



# TIBCO ActiveSpaces® - Enterprise Edition

## Security Guidelines

Version 5.0.0 | February 2025

# Contents

---

<b>Contents</b> .....	<b>2</b>
<b>About This Product</b> .....	<b>3</b>
<b>Product Overview and Security Features</b> .....	<b>4</b>
<b>Product Connectivity</b> .....	<b>5</b>
<b>Setting up a Secure TIBCO FTL Server</b> .....	<b>6</b>
<b>Setting up a Secure Data Grid</b> .....	<b>7</b>
<b>Securing Client-to-Proxy Communication</b> .....	<b>9</b>
<b>Transport Encryption on a Data Grid</b> .....	<b>11</b>
<b>Authentication and Authorization</b> .....	<b>12</b>
<b>Permissions</b> .....	<b>13</b>
<b>Commands to Start a Secure Data Grid</b> .....	<b>14</b>
Initial Setup to Start a Secure Data Grid .....	16
Create Directories Needed to Run the Processes .....	18
Setting Up and Starting TIBCO FTL Servers .....	19
Starting ActiveSpaces Processes .....	21
<b>TIBCO Documentation and Support Services</b> .....	<b>24</b>
<b>Legal and Third-Party Notices</b> .....	<b>25</b>

# About This Product

---

The TIBCO ActiveSpaces® - Enterprise Edition software is a distributed in-memory data grid product. Some features of ActiveSpaces® - Enterprise Edition include the use of familiar database concepts, high I/O capacity, and network scalability. It is ideal for all application development projects, and for deploying and managing applications in the production environment of an enterprise.

TIBCO FTL® is an embedded and bundled component of ActiveSpaces® - Enterprise Edition.

# Product Overview and Security Features

---

This document describes guidelines to ensure security within the components of ActiveSpaces and the communication between them. It also provides additional security-related guidance and recommendations for other aspects of internal and external communication. In particular, this document provides details of product connectivity and configuration of security options.

ActiveSpaces software includes the following security features that are layered above the TIBCO FTL security features:

- Every data grid can be configured to encrypt connections
- Every process has authentication and trust file options

ActiveSpaces software uses TIBCO FTL for the following security features:

- Secure transports for communication among data grid processes and between applications and the data grid processes
- TLS to secure TCP transports
- HTTPS to secure connections to the TIBCO FTL server
- Authentication and authorization service

For more information about TIBCO FTL security features, see *TIBCO FTL<sup>®</sup> Security*.

# Product Connectivity

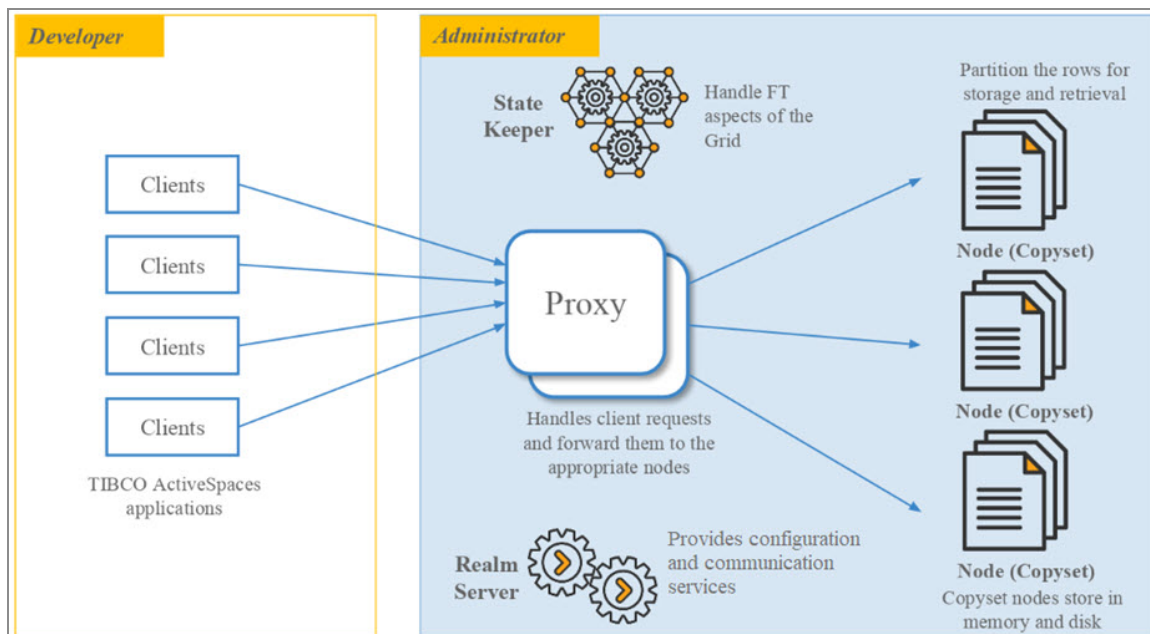
ActiveSpaces product connectivity can be broken down into the following categories:

- ActiveSpaces client application to data grid process connectivity
- ActiveSpaces data grid process to data grid process connectivity

Both client applications and data grid processes communicate with the realm service in the TIBCO FTL server. After the initial realm communication, client applications communicate with proxy processes. The proxy processes forward requests internally to the data grid and then forward replies to the external client application. Internal grid communication happens between proxy, state keeper, and node processes at different points in time.

As an administrator, with the help of the security guidelines, you can secure both internal grid communication and external client-to-proxy communication. You can also help application developers configure a client application and connect to a secure data grid. The following high-level diagram shows the connectivity information.

Figure 1: Connectivity information



# Setting up a Secure TIBCO FTL Server

---

In secure environments, except those using FTL generated certificates, the Admin Service must be used and not standalone Admin Daemons.

For a production deployment, perform the following steps:

## Procedure

1. Set up the secure TIBCO FTL server. For details about securing TIBCO FTL servers, see "Securing FTL Servers" in *TIBCO FTL® Security*.
2. Set up the YAML configuration file, and configure the FTL servers to use TLS security in their configuration files.

```
globals:  
    tls.secure: <keystore_password>
```

3. Run `tibftlserver --init-security` with a `keystore_password` file to generate the `.p12` keystore file and `ftl-trust.pem` file.
4. Distribute the `ftl-trust.pem` file for use in all other applications.
5. Start the TIBCO FTL server.

## What to do next

To start a secure data grid, follow the steps in [Setting up a Secure Data Grid](#).

## Example Scripts

Sample scripts to secure a data grid are available at `TIBCO_HOME/as/<version>/samples/scripts`. You can also start a secure TIBCO FTL Server and a secure data grid by using `as-start` with the `-s` command-line option.



**Note:** The installation environment of ActiveSpaces is referenced as `TIBCO_HOME`. For example, on Microsoft Windows, `TIBCO_HOME` might be `C:\tibco`.

# Setting up a Secure Data Grid

---

## Before you begin

Ensure that a secure TIBCO FTL server is running.

## Procedure

1. To configure a secure data grid in one command, create a `.tibdg` configuration file that can be passed to the `tibdg` administration tool.
2. In the `.tibdg` file, when defining the data grid, set `encrypted_connections=all` as shown in the following code snippet:

```
grid create copyset_size=2 encrypted_connections=all grid1
```

This property forces all internal grid communication and all client-to-proxy communication to use TIBCO FTL secure TCP transports.

3. Configure the firewall to open ports for client-to-proxy communication.

For each proxy that is listening for client connections, configure `proxy_client_listen_port` to the preferred port to which the proxy must bind and listen. Example:

```
proxy create proxy_client_listen_port=7771 p_01
```

You can use other optional configuration options in the proxy that help configure the specific host interface. For example, you can use the `proxy_client_listen_subnet_mask` configuration option to configure network interfaces. You can specify this option at the data grid and proxy level to control the network interface to which the proxy binds when listening for connections from clients. For details, see "Configure Network Interfaces" in *TIBCO ActiveSpaces® - Enterprise Edition Administration*.

4. Run the `tibdg` tool by providing the following command-line options:
  - A completed `.tibdg` configuration file
  - A trust file

The following command is an example of running the `tibdg` tool:

```
>tibdg -r https://host1:8085 -s  
/home/youruser/as/init/grid1/grid1.tibdg --trust-file  
/home/youruser/as/grid1/ftl-trust.pem
```



**Warning:** If you do not provide the trust file as a command-line option, the command fails when communicating with a secure TIBCO FTL server.

### What to do next

After the data grid has been successfully configured in the TIBCO FTL server, you can start the `tibdgkeeper`, `tibdgproxy`, and `tibdgnode` processes. Ensure that you provide the appropriate trust file on the command-line as follows with the `--trust-file` option.

```
tibdgkeeper -r  
"https://host1:8085|https://host2:8185|https://host3:8285" --trust-file  
/home/youruser/as/grid1/ftl-trust.pem -g grid1 -n k_1
```



# Securing Client-to-Proxy Communication

---

After creating and starting a secure data grid, set the properties of the ActiveSpaces client application to connect to a secure data grid and start secure communications. The properties must be passed to the `DataGrid.connect()` API function. The HTTPS protocol must be used in the URL parameter to connect to a secure realm service. For more information about how these properties work, see the `Operations` code sample at `TIBCO_HOME\as\<version>\samples\src\java\Operations`. The following procedure also elaborates on these properties.

**i Note:** The installation environment of ActiveSpaces is referenced as `TIBCO_HOME`. For example, on Microsoft Windows, `TIBCO_HOME` might be `C:\tibco`.

## Before you begin

Ensure that you have the following information from your administrator before you begin the procedure:

- The TIBCO FTL server trust file that was generated when setting up the secure TIBCO FTL server.
- The correct username and password for the ActiveSpaces client application (if the administrator has set up authentication in the TIBCO FTL server).

## Procedure

1. In the URL parameter passed to the `DataGrid.connect()` function call, use `https://` for each realm URL in the list.

When specifying a list of three TIBCO FTL servers, the URL string parameter must be as listed in this example:

```
https://ftlsvr1:8085|https://ftlsvr2:8185|https://ftlsvr3:8285.
```

2. To connect to a secure data grid, set a specific trust type in the properties passed to the `DataGrid.connect()` function call.
  - a. Place the PEM trust file in the file system so that it can be accessed securely by the ActiveSpaces client application.

- b. In the ActiveSpaces client application, set the connection TRUST\_TYPE property to the enum representing USE\_SPECIFIED\_TRUST\_FILE.
- c. In the ActiveSpaces client application, set the TRUST\_FILE property to the file system path of the trust file received by the administrator.

The following Java code snippet is an example:

```
Properties props = new Properties();
props.setProperty(Connection.TIBDG_CONNECTION_PROPERTY_STRING_
TRUST_TYPE, Connection.TIBDG_CONNECTION_HTTPS_CONNECTION_USE_
SPECIFIED_TRUST_FILE);
props.setProperty(Connection.TIBDG_CONNECTION_PROPERTY_STRING_
TRUST_FILE, trustFilePath);
DataGrid.connect(url, gridName, props);
```

3. If the administrator has set up authentication in the TIBCO FTL server and provided a username and password, then in the properties object passed to the DataGrid.connect() function call, include the USERNAME and USERPASSWORD properties as shown in the following examples:

```
props.setProperty(Connection.TIBDG_CONNECTION_PROPERTY_STRING_
USERNAME, username);
props.setProperty(Connection.TIBDG_CONNECTION_PROPERTY_STRING_
USERPASSWORD, password);
DataGrid.connect(url, gridName, props);
```

# Transport Encryption on a Data Grid

---

You can encrypt any network communication between the processes of your data grid to protect that communication from packet sniffing. For more information about encrypting a data grid, see "Enabling Transport Encryption on a Data Grid" in *TIBCO ActiveSpaces® - Enterprise Edition Administration*.

Use transport encryption with authentication and authorization.

# Authentication and Authorization

---

Authentication and authorization uses usernames and passwords to authenticate the data grid users and prevent unwanted access.

When authentication and authorization is enabled, each ActiveSpaces process uses credentials from the password file to authenticate itself to a secure realm service. For more information, see "Authentication and Authorization" in *TIBCO ActiveSpaces® - Enterprise Edition Administration*.

TIBCO recommends configuring a secure data grid with transport encryption, authentication, and authorization.

# Permissions

---

In ActiveSpaces, you can set permissions on tables to control who has access to the data in the tables. On a specific table, you can grant read or write permissions to users and roles.

For more information about enabling permission checking and granting and revoking table-level permissions in the data grid, see "Enabling Permission Checking when Creating or Modifying a Data Grid" in *TIBCO ActiveSpaces® - Enterprise Edition Administration*.

# Commands to Start a Secure Data Grid

---

**Goal:** Create a secure data grid named `grid1` running across four computers and access it from a client application running on a separate computer.

**Hosts:** `host1`, `host2`, `host3`, `host4`, `host5` (for client application)

## Procedure

1. Perform the steps listed in [Initial Setup to Start a Secure Data Grid](#).
2. Perform the steps listed in [Create Directories Needed to Run the Processes](#).
3. Perform the steps listed in [Setting Up and Starting TIBCO FTL Servers](#).
4. In a browser, browse to `https://host1:8085` or `https://host2:8185` or `https://host3:8285`.

An empty realm server with a working GUI is displayed.

5. Initialize the data grid from `host1`.

```
>tibdg -r https://host1:8085 -s
/home/youruser/as/init/grid1/grid1.tibdg --trust-file
/home/youruser/as/grid1/ftl-trust.pem
```



**Warning:** If you do not provide the trust file as a command-line option, the command fails when communicating with a secure TIBCO FTL server.

6. Check the status after configuring the data grid (no processes are running as expected).

```
>tibdg -r https://host1:8085 --trust-file
/home/youruser/as/grid1/ftl-trust.pem -g grid1 status
Grid grid1:
Grid is not functioning.
FTL healthy. Up for 824 seconds.
Admin server is not running
```

## PROCESSES

EST	TYPE	NAME	HOST	PID	REV	TXNS	REQS	COPYSET	ROLE
	SIZE	FS USED	FS CAP	DATA DIR		MAX	WRITE		
	node	cs_01.n_1	NOT	RUNNING					
	node	cs_01.n_2	NOT	RUNNING					
	node	cs_02.n_1	NOT	RUNNING					
	node	cs_02.n_2	NOT	RUNNING					

TYPE	NAME	HOST	PID	REV	ROLE	STATE	DIR
keeper	k_1	NOT	RUNNING				
keeper	k_2	NOT	RUNNING				
keeper	k_3	NOT	RUNNING				

QRY	TYPE	NAME	HOST	PID	REV	CLIENTS	REQ	TXN	ITER	STMT
	LSNR	MODE								
	proxy	p_01	NOT	RUNNING						
	proxy	p_02	NOT	RUNNING						
	proxy	p_03	NOT	RUNNING						
	proxy	p_04	NOT	RUNNING						

7. Perform the steps listed in [Starting ActiveSpaces Processes](#).
8. Start a `tibdgradmind` process to accept administration commands.

```
# On host1
>tibdgradmind -r "https://host1:8085" --trust-file
/home/youruser/as/grid1/ftl-trust.pem -l localhost:7171
```

9. Start a sample client to run operations.

```
>/opt/tibco/as/4.2/samples/bin/operations -r
"https://host1:8085|https://host2:8185|https://host3:8285" --trust-
file /home/youruser/as/grid1/ftl-trust.pem -g grid1

AS Product Version: 4.2.0 V5
```

```

Connected to table: t1

Operations commands:
    Enter 'p' to put a row into the table
    Enter 'g' to get a row from the table
    Enter 'd' to delete a row from the table
    Enter 'pm' to put multiple rows into the table
    Enter 'gm' to get multiple rows from the table
    Enter 'dm' to delete multiple rows from the table
    Enter 'i' to iterate the rows in a table
    Enter 'l' to listen to changes to the table
    Enter 's' to create an SQL SELECT or DML statement and
execute it
    Enter 'u' to execute an SQL DDL update
    Enter 'md' to display metadata about the grid and tables
    Enter 'h' to display this help menu
    Enter 'q' to quit

Main: [p/g/d/pm/gm/dm/i/l/s/u/md/h/q]: p
Put: Enter the key (long): 1
Put: Enter the value (string): 1
Put Success

Main: [p/g/d/pm/gm/dm/i/l/s/u/md/h/q]: g
Get: Enter the key (long): 1
result: {long:key=1, string:value="1"}

```

## Initial Setup to Start a Secure Data Grid

### Procedure

1. Set up PATH to point to TIBCO FTL and ActiveSpaces.

```

export TIBFTL_ROOT=/opt/tibco/ftl/<version>
export TIBDG_ROOT=/opt/tibco/as/<version>
export PATH=$TIBFTL_ROOT/bin:$TIBDG_ROOT/bin:$PATH

```

2. On a computer with TIBCO FTL and ActiveSpaces, create the directories to hold the initial setup and configuration files.



```
>cd /home/youruser
>mkdir -p as
>cd as
>mkdir -p init
>cd init
>mkdir grid1
>cd grid1
>mkdir ftl_security
```

### 3. Initialize the files for a secure ftlserver.

```
>cd ftl_security
>vi keystore_password.txt (enter a single-line password and save
file)
>tibftlserver --init-security
file:/home/youruser/as/init/grid1/ftl_security/keystore_
password.txt
Initializing TIBCO FTL server security.
Generating keystore 'ftl-tport.p12' and trust file 'ftl-trust.pem'.
```

### 4. Create the TIBCO FTL server YAML configuration file.

```
cd..
vi ftl.yaml (paste the config below)
globals:
  core.servers:
    ftl1: host1:8085
    ftl2: host2:8185
    ftl3: host3:8285
  tls.secure: file:/home/youruser/as/ftlservers/keystore_
password.txt
servers:
  ftl1:
    - realm:
      ftl: host1:8088
      data: /home/youruser/as/ftlservers/ftl1/realm_data
      logfile: /home/youruser/as/logs/ftlservers/ftl1-rs-log.txt
  ftl2:
    - realm:
      ftl: host2:8188
      data: /home/youruser/as/ftlservers/ftl2/realm_data
      logfile: /home/youruser/as/logs/ftlservers/ftl2-rs-log.txt
```

```
ftl3:
- realm:
  ftl: host3:8288
  data: /home/youruser/as/ftlservers/ftl3/realm_data
  logfile: /home/youruser/as/logs/ftlservers/ftl3-rs-log.txt
services:
  realm: {}
```

5. Create the `grid1.tibdg` file. This configuration file is used to configure the data grid later after the TIBCO FTL server is running.

```
vi grid1.tibdg (paste the config below)
grid create copyset_size=2 encrypted_connections=all grid1
copyset create cs_01
copyset create cs_02
node create --copyset cs_01 --dir /home/youruser/as/grid1/cs_01.n_
1_data cs_01.n_1
node create --copyset cs_01 --dir /home/youruser/as/grid1/cs_01.n_
2_data cs_01.n_2
node create --copyset cs_02 --dir /home/youruser/as/grid1/cs_02.n_
1_data cs_02.n_1
node create --copyset cs_02 --dir /home/youruser/as/grid1/cs_02.n_
2_data cs_02.n_2
keeper create --dir /home/youruser/as/grid1/k_1_data k_1
keeper create --dir /home/youruser/as/grid1/k_2_data k_2
keeper create --dir /home/youruser/as/grid1/k_3_data k_3
proxy create proxy_client_listen_port=7771 p_01
proxy create proxy_client_listen_port=7772 p_02
proxy create proxy_client_listen_port=7773 p_03
proxy create proxy_client_listen_port=7774 p_04
table create t1 key long
column create t1 value string
```

## Create Directories Needed to Run the Processes

### Procedure

1. Create the directories needed to run the processes on host1:

```
>cd /home/youruser/as
```

```
>mkdir -p logs/ftlservers
>mkdir -p logs/grid1
>mkdir -p ftlservers/ftl1/realm_data
>mkdir -p grid1
>mkdir -p grid1/k1_data
>mkdir -p grid1/cs_01.n_1_data
```

2. Create the directories needed to run the processes on host2:

```
>cd /home/youruser/as
>mkdir -p logs/ftlservers
>mkdir -p logs/grid1
>mkdir -p ftlservers/ftl2/realm_data
>mkdir -p grid1
>mkdir -p grid1/k2_data
>mkdir -p grid1/cs_01.n_2_data
```

3. Create the directories needed to run the processes on host3:

```
>cd /home/youruser/as
>mkdir -p logs/ftlservers
>mkdir -p logs/grid1
>mkdir -p ftlservers/ftl3/realm_data
>mkdir -p grid1
>mkdir -p grid1/k3_data
>mkdir -p grid1/cs_02.n_1_data
```

4. Create the directories needed to run the processes on host4:

```
>cd /home/youruser/as
>mkdir -p logs/ftlserver
>mkdir -p logs/grid1
>mkdir -p grid1
>mkdir -p grid1/cs_02.n_2_data
```

## Setting Up and Starting TIBCO FTL Servers

This procedure lists how to set up the TIBCO FTL environment and then start the TIBCO FTL server.

### Procedure

1. Copy the TIBCO FTL files that are needed to start the TIBCO FTL servers.

```
# FTL yaml file to start the ftlserver
>scp /home/youruser/as/init/grid1/ftl.yaml
youruser@host1:/home/youruser/as/ftlservers/ftl.yaml
>scp /home/youruser/as/init/grid1/ftl.yaml
youruser@host2:/home/youruser/as/ftlservers/ftl.yaml
>scp /home/youruser/as/init/grid1/ftl.yaml
youruser@host3:/home/youruser/as/ftlservers/ftl.yaml
```

2. Copy the TIBCO FTL keystore password to start ftlserver securely

```
>scp /home/youruser/as/init/grid1/ftl_security/keystore_
password.txt youruser@host1:/home/youruser/as/ftlservers/keystore_
password.txt
>scp /home/youruser/as/init/grid1/ftl_security/keystore_
password.txt youruser@host2:/home/youruser/as/ftlservers/keystore_
password.txt
>scp /home/youruser/as/init/grid1/ftl_security/keystore_
password.txt youruser@host3:/home/youruser/as/ftlservers/keystore_
password.txt
```

3. Copy the TIBCO FTL keystore file to start ftlserver securely. For more information on keystore files, see "Secure FTL Servers" in *TIBCO FTL® Administration*.

```
>scp /home/youruser/as/init/grid1/ftl_security/ftl-tport.p12
youruser@host1:/home/youruser/as/ftlservers/ftl1/realms_data/ftl-
tport.p12
>scp /home/youruser/as/init/grid1/ftl_security/ftl-tport.p12
youruser@host2:/home/youruser/as/ftlservers/ftl2/realms_data/ftl-
tport.p12
>scp /home/youruser/as/init/grid1/ftl_security/ftl-tport.p12
youruser@host3:/home/youruser/as/ftlservers/ftl3/realms_data/ftl-
tport.p12
```

4. Copy the TIBCO FTL public trust file needed by TIBCO FTL servers (in realms\_data directory)

```
>scp /home/youruser/as/init/grid1/ftl_security/ftl-trust.pem
youruser@host1:/home/youruser/as/ftlservers/ftl1/realms_data/ftl-
trust.pem
```

```
>scp /home/youruser/as/init/grid1/ftl_security/ftl-trust.pem
youruser@host2:/home/youruser/as/ftlservers/ftl2/real_data/ftl-
trust.pem
>scp /home/youruser/as/init/grid1/ftl_security/ftl-trust.pem
youruser@host3:/home/youruser/as/ftlservers/ftl3/real_data/ftl-
trust.pem
```

5. Copy the TIBCO FTL public trust file needed by ActiveSpaces processes in grid1:

```
>scp /home/youruser/as/init/grid1/ftl_security/ftl-trust.pem
youruser@host1:/home/youruser/as/grid1/ftl-trust.pem
>scp /home/youruser/as/init/grid1/ftl_security/ftl-trust.pem
youruser@host2:/home/youruser/as/grid1/ftl-trust.pem
>scp /home/youruser/as/init/grid1/ftl_security/ftl-trust.pem
youruser@host3:/home/youruser/as/grid1/ftl-trust.pem
```

6. Start the TIBCO FTL servers

```
# On host1
>cd /home/youruser/as
>tibftlserver -c ftlservers/ftl.yaml -n ftl1
# On host2
>cd /home/youruser/as
>tibftlserver -c ftlservers/ftl.yaml -n ftl2
# On host3
>cd /home/youruser/as
>tibftlserver -c ftlservers/ftl.yaml -n ftl3
```

## Starting ActiveSpaces Processes

### Before you begin

Complete the steps 1 to 6 from the procedure listed in [Commands to Start a Secure Data Grid](#).

### Procedure

1. Start the data grid state keeper processes.

```
# On host1
>cd as
>tibdkeeper -r
"https://host1:8085|https://host2:8185|https://host3:8285" --trust-
file /home/youruser/as/grid1/ftl-trust.pem --logfile
/home/youruser/as/logs/grid1/k_1-log.txt -g grid1 -n k_1

# On host2
>tibdkeeper -r
"https://host1:8085|https://host2:8185|https://host3:8285" --trust-
file /home/youruser/as/grid1/ftl-trust.pem --logfile
/home/youruser/as/logs/grid1/k_2-log.txt -g grid1 -n k_2

# On host3
>tibdkeeper -r
"https://host1:8085|https://host2:8185|https://host3:8285" --trust-
file /home/youruser/as/grid1/ftl-trust.pem --logfile
/home/youruser/as/logs/grid1/k_3-log.txt -g grid1 -n k_3
```

## 2. Start the data grid proxy processes.

```
# On host1
>tibdproxy -r
"https://host1:8085|https://host2:8185|https://host3:8285" --trust-
file /home/youruser/as/grid1/ftl-trust.pem --logfile
/home/youruser/as/logs/grid1/p_01-log.txt -g grid1 -n p_01

# On host2
>tibdproxy -r
"https://host1:8085|https://host2:8185|https://host3:8285" --trust-
file /home/youruser/as/grid1/ftl-trust.pem --logfile
/home/youruser/as/logs/grid1/p_02-log.txt -g grid1 -n p_02

# On host3
>tibdproxy -r
"https://host1:8085|https://host2:8185|https://host3:8285" --trust-
file /home/youruser/as/grid1/ftl-trust.pem --logfile
/home/youruser/as/logs/grid1/p_03-log.txt -g grid1 -n p_03

# On host4
>tibdproxy -r
"https://host1:8085|https://host2:8185|https://host3:8285" --trust-
```

```
file /home/youruser/as/grid1/ftl-trust.pem --logfile  
/home/youruser/as/logs/grid1/p_04-log.txt -g grid1 -n p_04
```

### 3. Start the data grid node processes.

```
# On host1  
>tibdgnode -r  
"https://host1:8085|https://host2:8185|https://host3:8285" --trust-  
file /home/youruser/as/grid1/ftl-trust.pem --logfile  
/home/youruser/as/logs/grid1/cs_01.n_1-log.txt -g grid1 -n cs_01.n_  
1  
  
# On host2  
>tibdgnode -r  
"https://host1:8085|https://host2:8185|https://host3:8285" --trust-  
file /home/youruser/as/grid1/ftl-trust.pem --logfile  
/home/youruser/as/logs/grid1/cs_01.n_2-log.txt -g grid1 -n cs_01.n_  
2  
  
# On host3  
>tibdgnode -r  
"https://host1:8085|https://host2:8185|https://host3:8285" --trust-  
file /home/youruser/as/grid1/ftl-trust.pem --logfile  
/home/youruser/as/logs/grid1/cs_02.n_1-log.txt -g grid1 -n cs_02.n_  
1  
  
# On host4  
>tibdgnode -r  
"https://host1:8085|https://host2:8185|https://host3:8285" --trust-  
file /home/youruser/as/grid1/ftl-trust.pem --logfile  
/home/youruser/as/logs/grid1/cs_02.n_2-log.txt -g grid1 -n cs_02.n_  
2
```

# TIBCO Documentation and Support Services

---

## How to Access TIBCO Documentation

Documentation for TIBCO products is available on the [Product Documentation website](#), mainly in HTML and PDF formats.

The [Product Documentation website](#) is updated frequently and is more current than any other documentation included with the product.

## Product-Specific Documentation

The documentation for this product is available on the [TIBCO ActiveSpaces® - Enterprise Edition Documentation](#) page.

## How to Contact Support for TIBCO Products

You can contact the Support team in the following ways:

- To access the Support Knowledge Base and getting personalized content about products you are interested in, visit our [product Support website](#).
- To create a Support case, you must have a valid maintenance or support contract with a Cloud Software Group entity. You also need a username and password to log in to the [product Support website](#). If you do not have a username, 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 CLOUD SOFTWARE GROUP, INC. (“CLOUD SG”) SOFTWARE AND CLOUD SERVICES EMBED, BUNDLE, OR OTHERWISE INCLUDE OTHER SOFTWARE, INCLUDING OTHER CLOUD SG SOFTWARE (COLLECTIVELY, “INCLUDED SOFTWARE”). USE OF INCLUDED SOFTWARE IS SOLELY TO ENABLE THE FUNCTIONALITY (OR PROVIDE LIMITED ADD-ON FUNCTIONALITY) OF THE LICENSED CLOUD SG SOFTWARE AND/OR CLOUD SERVICES. THE INCLUDED SOFTWARE IS NOT LICENSED TO BE USED OR ACCESSED BY ANY OTHER CLOUD SG SOFTWARE AND/OR CLOUD SERVICES OR FOR ANY OTHER PURPOSE.

USE OF CLOUD SG SOFTWARE AND CLOUD SERVICES IS SUBJECT TO THE TERMS AND CONDITIONS OF AN AGREEMENT FOUND IN EITHER A SEPARATELY EXECUTED AGREEMENT, OR, IF THERE IS NO SUCH SEPARATE AGREEMENT, THE CLICKWRAP END USER AGREEMENT WHICH IS DISPLAYED WHEN ACCESSING, DOWNLOADING, OR INSTALLING THE SOFTWARE OR CLOUD SERVICES (AND WHICH IS DUPLICATED IN THE LICENSE FILE) OR IF THERE IS NO SUCH LICENSE AGREEMENT OR CLICKWRAP END USER AGREEMENT, THE LICENSE(S) LOCATED IN THE “LICENSE” FILE(S) OF THE SOFTWARE. USE OF THIS DOCUMENT IS SUBJECT TO THOSE SAME 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.

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. You acknowledge that all rights to these third party marks are the exclusive property of their respective owners. Please refer to Cloud SG’s Third Party Trademark Notices (<https://www.cloud.com/legal>) for more information.

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.

Cloud SG 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 a specific version of Cloud SG software 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 SG MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT(S), THE PROGRAM(S), AND/OR THE SERVICES DESCRIBED IN THIS DOCUMENT AT ANY TIME WITHOUT NOTICE.

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 "README" FILES.

This and other products of Cloud SG may be covered by registered patents. For details, please refer to the Virtual Patent Marking document located at <https://www.cloud.com/legal>.

Copyright © 2009-2025. Cloud Software Group, Inc. All Rights Reserved.