



TIBCO Enterprise Message Service™ Appliance Installation and Reference

*Software Release 3.1.0
December 2019*

Important Information

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.

ANY SOFTWARE ITEM IDENTIFIED AS THIRD PARTY LIBRARY IS AVAILABLE UNDER SEPARATE SOFTWARE LICENSE TERMS AND IS NOT PART OF A TIBCO PRODUCT. AS SUCH, THESE SOFTWARE ITEMS ARE NOT COVERED BY THE TERMS OF YOUR AGREEMENT WITH TIBCO, INCLUDING ANY TERMS CONCERNING SUPPORT, MAINTENANCE, WARRANTIES, AND INDEMNITIES. DOWNLOAD AND USE OF THESE ITEMS IS SOLELY AT YOUR OWN DISCRETION AND SUBJECT TO THE LICENSE TERMS APPLICABLE TO THEM. BY PROCEEDING TO DOWNLOAD, INSTALL OR USE ANY OF THESE ITEMS, YOU ACKNOWLEDGE THE FOREGOING DISTINCTIONS BETWEEN THESE ITEMS AND TIBCO PRODUCTS.

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 TIBCO Software Inc.

TIBCO, the TIBCO logo, and the TIBCO O logo are either registered trademarks or trademarks of TIBCO Software 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.

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. Please see the readme.txt 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. TIBCO SOFTWARE 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 TIBCO Software Inc. may be covered by registered patents. Please refer to TIBCO's Virtual Patent Marking document (<https://www.tibco.com/patents>) for details.

The following information is for FCC compliance: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-

frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

Modifying the equipment without Pluribus Networks' written authorization may result in the equipment no longer complying with FCC requirements for Class A digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Pluribus Networks equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

- Turn the television or radio antenna until the interference stops.
- Move the equipment to one side or the other of the television or radio.
- Move the equipment farther away from the television or radio.
- Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Pluribus Networks, Inc. could void the FCC approval and negate your authority to operate the product.

Copyright © 1997-2019 TIBCO Software Inc. All rights reserved.

TIBCO Software Inc. Confidential Information

Contents

Figures	8
TIBCO Documentation and Support Services	9
Introduction	11
Product Overview	11
Models	11
Appliance Components	12
Installation	14
Installation Requirements	14
Installing the Hardware	14
Unpacking the Equipment	14
Installing the Rack Kit	15
Grounding the Appliance	15
Preventing Electrostatic Discharge Damage	17
Connecting the Power Supply to an AC Power Source	18
Verifying LED Operation	18
Connecting Two TIBCO Enterprise Message Service Appliances	18
Connecting the Appliance Management Port to the Network	19
Connecting the Appliance to Your Network	19
Uplink Configuration	19
Connecting Directly to the Appliance for Initial Setup	19
Initializing the Software	20
Accessing the Appliance System	20
Configuring the Management Information	21
Restarting the Software Initialization Process	21
Configuring Appliance Users	21
Re-configuring Management Information	22
Configuring Host Information	22
Configuring EMS Server Information	22
Configuring Fault Tolerant Behavior	23
Configuring Disaster Recovery	24
Beginning Appliance Operations	25
Configuration	26
Predefined Appliance User Accounts	26
Working with the File Transfer Directory	26
TIBCO Enterprise Message Service Server States	28
Appliance Monitoring	29

TIBCO Enterprise Message Service™ Instances	29
Maximum Connections	30
Configuration	30
Single Appliance Configuration	30
Fault Tolerant Configuration	30
Configuration Changes on Fault-Tolerant Servers	31
Authorization and Fault-Tolerant Servers	31
Startup Process	32
Failover Process	32
Restoring After a Failover	33
Failover Events	33
Disaster Recovery Configuration	34
Disaster Recovery Process	35
Enabling Disaster Recovery	36
Initial Setup	36
Verify that the EMS Server Instance on Each Appliance is Operational	36
Establish Communications Between the Quad Appliances	36
Activate Disaster Recovery Support	37
Rejoining the Quad	37
DR Members	37
DR Leader	37
Recovering to a Backup Site	37
Restoring the Production Site	38
Encrypted Data Store (EDS) Configuration	38
Configuring the Encrypted Data Store on EMS Appliance	39
Disaster Recovery	39
Commands	40
CLI Overview	40
Using the CLI to Make Configuration Changes	40
Command Overview	41
General Commands	44
date	44
diagnostics-enable	44
eds-key-refresh	45
ems-gateway	45
exit	45
export	45
export-support-logs	47
forcestart	47

halt	47
help	47
import	47
info	48
initialization-progress	48
log-show	48
log-test	48
quit	49
reboot	49
restore-primary-active	49
services	49
setup-enable	50
setup-show	50
show	50
start	51
stop	51
upgrade-software	51
version-show	52
Disaster Recovery Commands	52
dr-activate	52
dr-recover	53
dr-restore	53
key-accept	54
key-join	54
key-reset	54
Configuration Setup Commands	54
config-apply	54
config-pending	55
config-revert-pending	55
config-revert-unsaved	55
config-review	55
config-save	55
dr-config	55
eds-config	55
ems-config	57
ft-config	57
health-check-config	57
hostinfo-config	58
initial-config	58

mgmt-config	58
set-timezone	58
syslog-config	58
Instance Management Commands	59
call-tibemsadmin	59
forcestart-instance	59
start-instance	59
stop-instance	59
switch-active	59
Diagnostics and Troubleshooting Commands	60
disk-check	60
dr-check	60
log-audit	60
log-remove	60
log-rotate	61
log-truncate	61
network-check	61
peer-login	62
port-disable	62
port-enable	62
port-show	63
pstack-instance	63
remove-certs	63
remove-cores	63
remove-snapshots	64
remove-transfers	64
reset-all	64
session-timeout	64
uplink-config	64
zone-admin	66

Figures

Fault Tolerant Configuration 11

TIBCO Enterprise Message Service Appliance Components 13

TIBCO Documentation and Support Services

TIBCO is proud to announce the latest release of TIBCO Enterprise Message Service™ Appliance software. This release is the latest in a long history of TIBCO products that leverage the power of the Information Bus® technology to enable truly event-driven IT environments. To find out more about how TIBCO Enterprise Message Service Appliance software and other TIBCO products are powered by TIB® technology, visit us at www.tibco.com.

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. To access the latest documentation, visit <https://docs.tibco.com>.

TIBCO Enterprise Message Service Appliance Documentation

The following documents for this product can be found on the TIBCO Documentation site:

- *TIBCO Enterprise Message Service Appliance Installation and Reference*
- *TIBCO Enterprise Message Service Appliance Release Notes*
- *Rack Mounting Your TIBCO Chassis With Included Rail Kit*

TIBCO Enterprise Message Service Documentation

The following documents form the TIBCO Enterprise Message Service documentation set:

- *TIBCO Enterprise Message Service User's Guide*
- *TIBCO Enterprise Message Service Central Administration*
- *TIBCO Enterprise Message Service Installation*
- *TIBCO Enterprise Message Service C and COBOL Reference*
- *TIBCO Enterprise Message Service Java and .NET API Reference*
- *TIBCO Enterprise Message Service Release Notes*

Other TIBCO Product Documentation

You may find it useful to read the documentation for the following TIBCO products:

- TIBCO EMS® Client for z/OS (CICS)
- TIBCO EMS® Client for z/OS (MVS)
- TIBCO EMS® Client for IBM i

Third-Party Documentation

- Java™ Message Service specification, available through <http://www.oracle.com/technetwork/java/jms/index.html>.
- *Java™ Message Service* by Richard Monson-Haefel and David A. Chappell, O'Reilly and Associates, Sebastopol, California, 2001.

How to Contact TIBCO Support

You can contact TIBCO Support in the following ways:

- For an overview of TIBCO Support, visit <http://www.tibco.com/services/support>.
- For accessing the Support Knowledge Base and getting personalized content about products you are interested in, visit the TIBCO Support portal at <https://support.tibco.com>.
- 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 <https://support.tibco.com>. 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 <https://community.tibco.com>.

Introduction

This chapter describes the TIBCO Enterprise Message Service Appliance and its major features.

Product Overview

The TIBCO Enterprise Message Service Appliance is a state-of-the-art hardware platform that offers the full functionality of a TIBCO Enterprise Message Service server.

The appliance offers:

Full EMS Server Compatibility

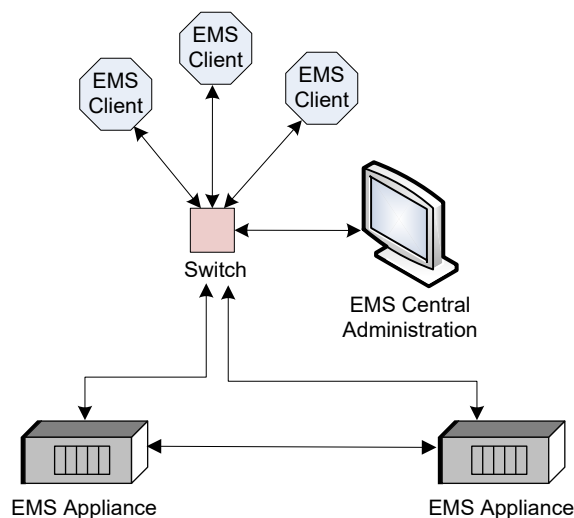
The appliance is fully compatible with current TIBCO Enterprise Message Service deployments, including TIBCO Enterprise Message Service clients and remote TIBCO Enterprise Message Service servers.

Multiple Configuration Options

Several setup configuration options are available:

- **Single Appliance:** Full TIBCO Enterprise Message Service server functionality with a single appliance.
- **Fault Tolerance:** Fault tolerant, guaranteed messaging for event-driven applications. This configuration requires two appliances.
- **Disaster Recovery:** Backup and recovery between a production and backup site. This configuration requires four appliances.

Fault Tolerant Configuration



Models

Two models of the TIBCO Enterprise Message Service Appliance are available.

TIBCO Enterprise Message Service Appliance Standard/SSD Edition

Designed for use with SOA installations that do not have performance requirements, the standard edition appliance includes a single standard-performance file system for message persistence. (In the

CLI and in some disk warning messages, the standard performance file system is referred to as the HDD location.)

TIBCO Enterprise Message Service Appliance High-Performance Edition

For use in high performance installations. In addition to the HDD location included in the standard model, the high performance model also includes a much faster high-performance file system for message persistence. Additionally, the high performance model has increased memory and a faster processor. (In the CLI and in some disk warning messages, the high performance file system is referred to as the SSD location.)



When using a fault tolerant or disaster recovery (DR) configuration, all appliances in that configuration must be the same model.

Appliance Components

It is important to understand the roles played by the components of the TIBCO Enterprise Message Service Appliance.

EMS Server Instance

The appliance comes with the TIBCO Enterprise Message Service server installed and ready to run. An *EMS server instance* is a TIBCO Enterprise Message Service server running on the appliance. The availability of EMS server instances depends on the appliance configuration selected, whether single, fault tolerant, or disaster recovery.

See [TIBCO Enterprise Message Service Instances](#) for more information.

HDD Location

The HDD location is standard on all appliance models. An active EMS server instance writes store files to the HDD location.

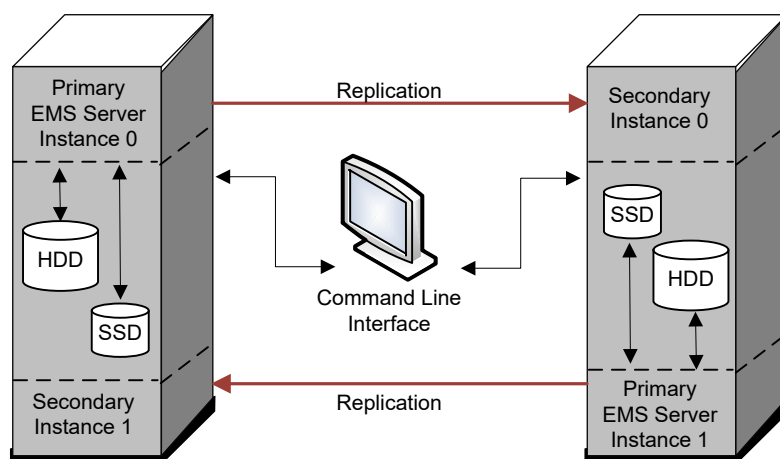
SSD Location

The SSD location is available only on the high performance model of the appliance. This store file location is allocated on a high performance file system. On a high performance model appliance, store files are placed on the SSD location by default.

Command Line Interface

Once powered on, the appliance is controlled using commands issued on the command line interface (CLI). For more information, see [Chapter 4, Commands](#).

The figure below shows the relationship between these primary appliance components in a fault tolerant configuration.

TIBCO Enterprise Message Service Appliance Components

Installation

This section describes the installation of the TIBCO Enterprise Message Service Appliance.

Installation Requirements

When installing the TIBCO Enterprise Message Service Appliance, follow these guidelines.

- Ensure that there is adequate space around the appliance to allow for servicing the appliance and for adequate airflow.
Airflow enters the chassis through the bezel and fan modules and exhausts through the port connections end of the chassis. You must install the TIBCO Enterprise Message Service Appliance with its bezel and fan modules located in a cold aisle.
- Ensure that the air conditioning meets the heat dissipation requirements:
 - Temperature: 32 to 104F (0 to 40°C)
 - Humidity: 10 to 85% (non condensing)
- Ensure that the appliance is going to be positioned so that it takes air from a cold aisle and exhausts air to a hot aisle. The end of the chassis with the bezel and fan modules must be positioned in a cold aisle.
- Ensure that the chassis can be adequately grounded. If the appliance is not mounted in a grounded rack, we recommend connecting both the system ground on the chassis and the power supply ground directly to an earth ground.
- Ensure that the site power meets the power requirements:
 - Maximum output power: 510 W
 - Input voltage: 100 to 240 VAC
 - Frequency: 50 to 60 Hz
 - Efficiency: 90/92% (110/240 Vin) at typical power draw and 88/91% (110/240 Vin) at max power draw
 - RoHS-6 compliant

If available, you can use an uninterruptible power supply (UPS) to protect against power failures.

- Ensure that circuits are sized according to local and national codes. For North America, the power supply requires a 15 Amp or 20 Amp circuit.

Installing the Hardware

Unpacking the Equipment

Follow these guidelines when lifting the switch chassis.

- Disconnect all power and external cables before lifting the switch.
- Ensure that your footing is solid and the weight of the switch is evenly distributed between your feet.
- Lift the switch slowly, keeping your back straight. Lift with your legs, not with your back. Bend at the knees, not at the waist.

Compare the shipment to the equipment list provided by your customer service representative and verify that you have received all items, including the following:

- Grounding lug kit
- Rack-mount rail-kit
- ESD wrist strap
- Cables with connectors
- Any optional items ordered

Check for damage and report any discrepancies or damage to your customer service representative.

Installing the Rack Kit

The TIBCO Enterprise Message Service Appliance can be installed in the following types of racks using a rail-kit shipped with the appliance:

- Open EIA rack
 - The minimum vertical rack space per chassis must be two rack units (RU), equal to 3.47 inches (8.8 cm).
 - The horizontal distance between the chassis and any adjacent chassis should be 6 inches (15.2 cm), and the distance between the chassis air vents and any walls should be 2.5 inches (6.4 cm).
- Perforated EIA cabinet
 - The front and rear doors must have at least a 60 percent open area perforation pattern, with at least 15 square inches (96.8 cm²) of open area per rack unit of door height.
 - The roof should be perforated with at least a 20 percent open area.
 - The cabinet floor should be open or perforated to enhance cooling.

The rail-kit enables you to install the appliance into racks of varying depths. You can use the rail-kit parts to position the appliance with easy access to either the port connections end of the chassis or the end of the chassis with the fan modules. For instructions on how to use the rail-kit, see the *Rack Mounting Your TIBCO Chassis With Included Rail Kit* document included with the appliance.

Grounding the Appliance

Grounding is one of the most important parts of equipment installation. Proper grounding practices ensure that the buildings and the installed equipment within them have low-impedance connections and low-voltage differentials between chassis. When you properly ground systems during installation, you reduce or prevent shock hazards, equipment damage due to transients, and data corruption.

Proper Grounding Guidelines

Environment	Electromagnetic Noise Severity Level	Grounding Recommendations
<p>Commercial building is subjected to direct lightning strikes.</p> <p>For example, some places in the United States, such as Florida, are subject to more lightning strikes than other areas.</p>	High	<p>All lightning protection devices must be installed in strict accordance with manufacturer recommendations.</p> <p>Conductors carrying lightning current should be spaced away from power and data lines in accordance with applicable recommendations and codes.</p> <p>Best grounding recommendations must be closely followed.</p>
Commercial building is located in an area where lightning storms frequently occur but is not subject to direct lightning strikes.	High	Best grounding recommendations must be closely followed.
Commercial building contains a mix of information technology equipment and industrial equipment, such as welding.	Medium to High	Best grounding recommendations must be closely followed.
Existing commercial building is not subject to natural environmental noise or manmade industrial noise. This building contains a standard office environment. This installation has a history of malfunctions due to electromagnetic noise.	Medium	<p>Determine source and cause of noise if possible, and mitigate as closely as possible at the noise source or reduce coupling from the noise source to the affected equipment.</p> <p>Best grounding recommendations must be closely followed.</p>
New commercial building is not subject to natural environmental noise or manmade industrial noise. This building contains a standard office environment.	Low	<p>Electromagnetic noise problems are not anticipated, but installing a grounding system in a new building is often the least expensive route and the best way to plan for the future.</p> <p>Best grounding recommendations should be followed as much as possible.</p>

Environment	Electromagnetic Noise Severity Level	Grounding Recommendations
Existing commercial building is not subject to natural environmental noise or manmade industrial noise. This building contains a standard office environment.	Low	Electromagnetic noise problems are not anticipated, but installing a grounding system is always recommended. Best grounding recommendations should be followed as much as possible.

To ground the TIBCO Enterprise Message Service Appliance and prevent damage from electrostatic discharge:

Procedure

1. Use a wire-stripping tool to remove approximately 0.75 inches (2 cm) of the insulation from the end of the grounding cable.
2. Insert the stripped end of the grounding cable into the open end of the grounding lug.
3. Use the crimping tool to secure the grounding cable in the grounding lug.
4. Remove the adhesive label from the grounding pad on the chassis.
5. Place the grounding lug against the grounding pad so that there is solid metal-to-metal contact, and insert the two M4 screws with washers through the holes in the grounding lug and into the grounding pad.
6. Ensure that the lug and cable do not interfere with other equipment.
7. Prepare the other end of the grounding cable and connect it to an appropriate grounding point in your site to ensure adequate earth ground.

Preventing Electrostatic Discharge Damage

Electrostatic discharge (ESD) damage, which can occur when modules and other field-replaceable units (FRUs) are improperly handled, results in intermittent or complete failures.

Modules consist of printed circuit boards that are fixed in metal carriers. Electromagnetic interference (EMI) shielding and connectors are integral components of the carrier. Although the metal carrier helps to protect the board from ESD, always use an ESD grounding strap when handling modules.

If you choose to use the disposable ESD wrist strap supplied with most FRUs or an ESD wrist strap equipped with an alligator clip, you must attach the system ground lug to the chassis in order to provide a proper grounding point for the ESD wrist strap.

Procedure

1. Attach the ESD wrist strap to bare skin as follows:
 - a) If you are using the ESD wrist strap supplied with the FRUs, open the wrist strap package and unwrap the ESD wrist strap. Place the black conductive loop over your wrist and tighten the strap so that it makes good contact with your bare skin.
 - b) If you are using an ESD wrist strap equipped with an alligator clip, open the package and remove the ESD wrist strap. Locate the end of the wrist strap that attaches to your body and secure it to your bare skin.

2. Grasp the spring or alligator clip on the ESD wrist strap and briefly touch the clip to a bare metal spot (unpainted surface) on a grounded rack. We recommend that you touch the clip to an unpainted rack rail so that any built-up static charge is safely dissipated to the entire rack.
3. Attach either the spring clip or the alligator clip to an earth ground (grounded rack or the screw holding a grounding lug to the chassis):
 - a) If you are using the ESD wrist strap that is supplied with the FRUs, squeeze the spring clip jaws open, position the spring clip to one side of the system ground lug screw head, and slide the spring clip over the lug screw head so that the spring clip jaws close behind the lug screw head.
 - b) If you are using an ESD wrist strap that is equipped with an alligator clip, attach the alligator clip directly over the head of the system ground lug screw or to the system ground lug barrel.

To attach the ESD wrist strap to the system ground lug screw for the TIBCO Enterprise Message Service Appliance, clip the grounding wire to the screw that attaches the grounding lug to the switch chassis.

Connecting the Power Supply to an AC Power Source

After the appliance is connected to an AC power source and the power switch on the back of the box is turned on, it automatically begins to boot up.

Procedure

1. Verify that the AC power source is turned off at the circuit breaker.
2. Plug the power cable into the power receptacle on the power supply.
3. Attach the other end of the power cable to the AC power source.
4. Turn on the power at the circuit breaker.
5. Turn the power switch on, and verify that the power supply is functioning.

Verifying LED Operation

After the appliance boots, verify the LED operation.
The LED operation should be as follows:

- PWR — Power LED is green.
- STAT — Status LED is green.
- ATTN — Attention LED is off.
- FAIL — Failure LED is off.

If after the switch boots the system status (STAT) LED is amber, one or more chassis environmental or diagnostics monitors is reporting a problem.

Connecting Two TIBCO Enterprise Message Service Appliances

To connect two TIBCO Enterprise Message Service Appliances for use in a fault tolerant configuration, connect ports numbered 30, 31, and 32 on the first box with the matching ports on the second box. This establishes the *crosslink* connection between the appliances.

- For best performance, use fiber optic cables to connect the two appliances.
 - Three connections are required.

Connecting the Appliance Management Port to the Network

The Management (MGMT) network connection is used for administrative and maintenance access to the appliance CLI, including initial setup of the appliance.

To connect an external switch to the appliance:

Procedure

1. Connect the appropriate cable to the Ethernet connector on your network switch.
2. Connect the other end of the cable to the MGMT1 port on the appliance.



Do not connect MGMT2 port to your network. It is only used for a direct connection.

Connecting the Appliance to Your Network

The TIBCO Enterprise Message Service Appliance is configured to support dual uplink ports to the network.

To connect the appliance to your network:

Procedure

1. Insert transceiver adaptors into ports 41 and 42 (or one of them). Connect to your network using the **10Gb/s SFP+** transceiver.



Pluribus Certified 1Gb/s transceivers are deprecated, but still supported.

2. Connect the transceivers to your network using the appropriate cables.

Uplink Configuration

Ports 41 and 42 are configured in an active-passive-mode Link Aggregation Control Protocol (LACP) trunk. These ports should uplink to network switch ports that are also trunked, and configured for active-passive LACP with port mode *fast*.

Ports 41 and 42 can be uplinked to two separate network switches as long as these switches support LACP ports across multiple switches. By default, only port 41 is enabled at startup. If you need a different uplink configuration, this can be configured after the software installation is complete using the **uplink-config** command. Consult your switch manufacturer's documentation to configure this option on the network switch.

Connecting Directly to the Appliance for Initial Setup

Initial software setup must be completed by directly connecting to the appliance. There are three supported methods for this: Ethernet cable, serial cable, or keyboard and monitor. We recommend using Ethernet for direct connections to the appliance.

Connect directly to the appliance using one of these methods:

Connect Using Ethernet

Recommended. This is the simplest connection method, and avoids console log messages that are printed during the setup dialog.

1. Using a CAT-5 cable, connect a computer to the MGMT2 port on the back of the appliance.
2. The MGMT2 interface has a statically assigned IP address of 169.254.254.3/16.

After you directly connect your computer to the appliance, you should be automatically assigned a usable IP address to SSH to the appliance. If the assigned IP address is not usable, you should assign a static IP address of 169.254.254.1 with a netmask of 255.255.0.0 in order to connect.

3. Using a terminal program, SSH to the switch at tibadm@169.254.254.3.

If the login prompt does not automatically appear, press Enter on the keyboard.

Connect a Computer Using an RJ-45 to DB-9 Serial Cable

1. Configure the terminal emulator program to match the following default port characteristics: 9600 baud, 8 data bits, 1 stop bit, no parity.
2. Connect the RJ-45 connector of the console cable to the CONSOLE port and the appropriate connector to the computer serial port.

Connect a Monitor and Keyboard to the Appliance

1. Connect a USB keyboard to the appliance. You may use any USB port on the appliance, front or back.
2. Connect a monitor using the 15-pin VGA port on the back of the back of the appliance.
3. Ensure that the monitor is plugged in and powered on. If a prompt does not automatically appear on the monitor screen, press Enter on the keyboard.

Initializing the Software

After the TIBCO Enterprise Message Service™ Appliance has been installed, you must initialize the software before the appliance can be used.

The initialization process configures the default appliance users, creates the TIBCO Enterprise Message Service™ server instance(s), and sets the IP addresses used to administer the appliance and connect to the TIBCO Enterprise Message Service™ servers using Central Administration.

Accessing the Appliance System

Directly connect to the appliance in order to begin the software initialization process.

Procedure

1. Power on the TIBCO Enterprise Message Service™ Appliance system.
2. Access the appliance as described in [Directly Connect to the Appliance for Initial Setup](#).



The appliance runs a health check before starting the software initialization process. If it detects any problems, such as an error in the operating system or hardware, it reports an error. Do not proceed with the software initialization process without first addressing and resolving any errors. Contact TIBCO Support if you require assistance.

3. Log in to the appliance using the tibadm username and default password of test123.
4. When prompted, enter the information specific to your system. The sections below describe the information requested in greater detail.



Note that all IP addresses must be specified using IPv4 addresses. The appliance does not support IPv6.

Configuring the Management Information

Assign a management IP address, enabling remote access. This connection can be used to access the CLI and complete the software initialization process.

Prompt	Description
Hostname():	Enter a name to identify this TIBCO Enterprise Message Service™ Appliance.
Mgmt IP/Netmask (/):	Enter the IP address that will be used by the predefined appliance users to access the management interface of the TIBCO Enterprise Message Service™ Appliance, followed by the network mask. For example: 10.101.1.100/24
Mgmt Gateway IP ():	For example: 10.101.1.1

Restarting the Software Initialization Process

To continue the installation, restart the software initialization process by logging into the appliance using the tibadm login.


Since the Management IP is now set up, you can log in either locally using the direct connection or remotely using the Mgmt-IP to finish the full setup dialog. See [CLI Overview](#) for information on accessing the appliance using the CLI.



The appliance runs a health check before restarting the software initialization process. If it detects any problems, such as an error in the operating system or hardware, it reports an error. Do not proceed with the software initialization process without first addressing and resolving any errors. Contact TIBCO Support if you require assistance.

Configuring Appliance Users

Set initial passwords for the predefined tibadm and tibfile users. These user logins are for administering the appliance.

Prompt	Description
Set passwords? [y/n] (yes):	Enter y to change the default passwords for the appliance users. Enter n to accept the default passwords. The default password for the tibadm user is test123. The default password for the tibfile user is test123. To change the passwords after setup, you can use the initial-config command to rerun the entire initial setup dialog.
Password for tibadm:	Select a password for the tibadm user.
Re-enter Password:	Enter the tibadm user password again.  Record your tibadm password in a secure location. TIBCO cannot access the appliance or recover a system without the tibadm password.
Password for tibfile:	Select a password for the tibfile user.

Prompt	Description
Re-enter Password:	Enter the tibfile user password again.

Re-configuring Management Information

If desired, update the appliance Management information.

The prompts from [Configuring the Management Information](#) are repeated here.

As these values were already specified, the settings are pre-populated. Review the original values and make any necessary updates.

Configuring Host Information



Specify your TCP networking service parameters.

Prompt	Description
Primary DNS IP ():	(Optional.) For best results, enter a DNS IP address. For example 10.201.1.100
Secondary DNS IP ():	(Optional) For example 10.101.1.100
Domain Name ():	For example company.com
NTP Server ():	For example 0.us.pool.ntp.org
Time zone ():	Time zone of location in which appliance will be used. Specify the time zone by entering a time zone name from the tz database. For example, America/New_York or US/Eastern are both valid settings. Lists of time zone names are available online: https://en.wikipedia.org/wiki/List_of_tz_database_time_zones
Uplink Speed in gigabits:	Specify an uplink speed. The default is 10 Gb (gigabits).

Configuring EMS Server Information

Enter primary EMS server network information.

Prompt	Description
EMS Server IP/ Netmask():	This is the TIBCO Enterprise Message Service server IP address that will be used by client software when connecting to the TIBCO Enterprise Message Service server. For example: 192.168.3.51/24

Prompt	Description
EMS Server Gateway IP:	<p>(Optional) The EMS Server Gateway provides routed access to the EMS Server IP. Specify this setting if any of your EMS clients need routed access to the server. You do <i>not</i> need to specify the EMS Server Gateway IP if all of your EMS clients are on the same subnet as the EMS server.</p> <p>If an EMS Server Gateway IP is specified, then once the system is booted and operational all traffic goes through the EMS Server Gateway except SSH logins to the Mgmt IP.</p> <div>  If the EMS Server Gateway IP is specified, then network services such as LDAP, DNS, and KMIP must be reachable by way of this gateway. </div> <div>  The active gateway can be manually changed using the ems-gateway command. </div> <p>For example: 10.101.1.1/24.</p>
EMS Instance Name ():	Enter a name for the TIBCO Enterprise Message Service server instance. For example, <code>inst0</code> . For server naming conventions, see documentation for the <code>server</code> parameter in the <i>TIBCO Enterprise Message Service User's Guide</i> .
EMS Instance IP Port ():	<p>Enter the port number to be used by TIBCO Enterprise Message Service clients connecting to the primary EMS server instance.</p> <p>This port is used with the TIBCO Enterprise Message Service server IP address to create the server's listen setting. Appliances in a fault tolerant pair must use different port numbers. For example, if TIBCO Enterprise Message Service instance 0 uses port 7222, TIBCO Enterprise Message Service instance 1 might use port 7223.</p> <p>NOTE: When setting up a Backup Site appliance for disaster recovery, be aware that the port number entered here will only be used for initial testing. When the Production Site is recovered to the backup site, this information is overwritten and the port numbers will be the same as the original production site port numbers.</p>

Configuring Fault Tolerant Behavior

For fault tolerant configurations, specify peer appliance information.

Prompt	Description
Is this in a Fault-Tolerant pair (yes):	<p>Hit enter if this appliance is connected to a second Appliance as part of a fault-tolerant pair.</p> <p>If this appliance is intended to run as a single installation, type no and hit enter and proceed to Beginning Appliance Operations.</p>

Prompt	Description
Primary Instance (0 or 1) on local EMS Server ():	<p>Enter 0 if the primary TIBCO Enterprise Message Service™ server instance on this appliance should be identified as instance 0.</p> <p>Enter 1 if the primary EMS server instance should be instance 1.</p> <p>Both appliances in a fault tolerant pair may not use the same instance number to identify their primary EMS servers. One appliance must be configured to have its primary server be instance 0 and the other must have its primary server be instance 1.</p>
EMS Server Instance Name of the other host of the FT pair ():	<p>Enter the EMS Instance Name used to identify the EMS server instance on the second appliance in the fault tolerant pair. This name is set in Configuring EMS Server Information.</p> <p>For example inst1.</p>
EMS Server IP of the other host of the FT pair ():	<p>Enter the EMS server IP address for the other appliance in the fault tolerant pair.</p> <p>This address is used to configure the secondary listen URL for the secondary EMS server instance.</p>
EMS Server Port of the other host of the FT pair ():	<p>Enter the port number of the fault tolerant peer appliance's primary EMS server instance.</p>

Configuring Disaster Recovery

For disaster recovery configurations, specify information regarding other quad members.

Prompt	Description
Is this unit in a disaster recovery configuration? (yes/no):	<p>If this appliance will be part of a disaster recovery installation, enter yes.</p> <p>For more information on disaster recovery and its requirements, see Disaster Recovery Configuration.</p> <p>If the appliance is not part of a disaster recovery installation, type no and hit enter and proceed to Beginning Appliance Operations.</p>
Is this a backup unit for disaster recovery? (yes/no):	<p>Enter yes if this appliance is located at the backup site.</p> <p>Enter no if the appliance is part of the production site.</p>
EMS Server IP of the Backup-A appliance ():	<p>This prompt appears only if your previous responses have indicated this appliance:</p> <ul style="list-style-type: none"> • is instance 0 in its fault-tolerant pair • is part of a disaster recovery installation • is part of the production site <p>Specify the IP address of the Backup-A appliance.</p>

Prompt	Description
EMS Server IP of the Backup-B appliance():	<p>This prompt appears only if your previous responses have indicated this appliance:</p> <ul style="list-style-type: none"> • is instance 0 in its fault-tolerant pair • is part of a disaster recovery installation • is part of the production site <p>Enter the IP address for the Backup-B appliance.</p>
Data backup interval in minutes (must be >= 1.0) ():	<p>This prompt appears only if your previous responses have indicated this appliance:</p> <ul style="list-style-type: none"> • is instance 0 in its fault-tolerant pair • is part of a disaster recovery installation • is part of the production site <p>Specify the interval at which updated system information is sent from the production site to the backup site. For example, enter 5 to have an update sent every five minutes.</p>
EMS Server IP of the Production-A appliance ():	<p>This prompt appears only if your previous responses have indicated this appliance:</p> <ul style="list-style-type: none"> • is part of a disaster recovery installation • is part of the backup site <p>Enter the IP address for the Production-A appliance.</p>

Beginning Appliance Operations

Once you have responded to the final prompt, your configuration is saved, and the CLI is ready for use. Click Enter to automatically log in as the `tibadm` user and access the CLI prompt:

```
EMS CLI >
```

The EMS server instances start automatically and can be accessed through Central Administration, using the EMS server IP address and the EMS instance IP ports specified during software initialization.

When the EMS server is active, you can see the EMS server URL by entering the `info` command from the CLI.

Configuration

This section explains how to configure the TIBCO Enterprise Message Service™ Appliance.

Predefined Appliance User Accounts

Predefined users can access the TIBCO Enterprise Message Service Appliance through a network connection, or through a console connected to the appliance.

The appliance can only be accessed using predefined SSH or SFTP accounts using the IP address specified during software initialization. See [CLI Overview](#) for information accessing the appliance using SSH.

Three preconfigured users have access to the TIBCO Enterprise Message Service Appliance:

- **tibadm** The tibadm account is used to issue commands to manage the appliance. Use SSH to login to the appliance as tibadm.

The appliance automatically launches the CLI when the login process is complete. Using commands, this user is able to perform such administrative activities as starting a TIBCO Enterprise Message Service server instance, copying log and core files to the file transfer directory with the export command, and updating SSL certificate files by way of the import command.

The password for the tibadm user is determined when the appliance is first configured. See [Initializing the Software](#) for more information. If you need to change the password, run the **initial-config** command. If you have forgotten the password, contact TIBCO Support.
- **tibfile** The tibfile account is used to transfer files to and from the appliance.

Use SFTP to login to the appliance as tibfile, as described in [Working with the File Transfer Directory](#).

As tibfile you are able to:
 - Retrieve files placed in the directory by the tibadm user.
 - Add files to the directory for deployment by the tibadm user.
 Only SFTP transfers are available. SCP transfers cannot be used.

The password for the tibfile user is determined when the appliance is first configured.
- **admin** The admin user is for use only when working with TIBCO support, and has complete access to the appliance by way of SSH.

In order to log on as the admin user, you must first log in using the tibadm password, and then correctly respond to a challenge code prompt.

Working with the File Transfer Directory

The tibfile user can login to the appliance through SFTP at the Mgmt IP address or the EMS Server IP address if specified. This is the only user that can access the tib-transfer file directory.

The tibfile user automatically accesses the tib-transfer directory upon login. The file transfer directory holds several types of files:

- Copies of deployed configuration and SSL certificate files that have been added by the tibadm user.
- Log and core report files that have been moved to the file transfer directory by the tibadm user.
- Modified or new files that have been uploaded by the tibfile user.

File Transfer Directory Structure

Directory	Contents
/instance-X/certs	<p>Contains SSL certificate files.</p> <p>SSL certificate files can be uploaded to this directory by the <code>tibfile</code> user and then deployed to the appliance by the <code>tibadm</code> user. See the import command for details.</p> <p>The <code>tibadm</code> user can also export existing SSL certificate files for review. See the export command for details.</p>
/instance-X/certs/ ldap_tls_cacert_dir	<p>Contains extra LDAP-related SSL CA certificate files. These extra CA certificates are used by OpenLDAP when connecting to an LDAP server when there is more than one CA certificate in the verify chain.</p> <p>The extra LDAP-related SSL CA certificate files can be uploaded to this directory by the <code>tibfile</code> user and then deployed to the appliance by the <code>tibadm</code> user. See the import command for details.</p> <p>The <code>tibadm</code> user can also export existing extra LDAP-related CA certificate files for review. See the export command for details.</p>
/instance-X/config	<p>Contains the TIBCO Enterprise Message Service™ server configuration files. The <code>tibadm</code> user can export copies of these files to the config directory:</p> <ul style="list-style-type: none"> • <code>tibemsd.json</code>— the deployed EMS server configuration file. • <code>tibemsd.config</code>— EMS server command line arguments. • <code>emsd.pathmap</code>— logical store location mapping. • <code>emsa_params.json</code>— lists setup parameters configured in appliance. • <code>emsa_emsmon.config</code>— syslog subscriptions for server messages. <p>See the export command for details.</p>
/instance-X/cores	<p>Contains core reports.</p> <p>The <code>tibadm</code> user can export any core reports to this directory.</p> <p>See the export command for details.</p>
/instance-X/logs	<p>Contains log files.</p> <p>In addition to regular event log files, the <code>emsa_dr.config</code> log file is generated during initialization, and lists all disaster recovery parameters. It is located under the instance-specific config directory.</p> <p>The <code>tibadm</code> user can export any server log files to this directory. See the export command for details.</p>
/system/import	<p>Contains software updates.</p> <p>Upload TIBCO Enterprise Message Service™ Appliance software upgrade packages to this directory for installation. After the package has been uploaded, it can be installed by the <code>tibadm</code> user.</p> <p>For details, see the upgrade-software command.</p>

Directory	Contents
/system/export	Contains log files for TIBCO support that are created when the CLI command export-support-logs is issued.

TIBCO Enterprise Message Service Server States

The TIBCO Enterprise Message Service server state provides information about how the server is operating in the appliance.

Use the **info** command to determine the server state.

Singular

On an appliance, the TIBCO Enterprise Message Service server state described here is only applicable to single appliance configurations.

State	Description
active	The server is fully operational and ready to service clients.

Fault Tolerant

The TIBCO Enterprise Message Service server states described here are only applicable to TIBCO Enterprise Message Service servers in a fault tolerant configuration.

State	Description
active-paused	The server is in active state and is determining the correct action in reaction to a failure to replicate with the standby server.
active-replicating	The server is in active state and is replicating incoming data to the standby server.
active-standalone	The server is active but not synchronizing data nor replicating incoming data to the standby server because it cannot reach it.
active-synchronizing	The server is in active state and is synchronizing data to the standby server.
down	The server has been stopped by the user through the CLI command stop.
standby-paused	The server is in standby state and is determining the correct action in reaction to failure of the active server.
standby-replicating	The server is in standby state and is currently replicating incoming data from the active server.
standby-synchronizing	The server is in standby state and is currently synchronizing data from the active server.

State	Description
wait-for-peer	The TIBCO Enterprise Message Service server is waiting for its peer to connect. Most frequently, this state is seen when there is a delay between startup of the primary and secondary servers in a fault tolerant pair.

Appliance Monitoring

The appliance regularly writes log messages to a local file, which can be accessed through the `tibfile` user.

In addition to these default logs, you can configure the appliance to transmit messages of higher importance to a remote `syslog` daemon, or collector.

When `syslog` transmission is enabled, all messages of priority notice and higher are transmitted to a standard `syslog` collector. This can be used to monitor the appliance for significant events, including:

- Server state changes
- Appliance fan failure
- Power supply failure
- Low disk space
- Disk errors
- CLI command actions

Syslog monitoring is configured with the `syslog-config` command.

TIBCO Enterprise Message Service™ Instances

On a given appliance, a TIBCO Enterprise Message Service instance is an EMS server running on the appliance.

The TIBCO Enterprise Message Service™ Appliance identifies a running EMS server as either instance 0 or instance 1. The instance number is set when the appliance software is initialized. This process is described in [Initializing the Software](#).

The availability of EMS server instances depends on the appliance configuration.

- **Single Appliance Configuration**

In a single appliance deployment, only one instance is available. This instance is always instance 0, and runs in standalone mode.

- **Fault Tolerant Configuration**

When two appliances (Peer-A and Peer-B) are connected as a fault tolerant pair, there are two TIBCO Enterprise Message Service™ instances, and each appliance is running two EMS servers, instance-0 and instance-1. For a given instance, the servers of that instance on each peer coordinate in order to synchronize and replicate data, with one running as active and the other as warm-standby. This state replication mechanism synchronizes and replicates configuration and store files between two appliances in a fault tolerant pair.

During normal load-balanced Fault-Tolerant operation, each instance has an Active EMS server running on one peer and a Standby EMS server running on the other peer so that each appliance is running one Active and one Standby server. By default, an EMS server is Active on its primary appliance (Peer-A for instance-0 and Peer-B for instance-1) and Standby on its secondary appliance (Peer-B for instance-0 and Peer-A for instance-1).

- **Disaster Recovery Configuration**

When four appliances are configured for disaster recovery, each pair in the quad is set up similar to a fault tolerant configuration. That is, at each site there is an appliance with an EMS server instance 0 designated as primary, and a second appliance where the primary EMS server instance is identified as instance 1.


Note that during normal DR operations the EMS servers at the backup site are disabled.

Maximum Connections

Each EMS server instance in an appliance can have up to 10,000 client connections.

Configuration

Once the TIBCO Enterprise Message Service™ server instance is started, you should configure the server using Central Administration.

Some TIBCO Enterprise Message Service™ features are not available to appliance users. In many cases, these features are hidden in Central Administration in order to protect you from appliance misconfigurations. The Server List in the Central Administration web interface denotes appliances with the  icon.

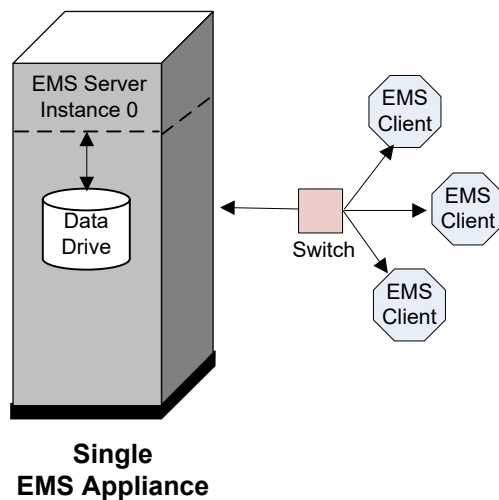
Accessing Central Administration

For more information on using Central Administration, see the *TIBCO Enterprise Message Service Central Administration* guide.

Single Appliance Configuration

Although most TIBCO Enterprise Message Service™ Appliance installations deploy two appliances in a fault tolerant pair, it is possible to run a single appliance.

In a single appliance scenario, fault tolerance is not available. If the TIBCO Enterprise Message Service™ server instance fails, there is no backup instance.



Fault Tolerant Configuration

Fault tolerance is deployed using two TIBCO Enterprise Message Service™ Appliances which are started at the same time and communicate over a cabled connection.

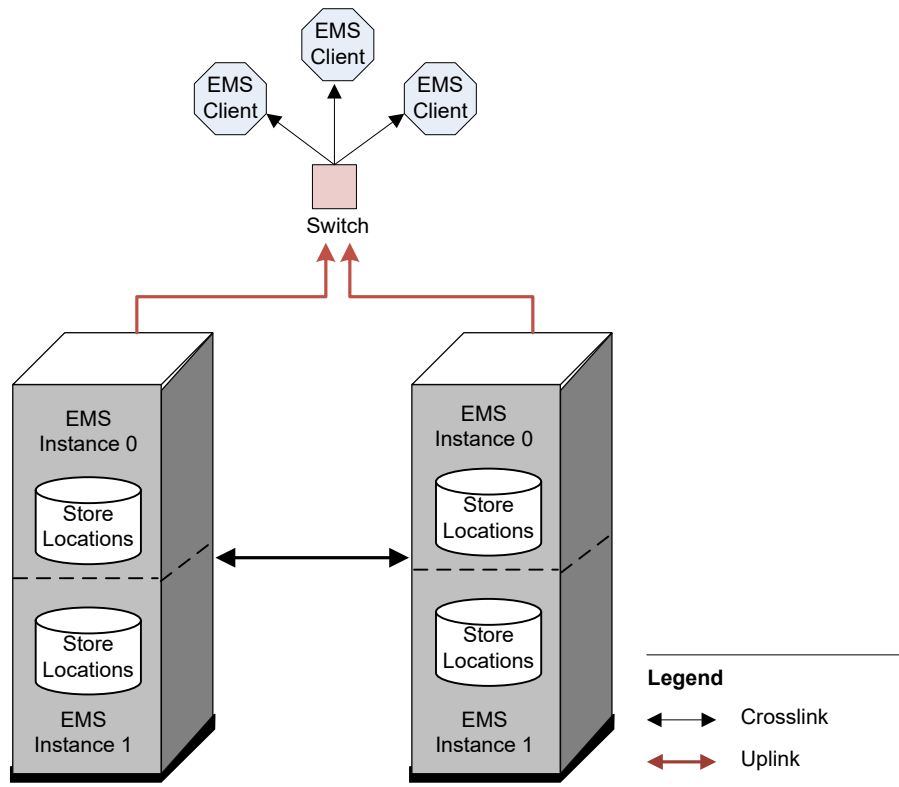
Each appliance contains a primary EMS server instance and a secondary server instance that is activated in the event of a failure of its primary instance. All switches and EMS clients are connected to

both appliances, allowing the secondary server instance to take over from the primary instance in the event of a failure.

In Fault Tolerant mode, data gets replicated between the active and standby EMS servers. So, both servers must be running and replicating when making configuration changes using Central Administration or the admin tool.



All appliances in a fault tolerant configuration should be of the same model, either standard or high performance. For best results, both appliances should use the same TIBCO Enterprise Message Service™ Appliance software version.



Configuration Changes on Fault-Tolerant Servers

In Fault Tolerant mode, data and configuration parameter settings get replicated between the active and standby TIBCO Enterprise Message Service™ servers.

Both servers must be running and replicating when making configuration changes using Central Administration or the admin tool.

Authorization and Fault-Tolerant Servers

When authorization is enabled for a fault tolerant configuration, the connection between the EMS servers in the fault tolerant pair is also authenticated. The standby server connects to the active server as a user whose name is its EMS instance name.

Before enabling authorization, you must therefore create a user with the EMS Instance Name and assign it the password configured for the EMS server. This user must be deployed to both servers in the fault tolerant pair. If the standby server does not have this user configured, it cannot connect to or replicate data from the active server.

In Central Administration:

- In the Users properties page, create a user with the EMS Instance Name.
- In the **Password** field on the Server Properties page, make sure that the same password granted to the new user is assigned to server.

Create the user when the appliance is in the active-replicating state, using either Central Administration or the admin tool. The username must be the same as the EMS Instance Name.



The EMS Instance Name is configured during software initialization, and can be viewed using the **setup-show** command, or changed using the **ems-config** configuration setup command. Use the **info** command to view the server state.

After the new user has been deployed to both active and standby servers, you can enable authentication.



If you enabled authorization before creating the EMS Instance Name user, or if the user was not deployed to the standby server when authorization was enabled, then the standby server will not be able to connect to the active server and will not be able to enter the replicating state. Disable authorization, then ensure that the user has been correctly created and replicated to the standby server before reenabling authorization.

Startup Process

When a pair of fault-tolerance appliances start up, the procedure described here takes place concurrently on each appliance.

Procedure

1. When the EMS server instance starts, it waits for its peer before proceeding with the startup sequence.
2. After contact occurs, the two EMS server instances check the state of their stores to determine which server has the most recent copy of the store data.
3. The EMS server that has the latest store data proceeds to the active state and begins servicing clients. The other server proceeds to the standby state.
4. The active and standby EMS servers synchronize data, such as store and configuration files, to ensure that both sides match. Synchronization is complete when both servers have the same records in their store files.
5. The active and the standby servers begin replicating data. Replication is the process whereby the active EMS server instance writes persistent data to both its own and the standby server store files.

Result

If only one appliance in a fault tolerant pair is available, you can force the EMS server instance(s) on the available appliance to start in standalone mode. Starting an EMS server instance in a standalone mode requires an explicit command from the administrator using the **forcestart** command on the CLI. Neither appliance will automatically start servicing messaging operations in the absence of the other.



When the second appliance is started, it synchronizes with the appliance that was forced to start. You should never force both appliances to start separately because they cannot properly synchronize their stores afterwards.

Failover Process

When a fault tolerant appliance loses contact with its peer, both the active and standby EMS server instances enter their paused states for a short time while the appliance determines the correct action.

The response of the appliance depends on the type of failure experienced:

- **System or Power Failure**

If the peer appliance is down, the remaining appliance's active EMS server instance enters the active-standalone state and continues to service clients. The standby EMS server instance also enters the active-standalone state, and begins servicing clients.



No replication occurs while the servers are in the standalone state.

- **Hardware Component Failure**

If both appliances are still running but one appliance has a hardware fault, the faulted appliance shuts down its active EMS server instance. Both server instances on the functional appliance begin servicing clients in the active-standalone state.

- **Connection Failure**

If the fiber optic cable connections between the appliances fail, preventing the EMS server instances from communicating, the appliances continue their active server instance in the standalone state and prevent their standby server instance from being able to activate.

- **Network Interface Failure**

If an appliance has a network interface failure that prevents its EMS server instances from servicing clients (even though the EMS server instances can communicate with their peers on the other appliance), the appliances react in the same way as they would to a hardware failure.

Restoring After a Failover

To restore the fully functional condition, simply start the appliance that is down.

If the EMS servers do not start automatically, you can start them manually using the **start** command.

The EMS server instances on the restarted appliance automatically contact their peers in the functional appliance. The servers in the functional appliance, which have been operating in active-standalone state, enter the active-synchronizing state while continuing to service messaging clients.

When synchronization is complete, both EMS server instances on the functional appliance transition to the active-replicating state. Both servers on the newly started appliance then transition to the standby-replicating state. Use the **restore-primary-active** command on the CLI to rebalance the server instances so that EMS server instance 0 is active on the primary appliance and EMS server instance 1 is active on the secondary appliance.



Restoring the primary EMS server to the active state causes client connections to drop and reconnect, as the active server moves from one appliance to the other.

Failover Events

The events that result in a failover, and the response to each event by the primary and secondary EMS server instances are described in this section.

Event	Active EMS Instance Reaction	Standby EMS Instance Reaction
Failure of the active EMS server instance, other than a write failure.	The EMS server attempts to restart and synchronize with the activated standby server.	Activates the EMS server instance and begins local writes.

Event	Active EMS Instance Reaction	Standby EMS Instance Reaction
Failure of the active EMS server hardware.	n/a	Activates the EMS server instance and begins local writes.
Failure of the standby EMS server hardware.	Performs local writes only.	n/a
An internal system error on the active appliance.	Stops the EMS server instance.	Activates the EMS server instance and begins local writes.
An internal system error on the standby appliance.	Performs local writes only.	Cannot be activated.
Active EMS server local write fails.	Stops the EMS server instance.	Activates the EMS server instance and begins local writes.
Standby EMS server local write fails.	Performs local writes only.	The EMS server restarts.
Failure of the standby EMS server, other than write failure.	Performs local writes only.	The EMS server attempts to restart and synchronize with the active server.

Disaster Recovery Configuration

You can configure your appliance installation for disaster recovery (DR).

A disaster recovery configuration consists of two appliances at a production site matched with two appliances at a back-up site. Should there be a failure in the production site, you can recover activity at the back-up location. When the production site is back online, you can then restore activity at that location.

Requirements

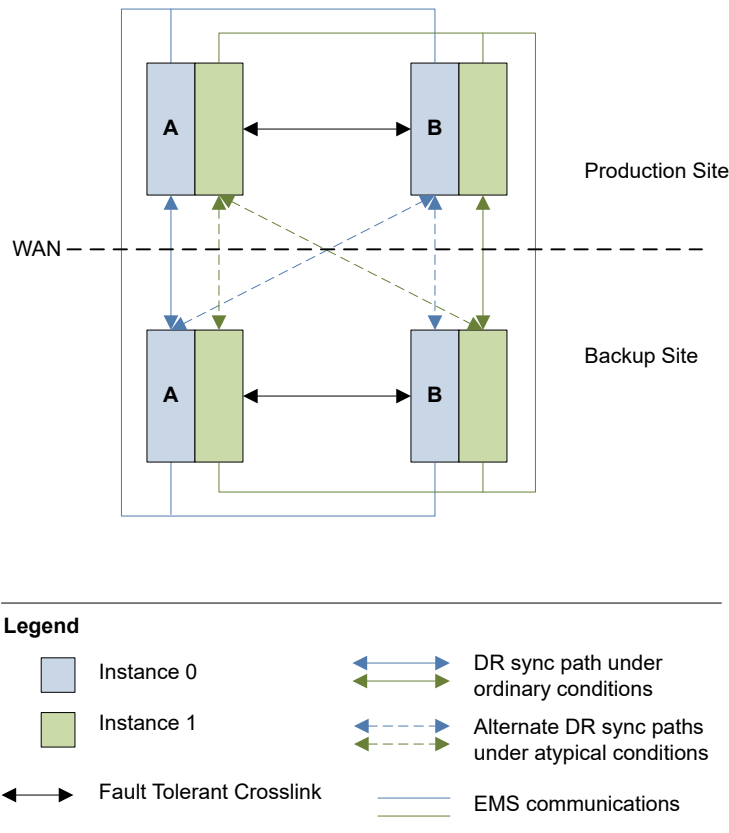
- All appliances in a DR configuration should be of the same model, either standard or high-performance. All appliances should also use the same TIBCO Enterprise Message Service Appliance software version.
- DR operations require that the following ports be allowed between members of the DR cluster. These DR communications all use the EMS-IP address.
 - SSH port 22
 - RSYNC port 873
 - Agent port 9990

Structure

Disaster recovery requires four appliances, known as a *quad*. A quad is divided into two fault-tolerant pairs, the production pair and the backup pair. The terms *production* and *backup* here indicate the physical location, or site, of the appliances.

The appliances at the production site are designated Production-A and Production-B, whereas the appliances at the backup site are designated Backup-A and Backup-B. An appliance's designation is distinct from but related to its role.

The relationships between the quad of appliances is shown in the following image.



Roles

There are two roles in disaster recovery

- DR leader
- DR member

In most cases, Production-A is the *DR leader*, while the three remaining appliances, Production-B, Backup-A and Backup-B, are *DR members*.

Disaster Recovery Process

When configured, disaster recovery works as follows:

Procedure

1. At regular intervals, the production site takes a snapshot of filesystem data from its active server instances and sends this snapshot to an appliance at the backup site.

Under normal, fully operational behavior, Production-A sends instance 0 snapshots to Backup-A, and Production-B sends instance 1 snapshots to Backup-B.

2. If Production-A fails, both EMS server instances 0 and 1 are running on Production-B. Assuming both backup site appliances are available, Production-B begins sending instance 0 snapshots to Backup-A, and continues sending instance 1 snapshots to Backup-B.



You should not start the EMS server instance on an appliance while it is acting as a backup. In case of a recovery event, the data from previous activity using those servers will be lost.

3. If both Production-A and Production-B fail, you must manually initiate the DR recovery procedure at the backup site. See [Recovering to a Backup Site](#) for details.
Note that disaster recovery does not imply that there is no data loss. Any activity that occurred after the most recent snapshot may be lost. The recovery process erases all prior data from the backup site and overwrites it with the data from the production site snapshot.
4. If at the time of a DR event only one appliance is available at the backup site, the disaster recovery process can be initiated on the available appliance. For example, if the backup site experienced an FT event or planned downtime on one of the appliances, the client operations can still be recovered at the backup site.
5. When the production site is restored, it must be reactivated manually using the `dr-restore` command.

Enabling Disaster Recovery

You can activate DR only after the initial setup is complete on all four appliances, connectivity exists, and all four roles have been correctly established.

Initial Setup

The first step in disaster recovery setup is to configure the software.

For each appliance in the quad, you specify that it will be used for disaster recovery and whether the appliance is part of the production or backup site. You also provide any needed IP addresses of other members of the quad.

You are prompted for this information during software initialization of a new appliance. However, you can also add DR configuration later using the `dr-config` command.

For information about the disaster recovery settings configured during software initialization, see [Initializing the Software](#).

Verify that the EMS Server Instance on Each Appliance is Operational

Before establishing communications between the quad appliances, ensure that the EMS server instance on each appliance is fully operational.

To verify the EMS server state, use the `info` command on the CLI.

For the Production-A and Backup-A appliances, the state of instance 0 should be active-replicating. The state of instance 1 should be standby-replicating.

For the Production-B and Backup-B appliances, the opposite is true: instance 0 should be standby-replicating, and instance 1 should be active-replicating.

Establish Communications Between the Quad Appliances

On each of the DR members, issue `key-join`.



Appliances in the DR cluster exchange SSH Secure Shell keys. Consequently, SSH port 22 and RSYNC port 873 must be open between members of the quad.

Additionally, agent port 9990 is used to exchange status information between cluster members and must be open.

This command establishes communications between the appliances in the DR cluster.

The key is a key-pair automatically generated by the DR leader during initial setup. When you issue **key-join**, the DR members retrieve and install the DR key. All DR members use the same DR key.

Activate Disaster Recovery Support

To start DR services on the quad, activate disaster recovery services on the DR leader (Production-A) using the **dr-activate** command.

See **dr-activate** for more information.

This command is only available on the DR leader, and will only be successful if **key-join** has been called on the other DR members to establish disaster recovery communications.

Rejoining the Quad

If an appliance loses and then regains communications with the quad, no special actions are required to restore DR activity. However, if an appliance requires configuration changes, there are some steps needed to rejoin the DR cluster.

DR Members

To restore a DR member that required a new setup to the quad:

Procedure

1. From the CLI, issue the **info** command to view the appliance configuration settings. Ensure that the DR member has the appropriate DR configuration settings for its role. See [Initial Setup](#) for more information.
2. On the DR member rejoining the quad, issue **key-join**.
3. Depending on whether the joining DR member is a production or backup appliance, enable or disable TIBCO Enterprise Message Service services.
 - If the joining member is a backup site appliance (either Backup-A or Backup-B), issue:


```
services all disable perm
```
 - If the joining member is Production-B, issue:


```
services all enable
```

DR Leader

Only in a non-DR recovery RMA scenario would a DR Leader be lost from the cluster. (For example, if the physical appliance is replaced.) However, if this occurs, the DR leader can rejoin using **key-join member-IP**.

If the production site is rejoining as part of a DR scenario, see [Restoring the Production Site](#) for details.

Recovering to a Backup Site

In the event of a production site failure, you manually activate the backup site.

To recover to the backup site, issue the **dr-recover** command at the backup site.

Recovering from a disaster only requires one appliance be available at the backup site. The full quad is required to setup the DR feature, but not to recover from a DR event. For example if one of the appliances at the backup site is down for repair, you can still recover to the available appliance.

- If both Backup-A and Backup-B are available, OR if only Backup-A is available, then issue **dr-recover** on Backup-A.
- If only Backup-B is available, issue **dr-recover** from Backup-B.

dr-recover erases all prior EMS server data from the backup site and overwrites it with the data from the production site snapshots.

Restoring the Production Site

After a DR event, you restore the production site to operation manually.

Procedure

1. Bring the appliances at the production site back on line and make sure they're properly configured. If the DR leader (Production-A) has been rebuilt and must re-join the cluster:
 - Run **dr-config** using the same setup and DR parameters as the original configured.
 - On production-A issue **key-join**.
2. Ensure that each pair of appliances in the quad is properly set-up as an FT pair and has re-joined the cluster, if necessary.
From the CLI for each appliance, issue the info command to view the appliance configuration settings. See [Task A, Initial Setup](#), for more information. Use the **dr-check** command to view DR join status.
3. At the backup site, issue the **dr-restore** command. This command restores activity at the production site and reestablishes DR processes. The **dr-restore** command is only active on the Backup site appliances and is normally issued from Backup-A.



dr-restore sends full copies of store data to the production site and re-initializes the production servers. This process can be time-consuming and should not be interrupted.

Encrypted Data Store (EDS) Configuration

The high-performance edition TIBCO Enterprise Message Service™ Appliance supports encrypted data store locations.

You can configure your high-performance edition TIBCO Enterprise Message Service™ Appliance for use with applications that require an encrypted data store. The high-performance edition appliance supports writing data to an encrypted data store by creating encrypted store file locations called ESSD on the appliance. Once you configure the encrypted store file location, you can select this encrypted data store (ESSD) from the drop down menu that is available in Central Administration when configuring the data store on your appliance. The appliance uses the Key Management Interoperability Protocol (KMIP) technology to connect to your key server for storage and retrieval of the associated data encryption key.

After the appliance is configured for encrypted data storage support, the appliance connects to your KMIP key server and creates a key that the appliance uses to access the ESSD data store. When an appliance is rebooted, the KMIP key server must be reachable, or the encrypted stores cannot be opened and the EMS server instances will fail to start.



If the key on the KMIP server has an expiration date, you must refresh the key by running the **eds-key-refresh** command. See [eds-key-refresh](#) details on this command.

The appliance then mounts the ESSD encrypted storage area using the encryption credentials that you provided during the encrypted data storage setup. If the connection to the KMIP key server fails, your TIBCO Enterprise Message Service™ servers on the appliance will not start. In such a situation, check the connection to the key server and make sure the address and port are correct in the appliance setup.

Configuring the Encrypted Data Store on EMS Appliance



In a Fault Tolerant Environment, you must stop all servers in the fault tolerant pair before you can configure the appliances for encrypted data storage support. Run the `eds-config` command on Peer A. To configure your TIBCO Enterprise Message Service™ Appliance to support a solution that requires an encrypted data store, follow these steps on the appliance:

Procedure

1. Make sure your KMIP key server is up and running.
2. Make sure the peer appliance is up and running.
3. Rename the KMIP key server certificate files to `KEYSERVER.pem` and `KEYSERVER_CA.pem` certificate files. These certificate files are used by the TIBCO Enterprise Message Service™ Appliance to connect to the KMIP key server.



Keep in mind that the TIBCO Enterprise Message Service™ Appliance automatically shuts down the TIBCO Enterprise Message Service™ servers before it applies the following changes.

4. Import the `KEYSERVER.pem` and `KEYSERVER_CA.pem` files into the TIBCO Enterprise Message Service™ Appliance's instance 0 certs directory. This is required in order for the appliance to securely communicate with the KMIP key server. See the command `import` for details.
5. Run the `eds-config` command from the CLI and set the encrypted data store size, KMIP key server host name or IP address and port number when prompted.
6. Save and apply your changes using the `config-save` and `config-apply` commands.
7. Connect to the EMS server using Central Administration in order to create store files that use the new ESSD encrypted storage area.

Disaster Recovery



When you choose the initial EDS pool size, keep in mind that the initial DR synchronization sends the fully allocated EDS store, for example, 5G by default. This could impact the DR synchronization initialization time as the full pool size will need to be transmitted to the backup site on the initial send. During any subsequent synchronizations only changed blocks get sent.

Do the following on the disaster recovery machines:

- Make sure that the disaster recovery machines are able to connect to the KMIP key server.
- Ensure that the KMIP key server port is open on the disaster recovery machines. This can be verified using the `network-check connect` command by supplying the key server host and port as the target. When recovering to the backup site, the backup site appliances must connect to the KMIP key server in order to remount the encrypted data stores.

Commands

The TIBCO Enterprise Message Service™ Appliance command line interface (CLI) is the interface to the software that you use whenever you access the system— whether from the console or through a remote network connection.

The CLI, which starts automatically on login, provides commands that you use to perform various tasks, including starting and stopping the EMS server instance, monitoring the system state, and accessing server files and logs.

CLI Overview

The TIBCO Enterprise Message Service Appliance CLI is a text-based interface for setup and management of the appliances.

The tibadm user can access the CLI through either a console connection to the system or through a Secure Shell (SSH) connection.

To access the appliance using SSH, login using the IP address specified during setup and initialization. Depending on the appliance configuration, this may be:

- The management IP address. This is the default setting.
- The EMS server IP address. This address may be used if the optional EMS Server Gateway IP was configured and is operational.

See [Initializing the Software](#) for information on initialization.

Some of the CLI commands are specifying an action on a particular EMS server instance. You are therefore required to identify the desired server instance, either 0 or 1. In a single appliance configuration, the instance is always 0.



In a fault tolerant configuration, some CLI commands act only on the appliance the CLI is running on. Commands that take an instance parameter do not write changes to the TIBCO Enterprise Message Service server instance on the fault tolerant peer. If you specify an instance number that is not primary for this appliance, the command acts on the secondary EMS server instance.

Using the CLI to Make Configuration Changes

The CLI offers a way to make some changes to the TIBCO Enterprise Message Service Appliance configuration.

To prevent inadvertent changes, commands that modify the appliance configuration are not available through the main CLI. To access these commands, you must enter the TIBCO EMS Appliance Setup menu, and explicitly save and apply changes made while in that interface.

Procedure

1. From the CLI, issue the **setup-enable** command to enter the TIBCO EMS Appliance Setup Interface.
2. Make the desired configuration changes using the available commands. See [Configuration Setup Commands](#) for more information.
3. Issue the **config-save** command to save the changes made.
4. Issue the **config-apply** command to apply the changes.
5. Use the **exit** or **quit** command to exit the TIBCO EMS Appliance Setup Interface and return to the main CLI.

Command Overview

The following table lists CLI commands.

General Commands

Command	Description
<code>date</code>	Prints the current system date and time.
<code>diagnostics-enable</code>	Enters the Diagnostics menu of the CLI which provides access to diagnostics and troubleshooting commands.
<code>eds-key-refresh</code>	Generates and applies a new data store key on the key server before the key expires.
<code>ems-gateway</code>	Manually enables or disables the EMS Server Gateway.
<code>exit</code>	Exits the current CLI interface.
<code>export</code>	Exports the specified files to the transfer directory.
<code>export-support-logs</code>	Exports configuration and log files for use by TIBCO Support.
<code>forcestart</code>	Activates the EMS server instance as a standalone server.
<code>halt</code>	Shuts down all system services in preparation for powering off the appliance.
<code>help</code>	Displays help information.
<code>import</code>	Moves a file from the file transfer directory to the operating directory.
<code>info</code>	Displays the state of the EMS server instance.
<code>initialization-progress</code>	Turns off or on status notification messages for the appliance initialization progress.
<code>log-show</code>	Displays the most recent lines of a log file.
<code>log-test</code>	Prints a syslog test message of the desired level.
<code>quit</code>	Exits the current CLI interface.
<code>reboot</code>	Stops and restarts all services and processes on the appliance.
<code>restore-primary-active</code>	Makes the default primary EMS servers active on each peer.
<code>services</code>	Starts, stops, or lists EMS and DR services on an appliance.
<code>setup-enable</code>	Initiates the Setup menu of the CLI session to modify configuration parameters.

Command	Description
<code>setup-show</code>	Prints a list of the currently applied appliance setup parameters.
<code>show</code>	Prints a list of files of the type specified.
<code>start</code>	Starts EMS servers.
<code>stop</code>	Stops running EMS server instance(s).
<code>upgrade-software</code>	Installs a TIBCO Enterprise Message Service™ Appliance software upgrade package.
<code>version-show</code>	Prints the version numbers for the software components on the TIBCO Enterprise Message Service™ Appliance.

Disaster Recovery Commands

Command	Description
<code>dr-activate</code>	Activates a previously-configured DR quad.
<code>dr-recover</code>	Activates the backup site after a DR event.
<code>dr-restore</code>	Brings the production site back online and reestablishes normal backup operations after an event.
<code>key-accept</code>	Allows DR members to fetch the DR key from the DR leader.
<code>key-join</code>	Causes a DR member to request the DR key from the DR leader.
<code>key-reset</code>	Pushes a new DR key from the DR leader to members.

Configuration Setup Commands

Command	Description
<code>config-apply</code>	Applies all saved and pending configuration changes.
<code>config-pending</code>	Displays a list of saved but unapplied configuration changes.
<code>config-revert-pending</code>	Removes pending (saved but not applied) configuration changes.
<code>config-revert-unsaved</code>	Removes unsaved configuration changes.
<code>config-review</code>	Displays a list of all configuration changes that have been made but not saved.
<code>config-save</code>	Saves (but does not apply) changes made during the current session.
<code>dr-config</code>	Adds or changes DR configuration information.

Command	Description
<code>eds-config</code>	Configures the TIBCO Enterprise Message Service™ Appliance to support encrypted data storage. It is currently available only on high-performance models.
<code>ems-config</code>	Adds or changes EMS configuration parameters.
<code>ft-config</code>	Adds or changes fault tolerance configuration parameters.
<code>health-check-config</code>	Transmit information about <code>isLive</code> or <code>isReady</code>
<code>hostinfo-config</code>	Changes host configuration parameters.
<code>initial-config</code>	Changes all configuration parameters.
<code>mgmt-config</code>	Changes management port configuration parameters.
<code>set-timezone</code>	Sets a new time zone for the appliance.
<code>syslog-config</code>	Supplies the IP address for a remote syslog collector to enable sending of important log messages to the collector.

Instance Management Commands

Command	Description
<code>call-tibemsadmin</code>	Locally logs into the EMS server's admin tool.
<code>forcestart-instance</code>	Forces the EMS server instance to go into a STANDALONE state.
<code>start-instance</code>	Starts the specified local EMS server instance.
<code>stop-instance</code>	Stops the specified local EMS server instance.
<code>switch-active</code>	Switches the active TIBCO Enterprise Message Service™ Appliance for the specified EMS server instance.

Diagnostics and Troubleshooting Commands

Command	Description
<code>disk-check</code>	Prints detailed information about storage devices on the appliance.
<code>dr-check</code>	Runs general Disaster Recovery diagnostics and reports the results to the CLI.
<code>log-audit</code>	Lists appliance log files that are larger than the size that you have specified in the command.
<code>log-remove</code>	Deletes the specified log file name or its rotations.

Command	Description
<code>log-rotate</code>	Rotates the appliance logs or the log file that is specified.
<code>log-truncate</code>	Edits the specified log file so that the first 100MB and last 100MB are saved.
<code>network-check</code>	Uses any of a variety of network utilities that may be used for debugging.
<code>peer-login</code>	Opens a CLI SSH session to the target TIBCO Enterprise Message Service™ Appliance.
<code>port-disable</code>	Disables the specified port on the appliance.
<code>port-enable</code>	Enables the specified port on the appliance.
<code>port-show</code>	Displays formatted information about the specified port.
<code>pstack-instance</code>	Creates a log file containing the <code>pstack</code> information.
<code>remove-certs</code>	Deletes certificates for EMS server instance.
<code>remove-cores</code>	Deletes core files for the specified EMS server instance.
<code>remove-snapshots</code>	Removes Disaster Recovery (DR) snapshots from the appliance.
<code>remove-transfers</code>	Deletes all files in the <code>/tib-transfer</code> directory and its subdirectories.
<code>reset-all</code>	Resets the appliance to a pre-setup state without rebooting.
<code>session-timeout</code>	Prints or changes the timeout of the current session.
<code>uplink-config</code>	Customizes the uplink connection used by the appliance to connect to the EMS network.
<code>zone-admin</code>	Reboots the management zone or exports the management zone log files.

General Commands

date

This command prints the current date and time configured in the appliance.

```
date
```

diagnostics-enable

This command allows you to enter the Diagnostics menu of the CLI, which provides access to diagnostics and troubleshooting commands.

```
diagnostics-enable
```

eds-key-refresh

This command allows you to generate and apply a new data store key on the key server before the key expires.

```
eds-key-refresh
```

ems-gateway

This command enables or disables the EMS Server Gateway.

```
ems-gateway [-force] {enable|disable}
```

By default, the EMS Server Gateway is automatically enabled when the appliance is set up and the uplink is connected. Disabling this gateway leaves the Mgmt Gateway as the only access point for the CLI. Enabling this gateway allows for access using either the EMS Server Gateway or the Mgmt Gateway. For more information on the EMS Server Gateway, see [Configure EMS Server Information](#).

exit

This command exits the current CLI menu.

```
exit
```

If you are at the CLI main menu, the command logs the user out and exits the CLI. If you are in a sub-menu, such as the Setup Interface that is accessed using the [setup-enable](#) command, then the **exit** command returns you to the main CLI menu.

export


This command places all files of the specified type into the file transfer directory, where they can be accessed by the `tibfile` user.

```
export <instance> <type>
```

<i>instance</i>	The EMS server instance. Can be one of the following values: <ul style="list-style-type: none"> • 0 refers to EMS server instance 0. • 1 refers to EMS server instance 1. • all refers to both instance 0 and 1 and all file rotations. If the <instance> option is not specified, the default behavior is all.
-----------------	--

type

The type can be one of the following values:

- **logs:** Copies all log files. This is the default behavior. If the type is not specified, the default is logs.
- 

To export a single log file, you must use type=logs.
- **log-filename:** Copy the specified file.
 - **log-filename-path/log-filename:** Copy the specified file from the path specified.
 - **cores:** Moves any core report. Note that this removes the core files from the operating directory.
 - **certs:** Copies the current SSL certificate files.
 - **config:** Copies the following files:
 - EMS server instance tibemsd.json
 - tibemsd.config
 - emsd.pathmap
 - appliance-wide emsa_params.json
 - emsa_emsmon.config

Here are some examples of using the command.

To export instance-specific cert files, use the following command:

```
export <0|1> certs
```

To export core files that are not instance-specific, use the following command:

```
export cores
```

To export config and log files that are both instance-specific and not instance-specific, use the following commands:

Command	Exports
export config	non-instance specific config files
export logs	non-instance specific log files
export <0 1> config	instance specific config files
export <0 1> logs	instance specific log files
export all config	both instance and non-instance specific config files
export all logs	both instance and non-instance specific log files
export all emsa.syslog	all rotations of non-instance specific emsa.syslog log file
export all emsd.log	all rotations for both instances for the instance specific emsd.log file

The appliance-wide files are copied regardless of the instance specified.

export-support-logs

This command creates and exports a compressed .tgz file containing configuration and log files and debug information to be used by TIBCO Support in the event of a support request.

```
export-support-logs [options]
```

The exported file is placed in the /system/export directory under the tibfile user's home. TIBCO Support will provide additional direction if any options are needed.

forcestart

This command forces the EMS server instances on the fault tolerant pair of appliances to transition from the wait-for-peer to active-standalone state.

```
forcestart
```

When activated, the EMS server begins serving clients even when its fault tolerant peer is not available.

Before you can use this command, the appliance must be in the wait-for-peer state. For details on states, see [TIBCO Enterprise Message Service Server States](#).

Under normal circumstances, an EMS server instance starts automatically when the appliance is powered on. However, the server instance will not start if the appliance is unable to synchronize with its peer.

This command is used to activate an EMS server instance in a fault tolerant pair when the connection to the other appliance is unavailable. This command should only be used to activate a server instance when the other machine in the fault tolerant pair cannot be made available and this machine is in the wait-for-peer state. If the fault tolerant pair is in any other state, this command will not be accepted. Furthermore, this skips any file synchronization between the two machines, resulting in the loss of any new data on the peer.

halt

This command prepares the appliance to be powered off.

```
halt
```

This command shuts down the appliance operating system in preparation for a power down, but does not itself power off the appliance. Physical access to the appliance is required to complete the power down, or to restart.

help

This command displays help information.

```
help [command]
```

Enter help for a summary of all available commands.

Enter help *command* for help on the specified command.

import

This command copies the certificate files from the file transfer directory to the operating directory for the specified TIBCO Enterprise Message Service™ server instance.

```
import instance certs
```

<i>instance</i>	The EMS server instance. Must be either 0 or 1.
-----------------	---

Any existing certificates are overwritten.



In a fault tolerant configuration, an import should be issued on both appliances, so that they both have the same resulting configuration.

See the section [Working with the File Transfer Directory](#) for details about files in the file transfer directory.

info

This command retrieves the state of the EMS server instances on the local appliance and prints the latest operator notification.

```
info [instance]
```

<i>instance</i>	The EMS server instance. If an instance is not specified, the info command prints a summary status of all instances. If specified, <i>instance</i> must be either 0 or 1.
-----------------	---

For information on possible appliance states, see [TIBCO Enterprise Message Service Server States](#).

initialization-progress

This command enables or disables progress notifications during TIBCO Enterprise Message Service™ Appliance initialization.

```
initialization-progress [on|off]
```

The default value is on.

log-show

This command allows you to view the most recent lines of a log file on the console.

```
log-show [-lines | -f] instance log-name
```

-lines	The number of lines to show. For example, specify -100 to show the last 100 lines of the log file. If -lines is not included, the last 50 lines are shown.
-f	Follow option. When entered, tails the log file until stopped with ^C.
<i>instance</i>	The EMS server instance. Must be either 0 or 1.
log-name	The name of the desired log file.

Any log file reported using the show *instance* logs command can be specified. For those logs that are not instance specific (as identified in the output of the show command), either instance number may be specified.

Example

```
EMS CLI> log-show 0 cli.log
```

You can still export and download the full log file, if desired.

log-test

This command prints a test message of the desired level.

```
log-test level [msg]
```


<code>level</code>	Can be any of the <code>syslog</code> severity levels defined in the <code>syslog</code> standard RFC 3164.
<code>msg</code>	(Optional) The <code>msg</code> can be any string. The resulting message prefixes the word <code>TEST</code> to the specified <code>msg</code> text. If no <code>msg</code> is entered, a default <code>TEST</code> message containing the current date and time is generated.

This command can be used to verify that your `syslog` collector is correctly set up to receive the desired log messages.

quit

This command exits the current CLI menu.

```
quit
```

If you are in the CLI main menu, this command logs the user out and exits the CLI. If you are in a sub-menu, such as the TIBCO EMS Appliance Setup Interface that is accessed using the `setup-enable` command, then the `quit` command returns you to the main CLI menu.

reboot

This command restarts all services and processes on the appliance.

```
reboot
```

This command can be used at any time to restart the TIBCO Enterprise Message Service™ Appliance.



Following a reboot, it is possible to log into the CLI before all required services have started. In this case, the CLI displays startup progress notifications, concluding with a message notifying you when the system is ready.

restore-primary-active

This command causes clients to disconnect from the EMS server instance, and reconnect to the other appliance.

```
restore-primary-active [-force]
```

`-force`

Include the `-force` to disconnect all clients silently by suppressing the warning prompts that require you to acknowledge client disconnects.

Transitions a fault tolerant pair of appliances so that the original primary active servers become active again. This is done when maintenance or a fault of some kind has caused a failover and one appliance is active for both instances.



Because this commands disconnects clients from the EMS server instance and reconnects to the other appliance, both EMS instances on the pair of appliances must be in a replicating state.

services

This command starts, stops, restarts, or lists the services running on an appliance without affecting the state of the appliance.

```
service group action [perm|noperm]
```

<i>group</i>	<p>The values for <i>group</i> can be:</p> <ul style="list-style-type: none"> • <code>ems</code> applies to all EMS server and related processes, including monitoring processes. • <code>dr</code> applies to the disaster recovery synchronization service. • <code>all</code> includes all configured services on the appliance.
<i>action</i>	<p>The values for <i>action</i> can be:</p> <ul style="list-style-type: none"> • <code>enable</code> to start service(s). • <code>disable</code> to stop service(s). • <code>restart</code> to stop and then restart the service(s). • <code>list</code> to list the service status. <p>When <i>action</i> is <code>enable</code> or <code>disable</code>, the optional <code>perm</code> attribute causes the new state to be preserved across appliance reboots. If <code>noperm</code> is included, the new state is not preserved across reboots. For the <code>enable</code> action, the default is <code>perm</code>. For the <code>disable</code> action, the default is <code>noperm</code>.</p>

This command is used to:

- Shutdown services on a DR backup site after testing and prior to DR activation.
- Shutdown services on an appliance in preparation for support or maintenance activities, or both.

setup-enable

This command initiates a TIBCO EMS Appliance Setup Interface session.

```
setup-enable
```

While in the TIBCO EMS Appliance Setup Interface, you may make modifications to the appliance configuration parameters.

For more information, [Using the CLI to Make Configuration Changes](#).

setup-show

This command prints a list of significant appliance setup parameters and their values.

```
setup-show
```

These parameters were configured during the software initialization, and may have been modified in a TIBCO EMS Appliance Setup Interface session. See [Initializing the Software](#) for a list of parameters.

show

This command prints a list of files of the specified type for the EMS server instance, and the timestamps indicating when each file was last modified. Only in the case of log files, this command also prints the size of each log file in bytes.

```
show instance logs|certs|cores
```

<i>instance</i>	The EMS server instance. Must be either 0 or 1.
-----------------	---

<code>logs</code>	Prints a list of log files.
<code>certs</code>	Prints a list of SSL certificate files.
<code>cores</code>	Prints a list of core reports, if any exist. The core reports are not instance-specific.



To view the contents of a file, use the **export** command to copy or move the files to the file transfer directory, then retrieve the files using the `tibfile` user.

To view the most recent lines in a log file, use the **log-show** command.

start

This command starts the EMS server instances on the appliance or on a fault tolerant pair of appliances.

```
start scope
```

<i>scope</i>	Valid values are: <ul style="list-style-type: none"> <code>local</code> Both EMS server instances on the local appliance are started. <code>ft-pair</code> All EMS server instances on both appliances in the fault tolerant pair are started.
--------------	--

stop

This command stops the EMS server instances on the appliance or on a fault tolerant pair of appliances.

```
stop scope
```

<i>scope</i>	Valid values are: <ul style="list-style-type: none"> <code>local</code> Both EMS server instances on the local appliance are stopped. <code>ft-pair</code> All EMS server instances on both appliances in the fault tolerant pair are stopped.
--------------	--

upgrade-software

Installs a TIBCO Enterprise Message Service™ Appliance software upgrade that has been previously uploaded to the file transfer directory by the `tibfile` user.

```
upgrade-software [file-name]
```

<i>file-name</i>	The name of the software package to be installed. If no file name is specified, upgrade-software displays a list of installation packages that have been uploaded and are available for installation.
------------------	---



Review any migration instructions in the Release Notes before using the **upgrade-software** command. Failure to review and follow any specific upgrade instructions contained therein may result in system downtime.

This command assumes that the upgrade will be applied to both appliances in a fault tolerant pair. To minimize downtime and ensure maximum data availability, after upgrading the first appliance in a pair you should wait for it to reboot fully and to successfully transition from wait-for-peer to standby-replicating state before upgrading its peer appliance.

To upgrade the software:

1. As the `tibfile` user, upload the software package to each machine by way of SFTP. The package must be added to the `/system/import` directory. For details, see [Working with the File Transfer Directory](#).
2. In the CLI for the first appliance, issue the `upgrade-software` command, specifying the uploaded package name. Use the command as shown in the following example:

Package Name	Command
TIB_emsa_3.0.1_illumos_F64.pkg	EMS CLI> <code>upgrade-software</code> TIB_emsa_3.0.1_illumos_F64.pkg

This command stops the EMS server instances on the appliance, applies the update, and reboots the machine in wait-for-peer state. For best results, wait for the servers to reach replicating state before upgrading the peer appliance.

3. In the CLI for the second appliance, issue the same **upgrade-software** command, specifying the software package name.

The command stops the EMS server instances, applies the update, and reboots the machine. The pair then synchronizes and resumes activity.



If you are using Central Administration to configure the EMS server on your appliance, then after completing the upgrade you must also refresh the server instances in Central Administration.

During system startup that follows the reboot triggered by an **upgrade-software** command, additional upgrade tasks take place if needed. If you log in to the CLI before all the upgrade and startup tasks have completed, the CLI displays progress information until the system is fully ready.



If additional user actions are required to complete the upgrade, these actions are also noted in the CLI. These actions can include additional reboots of the appliance. This is normal; you can log back in following the reboot to continue monitoring the upgrade progress.

Any and all additional upgrade tasks are described in the Release Notes. Review the migration instructions there to ensure that you are familiar with any additional upgrade tasks before beginning the upgrade procedure.

version-show

Prints the version numbers for selected software components. Include this information when communicating with TIBCO Support.

```
version-show
```

Disaster Recovery Commands

The commands listed here can be used for disaster recovery of the TIBCO Enterprise Message Service™ Appliance.

dr-activate

Issue this command on the DR leader to active disaster recovery backup services on a quad of appliances.

```
dr-activate
```

This command is only available on the DR leader, and will only be successful if [key-join](#) has already been called on the other DR members to establish disaster recovery communications. The **dr-activate** command does the following:

- Pushes the DR configuration information and DR key from the DR leader to DR members.
- Establishes communications with all DR members.
- Disables instance services at the backup site.
- Enable the data synchronization service for each EMS server instance on the production site appliances.

See [Enabling Disaster Recovery](#) for more information about configuring disaster recovery.

dr-recover

The **dr-recover** command is normally executed from the Backup-A appliance, but in the event that Backup-A is off-line, may be issued from Backup-B.

```
dr-recover
```

This command will only be successful if the production site is inactive or unreachable.

When called, **dr-recover** does the following:

1. Verify the production site is inactive.
2. Verify connectivity to Backup-B.
3. Synchronize with the most recent snapshot from the production site. Synchronization erases all prior EMS server data from the backup site and overwrites it with the server data from the production site snapshot.
4. Synchronize with Backup-B.
5. Activate TIBCO Enterprise Message Service™ services.
6. Verify that EMS instances on Backup-A and Backup-B are fully operational.

Should one of the Backup appliances also be down, the available backup appliance can be recovered in single appliance recovery mode.

dr-restore

This command restores activity to the production site and reestablishes DR backup processes following a DR scenario.

```
dr-restore [-force]
```

The **dr-restore** command is active only on the Backup site, and is normally issued from Backup-A. However, if Backup-A is unavailable, you can issue the command from Backup-B by specifying the **-force** flag.

When called, **dr-restore** does the following:

1. Verifies connectivity within the quad.
2. Deactivates EMS server instances on the production appliances, if any are running.
3. Deactivates EMS server instances on the backup appliances, if any are running.
4. Generates final file system snapshots on the backup site appliances.
5. Pushes snapshots to the Production site appliances.
6. Starts TIBCO Enterprise Message Service services.
7. Verify that EMS instances on Production-A and Production-B are fully operational.

For more information, see [Restoring the Production Site](#).

key-accept

This command allows DR members joining the quad to fetch the DR key. The command is only available on the DR leader (generally Production-A).

```
key-accept [off]
```

off

The optional off argument can be used to complete the keying sequence when an appliance needs to rejoin a running cluster. When included, the off argument terminates access to the public key and pushes key and DR information to connected and configured DR members.

Note that `key-accept off` is not needed if the `dr-activate` command is used.

This command is deprecated and may be removed in a future release. The `key-accept` command is no longer necessary. DR members automatically publish public data for other DR members to use during `key-join`.

During `key-join`, DR members automatically request an update from the DR leader so they can finish the join sequence.

key-join

This command causes a DR member to request the DR key from the DR leader.

```
key-join
```

key-reset

This command pushes a new DR key from the DR leader to DR members.

```
key-reset
```

The DR members must have already joined before `key-reset` is issued. Use `dr-check` to ensure that all members are appropriately joined before issuing `key-reset`.

Configuration Setup Commands

The commands listed here can be used to make changes to the configuration of the TIBCO Enterprise Message Service™ Appliance.

Before you can access these commands, you must initiate a TIBCO EMS Appliance Setup Interface session using the `setup-enable` command.

For details, see [Using the CLI to Make Configuration Changes](#).

config-apply

This command applies all pending configuration changes that have been saved in the current or a previous TIBCO EMS Appliance Setup Interface session.

```
config-apply
```



If changes were made to the fault tolerance or EMS server settings with `ft-config` or `ems-config`, issuing `config-apply` causes the EMS server instances to restart.



If `eds-config` run with `no` is applied, all encrypted store data will be completely removed from both machines in the fault tolerant pair.

Before applying configuration changes, you must save them using the `config-save` command.

config-pending

Prints a list of saved (but not yet applied) configuration changes.

```
config-pending
```

Before applying configuration changes, you must save them using the [config-save](#) command. The changes listed here will be applied when the [config-apply](#) command is issued.

config-revert-pending

The command causes the appliance to discard all configuration changes that have been saved but not yet applied.

```
config-revert-pending
```

Only changes that are listed by the [config-pending](#) command are discarded. Changes that have not been saved are not affected by this command.

config-revert-unsaved

The command causes the appliance to discard all configuration changes that have not been saved.

```
config-revert-unsaved
```

Only changes that are listed by the [config-review](#) command are discarded. Changes that have been saved are not affected by this command.

config-review

This command shows all configuration changes that have been made but not saved.

```
config-review
```

The listed changes will be saved when the [config-save](#) command is issued.

config-save

This command saves, but does not apply, all changes that have been made during the TIBCO EMS Appliance Setup Interface session.

```
config-save
```

The command affects all changes that are listed by the [config-review](#) command.



Unsaved changes are persisted till the end of the current CLI session. If you exit the Setup Interface, unsaved changes are still available to be saved if you reenter it. When you exit the main CLI session, all unsaved changes are discarded.

dr-config

If you initialized the software for an appliance without enabling DR, or if you would like to change your disaster recovery configuration settings, use this command to set up disaster recovery information.

```
dr-config
```

For an explanation of the prompts that follow this command and their settings, see [Configure Disaster Recovery](#). For details about enabling and activating disaster recovery, see [Enabling Disaster Recovery](#).



If DR is already active, services should be disabled prior to changing the configuration.

After making configuration changes, such as entering a new IP address, you must re-run the [key-join](#) and [dr-activate](#) commands.

eds-config

This command allows you to configure the appliance to support encrypted data storage.

```
eds-config
```

It is currently available only on high-performance models. Running this command on a standard model results in an error.

Before using this command, you must import the `KEYSERVER.pem` and `KEYSERVER_CA.pem` certificate files into the TIBCO Enterprise Message Service™ Appliance using the `import 0 certs` command. This enables the appliance to communicate with the KMIP key server.

The default certificate file names are `KEYSERVER.pem` and `KEYSERVER_CA.pem`. You do not need to modify these file names. However, if you need to modify them you can do so:

1. Use the `export 0 certs` command to export the `eds-params.json` file.
2. Modify `key_server` parameters to specify the new file names.
3. Re-import the `eds-params.json` file using the `import` command.

When issued, the `eds-config` command offers the following prompts.

Prompt	Description
Do you want to enable encrypted stores? [y/n](no):	Enter y to enable encrypted data storage. Note that when you enable encrypted stores, the EMS server instances on both appliances of a fault tolerant pair are stopped, and you will not be able to access them through the EMS-IP address. After the changes are applied and confirmed, the servers are restarted.
Do you want to proceed (y/n)?	Enter y to proceed, or n to exit the setup.
EDS Key Server IP Address [addr:port]():	Enter the IP address and port, or hostname and port for the encrypted data key server. For example: <code>interop3.cryptsoft.com:5696</code>
Encrypted store allocation(5G):	Enter the disk size for the storage. This represents the maximum amount of disk space the encrypted store can use on the appliance. Specify the size as an integer using M to indicate megabytes or G for gigabytes. For example, 350M or 6G. If no value is entered, a default of 5G is used. Once configured, the encrypted storage is treated like any other appliance disk. Low disk space is reported with appliance health checks.

Issue Ctrl-d at any time to exit the command. Note that if you exit after enabling encrypted data storage but before providing the key server address, you will receive an error if you try to apply your changes.

When you apply your encrypted data storage configuration, the appliance validates that the KMIP key server is reachable before proceeding to create the encrypted store. If the server is not reachable, or if the encrypted store fails to mount for any reason, the EMS servers are not started.



When you choose the initial EDS pool size, keep in mind that the initial DR synchronization sends the fully allocated EDS store, for example, 5G by default. This could impact the DR synchronization initialization time as the full pool size will need to be transmitted to the backup site on the initial send. During any subsequent synchronizations, only changed blocks are sent.

You can also use this command to disable the encrypted data storage. Keep in mind that the appliance automatically shuts down the EMS servers when disabling the encrypted data storage. Before disabling encrypted stores, you must remove all encrypted stores that are using the ESSD store location from the TIBCO Enterprise Message Service™ Appliance server configurations.

ems-config

Use this command to change the EMS server configuration that was specified during software initialization.

```
ems-config
```



If you make changes to the configuration of a server in a fault tolerant pair, you must also make change to its peer using the **ft-config** command. If the appliance settings are not in sync, the EMS servers will not be able to connect after a restart.

For an explanation of the prompts that follow this command and their settings, see [Configure EMS Server Information](#).

ft-config

Use this command to enable fault tolerance, or to change fault tolerant configuration settings that were entered during software initialization.

```
ft-config
```



If you make changes to the configuration of a server in a fault tolerant pair, you must also make change to its peer using the **ems-config** command. If all appliance settings or the EMS server settings are not the same, the EMS servers will not be able to connect after a restart.

For an explanation of the prompts that follow this command and their settings, see [Configure Fault Tolerant Behavior](#).

health-check-config

Option to enable an EMS status port for external entities, such as a load balancer, to easily check on EMS server readiness using a standard http interface.

This port supports two standard HTTP GET probes:

- `/isLive` returns 200 if the server is running
- `/isReady` returns 200 if the server is active (as opposed to standby).

Enter a port number to turn the setting **on**.

Once a port is set, enter two single quotes ' ' in lieu of an existing port value, to turn the setting **off**.

To set `health-check-config`, log into the appliance and open the EMS Setup CLI.

Run the `health-check-config` command as seen in the following example:

```
health-check-config
Now entering setup...
Ctrl-d can be used to prematurely exit.
Use ' ' (two single quotes) to delete an existing value.
Health Check webserver port for Instance 0(): <enter port number>
Health Check webserver port for Instance 1(): <enter port number>
```

Once you have entered the ports, save and then apply the changes using the following commands:

```
config-save
config-apply
```

The following ports numbers cannot be used for this command:

- Port 1024 and below.
- Port 9990.
- Additionally, any EMS or peer EMS ports that are currently set, are also unavailable.

hostinfo-config

Use this command to change generic host information, such as DNS servers.

```
hostinfo-config
```

For an explanation of the prompts that follow this command and their settings, see [Configure Host Information](#).

initial-config

Use this command to prompt for all configuration parameters.

```
initial-config
```

This command repeats the initial appliance setup. For an explanation of the prompts that follow this command, see [Initializing the Software](#), specifically these tasks:

1. [Configuring Appliance Users](#)
2. [Configuring Host Information](#)
3. [Configuring EMS Server Information](#)
4. [Configuring Fault Tolerant Behavior](#)
5. [Configuring Disaster Recovery](#)

mgmt-config

Use this command to change management interface networking parameters.

```
mgmt-config
```

For an explanation of the prompts that follow this command and their settings, see [Configure Management Information](#).

set-timezone

Sets a new time zone, as specified by time-zone.

```
set-timezone [time-zone]
```

time-zone	<p>If no time-zone is specified, or if time-zone is not a recognized time zone, the command-line enters an interactive mode which prompts you through the time zone selection process.</p> <p>Specify the time zone by entering a time zone name from the tz database.</p> <p>For example, America/New_York or US/Eastern are both valid settings. Lists of time zone names are available online: http://en.wikipedia.org/wiki/List_of_tz_database_time_zones.</p>
-----------	--



This command is saved and applied immediately, without need to issue the **config-save** or **config-apply** commands. However, the appliance must be rebooted before the new time zone setting takes effect.

syslog-config

This command configures the appliance to transmit important log messages to a remote syslog daemon, commonly known as a collector.

```
syslog-config
```

Only messages of priority notice and higher are transmitted to the collector. When entered, **syslog-config** returns the following prompt:

```
Enter the IP address where syslog messages will be sent ():
```

Enter the IP address where the collector is located to begin transmitting log messages.



Note that the **syslog-config** command does not stop the default logging behavior. Even after this command is called, the appliance continues to write log messages of all levels to a local log file.

Instance Management Commands

The following commands are used to manage a single EMS server instance.

The commands listed here are used to manage a single EMS server instance. This gives you greater control over the individual EMS server instances if an EMS server goes down in a fault-tolerant environment. These commands are only needed when maintenance must be performed on one EMS instance while the other instance is still in production servicing clients and must not be disturbed.

call-tibemsadmin

This command logs into the admin tool associated with the specified, local EMS server.

```
call-tibemsadmin instance
```

<i>instance</i>	The EMS server instance. Must be either 0 or 1.
-----------------	---

Refer to the *TIBCO Enterprise Message Service User's Guide* for more information on this tool.

forcestart-instance

This command forces the EMS server instance to go into a standalone state if the EMS server instance is in the wait-for-peer state.

```
forcestart-instance instance
```

<i>instance</i>	The EMS server instance. Must be either 0 or 1.
-----------------	---

start-instance

This command starts the specified local EMS server instance.

```
start-instance instance
```

<i>instance</i>	The EMS server instance. Must be either 0 or 1.
-----------------	---

stop-instance

This command stops the specified local EMS server instance.

```
stop-instance instance
```

<i>instance</i>	The EMS server instance. Must be either 0 or 1.
-----------------	---

switch-active

This command allows you to switch the active TIBCO Enterprise Message Service™ Appliance for the specified EMS server instance.

```
switch-active instance
```

<i>instance</i>	The EMS server instance. Must be either 0 or 1.
-----------------	---

This command is valid only in a fault-tolerant environment where there are two TIBCO Enterprise Message Service™ Appliances.

Diagnostics and Troubleshooting Commands

These commands are only available within the **Diagnostics** menu, that can be accessed using the `diagnostic-enable` command.

disk-check

This command prints out detailed information about storage devices on the TIBCO Enterprise Message Service™ Appliance.

```
disk-check [free-space|stores|devices]
```

<code>free-space</code>	(Default.) If used, this option lists the usage information about ROOT, HDD, and SSD disks.
<code>stores</code>	If used, this option lists all database files along with their sizes for each EMS server instance.
<code>devices</code>	If used, this option lists raw diagnostic information about the appliance's internal disks.

dr-check

This command runs general DR diagnostics and reports the results to the CLI.

```
dr-check [comm|snapshots]
```

<code>comm</code>	(Default.) If used, allows you to check the communication between cluster members.
<code>snapshots</code>	If used, this option lists the creation date and size of local DR snapshots.

log-audit

This command lists TIBCO Enterprise Message Service™ Appliance log files that are larger than the size that you have specified in the command.

```
log-audit [size]
```

<i>size</i>	<p><i>size</i> is a number or a number followed by B, K, M, or G (for Bytes, Kilobytes, Megabytes, Gigabytes).</p> <p>The default size is 2G.</p> <p>If you do not specify the letter after the number, the default size accepted will be in bytes.</p>
-------------	---

log-remove

This command removes the selected TIBCO Enterprise Message Service™ Appliance log files.

```
log-remove [instance] target [options]
```

<i>instance</i>	(Optional.) The instance optional argument specifies an instance-specific log file.
<i>target</i>	<p>Can be a log file name or rotations.</p> <p>If target is a log file, the named file gets deleted.</p>

The following *options* are available:

<code>-age <i>dates</i></code>	-age specifies the minimum number of days since a file was modified. Any file that hasn't been modified in more than the number of days specified with -age option gets deleted. The default is 30 days.
<code>-size <i>bytes</i></code>	-size specifies the minimum size of the file required to be deleted. Any file larger than the size specified is deleted. The default is 2G.

log-rotate

This command rotates the TIBCO Enterprise Message Service Appliance log files.

```
log-rotate [instance] filename
```

<i>instance</i>	(Optional.) The instance argument specifies an instance-specific log file where instance may be either 0 or 1.
<i>filename</i>	(Optional.) If you do not specify the filename argument, this command rotates the TIBCO Enterprise Message Service Appliance logs by default, otherwise the file you specify gets rotated. You can rotate any log file with this command.

log-truncate

This command edits the specified log file so that the first 100MB and last 100MB are saved.

```
log-truncate [instance] filename
```

<i>instance</i>	(Optional.) The <i>instance</i> argument specifies an instance-specific log file. Must be either 0 or 1. It can only be called on log files larger than 200MB. Files smaller than 200MB will be unchanged.
<i>filename</i>	If the filename is not a rotation, then it is forcefully rotated.

network-check

This command wraps a variety of network utilities that may be used for debugging.

```
network-check [options] action [parameters]
```

Missed heartbeats and other agent messages can be diagnosed with this command.

The following *action parameters* are available:

<code>connect <i>ipaddr</i> [-p <i>port</i>]</code>	Tests the ability to make a TCP connection to <i>ipaddr</i> (Default port is 22 for SSH).
<code>ping <i>arguments</i></code>	Calls the Solaris built-in ping with any given arguments.
<code>traceroute <i>arguments</i></code>	Calls the Solaris built-in traceroute with any given arguments.
<code>ifconfig</code>	Calls <code>ifconfig -a</code> , which prints out information about appliance interfaces.
<code>netstat</code>	Calls <code>netstat -nr</code> , which prints out routing tables for both IPv4 and IPv6.

The following values for *options* are available:

<code>-fg</code>	Runs the network-check command in the foreground and disables logging. The progress can be seen in the CLI window.
<code>-t <i>timeout</i></code>	Specifies the maximum time for the command to run before aborting. For example, the time it would take before the ping command would stop trying to ping an unreachable host.

peer-login

This command opens a CLI SSH session to the target TIBCO Enterprise Message Service™ Appliance.

`peer-login target`

<i>target</i>	<p>Values can be :</p> <ul style="list-style-type: none"> • <code>crosslink</code> The SSH connection is made using the dedicated crosslink connection to its fault tolerant peer • <code>ems</code> The connection is opened over the peer's TIBCO Enterprise Message Service server IP address. • <i>IP address</i> The connection is opened with SSH directly to the tibadm login at the given IP address.
---------------	--

port-disable

This command disables the specified port on the TIBCO Enterprise Message Service™ Appliance.

`port-disable port`

<i>port</i>	<p>Values can be:</p> <ul style="list-style-type: none"> • <code>crosslink</code> disables all ports used by the crosslink, which is the cabled connection between two appliances. These are ports 30, 31, and 32. • <code>uplink</code> disables all ports used by the uplink, which is the cabled connection to the EMS network. These are ports 41 and 42. • <i>number</i> disables the specified port, where <i>number</i> is one of the following ports: 30, 31, 32, 41, or 42. Enter multiple ports in a comma-separated list, with no spaces.
-------------	---

port-enable

This command enables the specified port on the TIBCO Enterprise Message Service™ Appliance.

`port-enable port`

<i>port</i>	<p>Values can be:</p> <ul style="list-style-type: none"> • crosslink enables all ports used by the crosslink, which is the cabled connection between two appliances. These are ports 30, 31, and 32. • uplink enables all ports used by the uplink, which is the cabled connection to the EMS network. These are ports 41 and 42. • number enables the specified port, where <i>number</i> is one of the following ports: 30, 31, 32, 41, or 42. Enter multiple ports in a comma-separated list, with no spaces.
-------------	--

port-show

This command displays formatted information about the specified port.

```
port-show port
```

<i>port</i>	<p>Values can be:</p> <ul style="list-style-type: none"> • crosslink Shows information about ports 30, 31, and 32. • uplink Shows information about ports 41 and 42.
-------------	--

pstack-instance

This command creates a log file containing the pstack information for the specified EMS server instance.

```
pstack-instance instance
```

<i>instance</i>	The EMS server instance. Must be either 0 or 1.
-----------------	---

The pstack information is captured in the `pstack.log` file, which can be accessed along with other log files using the [export](#) command.



Each subsequent issuance of the **pstack-instance** command automatically rotates the log file.

remove-certs

This command deletes certificates from the EMS server instance.

```
remove-certs instance
```

<i>instance</i>	The EMS server instance. Must be either 0 or 1.
-----------------	---

remove-cores

This command deletes core files from the EMS server instance.

```
remove-cores
```

remove-snapshots

This command removes Disaster Recovery (DR) snapshots from TIBCO Enterprise Message Service™ appliance.

```
remove-snapshots [-all]
```

-all	By default, the latest snapshot is not removed. If you use the option -all, the latest snapshot is also removed.
------	---

This command should only be run when DR services are disabled.

If used inappropriately, this command can prevent a successful recovery of the data. For example, if you remove snapshots from the production site without removing them from the backup site you could have problems with data recovery.



If you use the -all option to remove snapshots from a member of a DR cluster, then you should run **remove-snapshots -all** on both DR Backup appliances to ensure correct snapshot numbering going forward.

remove-transfers

This command deletes all files in the /tib-transfer directory and its subdirectories.

```
remove-transfers
```

reset-all

This command restores the appliance to a pre-setup state without requiring a reboot.

```
reset-all
```



All existing data on the appliance is deleted.

session-timeout

This command prints or changes the timeout, in minutes, of the current session.

```
session-timeout minutes
```

<i>minutes</i>	(Optional.) If provided, the command changes the timeout to the specified <i>minutes</i> .
----------------	--

uplink-config

This command allows you to change how the appliance connects to the EMS network by customizing the uplink configuration. The **uplink-config** command both applies the new setting immediately and saves the setting for use on subsequent system reboots.

```
uplink-config [ -show | -default | explicit-options ]
```

The uplink connection refers to the cabled connection between the appliance and your EMS network. By default, the appliance is connected to the network using two cables on ports 41 and 42. The connection is trunked using the LACP protocol. By default, on startup only port 41 is enabled. In the case of an outage on port 41, port 42 may be manually enabled. However, should port 41 fail on an appliance that is part of a fault tolerant configuration, client connectivity is maintained through failover to the peer appliance.



The default uplink configuration is compatible with most networks. Should your installation require a custom uplink configuration, verify that everything else is working properly before modifying the uplink.



Prior to making a permanent change to the configuration, you should test network switch LACP configuration using the **port-enable 42** command.



After making changes to the uplink configuration, verify with your network team that your new configuration is stable and performing properly.

Supported options are:

<code>-show</code>	Displays the current saved configuration settings of the uplink connection. Note: If the uplink has been manually modified, the saved configuration may be different from the currently running configuration. (For example, you might manually modify the connection using the port-enable or port-disabled commands.) Use port-show uplink to verify the currently active settings. Note: Depending on the trunk protocol, some fields in the uplink-config -show output are unused.
<code>-default</code>	Resets the uplink configuration and restores all settings to the default.

Explicit options are used to define a new uplink trunk configuration. The available *explicit-options* are:

<code>-proto {lacp lag}</code>	Specifies the protocol to use for the trunk.
<code>-enabled port[,port]</code>	Specifies the port(s) to be automatically enabled on startup. To enable both ports, separate the port numbers by a comma with no spaces. For example, <code>-enabled 41,42</code> . Only the specified ports will be enabled after the uplink-config command is issued with the <code>-enabled</code> option. That is, <code>uplink-config -enabled 42</code> results in only port 42 being enabled, even if port 41 was enabled before the command was issued.
<code>-speed</code>	Indicates the uplink speed. Note that this speed must match the type of the cable connecting the appliance to the network. This speed is set during the initial appliance setup, and normally does not need to be specified during uplink-config . The default is 10g.

Examples

This example shows the default uplink configuration.

```
uplink-config -proto lacp -enabled 41
```

The next example defines a standard two-port LAG trunk.

```
uplink-config -proto lag -enabled 41,42
```

This following example defines an LACP trunk with both ports enabled.

```
uplink-config -proto lacp -enabled 41,42
```

Troubleshooting

If performance using the EMS-IP address is erratic or not performing correctly after the initial setup, this may be an indication that the uplink network-switch has not been configured correctly.

The following issues are symptoms of a misconfigured uplink:

- timeouts

- slow connections
- network switch error messages regarding MAC moves

To address these errors, you can issue **uplink-config -default** to restore the uplink to its default settings, which is compatible with most networks and should resolve the problems while you work with your network team to make further configuration changes.

zone-admin

This **zone-admin** command is a diagnostic command to either reboot the management zone or export the management zone log files.

```
zone-admin <action>
```

where <action> can be any one of the following:

reboot	reboot the mgmt-zone
get-logs	export zone logs files

The mgmt-zone handles the Mgmt-gateway for SSH access when the EMS Gateway is active. In cases where SSH access through the Mgmt-IP stops working, this command can be used to restart the mgmt-zone without hindering the EMS server traffic.

```
zone-admin restart
```

To export the zone log files, use the following command:

```
zone-admin get-logs
```