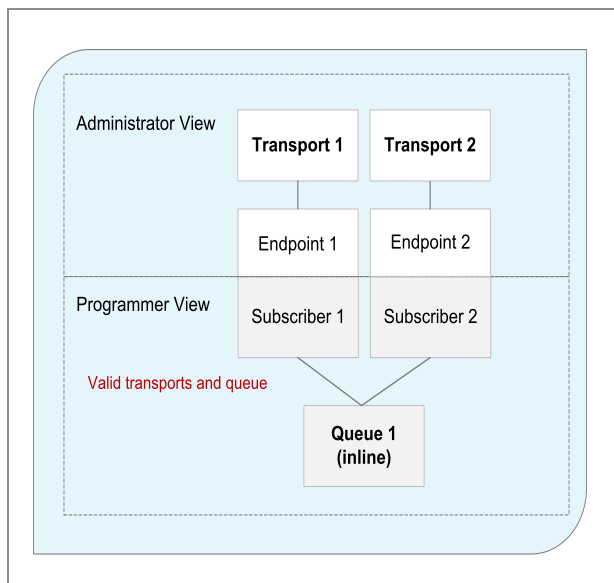
Figure 4: Legal Inline Queue, Separate Transports



Single Queue to Correct a Violation

In the fourth diagram, even though two subscribers (S1 and S2) share the same underlying transport (T1), they are associated with the same inline event queue (Q1). This arrangement does *not* violate the restriction.

Figure 5: Legal Inline Queue, Single Queue



FTL Server Interactions

FTL Server Connect Call

Every application program must connect as a client to an FTL server. The realm connect call identifies the client to the FTL server, and receives the realm definition from the realm service.

Developers must coordinate with administrators regarding the information that programs supply in the realm connect call:

- FTL Server URL List (required)
- Application Name (required)
- Application Instance Identifier (optional)
- Client Label (optional)
- Security Credentials (optional)
- Trust Properties (required to connect to a secure FTL server)

Application Name

The application name argument of the realm connect call selects the application definition, which contains administrative information that the application needs at run time, such as the binding of endpoints to transports, and message formats.

Null Application Name

To support coding experiments and rapid prototyping, the realm connect call accepts a null application name. A null argument selects the default application definition.

The default application definition supports any program that satisfies these conditions:

- Every call that creates a publisher or a subscriber specifies a null endpoint name.

- The program uses dynamic formats or built-in formats, but not managed formats.

To start an FTL server that contains the default application definition (and no other application definitions), omit the data directory parameter (data) from the FTL server configuration file. See "FTL Server Configuration" in TIBCO FTL [Administration](#).



Note: Do not use null application names when developing programs for production environments, nor in any situation that requires control over run time details.

Client Label

The *client label* is a human-friendly string that names the functional role of a client process. This label can help administrators recognize client application processes by their role within the enterprise. Client ID is given to the client by the realm (FTL server) but the client label is set by the client itself via `TIB_REALM_PROPERTY_STRING_CLIENT_LABEL`.

Programmers

It is good programming practice to supply a client label property in the realm connect call.

For flexibility, design programs to accept a client label value as a command line or configuration argument, which overrides a default value.

Administrators

The FTL server includes the client label in GUI displays, web API responses, and monitoring data.

Administrators can use identical client labels to maintain name recognition when several instances of an application run on different host computers. Conversely, you can use distinct client labels to distinguish among several instances of an application that run on the same host computer.

Administrators can use the client label to maintain continuity, so you can recognize a client process by its role even after it restarts. (In contrast, the FTL server assigns a unique client ID each time an application process restarts.)

Operation of the Realm Connect Call

When a client program contacts an FTL server, the realm connect call uses these algorithms:

One Server

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

If the program's realm object has only a single URL for the FTL server, the realm connect call sends requests to the FTL server at that URL.

If the server does not respond to repeated requests, the realm connect call throws an exception.

Fault-Tolerant Servers

```
"https://<host>:<port>|https://<host>:<port>|https://<host>:<port>"
```

If the program's realm object has a pipe-separated URL list for the FTL server, the realm connect call sends requests to those URLs until it succeeds in connecting to one of them.

If none of the FTL servers respond to repeated requests, the realm connect call throws an exception.

Trust Properties of the Realm Connect Method

In an enterprise with TLS security, client applications must trust the FTL server. Properties of the realm connect method specify the behavior of this interaction.

- **TIB_REALM_PROPERTY_LONG_TRUST_TYPE** - This property indicates the way that the client determines trust in the FTL server. Its value is one of the following constants:
 - **HTTPS_CONNECTION_USE_SPECIFIED_TRUST_FILE** - The client trusts the FTL server based on the trust file created by the FTL server and distributed by the administrator. Specify the file path of the trust file in an adjunct parameter,

TIB_REALM_PROPERTY_STRING_TRUST_FILE.

- HTTPS_CONNECTION_USE_SPECIFIED_TRUST_STRING - The client trusts the FTL server based a trust string. Specify that data content in an adjunct parameter, TIB_REALM_PROPERTY_STRING_TRUST_PEM_STRING.
- HTTPS_CONNECTION_TRUST_EVERYONE - The client trusts any FTL server without verifying trust in the server's certificate.



Warning: Do not use this value except for convenience in development and testing. It is *not* secure.

- TIB_REALM_PROPERTY_STRING_TRUST_FILE - The string value of this property is the file path of the trust file.
- TIB_REALM_PROPERTY_STRING_TRUST_PEM_STRING - The string value of this property is the trust string in PEM format.

The names of properties and constants vary slightly among the languages that the API supports.

Trust File

The content of the trust file instructs clients to trust the FTL server's certificate. Administrators and developers coordinate to supply the trust file to application programs, web browsers, and all FTL servers which include all core servers and auxiliary servers at all sites (including primary, satellite, and DR sites). .

A secure FTL server reads the trust file in its data directory. The trust file is named `ftl-trust.pem`. This file contains one or more PEM-encoded public certificates, each of which is typically 1 - 2 kilobytes of data.

Administrators distribute the trust file to clients: that is, developers and application administrators coordinate so that client programs can access the trust file at run time.

Users can load the trust file into a web browser's trust store.

Reconnect Properties of the Realm Connect Method

If the connect call cannot initially connect to the FTL server, it waits a period and tries again. The following properties characterize this reconnect behavior. These properties apply only to `tibRealm_Connect` and do not affect reconnects if the client loses connection to the FTL server.

- `TIB_REALM_PROPERTY_DOUBLE_CONNECT_INTERVAL` - The connect call waits this interval (in seconds) between connection attempts. The default value is 1.0 seconds.
- `TIB_REALM_PROPERTY_LONG_CONNECT_RETRIES` - If the connect call cannot connect to the FTL server after this maximum number of connection attempts, it fails with an exception. The default value is retry forever (0).

The names of properties and constants vary slightly among the languages that the API supports.

Update and Disable

After the initial connect call, the client and server remain in contact.

- Administrators can use the FTL server monitoring interface to view the status of client processes.
- Administrators can modify the realm definition, and deploy the updated definition to all clients.
- Administrators can disable individual client processes. A disabled client cannot use TIBCO FTL communications resources.

Logs

Developers, administrators, and TIBCO Support staff can use logging output for diagnostic purposes.

Application developers can set the log level. Administrators can subsequently change log level settings using the central logging facility.

Application developers can set the log output target.

Log Levels

The log level determines the level of detail and the quantity of log statements. Properly tuned logging can help diagnose unexpected behaviors. Excessively detailed logging can contribute to message latency and consume storage resources.

Application developers can set the log level using an API entry point. In addition, TIBCO FTL executable components accept the same log level specifications through command line arguments.

Log Level Tuning via API

You can tune the log level for all logging elements, or separately per individual elements.

Tuning for All Elements

In a log-level call, supply one of the string-valued constants in [Log Level Reference](#). For example (in C):

```
tib_SetLogLevel(tibEx e, TIB_LOG_LEVEL_WARN)
```

Alternatively, you can supply an **all** log element tag. See the next section.

Tuning for Selected Elements

Supply a string of this form:

```
"element:level; ... ;element:level"
```

Pair each element and its log level with a colon, and delimit the pairs with semicolons. For available elements, see [Log Element Tags Reference](#). For example (in C):

```
tib_SetLogLevel(tibEx e, "transports:warn;msg:debug")
```

When elements conflict, pairs that appear later in the list override earlier pairs. For example, `all:off;msg:warn` turns off logging for all elements, except for the messages (msg) element, which logs warnings and severe events, thus overriding the preceding `all` element.

Log Level Reference

These API constants and their string values denote the available log levels.

Log Level Constants and Values

Log Level Constant	String	Description
TIB_LOG_LEVEL_OFF	off	Disable all tracing.
TIB_LOG_LEVEL_SEVERE	severe	Output log entries only for severe events.
TIB_LOG_LEVEL_WARN	warn	Output log entries for warning and severe events.
TIB_LOG_LEVEL_INFO	info	Output log entries for information, warning, and severe events. If an application program does not explicitly set the log level, the library uses this default value.
TIB_LOG_LEVEL_VERBOSE	verbose	Output log entries for verbose, information, warning, and severe events.

Log Level Constant	String	Description
TIB_LOG_LEVEL_DEBUG	debug	Output log entries for debug, verbose, information, warning, and severe events.



Note: The output from debug and verbose can result in very large log files. This level of detail is generally not useful unless TIBCO staff specifically requests it.

Log Element Tags Reference

These strings denote the available log element tags.

Log Element Tags

Element	Description
all	Tune logging for all elements, embracing all the categories in this table.
application	Tune logging related to the application program, such as the program's use of API calls, message formats, and content matchers.
IO	Admin only. Tune logging related to data I/O, such as message data entering or leaving the program, and message packetization.
RS	Admin only. Tune logging related to the realm server. <ul style="list-style-type: none"> In FTL server client processes, this category includes client communication with the FTL server. In FTL server processes, this category includes operations within the FTL server, such as communication with clients, with affiliated FTL servers, and with services.
transports	Tune logging related to transports, including peer connections, subscriber interest, message send operations, protocols.
store	Admin only. Tune logging related to persistence stores and durables, such as

Element	Description
	store and durable operations, quorum formation, and leader election.
msg	Tune logging related to messages. The debug level logs each outbound message send and each inbound message callback by printing a representation of the message.
broker	Admin only. Tune logging related to clients of the eFTL service. (This element is available <i>only</i> in the eFTL service.)
route	Admin only. Tune logging related to wide-area durables.
mux	Admin only. Tune logging related to the FTL server as it redirects HTTP requests to the services it provides.
api	Tune logging related to API calls.

Log Output Targets

Developers can select the output target for log statements. Application programs can use one of three mutually exclusive targets.

Log Targets

Log Target	Description
Default Log Target	Output all log statements to stderr.
Log Files in Rotation	Output all log statements to a set of rotating log files.
Log Callback	The program defines a callback, which intercepts all log statements.

Each program process may set its log target only once. Attempting to set it again is an error.

Default Log Target

If a program does not set a log target, TIBCO FTL software directs all log statements to `stderr`.

Log Files in Rotation

Rotating log files organize log output into a set of files, and limit the file system storage that log statements can consume.

The call that arranges rotating log files accepts a file prefix, the file size that triggers rotation, and the maximum number of files.

Log files receive filenames consisting of the prefix you supply, a dot (.) character, and an integer suffix. Suffix zero indicates the current log file. Suffix 1 indicates the next most recent. Higher suffixes indicate older files.

Rotating renames each file in the set by incrementing its numeric suffix. If rotating would exceed the maximum number of files, then it discards the oldest file. These file I/O operations can affect message latency.

The TIBCO FTL library requires that the total length of any log file name must be strictly less than 1024 characters. The host computer's operating system may require a smaller file name length.

Log Callback

Applications can define and register a log callback. Instead of directing log statements to the file system, the TIBCO FTL library invokes the callback to process each log statement (that is, to enter it into the application's log system).

This type of target can introduce overhead costs and potential latency.

**Warning: Log Callback Restrictions**

- Programmers must ensure that the callback always returns promptly. The log callback executes inline, that is, synchronously, and can affect message latency.
- Your callback *must* not call any TIBCO FTL API entry point.
- Your callback *must* be thread-safe.
- For best results, your callback must not acquire any lock that might require a long wait time.

Log Content and Form

The form and content of trace log output are *not* part of a defined interface: they could change in subsequent releases.



Warning: Avoid programming techniques that rely on parsing log output, or depend on log content.

Advisory Messages

TIBCO FTL software presents asynchronous *advisory messages* to application programs. Advisory messages can indicate errors, warnings, or other information.

In contrast with exceptions and error codes, which indicate success or failure within a specific TIBCO FTL call, asynchronous advisory messages notify programs of incidents that occur outside of the program's direct flow of control.

When it is not possible to communicate through an advisory message, TIBCO FTL software presents an *out-of-band notification* instead (see [Notifications](#)).

Programs must arrange to receive and process information through both of these mechanisms: advisories and notifications.

Advisory Message Common Fields Reference

Advisory messages contain fields that present information to programs. Some fields are present on all advisory messages. Other fields are present only when information is available. Still other fields are associated only with specific advisory messages. Programs can use content matchers to select subsets of advisory messages from the advisory endpoint.

Advisory Message, Common Fields

Field	Present	Description
name	Always	The value denotes the general category of the advisory.
reason	Only as needed	The value distinguishes among several possible reasons for the advisory.
severity	Always	The value classifies the advisory according to the ability of TIBCO FTL software to fulfill its function as a message carrier.
module	Always	The value denotes the part of TIBCO FTL software to which

Field	Present	Description
		the advisory pertains.
timestamp	Always	<p>The <code>DateTime</code> value of this field indicates the time that the library generated the advisory.</p> <p>Although <code>DateTime</code> values can represent time with nanosecond precision, the actual resolution of the timestamp is only as fine-grained as the host computer's operating system supports.</p>
aggregation_ count	Only for aggregate data	The value represents the number of aggregated incidents.
aggregation_ time	Only for aggregate data	The value represents the length of the time interval, in seconds, for aggregated data.

Subscribing to Advisory Messages

To receive advisory messages, programs can create subscribers on a special endpoint named `_advisoryEndpoint`. (In each supported programming language, an API constant has the name of this endpoint as its value.)

Scope and Restrictions

i Note: The realm object scopes the advisories that a subscriber can receive on the special advisory endpoint, `_advisoryEndpoint`. That is, a subscriber to this endpoint receives only those advisories produced by other objects in the same program and the same realm as the advisory subscriber.

It is illegal to create publishers on the special advisory endpoint.

Procedure

1. Determine the set of advisory messages to receive.
2. Determine the action of your program in response to each advisory message.
3. Define message callbacks to process the advisory messages.
For example, an advisory callback might respond by logging the content of the advisory, by notifying an administrator, or by exiting.
4. Optional. Define content matchers.
A subscriber may receive all advisory messages without distinguishing among them, or it may select a specific subset of advisory messages using a content matcher.
5. Create subscribers on the special advisory endpoint.
6. Create a special event queue, dedicated only to dispatching and processing advisory messages.
This queue must never discard events.
7. Code a special dispatch thread within your program, dedicated only to dispatching the advisory event queue. Ensure that this thread always receives sufficient CPU cycles in a timely fashion, even when other dispatch threads might be stuck.
8. Add the advisory subscribers to the dedicated advisory event queue.

Advisory Messages Catalog

Application programs can receive the advisory messages in this table.

Advisory Message Catalog

Name and Reason	Description
DATALOSS FAILOVER_LOSS	Failover to a backup forwarding component, such as a transport bridge.
DATALOSS INCOMPLETE_MESSAGE	A transport could not reassemble the complete message.
DATALOSS QUEUE_LIMIT_EXCEEDED	An event queue discarded events.

Name and Reason	Description
DATALOSS SENDER_DISCARD	A transport discarded messages in accordance with its backlog settings (non-blocking send).
DATALOSS TPORT_DATALOSS	A transport lost data packets.
DATALOSS RECONNECT_LOSS	A connection-oriented transport became disconnected.
DATALOSS STORE_DISCARD_DATALOSS	A subscriber to a last-value durable has missed messages.
DATALOSS UPSTREAM_LOSS	A forwarding component detected an upstream dataloss advisory.
DATALOSS DIRECT_SUB_LOSS	A direct subscriber lost data.
RESOURCE_AVAILABLE	A resource is available.
RESOURCE_UNAVAILABLE	A resource is unavailable.
Groups	
ORDINAL_UPDATE	Change to a group ordinal.
Persistence Stores and Durables	
SUBSCRIBER_FORCE_CLOSE	A persistence store forced a subscriber object to close.
LOCK_LOST	The client program no longer holds a lock.
Multicast Retransmission	
RETRANSMISSION RETRANSMISSION_REQUEST	A subscriber requested retransmission.
RETRANSMISSION RETRANSMISSION_SENT	A publisher sent a retransmission.
RETRANSMISSION RETRANSMISSION_SUPPRESSED	A subscriber suppressed a retransmission request.

DATALOSS FAILOVER_LOSS

This advisory reports potential dataloss. The reason is failover to a backup forwarding component.

Details

Only connection-oriented transports can detect this condition.

This advisory does not indicate the volume of lost data, but rather the number of data loss incidents. Each data loss incident represents the *potential* for lost messages. (The volume of lost data could be zero.)

Actions

Report this advisory to an administrator. Check the forwarding component.

Fields

Field	Description
name	DATALOSS
reason	FAILOVER_LOSS
endpoints	<p>The string array value of this field lists the endpoints that could have lost data.</p> <p>Although data loss occurs primarily in a transport, its symptoms could affect all endpoints that use the transport, and by extension, any subscriber on those endpoints. Furthermore, transport names are meaningful to administrators, but usually not available to programmers. This advisory field reports the set of all endpoints through which the program could access the problematic transport, according to the configuration in the local realm object.</p>
aggregation_count	The long value of this field reports the cumulative number of failover incidents during the time interval (see <code>aggregation_time</code>).

Field	Description
	The base library aggregates this count separately for each transport.
aggregation_time	<p>The double floating point value, in seconds, of this field indicates the length of the time interval for aggregating the incidents that aggregation_count reports.</p> <p>The time interval ends shortly before the timestamp.</p>
timestamp	<p>The DateTime value of this field indicates the time that the library generated the advisory.</p> <p>Although DateTime values can represent time with nanosecond precision, the actual resolution of the timestamp is only as fine-grained as the host computer's operating system supports.</p>

DATALOSS SENDER_DISCARD

The advisory reports an unrecoverable dataloss. The reason is transport backlog overflow at the publisher, in accordance with the transport's backlog settings.

Details

This advisory reports only inbound dataloss to subscribing programs. It does *not* report outbound dataloss to the publishing program.

This advisory does not indicate the volume of lost data, but rather the number of dataloss incidents. Each dataloss incident represents *at least one* lost message, but could represent many lost messages.

For more information about backlog overflow, see [Send: Blocking versus Non-Blocking](#).

Actions

Report this advisory to an administrator.

Fields

Field	Description
name	DATALOSS
reason	SENDER_DISCARD
endpoints	<p>The string array value of this field lists the endpoints that could have lost data.</p> <p>Although data loss occurs primarily in a transport, its symptoms could affect all endpoints that use the transport, and by extension, any subscriber on those endpoints. Furthermore, transport names are meaningful to administrators, but usually not available to programmers. This advisory field reports the set of all endpoints through which the program could access the problematic transport, according to the configuration in the local realm object.</p>
aggregation_count	<p>The long value of this field reports the cumulative number of dataloss incidents during the time interval (see <code>aggregation_time</code>).</p> <p>The base library aggregates this count separately for each transport.</p>
aggregation_time	<p>The double floating point value, in seconds, of this field indicates the length of the time interval for aggregating the incidents that <code>aggregation_count</code> reports.</p> <p>The time interval ends shortly before the timestamp.</p>
timestamp	<p>The <code>DateTime</code> value of this field indicates the time that the library generated the advisory.</p> <p>Although <code>DateTime</code> values can represent time with nanosecond precision, the actual resolution of the timestamp is only as fine-grained as the host computer's operating system supports.</p>

DATALOSS QUEUE_LIMIT_EXCEEDED

The advisory reports dataloss. The reason is overflow of an event queue.

Details

The queue has discarded some events, in accordance with its property values.

Diagnoses

- Lengthy processing in callbacks could delay prompt dispatch of the queue.
- The program could not process the volume of inbound messages from its subscribers.
- The program is starved for CPU cycles. Its host computer is too heavily loaded.
- The maximum events limit of the event queue is too low.

Actions

Consider whether this behavior is reasonable and expected.

Report this advisory to an administrator.

Fields

Field	Description
name	DATALOSS
reason	QUEUE_LIMIT_EXCEEDED
endpoints	<p>The string array value of this field lists the endpoints that could have lost data.</p> <p>Although data loss occurs primarily in a transport, its symptoms could affect all endpoints that use the transport, and by extension, any subscriber on those endpoints. Furthermore, transport names are meaningful to administrators, but usually not available to programmers. This advisory field reports the set of all endpoints through which the program could access the problematic transport, according to the configuration in the local realm object.</p>
aggregation_	The long value of this field reports the cumulative number of events that the

Field	Description
count	queue discarded during the time interval (see <code>aggregation_time</code>). The base library aggregates this count separately for each transport.
aggregation_time	The double floating point value, in seconds, of this field indicates the length of the time interval for aggregating the incidents that <code>aggregation_count</code> reports. The time interval ends shortly before the timestamp.
timestamp	The <code>DateTime</code> value of this field indicates the time that the library generated the advisory. Although <code>DateTime</code> values can represent time with nanosecond precision, the actual resolution of the timestamp is only as fine-grained as the host computer's operating system supports.

DATALOSS INCOMPLETE_MESSAGE

Purpose

The advisory reports dataloss. The reason is an incomplete message.

The transport could not reassemble an inbound message because some data fragments did not arrive.

Diagnoses

- Network issues could interfere with message transmission.
- The sending process abruptly exited before transmitting all packets.
- When this advisory occurs alongside [DATALOSS SENDER_DISCARD](#), the problem could be within the sending process or a forwarding component.

Actions

Report this advisory to an administrator.

Fields

Field	Description
name	DATALOSS
reason	INCOMPLETE_MESSAGE
endpoints	<p>The string array value of this field lists the endpoints that could have lost data.</p> <p>Although data loss occurs primarily in a transport, its symptoms could affect all endpoints that use the transport, and by extension, any subscriber on those endpoints. Furthermore, transport names are meaningful to administrators, but usually not available to programmers. This advisory field reports the set of all endpoints through which the program could access the problematic transport, according to the configuration in the local realm object.</p>
aggregation_count	<p>The long value of this field reports the cumulative number of incomplete message incidents during the time interval (see <code>aggregation_time</code>).</p> <p>The base library aggregates this count separately for each transport.</p>
aggregation_time	<p>The double floating point value, in seconds, of this field indicates the length of the time interval for aggregating the incidents that <code>aggregation_count</code> reports.</p> <p>The time interval ends shortly before the timestamp.</p>
timestamp	<p>The <code>DateTime</code> value of this field indicates the time that the library generated the advisory.</p> <p>Although <code>DateTime</code> values can represent time with nanosecond precision, the actual resolution of the timestamp is only as fine-grained as the host computer's operating system supports.</p>

DATALOSS TPORT_DATALOSS

The advisory reports an unrecoverable dataloss. The reason is a transport malfunction.

Details

This advisory reports only inbound data loss, not outbound.

This advisory does not indicate the volume of lost data, but rather the number of data loss incidents. Each data loss incident represents the *potential* for lost messages. (The volume of lost data could be zero.)

Actions

Report this advisory to an administrator.

Fields

Field	Description
name	DATALOSS
reason	TPORT_DATALOSS
endpoints	<p>The string array value of this field lists the endpoints that could have lost data.</p> <p>Although data loss occurs primarily in a transport, its symptoms could affect all endpoints that use the transport, and by extension, any subscriber on those endpoints. Furthermore, transport names are meaningful to administrators, but usually not available to programmers. This advisory field reports the set of all endpoints through which the program could access the problematic transport, according to the configuration in the local realm object.</p>
aggregation_count	<p>The long value of this field reports the cumulative number of dataloss incidents during the time interval (see aggregation_time).</p> <p>The base library aggregates this count separately for each transport.</p>
aggregation_time	<p>The double floating point value, in seconds, of this field indicates the length of the time interval for aggregating the incidents that aggregation_count reports.</p> <p>The time interval ends shortly before the timestamp.</p>

Field	Description
timestamp	<p>The DateTime value of this field indicates the time that the library generated the advisory.</p> <p>Although DateTime values can represent time with nanosecond precision, the actual resolution of the timestamp is only as fine-grained as the host computer's operating system supports.</p>

DATALOSS RECONNECT_LOSS

The advisory reports potential dataloss. The reason is a temporary network disconnect between two connection-oriented transports.

Details

This advisory reports only inbound data loss, not outbound.

This advisory does not indicate the volume of lost data, but rather the number of data loss incidents. Each data loss incident represents the *potential* for lost messages. (The volume of lost data could be zero.)

Actions

Report this advisory to an administrator.

Fields

Field	Description
name	DATALOSS
reason	RECONNECT_LOSS
endpoints	The string array value of this field lists the endpoints that could have lost data.

Field	Description
	Although data loss occurs primarily in a transport, its symptoms could affect all endpoints that use the transport, and by extension, any subscriber on those endpoints. Furthermore, transport names are meaningful to administrators, but usually not available to programmers. This advisory field reports the set of all endpoints through which the program could access the problematic transport, according to the configuration in the local realm object.
aggregation_count	<p>The long value of this field reports the cumulative number of disconnect incidents during the time interval (see aggregation_time).</p> <p>The base library aggregates this count separately for each transport.</p>
aggregation_time	<p>The double floating point value, in seconds, of this field indicates the length of the time interval for aggregating the incidents that aggregation_count reports.</p> <p>The time interval ends shortly before the timestamp.</p>
timestamp	<p>The DateTime value of this field indicates the time that the library generated the advisory.</p> <p>Although DateTime values can represent time with nanosecond precision, the actual resolution of the timestamp is only as fine-grained as the host computer's operating system supports.</p>

DATALOSS STORE_DISCARD_DATALOSS

The advisory reports potential data loss at a subscriber to a last-value durable. The reason is that the subscriber has either missed one or more messages, or disconnected from the persistence store.

Details

A subscriber to a last-value durable receives every message that updates that durable. However, if the subscriber cannot keep up with the stream of updates from publishers, the subscriber might miss messages, as the durable stores only the most recent message.

If the subscriber disconnects from the persistence store, it could miss messages during the interval in which it remains disconnected.

This advisory reports only inbound data loss, not outbound.

This advisory does not indicate the volume of lost data, but rather the number of data loss incidents. Each data loss incident represents the *potential* for lost messages. (The volume of lost data could be zero.)

Actions

Report this advisory to an administrator.

Fields

Field	Description
name	DATALOSS
reason	STORE_DISCARD_DATALOSS
endpoints	<p>The string array value of this field lists the endpoints that could have lost data.</p> <p>Although data loss occurs primarily in a transport, its symptoms could affect all endpoints that use the transport, and by extension, any subscriber on those endpoints. Furthermore, transport names are meaningful to administrators, but usually not available to programmers. This advisory field reports the set of all endpoints through which the program could access the problematic transport, according to the configuration in the local realm object.</p>
aggregation_count	<p>The long value of this field reports the cumulative number of discard or disconnect incidents during the time interval (see <code>aggregation_time</code>).</p> <p>The base library aggregates this count separately for each transport.</p>
aggregation_time	<p>The double floating point value, in seconds, of this field indicates the length of the time interval for aggregating the incidents that <code>aggregation_count</code> reports.</p>

Field	Description
	The time interval ends shortly before the timestamp.
timestamp	<p>The DateTime value of this field indicates the time that the library generated the advisory.</p> <p>Although DateTime values can represent time with nanosecond precision, the actual resolution of the timestamp is only as fine-grained as the host computer's operating system supports.</p>

DATALOSS UPSTREAM_LOSS

The advisory reports potential dataloss. The reason is a dataloss advisory detected upstream at a forwarding component (such as a transport bridge).

Details

This advisory reports only inbound data loss, not outbound.

This advisory does not indicate the volume of lost data, but rather the number of data loss incidents. Each data loss incident represents the *potential* for lost messages. (The volume of lost data could be zero.)

Actions

Report this advisory to an administrator.

Fields

Field	Description
name	DATALOSS
reason	UPSTREAM_LOSS
endpoints	The string array value of this field lists the endpoints that could have lost

Field	Description
	<p>data.</p> <p>Although data loss occurs primarily in a transport, its symptoms could affect all endpoints that use the transport, and by extension, any subscriber on those endpoints. Furthermore, transport names are meaningful to administrators, but usually not available to programmers. This advisory field reports the set of all endpoints through which the program could access the problematic transport, according to the configuration in the local realm object.</p>
aggregation_count	<p>The long value of this field reports the cumulative number of dataloss incidents during the time interval (see aggregation_time).</p> <p>The base library aggregates this count separately for each transport.</p>
aggregation_time	<p>The double floating point value, in seconds, of this field indicates the length of the time interval for aggregating the incidents that aggregation_count reports.</p> <p>The time interval ends shortly before the timestamp.</p>
timestamp	<p>The DateTime value of this field indicates the time that the library generated the advisory.</p> <p>Although DateTime values can represent time with nanosecond precision, the actual resolution of the timestamp is only as fine-grained as the host computer's operating system supports.</p>

DATALOSS DIRECT_SUB_LOSS

The advisory reports an unrecoverable data loss at a direct subscriber.

Details

This advisory reports only inbound data loss, not outbound.

This advisory does not indicate the volume of lost data, but rather the number of data loss incidents. Each data loss incident represents the *potential* for lost messages. (The volume of lost data could be zero.)

Actions

Report this advisory to an administrator.

Fields

Field	Description
name	DATALOSS
reason	DIRECT_SUB_LOSS
endpoints	<p>The string array value of this field lists the endpoints that could have lost data.</p> <p>Although data loss occurs primarily in a transport, its symptoms could affect all endpoints that use the transport, and by extension, any subscriber on those endpoints. Furthermore, transport names are meaningful to administrators, but usually not available to programmers. This advisory field reports the set of all endpoints through which the program could access the problematic transport, according to the configuration in the local realm object.</p>
aggregation_count	<p>The long value of this field reports the cumulative number of data loss incidents during the time interval (see <code>aggregation_time</code>).</p> <p>The base library aggregates this count separately for each transport.</p>
aggregation_time	<p>The double floating point value, in seconds, of this field indicates the length of the time interval for aggregating the incidents that <code>aggregation_count</code> reports.</p> <p>The time interval ends shortly before the timestamp.</p>
timestamp	<p>The <code>DateTime</code> value of this field indicates the time that the library generated the advisory.</p> <p>Although <code>DateTime</code> values can represent time with nanosecond precision, the actual resolution of the timestamp is only as fine-grained as the host computer's operating system supports.</p>

ORDINAL_UPDATE

The advisory reports a change to a group ordinal.

Details

For background information, see [Groups of Applications](#).

Actions

Programs change the member's operating role and behavior according to the new ordinal.

Fields

Field	Description
name	ORDINAL_UPDATE
group	Group name. The name of the group to which the advisory pertains.
ordinal	Group member ordinal. The positive long value of the ordinal field represents the new ordinal of the group member. The value -1 indicates that the group object is disconnected from the group service. The group object automatically attempts to reconnect, and continues until the program explicitly destroys the object. Meanwhile, the group service could reassign the member's previous ordinal to another group member. Zero is a reserved value.

GROUP_STATUS

The advisory reports the status of a group and its members.

Group status messages differ in form and content, depending on the member and the state change. For more information, see [Group Status](#).

Fields of the Group Status Advisory Message

Field	Description
name	GROUP_STATUS
group	Group name. The name of the group to which the advisory pertains.
group_server_ available	When present, the long value of this field indicates whether the application process has a functioning connection to the group service.
group_ member_ status_list	When present, the value of this field is an array of submessages. Each submessage describes the status of one group member.

Fields of the Member Status Submessage

Field	Description
group_ member_ descriptor	The value of this field is a message that identifies a group member. Member programs can supply this optional member descriptor message when the program joins the group. If the member does not supply a descriptor, then this field is absent in the status submessage: the member is indistinguishable from any other member that omits a descriptor.
group_ member_ event	The long value of this field is an enumerated constant that indicates the connection status of the group member.

RESOURCE_AVAILABLE

The advisory reports that a resource is available.

Details

Persistence services are resources. For background information, see [Persistence: Stores and Durables](#).

Diagnosis

A resource that had been unavailable is now available. Operations that required that resource may proceed. The reason field indicates the resource.

Actions

Report this advisory to an administrator.

Fields

Field	Description
name	RESOURCE_AVAILABLE
reason	PERSISTENCE_STORE_AVAILABLE PERSISTENCE_STORE_AVAILABLE_AFTER_CLUSTER_DATALOSS
endpoints	The string array value of this field lists the endpoints that had been affected by a persistence service that had been unavailable but is now available again.
timestamp	The DateTime value of this field indicates the time that the library generated the advisory. Although DateTime values can represent time with nanosecond precision, the actual resolution of the timestamp is only as fine-grained as the host computer's operating system supports.

RESOURCE_UNAVAILABLE

The advisory reports that a resource is unavailable.

Details

Persistence services are resources. For background information, see [Persistence: Stores and Durables](#).

Diagnosis

A required resource is unavailable. The reason field indicates the resource.

- The persistence cluster lacks a quorum of available services for the store. Application clients must wait until a quorum forms.
- An insufficient number of persistence services are operating. Administrators must attend to FTL servers and persistence services.

Actions

Report this advisory to an administrator.

If this state continues for a long duration, investigate whether hardware or network issues are interfering with resource operation or communication.

Fields

Field	Description
name	RESOURCE_UNAVAILABLE
reason	PERSISTENCE_STORE_UNAVAILABLE
endpoints	The string array value of this field lists the endpoints affected by an unavailable persistence service.
timestamp	<p>The DateTime value of this field indicates the time that the library generated the advisory.</p> <p>Although DateTime values can represent time with nanosecond precision, the actual resolution of the timestamp is only as fine-grained as the host computer's operating system supports.</p>

RETRANSMISSION RETRANSMISSION_REQUEST

The advisory reports that a subscribing endpoint in the application process requested retransmission from a publisher.

Details

Retransmission is a normal occurrence for multicast transports. Retransmission advisories give applications access to data about network conditions.

When the subscribing endpoint of a multicast transport detects that it has missed one or more data packets, it requests that the publishing endpoint retransmit them. If possible, the publishing endpoint complies. Otherwise data loss occurs.

This advisory has severity DEBUG. It does not indicate impaired behavior. Applications can receive it *only* when the log level is set to DEBUG for the transports element. See also [Log Level Tuning via API](#).

Actions

This advisory contains information for debugging. Report this advisory to an administrator.

Fields

Field	Description
name	RETRANSMISSION
reason	RETRANSMISSION_REQUEST
endpoints	The string array value of this field lists the endpoints that detected missed data packets.
aggregation_ count	<p>The long value of this field reports the cumulative number of retransmission request incidents during the time interval (see aggregation_time).</p> <p>The base library aggregates this count separately for each transport.</p>
aggregation_ time	The double floating point value, in seconds, of this field indicates the length

Field	Description
	of the time interval for aggregating the incidents that <code>aggregation_count</code> reports. The time interval ends shortly before the timestamp.
timestamp	The <code>DateTime</code> value of this field indicates the time that the library generated the advisory. Although <code>DateTime</code> values can represent time with nanosecond precision, the actual resolution of the timestamp is only as fine-grained as the host computer's operating system supports.

RETRANSMISSION RETRANSMISSION_SENT

The advisory reports that a publishing endpoint in the application process retransmitted data packets as requested as requested by a subscribing endpoint.

Details

Retransmission is a normal occurrence for multicast transports. Retransmission advisories give applications access to data about network conditions.

When the subscribing endpoint of a multicast transport detects that it has missed one or more data packets, it requests that the publishing endpoint retransmit them. If possible, the publishing endpoint complies. Otherwise data loss occurs.

This advisory has severity `DEBUG`. It does not indicate impaired behavior. Applications can receive it *only* when the log level is set to `DEBUG` for the transports element. See also [Log Level Tuning via API](#).

Actions

This advisory contains information for debugging. Report this advisory to an administrator.

Fields

Field	Description
name	RETRANSMISSION
reason	RETRANSMISSION_SENT
endpoints	The string array value of this field lists the endpoints that re-sent missed data packets.
aggregation_count	<p>The long value of this field reports the cumulative number of data retransmission incidents during the time interval (see <code>aggregation_time</code>).</p> <p>The base library aggregates this count separately for each transport.</p>
aggregation_time	<p>The double floating point value, in seconds, of this field indicates the length of the time interval for aggregating the incidents that <code>aggregation_count</code> reports.</p> <p>The time interval ends shortly before the timestamp.</p>
timestamp	<p>The <code>DateTime</code> value of this field indicates the time that the library generated the advisory.</p> <p>Although <code>DateTime</code> values can represent time with nanosecond precision, the actual resolution of the timestamp is only as fine-grained as the host computer's operating system supports.</p>

RETRANSMISSION RETRANSMISSION_SUPPRESSED

The advisory reports that a subscribing endpoint in the application process would have requested retransmission, but the request was suppressed. Suppression of retransmit requests can occur when a multicast transport enables retransmission control, and a subscriber misses packets in excess of a specified threshold.

Details

Retransmission is a normal occurrence for multicast transports. Retransmission advisories give applications access to data about network conditions.

When the subscribing endpoint of a multicast transport detects that it has missed one or more data packets, it requests that the publishing endpoint retransmit them. If possible, the publishing endpoint complies. Otherwise data loss occurs.

This advisory has severity WARN.

Actions

Report this advisory to an administrator.

Fields

Field	Description
name	RETRANSMISSION
reason	RETRANSMISSION_SUPPRESSED
endpoints	The string array value of this field lists the endpoints that suppressed retransmission requests.
aggregation_count	<p>The long value of this field reports the cumulative number of retransmission request suppression incidents during the time interval (see <code>aggregation_time</code>).</p> <p>The base library aggregates this count separately for each transport.</p>
aggregation_time	<p>The double floating point value, in seconds, of this field indicates the length of the time interval for aggregating the incidents that <code>aggregation_count</code> reports.</p> <p>The time interval ends shortly before the timestamp.</p>
timestamp	<p>The <code>DateTime</code> value of this field indicates the time that the library generated the advisory.</p> <p>Although <code>DateTime</code> values can represent time with nanosecond precision, the actual resolution of the timestamp is only as fine-grained as the host computer's operating system supports.</p>

SUBSCRIBER_FORCE_CLOSE

The advisory reports that the persistence store closed a durable subscriber.

Details

For background information, see [Persistence: Stores and Durables](#).

Diagnosis

Each durable can serve at most one subscriber object at a time. A durable subscriber connected to the persistence store, and it maps to a durable that already serves another subscriber object. The store resolves collisions in favor of the more recent subscriber, deactivating the older subscriber.

Actions

Close the subscriber object. Clean up application state associated with the subscriber. Report this advisory to an administrator.

Fields

Field	Description
name	SUBSCRIBER_FORCE_CLOSE
reason	DURABLE_SUBSCRIBER_COLLISION
endpoints	The string array value of this field contains the single endpoint that the closed subscriber had instantiated.
subscriber_name	Subscriber name of the closed durable subscriber.
timestamp	The DateTime value of this field indicates the time that the library generated the advisory. Although DateTime values can represent time with nanosecond precision, the

Field	Description
	actual resolution of the timestamp is only as fine-grained as the host computer's operating system supports.

LOCK_LOST

The advisory reports that the client program no longer holds a lock.

Details

For background information, see [Locks](#).

Diagnosis

- Another client process has stolen the lock.
- This client process disconnected from the persistence service. All locks are invalid.

Actions

Request the lock again.

Fields

Field	Description
name	LOCK_LOST
reason	TIB_ADVISORY_REASON_LOCK_STOLEN TIB_ADVISORY_REASON_LOCK_LOST_ON_DISCONNECT
lock_name	The string value of this field contains the name of the lock that was stolen or lost.

Notifications

In some situations, the base library must notify programs of conditions that preclude the use of event queues as the communications medium. Instead of sending an advisory, the library notifies the program through an out-of-band mechanism.

All application programs must define a notification handler callback to process these out-of-band notifications, and register that callback using the set notification handler method.

Notifications Catalog

Out-of-Band Notification Catalog

Name and Reason	Description
<code>CLIENT_DISABLED</code>	The FTL server disabled this application process.

CLIENT_DISABLED

This notification alerts the application code that the FTL server administratively disabled this client process.

Diagnoses

- An administrator modified the realm definition, but this application process could not accept the changes, and the administrator disabled it (along with other processes that could not accept the changes).
- An administrator disabled this process to solve a problem (for example, consuming too much network bandwidth).

The administrator can supply an optional string to indicate a reason for disabling client processes. The notification callback receives this reason string as an argument.

Actions

Your notification callback must arrange for either of these two recovery actions:

- Create a new realm object and associated objects, and resume operation.
- Exit and restart.

To determine the appropriate recovery action, see [Recovery of a Disabled Process Restart versus Reopen the Realm](#).

To do either recovery action, see [Clean-Up](#).

Groups of Applications

Applications can use the group facility to coordinate fault-tolerant operation, or to distribute operating roles among application processes.

Introduction to Groups

A set of application processes can join a group. Each member of a group receives an *ordinal*, that is, a number representing its current position within the group. An application can specify a weight in a group member process to influence the ordinal assigned. Application program logic uses the ordinal to select one of several possible operating roles.

A *group service* tracks the group members as processes join and leave the group, and as they disconnect from and reconnect to the FTL server. At each of these events, the group facility revises ordinals to restore a one-to-one mapping between n members and the positive integers $[1, n]$.

Developers are responsible for the names of groups and for the API calls that join groups. Administrators are responsible for configuring group communication.

Simple Fault Tolerance with Groups

Application programs can use the group facility to coordinate fault-tolerant operation.

In the following diagram, consider an application program that can operate in either of two roles, according to its application logic:

- A1 is the active role: the program subscribes to messages, processes each message, and sends another message in response.
- A2 is the standby role: the program subscribes to messages, but neither processes them nor sends responses.

Simple Fault Tolerance, Role Behavior

Ordinal	Role	Description
1	A1	Actively process messages
2 or greater	A2	Standby

In the following diagram, when a process instance of the program starts, it joins Group_A, and receives its ordinal. The first process to start (Process P1) receives ordinal 1, so according to its application logic, it enters role A1 to subscribe, receive, process, and send messages. The second process to join the group (Process P2) receives ordinal 2, so it enters the A2 standby role. As other processes join the group, they receive ordinals 3, 4, and 5 in sequence and enter the A2 standby role. These are Process P3 through Process P5 in the diagram. In the following Timeline table, time t1 describes this state.

Simple Fault Tolerance, Timeline

Timeline: Processes Join Group_A					
Time	Process P1	Process P2	Process P3	Process P4	Process P5
t1	Ord=1 Role=A1	Ord=2 Role=A2	Ord=3 Role=A2	Ord=4 Role=A2	Ord=5 Role=A2
t2	Ord=-1 Role=A2 (or exit)	Ord=1 Role=A1	Ord=2 Role=A2	Ord=3 Role=A2	Ord=4 Role=A2
t3	Ord=5 Role=A2	Ord=1 Role=A1	Ord=2 Role=A2	Ord=3 Role=A2	Ord=4 Role=A2

Time t2 in the previous diagram illustrates the state when Process P1 exits, or becomes disconnected from the group service. All group members receive new ordinals within the group, usually decrementing their existing ordinal. In particular, Process P2 receives ordinal 1, enters role A1, and begins processing messages and sending responses. If Process P1 is still running while disconnected from the group service, then the group facility assigns it ordinal -1 and attempts to reconnect to the group service. The program can either exit, or enter the standby role A2, according to its program logic.

Time T3 illustrates the state when Process P1 restarts, or reconnects to the group service. Process P1 receives the lowest unassigned ordinal, and operates in the corresponding role, A2. Notice that Process P1 does not resume with ordinal 1. Instead, P2 retains ordinal 1.

Groups with More than Two Roles

You can extrapolate fault-tolerant behavior to an application with *several* distinct operating roles.

For example, consider an application that uses roles for graceful degradation of service. Each role subscribes to a different subset of messages by using different content matchers, and processes matching messages.

In the following diagram:

- B1 is an active role: The program processes high priority messages with matcher M1, and ignores the rest. The member with ordinal 1 operates in this role.
- B2 is an active role: The program processes medium priority messages with matcher M2, and ignores the rest. The member with ordinal 2 operates in this role.
- B3 is an active role: The program processes low priority messages with matcher M3, and ignores the rest. The member with ordinal 3 operates in this role.
- B4 is the standby role: The program does not process any messages. Any member with ordinal 4 or greater operates in this role.

More than Two Roles, Role Behavior

Ordinal	Role	Description	Matcher
1	B1	Actively process high priority messages	M1
2	B2	Actively process medium priority messages	M2
3	B3	Actively process low priority messages	M3
4 or greater	B4	Standby	

The following diagram shows ordinals and roles based on the number of processes running. When only one instance of application B is running, it has ordinal 1, role B1, and it

processes messages with the highest priority. It does not devote any time to messages with medium or low priority.

When two instances are running, one instance, with ordinal 1, role B1, processes messages with high priority. The other instance, with ordinal 2, role B2, processes messages with medium priority. Neither devotes any time to messages with low priority.

When three instances are running, each instance processes messages with a different priority, and together they cover all the priorities. That is, one instance has ordinal 1, role B1, and processes messages with high priority. Meanwhile, the second instance, with ordinal 2, role B2, processes messages with medium priority. The third instance, with ordinal 3, role B3, processes messages with medium priority.

When four or more instances are running, the instances with ordinal greater than 3 idle in standby role B4, ready to process messages if an instance in any of the processes in the three active roles were to become unavailable.



Tip: Notice that when the process with ordinal k becomes unavailable, all processes with ordinals greater than k shift their roles. When developing programs, design program logic to make this shift smoothly and rapidly.

More than Two Roles, Timeline

Processes Running	Process P1	Process P2	Process P3	Process P4	Process P5
1	Ord=1 Role=B1				
2	Ord=1 Role=B1	Ord=2 Role=B2			
3	Ord=1 Role=B1	Ord=2 Role=B2	Ord=3 Role=B3		
4 or more	Ord=1 Role=B1	Ord=2 Role=B2	Ord=3 Role=B3	Ord=4 Role=B4 standby	Ord=5 Role=B4 standby

Weights for Group Members

An application can assign a weight to a fault tolerance group member process. The weight influences the FTL group service's assignment of the ordinal, which determines the operating role, such as 1 (active). Use weights to make decisions based on hardware speed, hardware reliability, load factors, or other operating environment factors. Programs can adjust weights based on system conditions.

Weights, Ordinals, and Status

When a process joins a group, a member of greater weight always outranks members of lower weights. The group member process with the greatest weight is assigned ordinal 1 and the status is active (the leader member of the group).

For example, in the following diagram, Member A runs on a computer that is much faster than Member B, so Member A is assigned the greatest weight (200). The FTL group service assigns Member A ordinal 1 which is active status and Member B (weight 100) ordinal 2 which is standby status. Members C and D run on equally fast computers with approximately equal load factors so they are assigned an equal weight of 50 each, which results in the assignment of ordinals 3 and 4 and standby status.

Weights Assigned to Member Processes

Member	Weight Assigned	Ordinal Assigned	Status
Member A	200	1	Active
Member B	100	2	Standby
Member C	50	3	Standby
Member D	50	4	Standby

Greater Weight Processes Join

When an inactive member with a greater weight re-joins a group, the member preempts the active member of a lower weight. For example, in the following diagram, when three processes are running, Member B has the greatest weight (100) and is the active member. When Member A (weight 200) joins the group and four processes are running, the FTL

group service re-assigns ordinal 1 (active) to Member A and sends an ordinal update to the other processes.

More than Two Roles, Timeline

Processes Running	Member B Weight 100	Member C Weight 50	Member D Weight 50	Member A Weight 200
3	Ord=1 Role=Active	Ord=2 Role=Standby	Ord=3 Role=Standby	
4 (Member A joins)	Ord=2 Role=Standby	Ord=3 Role=Standby	Ord=4 Role=Standby	Ord=1 Role=Active

Members with Equal Weight

Members of equal weight do not outrank each other and the order of equally weighted members joining the group is irrelevant to rank.

Considerations:

- If two members have equal weight, you cannot assume either member outranks the other or that either member will be the first to become the active member.
- An inactive member that is joining never preempts an active member with the same weight. For example, if Members Y and Z have equal weight, and Member Z is already active (ordinal 1), then Member Y does not preempt Member Z.

Adjusting Weights

In addition to specifying weight when a process joins a group, programs can adjust their weight at any time to reflect changing conditions. For example, when a load factor of a host computer changes, a member process might track the change and adjust its weight accordingly.

When a member's weight is adjusted, the FTL group service recomputes the ordinals members of the group. For large groups this re-computation can affect performance.

API Weight Settings

Weight is controlled via the FTL Group API. Considerations:

- Weights must be positive integers.
- Zero cannot be used as a weight and is reserved for future use.
- In groups where member weights are assigned, members without a weight are assigned a default weight of 100.
- In groups where no member weights are assigned, the member that joined first gets ordinal 1.

Groups Principles of Operation

Group Service

Group services coordinate all the members of a group.

Every FTL server automatically provides a group service. Programs use the group facility's API calls to interact with the group service, and to coordinate appropriate behavior.

Group Members

Each group has a unique *group name*, which identifies its members to the group service.

In each group, every member must be able to assume any role, according to its current ordinal. You can satisfy this requirement in a natural way if all the members are process instances of one application program, compiled from source code with identical functionality (though they may execute on different hardware and operating system platforms).

Member applications and the group service are all within the same realm, and usually run on host computers within a local area network.

The first member to join a group establishes heartbeat and timeout parameters for the entire group, based on the *activation interval* property that the first member supplies in

the `join` call. For consistent behavior, ensure that all members of a group supply the same activation interval.

An application can join several groups. Nonetheless, an application must *not* join a group a second time, that is, if it is already a member of that group.

Interactions within a Group

The *join* call establishes communication between a member and the group service. After the join call returns successfully, the group library continues exchanging heartbeats with the group service. (Heartbeats and other group protocols are not visible to your program code.)

The *leave* call explicitly ends the stream of heartbeats from a member. The group service immediately adjusts the ordinals of the remaining members.

Other events can *implicitly* interrupt the heartbeat stream. For example, the member process could abruptly exit, or network segmentation could separate the member from the group service. In these situations, the group service also adjusts the ordinals of the remaining members, but after a calculated delay (see [Activation Interval](#)).

When a member's ordinal changes, the group facility informs program code by raising an `ORDINAL_UPDATE` advisory message. Programs subscribe to this advisory, and application callback code must take appropriate action to change the member's operating behavior.

The group service tracks member heartbeats to determine the health of each member.

Individual members of a group do not exchange group protocol messages with one another, but only with the group service.

Side Effects of Groups

Group protocol traffic consumes network bandwidth. With fewer than 10 members, using the default activation interval, expect only minimal impact on message latency. More members or a smaller activation interval can increase the impact.

Techniques for Programming with Groups

Program Structure for Groups

Programs using the group facility follow this template.

1. Determine the group name and property values.

(See also, [Restrictions on Names](#).)

2. Subscribe to ordinal update advisories.

Content matchers can filter for these advisories by matching the string value `ORDINAL_UPDATE` in the name field, and the group name in the group field.

The ordinal field contains the group member's new ordinal.

The subscriber callback must change the operating role of the application process according to the new ordinal.

3. Join the group, using the join API call.
4. Explicitly leave the group, using the leave API call.

Programs must leave all groups before closing the realm object.

Activation Interval

When a member becomes disconnected, the group facility revises the ordinals of the remaining members, which respond by adjusting their operating roles. This process is not instantaneous: it takes time to *detect*, to *revise*, and to *adjust*.

You can supply the activation interval property as a guide for the group service during the detect and revise phases. The group service derives appropriate heartbeat and timeout intervals from this property, aiming to complete these two phases within the activation interval you supply. That is, when a member becomes disconnected, you can expect that all affected group members receive new ordinals in approximately this time.

In contrast, the length of the adjust phase depends on the application, and the time it requires to switch operating roles.

In the interim, the application processes as a group might miss some messages. You can implement strategies to compensate for this possibility, as appropriate to application requirements.

If you omit the activation interval property, its default value is 5 seconds.

Disconnect

Ordinal -1 indicates that the group member is disconnected from the group service.

The group object automatically attempts to reconnect, and continues until the program explicitly destroys the object. Meanwhile, the group service could reassign the member's previous ordinal to another group member.

Appropriate program response depends on application requirements. For example, if it is not acceptable for two members to share the role, the program should respond by entering an idle or standby role. In contrast, if duplication of the role is acceptable, then the program could continue in that role while waiting to reconnect. Alternatively, the program could log an error and exit.

Group Status

Group status advisories report the state of group members.

Group members and observers can subscribe to receive group status advisories.

The group library presents members and observers with group status advisories, which can have one of three forms:

Total Status

A group status advisory that contains the group status of *all* existing member processes.

Change in Status

A group status advisory that contains the group status of *a subset* of members, including new members that joined the group, members that left the group, or members that became disconnected. Frequently, only one member at a time changes status, so the subset contains only that one member.

Server Unavailable

A group status advisory that indicates that the group service is unavailable or unreachable. This form does not contain the group status of any members.

When the state of the group changes, the group library presents members and observers with group status advisories. The form of the advisory depends on both the member and state change:

- When a *new member joins* a group, it receives a total status advisory, containing the status of all the members, excluding observers. All the other members and observers receive a change in status advisory.

When a *disconnected member reconnects*, this event results in the same set of status messages.

- When a *member leaves* a group, it does not receive a status advisory. All the other members and observers receive a change in status advisory.
- When a member becomes *disconnected* from the group service, it receives a server unavailable advisory. All the other members and observers also receive a change in status advisory.
- When a *new observer joins* a group, the group state does not change. The new observer receives a total status advisory, containing the status of all the other members, excluding any observers. Other members and observers do *not* receive a status advisory.
- When an *observer leaves* a group, or becomes *disconnected* from the group service, the group state does not change. The affected observer does *not* receive a status advisory, nor do any other members or observers.

For reference details about the group status advisory message, see [GROUP_STATUS](#).

Group Observer

An application program can join a group as an *observer*. Observers can monitor the group by subscribing to group status advisories, just as members can. However, the group service does not assign ordinals to observers: observers do not participate in the functional roles of the group.

When an observer joins or leaves a group, or becomes disconnected from the group service, the state of the group and its members does not change.

Programmer's Checklist Addenda for Groups

The items in this topic supplement the checklist items in [Information for Developers](#).

All Programming Languages

The FTL server and its group service must be available to application processes. For details, see TIBCO FTL [Administration](#).

C Programmer's Checklist

C programs must include the header file `tibgroup/group.h`.

On UNIX platforms, add the linker flag `-ltibroup`.

On Windows platforms, link the corresponding C library file `tibgroup.lib`, and run using `tibgroup.dll`.

Java Programmer's Checklist

Java programs must import the group package:

```
import com.tibco.ftl.group.*;
```

The CLASSPATH must include the `lib` directory, which must contain the archive file `tibftlgroup.jar`.

.NET Programmer's Checklist

To simplify coding, programs can include this statement:

```
using TIBCO.FTL.GROUP;
```

The assembly `TIBCO.FTL.GROUP.dll` must be in the general assembly cache (GAC). If the .NET framework is properly installed, then installing TIBCO FTL registers the assembly with the GAC.

Persistence: Stores and Durables

Persistence is the potential to store a message between sending and receiving it.

The topics that follow present persistence, stores, and durables from an application developer's perspective. These topics focus on the modifications to programs that enable durable subscribers and correct interaction with a persistence cluster.

For an intuitive introduction and terminology, see "Persistence: Stores and Durables" in TIBCO FTL [Concepts](#).

For advisories associated with persistence, see "Stores and Durables" in TIBCO FTL [Development](#).

For coordination between developers and administrators, see the "Application Coordination Form" in the FTL [Product Guides](#) list.

Purposes of Persistence

The persistence infrastructure of stores and durables can serve four purposes:

- Delivery assurance
- Apportioning message streams
- Last-value availability
- Key/value maps

These purposes correspond to four types of durables: standard durables, shared durables, last-value durables, and map durables.

Delivery Assurance

An ordinary subscriber receives messages from a publisher only when a transport connects the subscriber with that publisher. That is, an ordinary subscriber cannot receive a message through a direct path transport unless *both* of these conditions hold at the time that the publisher sends the message:

- The subscriber object exists.
- The transport is connected.

With persistence, subscribers can receive every message with high assurance, despite temporary lapses in these conditions. For example, a persistence store can retain data for subscriber recovery after application exit and restart, temporary network failure, or application host computer failure.

Stores can retain data indefinitely, until subscribers acknowledge delivery. (In contrast, even reliable transports retain data only for a finite interval.)

For delivery assurance, use standard durables. Standard durables serve one subscriber at a time, and assure that it can receive the whole message stream.

Apportioning Message Streams

In some situations it is convenient to use a shared durable to apportion a message stream among a set of cooperating subscribers so that only one subscriber receives and processes each message, but acting together the subscribers process every message in the stream. For details, see [Basic Definitions for Persistence](#), Shared Durable.

Last-Value Availability

When new subscribers need to receive the current state immediately, but do not need to receive a complete historical message stream, a persistence store can supply the most recent (i.e., *last-value*) message.

The store continues to forward subsequent messages to subscribers, discarding the previous message as each new message arrives.

For last-value availability, use last-value durables. Last-value durables can serve many subscribers.

A last-value durable divides its input message stream into distinct output streams based on the value of a distinguished key field. In this way, one last-value durable holds more than one last value: one for each key.

Key/Value Map

A key/value map is like a last-value durable without a message stream. It behaves like a simple database table with two columns.

Instead of an inbound message stream to supply values, programs use the map API calls to store and access values. See "Key/Value Maps" in TIBCO FTL [Development](#).

Basic Definitions for Persistence

Store

A data structure that collects a stream of messages.

Durable

A data structure within a store that represents subscriber interest, holds messages for a specific subscriber identity, and tracks acknowledgments as a subscriber object consumes those messages. Each store can contain many durables.

A durable can exhibit one of these behavior types: *standard*, *shared*, *last-value*, or *map* (see the definitions that follow).

Independent of its behavior type, a durable can exist either as *static* or *dynamic* (see the definitions that follow).

Standard Durable

A durable that represents the interest of one subscriber object, strengthening delivery assurance for that subscriber.

Use a standard durable when a subscriber must receive every message in a message stream, even if the subscriber is intermittently disconnected from the message bus. The type of persistence for a standard durable depends on whether the *prefetch* feature is enabled or disabled:

- Prefetch Enabled — Messages are received and sent by the server to subscribers. The durable functions as a message broker, with no messages traveling peer-to-peer from publisher to subscriber.
- Prefetch Disabled — Under normal conditions, messages flow directly from publisher to subscriber, with the store serving as a backup.

Shared Durable

A durable that represents the identical interest of *two or more* cooperating subscriber objects, apportioning a message stream among those subscribers.

Use a shared durable when a set of subscribers collectively process a message stream in a distributed or parallel fashion, processing every message exactly once.

Last-Value Durable

A durable that represents the interest of potentially many subscriber objects. It stores only the most recent message from one or more message streams.

Use a last-value durable to hold recent context for initializing new subscribers.

Map Durable

A durable that stores a key/value mapping. When a message arrives, a map durable uses the value in the message's key field as the key, and stores the full message as its value. For each distinct key, the durable stores only the most recent value. (Notice that one map durable can hold many key/value pairs.)

Applications can use the map API to get the current value of a key, or to store a key/value pair.

Key values must be strings.

Static Durable

A durable that the administrator defines as part of the store definition. It exists in the store and expresses interest in its message stream even before an application subscribes to it.

Dynamic durables are more convenient than static durables. Use static durables in situations that require administrative control over durables, or to support existing applications.

Dynamic Durable

A durable that an application creates at run time. The store creates it dynamically when an application subscribes to it. It expresses interest in a message stream only from the moment of first subscription. It continues to express interest until a program or an administrator explicitly deletes it from the store. Inbox durables are always dynamic durables.



Tip: Dynamic durables are the simplest way to create and use durables.

Dynamic Durable Template

An administrative definition that supplies parameters for a set of dynamic durables.

✓ **Tip:** The simplest way to enable dynamic durables is to use the built-in dynamic durable templates when configuring an endpoint; see "Enabling Dynamic Durables," "Enabling Maps," and "Built-In Dynamic Durable Templates" in TIBCO FTL [Administration](#).

Publisher Mode and Send Policy

Administrators set the publisher's mode when configuring a store. The publisher mode is either `store_confirm_send`, which offers maximum delivery assurance, or `store_send_noconfirm`, which offers minimal delivery assurance. For details, see the FTL Administration guide, [Publisher Mode](#).

Applications may set the publisher's send policy when creating a publisher object. In addition, administrators may set a default send policy in the realm configuration. See the [Administration](#) guide, [Publisher Mode and Send Policy](#).

The send policy may be inline or non-inline. In general inline send offers better latency, while non-inline send offers better throughput.

When the publisher mode is `store_send_noconfirm`, the send call returns immediately, regardless of the send policy. The application is not notified as to whether the message was persisted or lost. In this case, the non-inline send policy may offer somewhat improved throughput in exchange for higher latency.

When the publisher mode is `store_confirm_send`, the FTL library will attempt to persist the message for the publisher's retry duration. The retry duration can be set by the application. Administrators may set a default value in the realm configuration. See the [Administration](#) guide, [Realm Properties Details Panel](#), section [Persistence Retry](#).

If the publisher mode is `store_confirm_send`, and the send policy is inline, then the send call will block until the message is persisted, or the retry duration has elapsed. If the FTL library could not ensure that the message was persisted, an exception is raised by the send call. This is a synchronous send call, where performance is tied directly to the latency to the persistence service. It may be necessary to use the batched send call (`tibPublisher_SendMessages`), or multiple publishers in parallel, to achieve acceptable performance.

If the publisher mode is `store_confirm_send`, and the send policy is non-inline, the send call may return immediately, provided that the maximum batch count has not yet been reached. The application may set the maximum batch count. See the next section below.

When the send policy is non-inline, the FTL library attempts to persist the message in the background for the publisher's retry duration. If the latency to the persistence service is large, a non-inline send may offer a substantial improvement in throughput compared to inline send. However, failures are signaled to the application asynchronously, and handling failures may require a more sophisticated application.

If using a non-inline send, it is critical that the application flushes or closes the publisher before exiting. If the application merely exits, the send call may not be complete, and the message may be lost.

i Note: Calls to set keys in a map (`tibMap_Set` and `tibMap_SetMultiple`) are always synchronous. That is, they behave as if the publisher mode is `store_confirm_send` and the send policy is inline.

Configuring Publisher Send Policy

Send policy is configurable via the realm properties and at the API level. The API property set for inline or non-inline sends during publisher creation takes precedence over the realm property.

Dynamic update of the send policy realm property is allowed. However it applies only to the newly created publishers. Existing publishers are not affected by the new value. See the [Administration](#) guide, [Publisher Mode and Send Policy](#).

Applications may override the send policy when creating a publisher object (`TIB_PUBLISHER_PROPERTY_INT_SEND_POLICY`).

When using non-inline send, the application may specify a maximum batch count (`TIB_PUBLISHER_PROPERTY_INT_MAX_BATCH_COUNT`) when creating the publisher. The maximum batch count is an upper limit on how many messages the FTL library may have that are not yet persisted (in other words, how many messages are in flight to the persistence service). If this limit is reached, the send call will block. This limit may also be used to determine which messages might have been lost in the event of a failure.

If using non-inline send, a situation may occur where an application closes a publisher shortly after making a send call. Since the send may not be complete, the FTL library will linger for some amount of time while the send is retried. If the message cannot be persisted within the linger period it may be lost. The application may override the

publisher close linger period when creating the publisher (TIB_PUBLISHER_PROPERTY_DOUBLE_PERSISTENCE_CLOSE_LINGER).

FTL provides APIs that an application may use to determine the send policy and max batch count of a publisher object.

Detecting Failures with Non-Inline Send

When the send policy is non-inline, and a message cannot be persisted (perhaps because the retry duration has elapsed), the failure may occur in the background. The application will be notified, possibly after the fact, in one of two ways:

- An exception is generated by an ongoing or future send call
- An exception is generated by an ongoing or future flush call

However if the failure occurs during the publisher close linger period (for example, if a close call is made while the FTL library has messages that are not yet persisted), no exception is generated. Applications may wish to make a flush call before the close call.

When an exception is generated, the application must assume that up to maximum batch count messages might have been lost. This includes the message that was passed to a failed send call. Applications may wish to keep information about the most recent messages for diagnostic or other purposes. Re-sending the most recent messages is possible, but may result in duplicates.

If the application does not make send or flush calls frequently, it may subscribe to an advisory for non-inline send loss (TIB_ADVISORY_NAME_NON_INLINE_SEND_LOSS). When this advisory is received, it is a hint to the application that an error has occurred in the background, and that a future flush or send call will generate an exception.

Durable Subscribers

A *durable subscriber* is a subscriber object in an application process that maintains its identity even if the process exits and restarts. It can receive messages from a durable in a persistence store.

A durable is a data structure within a store. Within a store, each durable has a unique name.

When a program creates a subscriber object, it can link that subscriber to a durable in either of two ways:

Durable Name

The program supplies a durable name in the create subscriber call. This name is a request to link the subscriber with a specific durable. Supply the name as the value of the *durable name* property.

If a durable with that name already exists, the subscriber links to that durable.

Otherwise, the store dynamically creates a durable with that name, and the subscriber links to that new durable. (Pre-requisite: The administrator has enabled dynamic durables.)

✓ **Tip:** Using durable names is simpler than using subscriber names, because you need not define a subscriber name mapping.

Subscriber Name

i **Note:** Subscriber name mapping is an advanced topic.

Within an application instance, the administrator defines a mapping from subscriber names to durable names. The program supplies a subscriber name in the create subscriber call, and the mapping determines the durable for the subscriber. Supply the name as the value of the *subscriber name* (or *name*) property.

The durable must already exist: that is, the administrator must define it as a static durable.

✓ **Tip:** For flexibility, design applications can obtain their durable names and subscriber names from an external source, such as a command line argument or configuration file. Do not hard-code these names into application programs.

Developers and administrators coordinate the details of durable subscribers. See the "Durable Coordination Form" in the FTL [Product Guides](#) list.

Standard Durables

A *standard durable* strengthens delivery assurance for a subscriber.

A standard durable with prefetch disabled is intended to be used alongside a direct path to strengthen delivery assurance for a subscriber. However, the direct path remains the primary path.

A standard durable with prefetch enabled uses no direct path. Messages are always brokered by the persistence service.

Browsing is not supported for standard durables and is only supported for shared durables.

Quality of Service

A standard durable ensures that every message is received and acknowledged by its subscriber.

If the subscriber does not acknowledge a message, the persistence store retains the message, and the subscriber automatically recovers the message.

Delivery Count and Maximum

A standard durable with a nonzero prefetch setting counts the delivery attempts for each message. If the administrator sets an optional maximum limit for a durable, the durable can discard a message after the number of failed delivery attempts exceeds that limit.

While this mechanism never discards a message before reaching the limit, it does *not* guarantee a discard at exactly the limit.

Message Retention

A standard durable retains each message until its subscriber acknowledges it.

Subscribers

A standard durable can serve at most one subscriber at a time. That subscriber receives the entire message stream.

If a standard durable already serves a subscriber object in one client process, and another client process creates a subscriber that connects to the same standard durable, then the persistence store resolves collisions in favor of the more recent subscriber, deactivating the older durable subscriber. See "SUBSCRIBER_FORCE_CLOSE" in TIBCO FTL [Development](#).

If a subscriber to a standard durable already exists within a client process, and the same client process subsequently attempts to create another subscriber on the same standard durable, that subscriber create call fails.

Direct Path

Administrators may configure a direct path from publisher to subscriber. In this arrangement, a standard durable provides a parallel path through the persistence service, which adds an intermediary hop. This durable path is only for recovering missed messages. See “Stores for Delivery Assurance” in TIBCO FTL® [Administration](#).

However, in some use cases, a direct path is not required for standard durables:

- When using a message broker
- When using a wide-area store

Content Matcher

A standard durable accepts, but does not require, a content matcher.

If it has a content matcher, then the subscriber must specify either an identical content matcher, or no content matcher.

Acknowledgments

A standard durable tracks acknowledgments from subscribers.

Dynamic Durable

Before a program can create a dynamic standard durable, the administrator must have already enabled standard dynamic durables on the endpoint. In TIBCO FTL® [Administration](#), see “Enabling Dynamic Durables” and “Inbox Durable Templates”.

When a program creates a dynamic durable, it must supply the following information in the subscriber create call:

- Endpoint Name
- Durable Name
- Key Field Name

When creating a new dynamic durable, the key field name becomes part of its content matcher.

- Content Matcher

When creating a new dynamic durable, the content matcher becomes part of the new durable. The content matchers of subsequent subscribers to the durable must be identical.

If a durable with the specified durable name and key field name already exists, that durable forwards messages to the new subscriber.

If a durable with the specified durable name does *not* yet exist, the persistence store creates a dynamic durable using the durable name, key field name, and content matcher supplied in the subscriber create call.

Static Durable

Before a program can subscribe to a static durable, the administrator must have already defined that durable in the persistence store associated with the endpoint. See “Defining a Static Durable” in TIBCO FTL® [Administration](#)

When a program subscribes to a static standard durable, it must supply the following information in the subscriber create call:

- Endpoint Name
- Durable Name or Subscriber Name

To understand this distinction, see “Durable Subscribers” in TIBCO FTL® [Development](#).

- Optional: Content Matcher

The content matcher must either be null, or be identical to the content matcher of the durable as configured by the administrator. The best practice is to supply null.

Shared Durables

A *shared durable* apportions a message stream among its subscribers.

Quality of Service

A shared durable ensures that every message is received and acknowledged by a subscriber. Each subscriber receives a portion of the input message stream. Together, the subscribers receive the entire message stream.

If a subscriber does not acknowledge a message, the durable can redeliver it to another subscriber.

Delivery Count and Maximum

A shared durable counts the delivery attempts for each message. If the administrator sets an optional maximum limit for a durable, the durable can discard a message after the number of failed delivery attempts exceeds that limit.

While this mechanism never discards a message before reaching the limit, it does *not* guarantee a discard at exactly the limit.

Message Retention

A shared durable retains each message until a subscriber acknowledges it, or until its delivery count reaches the maximum limit.

Subscribers

A shared durable can support multiple subscribers simultaneously.

Each subscriber receives a portion of the message stream.

Direct Path

Subscribers receive messages *only* through the persistence store. The shared durable semantic precludes direct-path delivery, even if a direct path is configured.

Content Matcher

A shared durable accepts, but does not require, a content matcher.

If it has a content matcher, then every subscriber must specify either an identical content matcher, or no content matcher.

Acknowledgments

A shared durable tracks acknowledgments from subscribers.

Shared Durable Browsing

Use a client API to browse messages stored in a shared durable, for example, to run analytics on the data or delete a message. Messages are browsed from oldest to newest. A matcher can be used to browse a subset of the messages. Browsing does not affect delivery of messages to subscribing clients. Messages can be delivered to other subscribing clients while simultaneously being browsed. The effective matcher is a logical AND of the browser matcher and the durable matcher.

Messages returned to a durable while a browser is running are not browsed unless the browser is restarted or re-created. This may happen, for example, because a consumer failed while processing some messages.

In the event of leader failover or connection loss, browsers need to be restarted or closed.



Warning: Creating too many browsers is not recommended, as it can put a strain on the persistence service resources, including both CPU and memory usage.

Monitoring

The REST API and UI show the number of browsers on a shared durable. See [GET persistence/clusters/<clus_name>/stores/<stor_name>/durables](#).

Logging

A log message warns if there are too many browsers on a shared durable.

Dynamic Durable

Before a program can create a dynamic shared durable, the administrator must have already enabled shared dynamic durables on the endpoint, In TIBCO FTL® [Administration](#), see “Enabling Dynamic Durables” and “Inbox Durable Templates”.

When a program creates a dynamic durable, it must supply the following information in the subscriber create call:

- Endpoint Name
- Durable Name
- Key Field Name

When creating a new dynamic durable, the key field name becomes part of its content matcher.

- Content Matcher

When creating a new dynamic durable, the content matcher becomes part of the new durable. The content matchers of subsequent subscribers to the durable must be identical.

If a durable with the specified durable name and key field name already exists, that durable forwards messages to the new subscriber.

If a durable with the specified durable name does *not* yet exist, the persistence store creates a dynamic durable using the durable name, key field name, and content matcher supplied in the subscriber create call.

Static Durable

Before a program can subscribe to a static durable, the administrator must have already defined that durable in the persistence store associated with the endpoint. See “Defining a Static Durable” in TIBCO FTL [Administration](#).

When a program subscribes to a static shared durable, it must supply the following information in the subscriber create call:

- Endpoint Name
- Durable Name or Subscriber Name

To understand this distinction, see “Durable Subscribers” in TIBCO FTL [Development](#).

- Optional: Content Matcher

The content matcher must either be null, or be identical to the content matcher of the durable. The best practice is to supply null.

Last-Value Durables

A *last-value durable* preserves only the most recent message for subscribers. It does not track message acknowledgments from subscribers.

Browsing is not supported for last-value durables and is only supported for shared durables.

Quality of Service

A last-value durable divides its input message stream into output sub-streams based on the string value of a key field in each message. For each sub-stream, the durable stores the most recent message.

A last-value durable ensures that every new subscriber immediately receives the most recent message, if one is stored. The subscriber continues to receive the sub-stream of subsequent messages until the subscriber closes, but without any assurance of delivery.

Message Retention

A last-value durable retains only one message for each output sub-stream.

Subscribers

A last-value durable can support multiple subscribers simultaneously.

Each subscriber can receive exactly one output sub-stream.

Direct Path

Subscribers receive messages *only* through the persistence store. The last-value durable semantic precludes direct-path delivery, even if a direct path is configured.

Content Matcher

Subscribing to a last-value durable requires a content matcher.

For static last-value durables, the administrator configures the key field name, and the program must match a specific value of that field in the create subscriber call.

For dynamic last-value durables, the program must supply the key field name as a property in the create subscriber call, and match a specific value of that field.

The key field must contain data of type string. Content matchers must match a string value against the key field.

Notice that each subscriber must test the key field, but each subscriber can match a different value of that field. The value determines the output sub-stream that the subscriber requests from the last-value durable.



Caution: A logical OR match is not permitted on the key field in the matcher used by a last-value durable subscriber. A subscriber must specify exactly one string value for the key field.

Acknowledgments

A last-value durable does not track acknowledgments from subscribers.

Unlike standard and shared durables, a subscriber to a last-value durable subscriber does not consume messages from the durable. Instead, new subscribers to a sub-stream continue to receive the stored value until a publisher sends a new value, which replaces it.

Dynamic Durable

Before a program can create a dynamic last-value durable, the administrator must have already enabled dynamic last-value dynamic durables on the endpoint. In TIBCO FTL® Administration, see “Enabling Dynamic Durables” and “Inbox Durable Templates”.

When a program creates a dynamic durable, it must supply the following information in the subscriber create call:

- Endpoint Name
- Durable Name
- Key Field Name

When creating a new dynamic durable, the key field name becomes part of its content matcher.

- Content Matcher

When creating a new dynamic durable, the content matcher becomes part of the new durable. The content matchers of subsequent subscribers to the durable must be identical.

If a durable with the specified durable name and key field name already exists, that durable forwards messages to the new subscriber.

If a durable with the specified durable name does *not* yet exist, the persistence store creates a dynamic durable using the durable name, key field name, and content matcher supplied in the subscriber create call.

For example, suppose the store does not yet contain a durable named ticker. A program then creates a subscriber to a last-value durable named ticker, with key field name Symbol and content matcher {"Symbol":"IBM","Exchange":"NYSE"}. In response, the store creates a new dynamic durable named ticker, with content matcher {"Symbol":true,"Exchange":"NYSE"}. That is, the new durable generalizes from the key field name to a content matcher clause that tests for the *presence* of the key field rather than a specific value, and integrates the rest of the clauses from the subscriber's content matcher.

If the create subscriber call does not supply a content matcher, the new durable uses only the key field clause as its content matcher.

Subsequent subscribers to the durable must specify compatible content matchers: that is, they must be identical except for the key field value, which can be different. A subscriber create call with an incompatible content matcher throws an exception.

Static Durable

Before a program can subscribe to a static durable, the administrator must have already defined that durable in the persistence store associated with the endpoint. See “Defining a Static Durable” in TIBCO FTL® [Administration](#).

When a program subscribes to a static last-value durable, it must supply the following information in the subscriber create call:

- Endpoint Name
- Durable Name or Subscriber Name

To understand this distinction, see “Durable Subscribers” in TIBCO FTL [Development](#).

- Content Matcher

The content matcher must include a test for a specific value of the key field: that is, it must express interest in a sub-stream of the last-value durable, as determined by a specific key string.

Acknowledgment of Message Delivery

A durable subscriber can acknowledge consuming a message to its durable in either of two ways.

Automatic Acknowledgment

With *automatic* acknowledgment, the base library automatically acknowledges the message when the application callback returns. This choice is appropriate when an application's callback completely processes the inbound message and then returns.

Explicit Acknowledgment

With *explicit* acknowledgment, the application program must use the `acknowledge` call to explicitly acknowledge each message. This choice is appropriate when an application's callback delegates processing of the inbound message to a separate thread. It could also be appropriate if the application must verify the success of each acknowledgment.

To enable explicit acknowledgment, programs pass a property to the subscriber create call. Otherwise, the default behavior is automatic acknowledgment.

The subscriber must acknowledge each message as received directly from the durable, using the `Acknowledge` call.



Note: The choice between these two mechanisms for acknowledging messages is orthogonal to the administrator's choice of [Acknowledgment Mode](#): synchronous versus asynchronous.

Acknowledgment is not relevant with last-value durables.

Message Delivery Behavior

Duplicate Delivery

While persistence stores and durables can strengthen delivery assurance, they also introduce the possibility of duplicate delivery. Application developers must design subscribing programs to process duplicate messages gracefully.

Message Order

A persistence store preserves message order *within* each of its publisher streams. That is, if a publisher sent message M1 before message M2, then the store delivers M1 before M2. Every subscriber that attempts to recover both messages receives them in the correct order.

However, a persistence store that merges message streams from two or more publishers does *not* preserve global order among its publisher streams. That is, if publisher A sent message A1 before publisher B sent message B2, the store could deliver these messages in either order. Furthermore, two subscribers S and T that recover these two messages could receive them in a different order: S receiving A1 first, and T receiving B2 first.

Maximum Message Size

When an endpoint is associated with a persistence store, limit the maximum size of messages to 10MB each. Messages that exceed the environment's maximum message size could disrupt the quorum of persistence services, and prevent them from reforming a quorum.



Warning: Persistence services and quorums are the responsibility of administrators, so developers generally do not need to know about them. Nonetheless, developers must understand that sending messages that exceed this maximum size limit could disrupt executable components.

The actual maximum can vary depending on network and host hardware. To determine the actual maximum, test empirically in each deployment environment.

Delivery Count for Standard and Shared Durables

When a shared durable or a standard durable with prefetch enabled delivers a message to a subscriber, the message includes a delivery count, indicating the number of times the persistence service has already delivered the message to this and other subscribers. It is good practice for message callbacks to check this value to confirm expected behavior.

i Note: Delivery count does not apply to standard durables with prefetch disabled.

Delivery Count = 1

If the delivery count is 1, you can infer that the subscriber is the first to receive the message.

Delivery Count Greater than 1

If the delivery count is greater than 1, it is possible that another subscriber received the message, but did not successfully process and acknowledge the message.

A higher delivery count could indicate a problem with the message. A message callback could shunt the message away from normal processing and output a log.

Administrators can set a shared durable parameter to limit the maximum delivery attempts. .

Delivery Count = -1

A delivery count of -1 can indicate any of the following conditions:

- The message is from a standard durable with prefetch disabled, or from a last-value durable.
- The message arrived through a direct path (e.g., standard durable with prefetch disabled), rather than from a persistence service.
- The persistence service predates the tracking of delivery counts.

A message callback can ignore this value and continue processing the message.

Programmer's Checklist Addenda for Stores and Durables

This topic provides a checklist for programmers using persistence stores and durables.

The following items supplement the checklist items in [Information for Developers](#).

All Programming Languages

- Ensure that the library load path includes the location of the most recent TIBCO FTL libraries *before* the locations of any older TIBCO FTL releases.
- The realm administrator must configure a persistence cluster and its persistence services. The persistence services must be available to application processes. For details, see TIBCO FTL [Administration](#).

Minimum Release

For best results, use the most recent release. Nonetheless, when using an older release, ensure that it includes the persistence features that the applications require.

Persistence Feature	Minimum Release
Delivery Count	5.4
Dynamic Durables	4.2
Last-Value Durables	
Key/Value Maps	
Apportion Message Streams	4.0
Delivery Assurance	3.1

Key/Value Maps

Programs can use maps to store key/value pairs in a persistence store.

A map behaves like a simple database table with two columns: key and value. The key is a string, and the value is a message.

Programs assign a name to each map. A store may contain many maps, each with a unique name.

API methods can do these operations:

- Create a map.
- Set a key/value pair or multiple key/value pairs.
- Get a key's value.
- Remove a key/value pair.
- Iterate over all the key/value pairs in a map, or some of the key/value pairs using a string matcher.
- Close a map object.
- Delete a map from the store.

In addition, most of these methods are available as locked operations. That is, you can use a lock to ensure that map operations in different processes do not interfere with one another (see [Locks](#)).

In order for a program to use maps, administrators must enable dynamic last-value durables in a persistence store. For more information, see “Enabling Key/Value Maps” in TIBCO FTL [Administration](#).

Locks

A lock is used to ensure exclusivity of a series of map operations in a persistence service.

If a series of client map API calls using a lock completes without an exception, then an application may be assured that no other writer using the same lock concurrently modified

a map in the persistence service, and that the modifications will be visible to future readers using the same lock.

If a map API call using a lock fails, then nothing may be assumed about the result of that operation, and the lock must be returned or destroyed before trying again.

A typical use is to implement atomic test-and-set on a particular row of a map. See the sample program `tibftlmap-lock`.

Lock Name

When a program creates a lock object, it assigns a lock name. A persistence cluster may contain many locks, each with a unique name. Two lock objects with the same name represent the same lock, so two or more application processes can use the lock to cooperate.

Programmers choose the name of a lock to indicate the purpose of the lock: for example, `ServerStatusMapLock` might lock an entire map that stores the states of server hardware within an enterprise, while `BlueLock` might lock the row of that map that describes the state of the server named Blue.

Methods of Lock Objects

API methods can do these operations:

- Create a lock.
- Return (that is, release) a lock that the process holds.
- Steal a lock that another process holds.
- Destroy a lock object to reclaim resources.

Methods with Locks and without Locks: Effective Use

Map operations are available in two forms: *with lock* and *without lock*. Methods that take a lock argument respect the state of that lock: that is, if another process holds the lock, then the method throws an exception and does not complete its map operation.

However, methods that do not take a lock argument do not respect the state of any lock: even if another process holds a lock for the map or for the key row, the method does not test the lock, and completes its map operation.

For locks to effectively prevent interference, *all* your application processes must access the map using only methods with locks.

Pattern for Programming with Locks

1. Create a lock object.
2. Call one or more methods with that lock.

A program can call many methods with that lock, even within a loop, as with a map iterator.

While the process still holds the lock, these methods succeed. Otherwise they throw an exception.

3. Return the lock.

A program can re-use a lock object, omitting step 1.

Locks and Stores

When a process acquires a lock, it associates the lock with a specific persistence cluster. When a process releases a lock, it cancels the association, making the lock available to use with any persistence cluster.

While a lock is associated with one persistence cluster, it is illegal to use it in a map operation on any other persistence cluster. Method calls that violate this restriction throw an exception.

Steal: Only to Circumvent a Blocked Lock

If a program process, A, holds a lock and does not return it in a timely fashion, the corresponding map or row remains inaccessible to other process that request that lock. To circumvent this blockage, another program process, B, can *steal* the lock.

When process A subsequently uses that lock in a map method call, the method throws an exception.

Direct Publishers and Subscribers

Direct publishers and subscribers use direct memory access to achieve the fastest data transfer and lowest latency.

A publishing application writes data directly into memory that is accessible to subscribing applications. Subscribing applications read data directly from memory written by the publishing application.

The implementation minimizes or eliminates sources of latency.

The following table summarizes the differences between regular and direct publishers and subscribers. Subsequent topics contain greater detail.

Aspect	TIBCO FTL Publishers and Subscribers	Direct Publishers and Subscribers
Messages	Applications exchange message objects.	Applications exchange data in buffers.
Structuring Data	Applications structure message objects using fields that contain typed data.	Applications structure data within buffers using an array of sizes.
Copying Data	The library copies message data as needed.	The library eliminates copying data wherever possible. The sending application populates a data buffer, and receiving applications have direct access to that same data buffer.
Memory Management	Applications can create and destroy publisher and subscriber objects.	Applications create direct publisher and subscriber objects, but cannot reclaim their memory. Application programs neither allocate data buffers, nor free them.

Aspect	TIBCO FTL Publishers and Subscribers	Direct Publishers and Subscribers
	The library and application programs can both create and destroy message objects.	
Subscribers and Threads	Subscribers are thread-safe.	Applications must not use a direct subscriber in more than one thread. Instead, applications can create a separate direct subscriber for each thread.
Delivery	The library distributes inbound messages through event queues.	Applications dispatch inbound data buffers directly to callback methods.
Content Matchers	Applications can use content matchers to select a sub-stream of messages.	Applications receive the entire data stream. Selectivity based on data content is not available.
API Language Support	The API supports multiple programming languages.	The API supports only the C language.
Protection	The implementation protects against many common types of programming errors.	The implementation protects against fewer types of errors. For example, programmers must be careful to not overrun the length of data buffers, because the library does not guard against this error.
Publishers	Many publishers can send through an endpoint.	A direct shared memory bus supports only one direct publisher object.

Aspect	TIBCO FTL Publishers and Subscribers	Direct Publishers and Subscribers
Transport	Choose from a variety of transport types.	Only a direct shared memory transport can implement a direct publisher or subscriber endpoint.
Persistence	Available.	The persistence feature does not support direct publishers and subscribers.

Use Cases for Direct Publishers and Subscribers

Direct publishers and subscribers are appropriate only in very specialized use cases in which a few nanoseconds of latency can make a critical difference.

Direct publishers and subscribers are less flexible than regular TIBCO FTL communications. Direct publishers omit several features in exchange for greater speed and lower latency:

- The implementation has fewer protections against incorrect use of the API calls. For example, it does not check arguments nor data types. The implementation does not protect against writing beyond buffer boundaries.
- Data is in buffers, rather than in messages with typed fields.
- Event queues are not available.
- Content matchers are not available.
- Persistence is not available.
- C is the only supported programming language.

Direct shared memory transports support only one direct publisher per bus. This restriction precludes the request/reply pattern, which requires two-way communication. Nonetheless, you could use a separate bus for replies.

Programming with Direct Publishers

Create a direct publisher object. Code a *reserve-fill-send* loop. Close the direct publisher and exit.

Number of Publisher Objects

A suite of application processes that communicate over a direct shared memory bus may contain *only one* direct publisher object at a time. It is the shared responsibility of the application developers and the administrators to ensure this condition.

One Reserved Buffer

A direct publisher can reserve at most one buffer at a time.

- If direct publisher has already reserved a buffer in one thread, any subsequent reserve calls in other threads block until the direct publisher has sent the reserved buffer.
- Do *not* call reserve twice within the same thread without an intervening send call.

The Reserve-Fill-Send Loop

Avoid delays in the reserve-fill-send loop: as soon as the reserve call returns a buffer, fill it with data, and send it.

Procedure

1. Create a direct publisher object.

The object will exist in memory until the process terminates.

Programs may use a direct publisher in multiple threads. However, contention to reserve a buffer can decrease performance and increase latency.

The reserve-fill-send loop begins here.

2. Reserve a buffer.

Supply the total size of the data, and the number of data elements.

The reserve call returns a pointer to the buffer.

If the program specifies more than one data element, the reserve call also yield a size array.

i Note: One reserve call can reserve a maximum block of 64 kilobytes. The data buffer *and* the size array must fit together within that maximum block.

3. Fill the buffer with data.

If another thread has already reserved a buffer with this direct publisher, this reserve call blocks until that other thread sends its buffer.

- **One Data Element:** Write the data into the buffer.
- **Multiple Data Elements:** Use a loop to write each data element into the buffer, and its corresponding size, in bytes, into the size array.

4. Send the reserved buffer.

The send reserved call makes the buffer available to direct subscribers.

After this call, the direct publisher is ready to reserve another buffer.

5. Loop to reserve the next buffer.

Clean up before the application process exits.

6. Close the direct publisher object.

Closing a direct publisher causes any blocked reserve calls to return. Closing also invalidates the direct publisher, which disallows any subsequent method calls.

However, closing a direct publisher does *not* free its memory.

Programming with Direct Subscribers

Create a direct subscriber object. Code a callback method. Code a *dispatch* loop. Close the direct subscriber.

Procedure

1. Code a direct callback method.

Within the callback, loop to unpack the data items.

Avoid introducing latency within the callback.

Programs can use the same callback with more than one direct subscriber object, and in more than one thread.

2. Create a direct subscriber object.

The object will exist in memory until the process terminates.

Programs may use a direct subscriber in multiple threads. However, contention to dispatch a direct subscriber object can decrease performance and increase latency.

3. Code a dispatch loop for the direct subscriber.

A dispatch loop repeatedly calls the dispatch method.

The dispatch method checks whether inbound data is available for a direct subscriber object.

- **Data** - If a data buffer is available, dispatch invokes the callback method, passing the buffer and a closure object as arguments to the callback. When the callback returns, the direct subscriber automatically acknowledges that it has received the buffer. Then the dispatch call returns.
- **No Data** - If a data buffer is not available, dispatch waits until data becomes available, or until the timeout expires.

You can supply a closure object that is specific to the direct subscriber object, or you can supply a global closure object common to more than one direct subscriber.

Clean up before the application process exits.

4. Close the direct subscriber object.

Closing a direct subscriber causes any executing dispatch calls to return immediately. Closing also invalidates the direct subscriber, which disallows any subsequent method calls.

However, closing a direct subscriber does *not* free its memory.

Multithreading with Direct Publishers and Subscribers

On hardware with multiple processor cores, multithreading can boost performance of applications that communicate using direct publishers and direct subscribers. You can use multithreading to implement a variety of communicating sub-applications within a single process, and to decrease context-switching latency as they communicate.

For best results, match the size of a multithreaded application program to the host computer hardware. Allot one processor core for each direct publisher and its reserve-fill-send loop, and one processor core for each direct subscriber object and its dispatch loop. Too few cores can increase latency.

i Note: A suite of application processes that communicate over a direct shared memory bus may contain *only one* direct publisher object at a time. It is the shared responsibility of the application developers and the administrators to ensure this condition.

Multiple Direct Subscribers

A program can create more than one direct subscriber on an endpoint. Each direct subscriber object receives every buffer published on the bus.

- You can use multiple direct subscribers to process the same inbound data stream with different callback semantics.
- You *cannot* use multiple direct subscribers to increase throughput by dividing an inbound data stream.

✓ Tip: In multithreaded application programs, use a separate direct subscriber object and a separate dispatch loop in each thread.

For best results, if an application program uses more than one direct subscriber object, create them all before starting the any of their dispatch loops.

✓ Tip: Programs may use a direct subscriber in multiple threads. However, contention to dispatch a direct subscriber object can decrease performance and increase latency.

Create only a finite number of direct subscriber objects. Re-use them as needed. Close them only when cleaning up to prepare for the process to exit.

Coordination Forms

Coordination forms help developers and administrators to agree upon application details and to document those details.

From the FTL [Product Guides](#) list, you can download the PDF forms listed below, rename the copies, and complete them online. Alternatively, you can print the downloaded forms and complete them on paper.

- Application Coordination Form
- Durable Coordination Form
- Endpoint Coordination Form
- Format Coordination Form

TIBCO Documentation and Support Services

For information about this product, you can read the documentation, contact TIBCO Support, and join [TIBCO Community](#).

How to Access TIBCO Documentation

Documentation for TIBCO products is available on the [TIBCO Product Documentation](#) website, mainly in HTML and PDF formats.

The [TIBCO Product Documentation](#) website is updated frequently and is more current than any other documentation included with the product.

Product-Specific Documentation

Documentation for TIBCO FTL® is available on the [TIBCO FTL® Product Documentation](#) page.

TIBCO FTL® Documentation Set

The following documents can be found on [TIBCO FTL](#) Product Documentation as [Web Help](#) or PDFs.

- *Installation*: Read this guide before installing or uninstalling the product.
- *Concepts*: Review this guide for an introduction to FTL software fundamentals.
- *Quick Start*: Use this guide to quickly start FTL and send and receive a message.
- *Getting Started*: Use the guide to set up, start, and run various TIBCO FTL sample programs that demonstrate typical messaging functionality.
- *FTL Tutorials*: Use this guide for a step-by-step approach to build TIBCO FTL applications. You use options and properties, exception handling, programming models, and the user interface for configuration and monitoring.
- *Administration*: Administrators read this manual to learn how to use the FTL server, its interfaces, and its services, and how to define a realm. Developers can also benefit from understanding FTL software from an administrator's perspective.

- *Development:* Application developers and architects read this manual to understand concepts relevant in any supported programming language.
- *Monitoring:* Administrators read this manual to learn about monitoring and metrics. Developers read this manual to learn how an application can subscribe to the stream of monitoring data.
Important: As of FTL 6.10.0, [TIBCO® Messaging Monitor for TIBCO FTL®](#) must be used. This replaces the FTL monitoring (monitoring directory) including Grafana and tibmongateway which are removed. Monitoring metric types are also removed as of FTL 6.10.0.
- *Shifting to FTL:* This manual contrasts TIBCO FTL with TIBCO Enterprise Message Service™, and offers suggestions to smooth your transition to TIBCO FTL. Application developers, architects, and administrators familiar with TIBCO Enterprise Message Service read this manual.
- *Security:* This manual contains security-related tasks for administrators and security tips for application developers.
- *API Documentation:* Application developers use this documentation to learn the details of the FTL API in specific programming languages. This is available as [Web Help](#) only.
- *TIBCO FTL Glossary:* The glossary contains brief definitions of key terms used in all other parts of the documentation set.
- *Release Notes:* Read the release notes for a list of new and changed features. This document also contains lists of known issues and closed issues for this release.

Additional information resources can be found, after file extraction, in the samples directory. These include a Getting Started guide, Tutorials, readme.txt files, and sample applications.

Updated Resources on TIBCO Community

Supplemental resources are now distributed at the [TIBCO FTL Community Wiki](#) in the Reference Info tab. You can always find the latest versions of these resources in that location.

Those resources include *TIBCO FTL Getting Started Guide* and *TIBCO FTL Tutorials*. They also include sample FTL server configuration files and sample realm definition files.

TIBCO eFTL™ Documentation Set

TIBCO eFTL software is documented separately. Administrators use the FTL server GUI to configure and monitor the eFTL service. For information about these GUI pages, see the documentation set for TIBCO eFTL software.

How to Contact TIBCO Support

Get an overview of [TIBCO Support](#). You can contact TIBCO Support in the following ways:

- For accessing the Support Knowledge Base and getting personalized content about products you are interested in, visit the [TIBCO Support](#) website.
- For creating a Support case, you must have a valid maintenance or support contract with TIBCO. You also need a user name and password to log in to [TIBCO Support](#) website. If you do not have a user name, you can request one by clicking **Register** on the website.

How to Join TIBCO Community

TIBCO Community is the official channel for TIBCO customers, partners, and employee subject matter experts to share and access their collective experience. TIBCO Community offers access to Q&A forums, product wikis, and best practices. It also offers access to extensions, adapters, solution accelerators, and tools that extend and enable customers to gain full value from TIBCO products. In addition, users can submit and vote on feature requests from within the [TIBCO Ideas Portal](#). For a free registration, go to [TIBCO Community](#).

Legal and Third-Party Notices

SOME TIBCO SOFTWARE EMBEDS OR BUNDLES OTHER TIBCO SOFTWARE. USE OF SUCH EMBEDDED OR BUNDLED TIBCO SOFTWARE IS SOLELY TO ENABLE THE FUNCTIONALITY (OR PROVIDE LIMITED ADD-ON FUNCTIONALITY) OF THE LICENSED TIBCO SOFTWARE. THE EMBEDDED OR BUNDLED SOFTWARE IS NOT LICENSED TO BE USED OR ACCESSED BY ANY OTHER TIBCO SOFTWARE OR FOR ANY OTHER PURPOSE.

USE OF TIBCO SOFTWARE AND THIS DOCUMENT IS SUBJECT TO THE TERMS AND CONDITIONS OF A LICENSE AGREEMENT FOUND IN EITHER A SEPARATELY EXECUTED SOFTWARE LICENSE AGREEMENT, OR, IF THERE IS NO SUCH SEPARATE AGREEMENT, THE CLICKWRAP END USER LICENSE AGREEMENT WHICH IS DISPLAYED DURING DOWNLOAD OR INSTALLATION OF THE SOFTWARE (AND WHICH IS DUPLICATED IN THE LICENSE FILE) OR IF THERE IS NO SUCH SOFTWARE LICENSE AGREEMENT OR CLICKWRAP END USER LICENSE AGREEMENT, THE LICENSE(S) LOCATED IN THE “LICENSE” FILE(S) OF THE SOFTWARE. USE OF THIS DOCUMENT IS SUBJECT TO THOSE TERMS AND CONDITIONS, AND YOUR USE HEREOF SHALL CONSTITUTE ACCEPTANCE OF AND AN AGREEMENT TO BE BOUND BY THE SAME.

This document is subject to U.S. and international copyright laws and treaties. No part of this document may be reproduced in any form without the written authorization of Cloud Software Group, Inc.

TIBCO, the TIBCO logo, the TIBCO O logo, FTL, eFTL, and Rendezvous are either registered trademarks or trademarks of Cloud Software Group, Inc. in the United States and/or other countries.

Java and all Java based trademarks and logos are trademarks or registered trademarks of Oracle Corporation and/or its affiliates.

This document includes fonts that are licensed under the SIL Open Font License, Version 1.1, which is available at: <https://scripts.sil.org/OFL>

Copyright (c) Paul D. Hunt, with Reserved Font Name Source Sans Pro and Source Code Pro.

All other product and company names and marks mentioned in this document are the property of their respective owners and are mentioned for identification purposes only.

This software may be available on multiple operating systems. However, not all operating system platforms for a specific software version are released at the same time. See the readme file for the availability of this software version on a specific operating system platform.

THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT.

THIS DOCUMENT COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN; THESE CHANGES WILL BE INCORPORATED IN NEW EDITIONS OF THIS DOCUMENT. CLOUD SOFTWARE GROUP, INC. MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT(S) AND/OR THE PROGRAM(S) DESCRIBED IN THIS DOCUMENT AT ANY TIME.

THE CONTENTS OF THIS DOCUMENT MAY BE MODIFIED AND/OR QUALIFIED, DIRECTLY OR INDIRECTLY, BY OTHER DOCUMENTATION WHICH ACCOMPANIES THIS SOFTWARE, INCLUDING BUT NOT LIMITED TO ANY RELEASE NOTES AND "READ ME" FILES.

This and other products of Cloud Software Group, Inc. may be covered by registered patents. Please refer to TIBCO's Virtual Patent Marking document (<https://www.tibco.com/patents>) for details.

Copyright © 2009-2023. Cloud Software Group, Inc. All Rights Reserved.