

# **TIBCO Enterprise Message Service™**

## **Central Administration**

*Software Release 8.4  
August 2017*

## 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.

This document contains confidential information that 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, Two-Second Advantage, TIB, Information Bus, TIBCO Enterprise Message Service, TIBCO Rendezvous, TIBCO Enterprise, TIBCO SmartSockets, TIBCO ActiveMatrix BusinessWorks, and TIBCO Hawk are either registered trademarks or trademarks of TIBCO Software Inc. in the United States and/or other countries.

Enterprise Java Beans (EJB), Java Platform Enterprise Edition (Java EE), Java 2 Platform Enterprise Edition (J2EE), and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle Corporation in the U.S. and 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. SEE THE README FILE FOR THE AVAILABILITY OF THIS SOFTWARE VERSION ON A SPECIFIC OPERATING SYSTEM PLATFORM.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT.

THIS DOCUMENT COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN; THESE CHANGES WILL BE INCORPORATED IN NEW EDITIONS OF THIS DOCUMENT. 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.

Copyright © 1997-2017 TIBCO Software Inc. All rights reserved.

TIBCO Software Inc. Confidential Information

# Contents

<b>Figures</b> .....	<b>vii</b>
<b>Tables</b> .....	<b>ix</b>
<b>Preface</b> .....	<b>xi</b>
Related Documentation .....	xii
TIBCO Enterprise Message Service Documentation .....	xii
Other TIBCO Product Documentation .....	xii
Third Party Documentation .....	xiii
Typographical Conventions .....	xiv
Connecting with TIBCO Resources .....	xvii
How to Join TIBCOCommunity .....	xvii
How to Access TIBCO Documentation .....	xvii
How to Contact TIBCO Support .....	xvii
<b>Chapter 1 Introduction</b> .....	<b>1</b>
Overview of Central Administration .....	2
Requirements .....	2
Structure .....	3
How Configuration Changes are Saved and Deployed .....	4
JSON Configuration Files .....	6
<b>Chapter 2 Running the Central Administration Server</b> .....	<b>7</b>
Starting and Stopping the Central Administration Server .....	8
Create a Data Directory .....	8
Create a Configuration File .....	8
Start the Central Administration Server .....	9
Stop the Central Administration Server .....	16
Running the Central Administration Server as a Windows Service .....	17
Removing the Central Administration Server Windows Service .....	18
Security Considerations .....	19
Configuring JAAS Authentication .....	20
Configuring SSL Connections with EMS Servers .....	21
Configuring HTTPS Connections with Web Browsers .....	22
Configuring Cipher Suites .....	23

<b>Chapter 3 Navigating Central Administration</b>	<b>25</b>
Accessing the Central Administration Web Interface	26
Navigating the Web Interface	27
Server List Page	27
Server Overview Page	28
Deployments Page	29
Common Navigation Tools	29
<b>Chapter 4 Using Central Administration</b>	<b>33</b>
Adding EMS Servers to Central Administration	34
Add a Server	34
Duplicate an Existing Server	34
Rename a Server Configuration	35
Remove a Server from Central Administration	36
Viewing the Server Configuration	37
Locking the Server	38
Lock Conflicts	38
Revert — Release a Lock	38
Editing Server Configurations	39
Overview of Editing Process	39
Using Index Pages	40
Deploying Configurations	42
Deploy All Locked Servers	44
Redeploy a Previous Configuration	45
Review the Deployment Logs	46
Refreshing the Server Configuration	48
Monitoring Servers	49
Temporary Server Tracing Options	49
Monitor Destination Activity	50
Detail Pages	51
<b>Chapter 5 Properties Pages</b>	<b>53</b>
Destinations	54
Topics	54
Queues	54
Durables	54
Bridges	54
Connections	55
Transports	55
Factories	56
RVCM	56

Routes .....	56
Server .....	57
Server Properties .....	57
Stores .....	58
Fault Tolerance .....	58
Trace/Log .....	58
Validation .....	58
JSON Source .....	59
Security .....	60
Users .....	60
Groups .....	60
ACLs .....	61
LDAP .....	61
SSL .....	61
<b>Appendix A Converting Server Configuration Files to JSON .....</b>	<b>63</b>
<b>Index .....</b>	<b>65</b>



# Figures

Figure 1      Central Administration Structure .....3

Figure 2      Central Administration — Flow of Information .....5





# Tables

Table 1	General Typographical Conventions . . . . .	xiv
Table 2	Syntax Typographical Conventions . . . . .	xv
Table 3	Central Administration Server Options . . . . .	9
Table 4	Command Icons . . . . .	30
Table 5	Manipulating Items Icons . . . . .	31
Table 6	Filtering Lists — Regular Expression Semantics . . . . .	40



# Preface

TIBCO is proud to announce the latest release of TIBCO Enterprise Message Service™ 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 software and other TIBCO products are powered by TIB® technology, please visit us at [www.tibco.com](http://www.tibco.com).

TIBCO Enterprise Message Service software lets application programs send and receive messages according to the Java Message Service (JMS) protocol. It also integrates with TIBCO FTL, TIBCO Rendezvous, and TIBCO SmartSockets messaging products.

## Topics

---

- [Related Documentation, page xii](#)
- [Typographical Conventions, page xiv](#)
- [Connecting with TIBCO Resources, page xvii](#)

## Related Documentation

---

This section lists documentation resources you may find useful.

### TIBCO Enterprise Message Service Documentation

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

- *TIBCO Enterprise Message Service User's Guide* Read this manual to gain an overall understanding of the product, its features, and configuration.
- *TIBCO Enterprise Message Service Central Administration* Read this manual for information on the central administration interface.
- *TIBCO Enterprise Message Service Installation* Read the relevant sections of this manual before installing this product.
- *TIBCO Enterprise Message Service C & COBOL Reference* The C API reference is available in HTML and PDF formats.
- *TIBCO Enterprise Message Service Java API Reference* The Java API reference can be accessed only through the HTML documentation interface.
- *TIBCO Enterprise Message Service .NET API Reference* The .NET API reference can be accessed only through the HTML documentation interface.
- *TIBCO Enterprise Message Service Release Notes* Read the release notes for a list of new and changed features. This document also contains lists of known issues and closed issues for this release. This document is available only in PDF format.

### Other TIBCO Product Documentation

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

- TIBCO FTL<sup>®</sup>
- TIBCO Rendezvous<sup>®</sup>
- TIBCO SmartSockets<sup>®</sup>
- TIBCO EMS<sup>®</sup> Client for z/OS (CICS)
- TIBCO EMS<sup>®</sup> Client for z/OS (MVS)
- TIBCO EMS<sup>®</sup> 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.
- Java™ Authentication and Authorization Service (JAAS) *LoginModule Developer's Guide* and *Reference Guide*, available through <http://www.oracle.com/technetwork/java/javase/jaas/index.html>.

# Typographical Conventions

The following typographical conventions are used in this manual.

Table 1 General Typographical Conventions

Convention	Use
<i>TIBCO_HOME</i> <i>ENV_NAME</i> <i>EMS_HOME</i>	<p>TIBCO products are installed into an installation environment. A product installed into an installation environment does not access components in other installation environments. Incompatible products and multiple instances of the same product must be installed into different installation environments.</p> <p>An installation environment consists of the following properties:</p> <ul style="list-style-type: none"><li>• <b>Name</b> Identifies the installation environment. This name is referenced in documentation as <i>ENV_NAME</i>. If you specify a custom environment name, on Microsoft Windows the name becomes a component of the path to the product shortcut in the Windows Start &gt; All Programs menu.</li><li>• <b>Path</b> The folder into which the product is installed. This folder is referenced in documentation as <i>TIBCO_HOME</i>. The value of <i>TIBCO_HOME</i> depends on the operating system. For example, on Windows systems, the default value is C:\tibco.</li></ul> <p>TIBCO Enterprise Message Service installs into a directory within <i>TIBCO_HOME</i>. This directory is referenced in documentation as <i>EMS_HOME</i>. The value of <i>EMS_HOME</i> depends on the operating system. For example on Windows systems, the default value is C:\tibco\ems\8.4.</p>
code font	<p>Code font identifies commands, code examples, filenames, pathnames, and output displayed in a command window. For example:</p> <p>Use MyCommand to start the foo process.</p>
bold code font	<p>Bold code font is used in the following ways:</p> <ul style="list-style-type: none"><li>• In procedures, to indicate what a user types. For example: Type <b>admin</b>.</li><li>• In large code samples, to indicate the parts of the sample that are of particular interest.</li><li>• In command syntax, to indicate the default parameter for a command. For example, if no parameter is specified, MyCommand is enabled: MyCommand [<b>enable</b>   disable]</li></ul>

Table 1 General Typographical Conventions (Cont'd)




Convention	Use
<i>italic font</i>	<p>Italic font is used in the following ways:</p> <ul style="list-style-type: none"> <li>To indicate a document title. For example: See <i>TIBCO ActiveMatrix BusinessWorks Concepts</i>.</li> <li>To introduce new terms. For example: A portal page may contain several portlets. <i>Portlets</i> are mini-applications that run in a portal.</li> <li>To indicate a variable in a command or code syntax that you must replace. For example: <code>MyCommand PathName</code></li> </ul>
Key combinations	<p>Key name separated by a plus sign indicate keys pressed simultaneously. For example: <code>Ctrl+C</code>.</p> <p>Key names separated by a comma and space indicate keys pressed one after the other. For example: <code>Esc, Ctrl+Q</code>.</p>
	The note icon indicates information that is of special interest or importance, for example, an additional action required only in certain circumstances.
	The tip icon indicates an idea that could be useful, for example, a way to apply the information provided in the current section to achieve a specific result.
	The warning icon indicates the potential for a damaging situation, for example, data loss or corruption if certain steps are taken or not taken.

Table 2 Syntax Typographical Conventions

Convention	Use
[ ]	<p>An optional item in a command or code syntax.</p> <p>For example:</p> <pre>MyCommand [optional_parameter] required_parameter</pre>
	<p>A logical OR that separates multiple items of which only one may be chosen.</p> <p>For example, you can select only one of the following parameters:</p> <pre>MyCommand para1   param2   param3</pre>

Table 2 Syntax Typographical Conventions

Convention	Use
{ }	<p>A logical group of items in a command. Other syntax notations may appear within each logical group.</p> <p>For example, the following command requires two parameters, which can be either the pair param1 and param2, or the pair param3 and param4.</p> <pre>MyCommand {param1 param2}   {param3 param4}</pre> <p>In the next example, the command requires two parameters. The first parameter can be either param1 or param2 and the second can be either param3 or param4:</p> <pre>MyCommand {param1   param2} {param3   param4}</pre> <p>In the next example, the command can accept either two or three parameters. The first parameter must be param1. You can optionally include param2 as the second parameter. And the last parameter is either param3 or param4.</p> <pre>MyCommand param1 [param2] {param3   param4}</pre>



## Connecting with TIBCO Resources

---

### How to Join TIBCOCommunity

TIBCOCommunity is an online destination for TIBCO customers, partners, and resident experts. It is a place to share and access the collective experience of the TIBCO community. TIBCOCommunity offers forums, blogs, and access to a variety of resources. To register, go to <https://community.tibco.com>.

### How to Access TIBCO Documentation

Documentation for this and other TIBCO products is available on the TIBCO Documentation site. This site is updated more frequently than any documentation that might be included with the product. To ensure that you are accessing the latest available help topics, please visit us at:

<https://docs.tibco.com/products/tibco-enterprise-message-service>

Documentation for TIBCO products is not bundled with the software. Instead, it is available on the TIBCO Documentation site at <https://docs.tibco.com>.

### How to Contact TIBCO Support

For comments or problems with this manual or the software it addresses, contact TIBCO Support as follows:

- For an overview of TIBCO Support, and information about getting started with TIBCO Support, visit this site:

<https://www.tibco.com/services/support>

- If you already have a valid maintenance or support contract, visit this site:

<https://support.tibco.com>

Entry to this site requires a user name and password. If you do not have a user name, you can request one.



## Chapter 1 **Introduction**

This chapter contains a general overview of Central Administration components and architecture.

### Topics

---

- [Overview of Central Administration, page 2](#)
- [Structure, page 3](#)
- [JSON Configuration Files, page 6](#)

## Overview of Central Administration

---

Central Administration for TIBCO Enterprise Message Service is a tool that allows administrators to make changes to multiple EMS server configurations and deploy those as a single action.

The major benefits of Central Configuration are:

- **Graphical User Interface** Central Administration provides a web-based graphical user interface (GUI) for configuring TIBCO Enterprise Message Service servers.
- **Centralized Configuration** You can also apply configuration changes across multiple TIBCO Enterprise Message Service servers from a single location.

## Requirements

In order to use Central Administration, you must meet these requirements:

- **Administrative Privileges** The Central Administration user who deploys changes to an EMS server must have administrative permissions to modify any EMS server setting.

The same username and password used to log in to the Central Administration web interface is used to log on to the EMS server. When JAAS authentication is not configured, the Central Administration server uses the default credentials of user `admin` with no password.

See [How the Central Administration Server Connects to the EMS Server on page 19](#) for more information.

- **JSON Configuration Files** EMS servers must use configuration files based on JavaScript Object Notation (JSON). In software release 7.0, TIBCO Enterprise Message Service introduced an EMS server configuration method based on JSON configuration files. Text-based `.conf` files are not supported using Central Administration.

See [JSON Configuration Files on page 6](#) for information about JSON files and steps to convert old server configuration files to JSON.

- **Supported Browser** The Central Administration web interface can be accessed using browsers supported by their respective vendors at the time of writing. HTML 5-compliant browsers with JavaScript enabled are supported. See the readme file for a full list of supported browsers.

## Structure

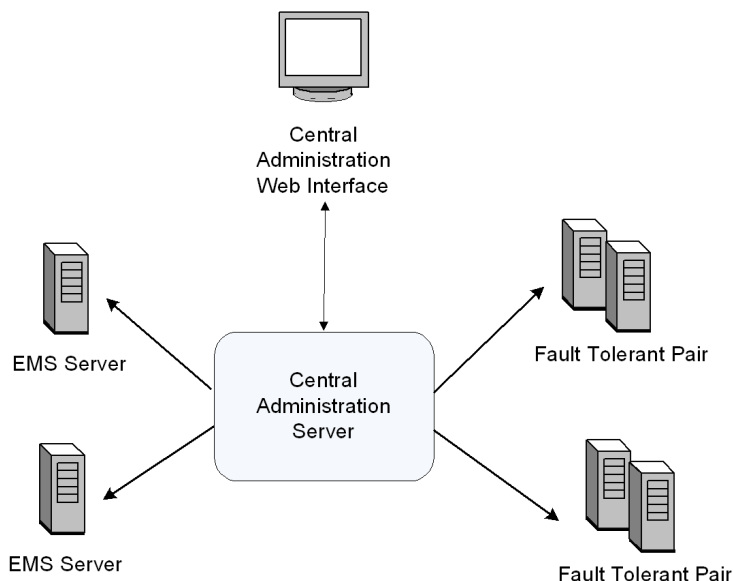
Central Administration offers a simple architecture. The Central Administration server connects to TIBCO Enterprise Message Service servers and stores a snapshot of the configuration from the running EMS server.



Be aware that the snapshot of the EMS server may not reflect its current running configuration. Because it's possible to modify the running EMS server with direct edits to the JSON configuration file, programming API calls, or commands issued through the administration tool, Central Administration may be out-of-sync with the running configuration.

Administrators connect to the Central Administration server through the web interface, and from there can view the snapshot server configurations, make changes, and deploy the new configurations.

*Figure 1 Central Administration Structure*



## How Configuration Changes are Saved and Deployed

The Central Administration server stores configuration files for each EMS server it manages in two directories:

- The **working directory** stores the last read configuration from the EMS server. It also stores the **lock file**, which contains the edits being made by a user to a server configuration.
- The **deployment directory** contains details on each deployment of the EMS server. This directory contains only records of configuration files that have already been deployed using Central Administration.

All commands issued through the Central Administration web interface modify the server configuration files in these two directories. [Figure 2](#) shows which files are modified for each action performed through the Central Administration web interface:

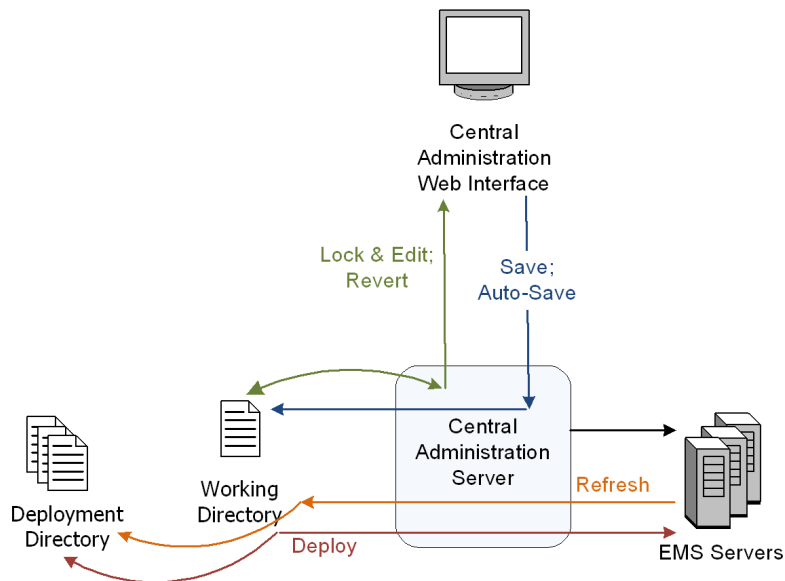
- **Lock & Edit** enables the user to make changes to the configuration. As the user edits the configuration, the edits are saved in the lock file.
- **Save** saves configuration changes made to the EMS server through the web interface to the lock file. Note that changes are also automatically saved at regular intervals, even if the user does not click Save.
- **Deploy** takes the configuration lock file from the working directory, and deploys it to the EMS server. If the deployment succeeds, the lock file is copied to the deployment directory for the current deployment and to the working file for the EMS server.

If deployment fails, the lock file is not copied to the deployment directory. It remains in the working directory and can be further edited and redeployed, or the lock can be reverted and changes discarded.

Note that the EMS server keeps a copy of the previous JSON configuration file upon receiving a deployment from the Central Administration server. When the deployment is successful, the previous configuration is kept in a file of the same name as the current configuration with an additional `.bak` suffix. For example, `tibemsd.json.bak`. During subsequent deployments, the backup file is overwritten.

- **Refresh** causes the Central Administration server to retrieve the currently deployed configuration file from the running EMS server, and save that file in the working directory. This is the only way to obtain configuration changes made directly to the EMS server. (That is, changes that were not made through Central Administration.)

Figure 2 Central Administration — Flow of Information



## JSON Configuration Files

---

When Central Administration is used, TIBCO Enterprise Message Service stores server configuration settings in a single JSON-based configuration file. This file holds the entire configuration of the server without the need of sub-files. Furthermore, a single JSON configuration file holds the configuration settings for a pair of fault tolerant servers. JSON-based configuration files use the `.json` file extension.

The JSON configuration standard was introduced in TIBCO Enterprise Message Service software release 7.0. With TIBCO Enterprise Message Service software release 6.x and earlier, the configuration of the EMS server was stored in a set of text-based configuration files with names ending in `.conf`. The main configuration file name defaults to `tibemsd.conf` and a set of sub-files such as `queues.conf` hold information on specific types of configuration items. These configuration files are described in Chapter 7, *Using the Configuration Files of the TIBCO Enterprise Message Service User's Guide*.

An EMS server can be started either with a set of `.conf` files or with a single `.json` file. However, the EMS server can be managed through the Central Administration feature only if it has been started with the JSON file. EMS servers started with a set of `.conf` files cannot be managed using the Central Administration server.

You can convert an EMS 6.x or later text-based server configuration to a single `tibemsd.json` file using the `tibemsconf2json` utility, which is described in [Appendix A, Converting Server Configuration Files to JSON](#).



## Chapter 2

# Running the Central Administration Server

This chapter describes the basic setup and configuration of the Central Administration server.

### Topics

---

- [Starting and Stopping the Central Administration Server, page 8](#)
- [Running the Central Administration Server as a Windows Service, page 17](#)
- [Security Considerations, page 19](#)

## Starting and Stopping the Central Administration Server

---

This section describes how to start and stop the Central Administration server.

### Create a Data Directory

Before starting the Central Administration server for the first time, you must create a data directory for the server. This directory is where the server stores deployment and working directories for each EMS server it manages.

You cannot share the data directory between Central Administration server instances. That is, each running Central Administration server requires its own data directory.

On startup, the Central Administration server looks for a data directory named `emsc_data` in the working directory. If you wish to specify a different name or location, use the `--data` command line option or related configuration file property to point the server to the correct location.

### Create a Configuration File

You can optionally create a configuration file to hold Central Administration server options, and pass this file to the server at startup. The properties that can be specified in the configuration file correspond to the startup options, and are described in [Table 3, Central Administration Server Options, on page 9](#).

The configuration file takes the form of a typical Java properties file and must use the `.properties` file extension. In a text-based file, specify one property on each line, using the format:

*property=value*

For example:

```
com.tibco.emsca.data.dir=/emsc_data
com.tibco.emsca.http.hostport=:8080
com.tibco.emsca.jaas=/emsc_security/emsc.jaas
```

By default, the Central Administration server looks for a file named `emsc.properties` in the current directory. However, you can direct the server to a different file using the `--config` command line option.



If an argument is passed to the Central Administration executable that is also configured in the file, the value provided in the command line overrides the value in the configuration file.

## Start the Central Administration Server

To start the Central Administration server from the command line, navigate to `EMS_HOME/bin` and run the script:

On UNIX

`tibemsca [options]`

On Windows

`tibemsca.bat [options]`



If the Central Administration server cannot locate the data directory, startup aborts. For more information see [Create a Data Directory](#) above.

To configure Central Administration server settings, use the command line arguments shown in [Table 3](#).

The command options to Central Administration server can also be passed using a configuration file described above in [Create a Configuration File](#). However, the command options override any value specified in the configuration file.

Table 3 Central Administration Server Options

Short	Long	Arguments	Description
-h	--help		Display a help message describing the command line parameters and options.
-d	--data	<i>path</i>	<p>Specifies the working data directory. The Central Administration server stores its working data files in the <i>path</i> given. This location must exist.</p> <p>If this argument is not specified, the default is to store working data files in a directory called <code>emsca_data</code> within the current working directory.</p> <p>You can also configure the working directory by setting the system property or configuration file property named <code>com.tibco.emsca.data.dir</code>.</p> <p>If you run several distinct Central Administration servers, you must supply a unique <i>path</i> location for each server.</p>

Table 3 Central Administration Server Options

Short	Long	Arguments	Description
-ht	--http	host:port	<p>Specifies the HTTP user interface host and port. Browsers send graphic user interface requests (using the HTTP protocol) to this service. You may specify <i>host:port</i>, or just <i>port</i>.</p> <p>If this argument is not present, the default is *:8080. Note that * implies all interfaces on the machine.</p> <p>When specifying the host and port on the command line, you must escape the argument if the * character is specified. For example, on Windows platforms:</p> <pre>-ht " *:4545 "</pre> <p>This is a requirement for shell scripts determined by the operating system.</p> <p>You can also configure the HTTP interface by specifying the configuration property <code>com.tibco.emsca.http.hostport</code>.</p>
-c	--config	path	<p>Points the Central Administration server to a file containing configuration properties. For more information see <a href="#">Create a Configuration File on page 8</a>.</p> <p>By default, the server looks for the file <code>emsca.properties</code> in the current directory.</p>

Table 3 Central Administration Server Options

Short	Long	Arguments	Description
-j	--jaas	<i>path</i>	<p>Configures the Central Administration server to configure security using the Java Authentication and Authorization Service (JAAS).</p> <p>When present, the Central Administration server configures security using the JAAS configuration file at <i>path</i>. When absent, the server neither requires nor verifies credentials.</p> <p>You can also configure JAAS using the property <code>com.tibco.emsca.jaas</code>.</p> <p>For more information on JAAS security, see <a href="#">Configuring JAAS Authentication on page 20</a>.</p>
-ja	--jaas-admins	<i>names</i>	<p>Replaces the default JAAS <code>emsca-admin</code> group with one or more admin group names. Administrators running Central Administration utility executables must be in one of these admin groups.</p> <p>Group names should not contain spaces or commas. Specify multiple admin groups in a comma-separated list.</p> <p>This parameter can also be specified in a configuration file as the property <code>com.tibco.emsca.jaas.admin.roles</code>.</p>
-jg	--jaas-guests	<i>names</i>	<p>Replaces the default <code>emsca-guest</code> group with one or more guest group names. JAAS guests can browse configurations, but are not able to modify, monitor, or deploy configurations.</p> <p>Group names should not contain spaces or commas. Specify multiple guest groups in a comma-separated list.</p> <p>This parameter can also be specified in a configuration file as the property <code>com.tibco.emsca.jaas.guest.roles</code>.</p>

Table 3 Central Administration Server Options

Short	Long	Arguments	Description
	<code>--concurrent-tasks</code>	<i>number</i>	<p>Specifies the number of concurrent deployment tasks that can be active at any one time during a deployment. Each deployment task implies a connection to an EMS server.</p> <p>The <i>number</i> given should be greater than 0. If this argument is not present, the default is 10 concurrent tasks.</p> <p>You can also configure the concurrent deployments using the property <code>com.tibco.emsca.concurrent.tasks</code>.</p>
	<code>--keep-max-deployments</code>	<i>number</i>	<p>Specifies the maximum number of deployments to keep. If the number of deployments exceeds this number, the older deployments are removed.</p> <p>Default is set to -1 (keep all deployments).</p> <p>This parameter can also be specified in a configuration file as the property <code>com.tibco.emsca.max.deployments</code>.</p>

Table 3 Central Administration Server Options

Short	Long	Arguments	Description
	<code>--ssl-ciphers</code>	<i>string</i>	<p>Optional. Can be used if <code>--ems-ssl-identity</code> or <code>--https-identity</code> is provided.</p> <p>Specifies the cipher suites to be used by SSL connections, either for the Central Administration server to connect to EMS servers using SSL or for accepting Web browser connections using the HTTPS protocol, or for both.</p> <p>The specified string must use the Java Client Syntax, as described in the <i>TIBCO Enterprise Message Service User's Guide</i>.</p> <p>For example:</p> <pre>-ALL:+TLS_RSA_WITH_AES_128_CBC_SHA:+TLS_RSA_WITH_AES_256_CBC_SHA</pre> <p>This parameter can also be specified in a configuration file as the property <code>com.tibco.ems.ssl.ciphers</code>.</p>

Table 3 Central Administration Server Options

Short	Long	Arguments	Description
<b>Central Administration to EMS Server SSL Communication Options</b>			
These options specify SSL settings between Central Administration and EMS servers. When configured in Central Administration, the server uses SSL to communicate with the EMS server. Note that neither hosts nor hostnames are verified.			
	<code>--ssl-policy</code>	<i>policy</i>	<p>Sets the SSL policy for the Central Administration server. This optional flag specifies the policy of iteration over the EMSCA Deployment Listens when communicating with an EMS server. Note that the Central Administration server only communicates with the EMS server using the EMSCA Deployment Listens specified on the <a href="#">Server Properties</a> page.</p> <p>Valid <i>policy</i> settings are:</p> <ul style="list-style-type: none"><li>REQUIRED — The Central Administration server only communicates with an EMS server using SSL listens. Any other type of listen is ignored.</li><li>PREFERRED — The Central Administration server attempts to communicate with an EMS server using SSL. If all the SSL listens for the EMS server fail, it then attempts non-SSL listens.</li><li>ANY — The Central Administration server attempts to connect through any of the listens defined in the configuration.</li></ul> <p>When absent, this option is set to ANY.</p> <p>You can also configure the SSL policy using the <code>com.tibco.emsca.ssl.policy</code> parameter.</p>



Table 3 Central Administration Server Options

Short	Long	Arguments	Description
	<code>--ems-ssl-identity</code>	<i>path</i>	<p>Optional flag specifying the path to a certificate providing the identity of the Central Administration server to EMS servers. The identity certificate must include its private key.</p> <p>If the <code>--ems-ssl-identity</code> option is provided and <code>--ems-ssl-password</code> is not, the login screen to the Central Administration web interface presents fields for username, password, and certificate password. This scenario is only supported when JAAS is configured.</p> <p>You can also include the identity by including the property <code>com.tibco.ems.ssl.identity</code>.</p> <p>For more information, see <a href="#">Configuring SSL Connections with EMS Servers</a> on page 21.</p>
	<code>--ems-ssl-password</code>	<i>string</i>	<p>Provides the SSL password associated with the private key or store set with the <code>--ems-ssl-identity</code> flag. This setting is optional.</p> <p>If the <code>--ems-ssl-password</code> option is provided with <code>--ems-ssl-identity</code>, the Central Administration server does <i>not</i> prompt for a certificate password.</p> <p>Note that providing a password on the command line is not recommended and may pose a security risk. Consider configuring this property using a configuration file. If you must provide the password on the command line or in a configuration file, please use <code>tibemsadmin -mangle</code> to generate an obfuscated version first.</p> <p>You can include the password in a configuration file using the <code>com.tibco.ems.ssl.password</code> parameter.</p>

Table 3 Central Administration Server Options

Short	Long	Arguments	Description
<b>Central Administration to Web Browser HTTPS Communication Options</b>			
These options specify HTTPS settings between Central Administration and web browsers.			
When configured, the Central Administration server uses HTTPS to communicate with web browsers.			
	<code>--https-identity</code>	<i>path</i>	<p>Optional flag specifying the path to a PKCS12 file or Java KeyStore that provides the identity of the Central Administration server to browsers. The file must include the certificate and the corresponding private key.</p> <p>When present, starts the web server port using the HTTPS protocol instead of HTTP.</p> <p>The <code>--https-identity</code> option must be specified with the <code>--https-password</code> option.</p> <p>This parameter can also be specified in a configuration file as the property <code>com.tibco.emsca.https.identity</code>.</p>
	<code>--https-password</code>	<i>string</i>	<p>Optional flag specifying the password to the identity file specified through <code>--https-identity</code>.</p> <p>Note that providing a password on the command line is not recommended and may pose a security risk. Consider configuring this property using a configuration file. If you must provide the password on the command line or in a configuration file, please use <code>tibemsadmin -mangle</code> to generate an obfuscated version first.</p> <p>This parameter can also be specified in a configuration file as the property <code>com.tibco.emsca.https.password</code>.</p>

Stop the Central Administration Server

You can stop the Central Administration server by ending the process using tools provided by your operating system.

## Running the Central Administration Server as a Windows Service

You can register the Central Administration server to run as a Windows service, enabling the server to start automatically.



This process is supported for version 8.3.0 or higher of EMS Central Administration. It is not supported for earlier versions.

### Task A Create an EMS Central Administration configuration file.

The configuration file is described in [Create a Configuration File on page 8](#).

For example, create a file `C:\directory\emscs.properties` with this content:

```
com.tibco.emsca.data.dir=C:/directory/emscs/data
com.tibco.emsca.http.hostport=*:8888
```

### Task B Register the Windows Service.

Use the `prunsrv` utility to register the Windows Service. The `prunsrv` utility is included in the `bin` directory of your EMS installation:

```
EMS_HOME\bin\prunsrv.exe
```

Model your command line on this template:

```
prunsrv install service-name
--DisplayName="TIBCO EMS Central Administration"
--Description="Allows administrators to make changes to multiple
EMS server configurations and deploy those as a single action."
--Install="EMS_HOME\bin\prunsrv.exe"
--Jvm="path-to-jvm.dll"
--StartMode=jvm
--StopMode=jvm
--StartClass=com.tibco.messaging.emsca.internal.CentralAdminServer
--StopClass=com.tibco.messaging.emsca.internal.CentralAdminServer
--StartParams=-c;"C:\directory\emscs.properties"
--StopMethod stop
--Classpath="EMS_HOME\bin\tibemscs.jar;EMS_HOME\lib\jms-2.0.jar
;EMS_HOME\lib\tibjms.jar;EMS_HOME\lib\tibjmsadmin.jar;EMS_HOM
E\bin\jetty-all.jar;EMS_HOME\bin\json_simple-1.1.jar"
```

Note the following aspects of this command line template:

- You need the *service-name* that you chose when you use the Windows `sc` command. For example, `sc start service-name`.
- `--Install` is the full path of the `prunsrv` executable.

- `--Jvm` is the full path to version 1.8 or later of `jvm.dll`. For example, `"C:\jre1.8.0\bin\server\jvm.dll"`.
- Specify `--StartMode`, `--StopMode`, `--StartClass`, `--StopClass` and `--StopMethod` exactly as shown in this template.
- `--StartParams` contains the command line parameters for EMS Central Administration, which you can adjust to your specification. Use a semicolon (;) to separate parameters. You must include the Central Administration configuration file that you created in [Task A](#).
- `--Classpath` lists the JAR files that EMS Central Administration requires. You must specify all of these files and replace `EMS_HOME` with the actual path.

### Task C *Optional*. Modify the parameters of the service as needed.

Once the Central Administration server has been registered through `prunsrv`, you can modify the parameters of the service using the `prunmgr` utility:

```
prunmgr //ES/service-name
```

The `prunmgr` utility is included in the `bin` directory of your EMS installation. More information about `prunsrv` and `prunmgr` is available through <http://commons.apache.org/proper/commons-daemon/>.

## Removing the Central Administration Server Windows Service

To remove the Central Administration server from the Windows Service registry, run the following command:

```
prunsrv delete service-name
```

where *service-name* is the name given when the service was installed.

## Security Considerations

By default, the Central Administration server does not impose security restrictions. That is, it is not automatically configured to use SSL connections or to require login credentials from users. However, you can configure the server to require user credentials, to use SSL when connecting with EMS servers, and to use HTTPS when accepting web browser connections.



The Central Administration server uses the same username and password to log into the EMS server as was used to log in to the Central Administration web interface. When JAAS authentication is not configured, the Central Administration server uses the default credentials of user `admin` with no password.

### How the Central Administration Server Connects to the EMS Server

The Central Administration server connects to the EMS server when:

- The EMS server is added to Central Administration.
- A user refreshes the EMS server configuration stored in Central Administration.
- A user deploys a configuration change.

#### Credentials

Each time it connects to the EMS server, the Central Administration server presents the credentials passed to it by the user when he or she logged on to the web interface.

- If JAAS authentication is *not* configured, the Central Administration server uses the `admin` user, with no password, to authenticate with all the EMS servers.
- If JAAS authentication *is* configured, the Central Administration server presents the user ID and password presented when the current user logged on. If the user is attempting to deploy configuration changes but does not have the necessary administrative privileges for the EMS server, the deployment fails.

#### SSL

When SSL is configured on the EMS server, the Central Administration server can optionally use SSL to communicate with the EMS server. In addition, the Central Administration server can use an identity certificate to authenticate itself to the EMS server.



When Central Administration uses SSL connections to communicate with an EMS server, neither the host nor hostname are validated by Central Administration.

## Configuring JAAS Authentication

You can configure the Central Administration server to use Java Authentication and Authorization Service (JAAS) authentication. JAAS authentication has two purposes:

- Authenticate users logging into the Central Administration server.

When JAAS is configured, users must enter credentials when logging into the Central Administration web interface. Central Administration users must be in one of these JAAS groups:

- `emsca-admin` — Grants administrative privileges to members. Administrators may lock and edit an EMS server in Central Administration, and deploy an updated server configuration. However, note that the user must *also* have administrative privileges for the EMS server before deploying.

You can change the group names with administrative privileges using the `--jaas-admins` option.

- `emsca-guest` — Grants read-only privileges to members. Guest users are not able to make changes or deploy configurations through Central Administration.

You can change the group names with guest privileges using the `--jaas-guests` option.

- Authenticate the Central Administration server to EMS servers.

When JAAS is configured, each time a user attempts to add or refresh an EMS server or deploy configuration changes, the Central Administration server uses the JAAS user ID and password presented by the user to authenticate with the EMS server. If the user does not have sufficient privileges, the action fails.



When using JAAS, you should not create a user name that has the same name as a JAAS group. Depending on the JAAS implementation, it is possible for a user name matching a group name to be included in the group.

Additionally, assigning conflicting JAAS roles, such as guest and admin, to the same user grants admin privileges.

To enable JAAS authentication, set the `--jaas` option at the command line, or through the related setting in the Central Administration configuration file.

JAAS can be configured to fetch user credentials from a property file or from an LDAP server. With LDAP, changes made to Central Administration user credentials are taken into account dynamically. With a property file, it is required to restart the Central Administration server upon altering user credentials.

For more information on JAAS security, see the sample configuration files in `EMS_HOME\samples\emsc\jaas`.

## Configuring SSL Connections with EMS Servers

You can configure the Central Administration server to use SSL when connecting to EMS servers.



The Central Administration server does *not* verify hostnames or hosts.

There are two supported configuration scenarios: when the EMS server requires an identity certificate from the Central Administration server, and when the EMS server does not require an identity. All EMS servers managed by Central Administration should use the same SSL configuration scenario.

The SSL scenario is determined by EMS server requirements. Depending on these requirements, further SSL settings are configured either through command line options when the Central Administration server is started, or by setting configuration parameters in the Central Administration configuration file:

- **SSL without Central Administration Identity**

The Central Administration server uses SSL to connect to the EMS server. This option is only available if EMS servers do not require an identity from connecting services.

This SSL configuration is determined entirely by the EMS server. No options or parameters are set in the Central Administration server.

- **SSL with Central Administration Identity**

If the EMS server requires an identity, the Central Administration server can be configured to supply an identity certificate and certificate password.

The syntax and use of these SSL configuration options are further documented in [Table 3, Central Administration Server Options, on page 9](#):

- Enable SSL using the `--ems-ssl-identity` command line option, or through the related setting in the Central Administration configuration file. This option sets the path to the identity certificate and private key that the Central Administration server uses when identifying itself to the EMS servers.
- Provide the SSL password associated with the private key by setting the `com.tibco.ems.ssl.password` parameter. The command line option `--ems-ssl-password` is also available, but providing a password on the command line is not recommended and may pose a security risk. Use

`tibemsadmin -mangle` to generate an obfuscated version before providing the password in either configuration file or command line.

If you do *not* provide the password using the parameter or flag, the Central Administration server requires the SSL decryption password when you log in. Note that this option is only available if JAAS is configured.

- Specify an SSL policy using the `--ssl-policy` command line option, or through the related setting in the Central Administration configuration file. By default, the Central Administration server attempts to connect through any of the listens defined in the EMS server configuration, regardless of whether they are SSL connections or not. Alternately, you can either "require" or "prefer" an SSL connection. If you require SSL, the server will not communicate with the EMS through a non-SSL connection. If you prefer SSL, SSL connections are attempted first.

For more information on using SSL in TIBCO Enterprise Message Service, see *Using the SSL Protocol in the TIBCO Enterprise Message Service User's Guide*.

## Configuring HTTPS Connections with Web Browsers

You can configure the Central Administration server to accept HTTPS connections from web browsers.

To configure this, provide Central Administration with an identity certificate and certificate password either through command line options when the Central Administration server is started or by setting configuration parameters in the Central Administration configuration file.

The syntax and use of these SSL configuration options are documented in [Table 3, Central Administration Server Options, on page 9](#):

- Enable HTTPS using the `--https-identity` command line option, or through the related setting in the Central Administration configuration file. This option sets the path to a PKCS12 file or Java KeyStore providing the identity of the Central Administration server to browsers. When HTTPS is enabled, it replaces HTTP on the same port number.
- Provide the SSL password associated with the private key by setting the `com.tibco.emsca.https.password` parameter. The command line option `--https-password` is also available, but providing a password on the command line is not recommended and may pose a security risk. Use `tibemsadmin -mangle` to generate an obfuscated version before providing the password in either configuration file or command line.



For testing purposes, you can configure Central Administration with the identity file `emsca_https_identity.p12` that is provided in the `samples/certs` directory and use the corresponding self-signed root certificate with your web browser. For restrictions and details, see the `readme.txt` file in the same directory.

## Configuring Cipher Suites

If desired, you can specify the cipher suites to be used when the Central Administration server uses SSL to connect to EMS servers or accepts web browsers connections with the HTTPS protocol.

To configure this feature, you can either provide a cipher suite specification with the `--ssl-ciphers` command line option when the Central Administration server is started, or set a configuration parameter in the Central Administration configuration file. Both methods accept the Java Client Syntax described in the *TIBCO Enterprise Message Service User's Guide*. This is further documented in [Table 3, Central Administration Server Options, on page 9](#).



## Chapter 3

# Navigating Central Administration

This chapter describes the Central Administration web interface. This includes the layout and navigation of the interface, as well as common navigational tools and icons.

## Topics

---

- [Accessing the Central Administration Web Interface, page 26](#)
- [Navigating the Web Interface, page 27](#)

## Accessing the Central Administration Web Interface

---

Once the Central Administration server is running, you can access it from a web browser. The location of the web interface is:

`http://host:port`

where *host* and *port* are specified when the Central Administration server is configured, either through the command line or in the configuration files. If no *host* or *port* are specified, the default is:

`http://localhost:8080`

**Login** If the Central Administration server has been configured to use JAAS security, you will need to log in. Enter your User Name and Password, and click **Login**.

**Browser Support** HTML 5-compliant browsers with JavaScript enabled are supported. For a list of supported browsers, see the readme file.

## Navigating the Web Interface

---

The Central Administration web interface is designed to be intuitive and easy to navigate. Upon login, you are presented with the [Server List Page](#), which shows a list of all EMS servers managed by this Central Administration instance. To view or edit the configuration settings for an EMS server, click the server name and you are taken to the [Server Overview Page](#). This page is a gateway to all configuration options for that server.


The [Deployments Page](#) is also accessed from the Server List page. This page provides details about every deployment executed from Central Administration. [Common Navigation Tools](#), such as breadcrumbs and sidebars, provide quick access to top-level pages from sub-pages.

The sections below describe each of these primary pages and the tasks you can perform from the page.

### Server List Page

The Server List page is the home page of the Central Administration web interface. Its main content is a complete list of EMS servers managed by the Central Administration server.

From this page, you can:

- Create or add new servers to Central Administration, and remove existing servers. See [Adding EMS Servers to Central Administration on page 34](#).
- Change the name used to identify an EMS server in Central Administration. See [Rename a Server Configuration on page 35](#).
- Refresh an EMS server's JSON configuration file that is stored in Central Administration. See [Refreshing the Server Configuration on page 48](#).
- Navigate to an EMS server's overview page, from which edits to the server configuration can be made. See [Server Overview Page](#) below.
- Navigate to the Deployments page. From here, you can view details about deployments, and revert to an earlier deployment if needed. See [Deployments Page on page 29](#).
- Navigate to the monitoring page for a listed server. To view the monitoring page for a server, click the  icon. See [Monitoring Servers on page 49](#) for details about monitoring.

## Server Overview Page

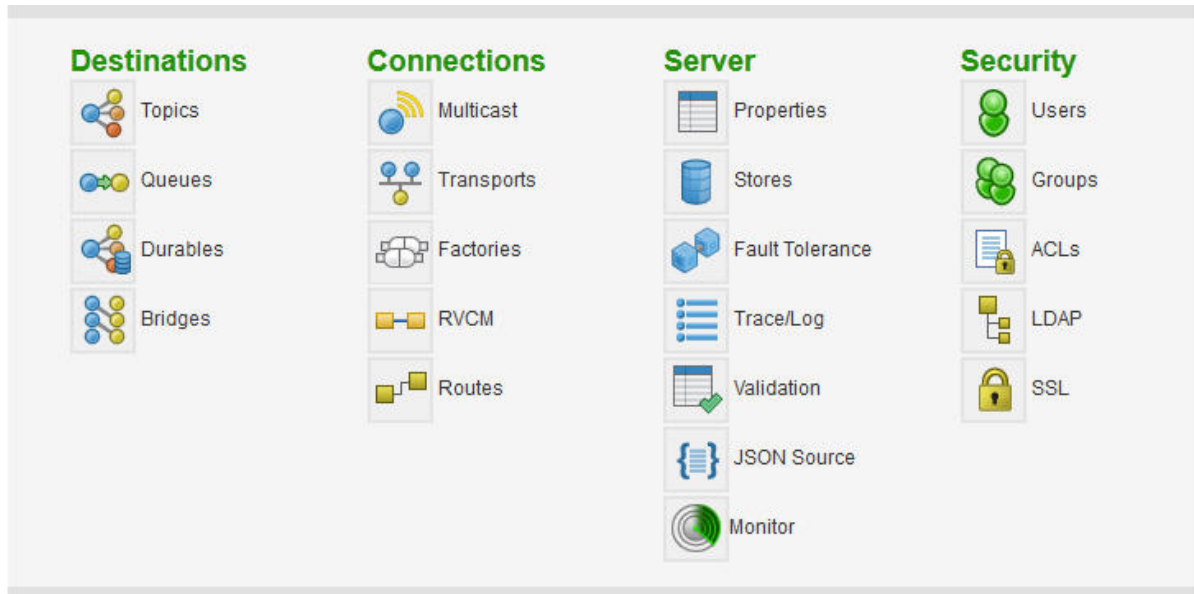
To access the overview page for an EMS server, locate the server in the Server List page and click the server name. You are taken to that server's overview page.

The Server overview page is the primary page from which you access the configuration settings of an EMS server. Its main content is a set of links to the various properties pages of the Central Administration interface.

The properties page links are organized into columns, corresponding to their uses:

- [Destinations](#) — settings related to destinations.
- [Connections](#) — settings related to connections between the server and other servers and clients.
- [Server](#) — primary server configuration settings and monitoring.
- [Security](#) — settings related to security, including user configuration, access control lists, SSL, and so forth.

Complete descriptions of these properties pages are provided in subsequent chapters.



## Deployments Page

To access the Deployments page, click the Deployments link that appears in the sidebar for the Server List page:



From this page, you can:

- View details about previous deployments. See [Review the Deployment Logs on page 46](#).
- Revert to an earlier deployment if needed. See [Redeploy a Previous Configuration on page 45](#).
- Delete a deployment from the deployment history. See [Delete a Deployment Record on page 47](#).

## Common Navigation Tools

### Home Logo

Clicking the TIBCO EMSCA logo at the top of each page returns to the main Server List page.




### Page Name and Breadcrumbs

The large titles at the top of each page indicate where you are within the server configuration. The black title indicates the name of the current page or object configuration being viewed. The green titles summarize the context of the page you are on, and let you return to pages you have recently viewed.



### Sidebar

The sidebar (visible on most pages) speeds navigation to other pages. The content of the sidebar is dependent on your current location.

- On the Server List and Deployments pages, the sidebar provides links between these two pages.
- On the EMS server property pages, the sidebar provides links to the other property pages, as well as a link back to the Server Overview page. Click server name that appears next to the home  icon.

In addition, a **Servers** link is available to return you to the Server List page.

- On all pages, a **Logout *username*** link logs the current user out of Central Administration. Note that this feature is only visible when JAAS authentication is configured.

Icons

Icons are used throughout the Central Administration web interface to give access to commonly used commands and tasks. These icons are divided into two general categories, and are described in the tables below:

- **Command Icons** Icons in the upper right corner denote commands. The available set of command icons varies depending on the state and location within the Central Administration web interface. These icons are described in [Table 4](#).
- **Manipulating Items Icons** These general-use icons can appear in several contexts within the Central Administration web interface. These icons are described in [Table 5](#).

Table 4 Command Icons



Icon	Name	Description
	Lock & Edit	<p>Grab the lock and start editing.</p> <ul style="list-style-type: none"><li>• Create a modifiable copy of the EMS server configuration file, and store it in the working directory.</li><li>• Lock the EMS server configuration file so only the current user can modify it.</li></ul> <p>If another user holds the lock, the <a href="#">Lock Conflicts</a> page opens.</p>
	Deploy	<p>Finish editing and deploy all modified EMS server configurations.</p> <ul style="list-style-type: none"><li>• Auto-save the modified configuration files of all EMS servers locked by the user to the working directory, and package them as a deployment.</li><li>• Send the deployment package to EMS servers.</li><li>• If the deployment succeeds, the web interface releases the lock, and displays the <a href="#">Deployments Page</a>.</li></ul>



Table 4 Command Icons





Icon	Name	Description
	Refresh	<p>Discard all modifications and retrieve the current configuration file from the EMS server.</p> <p>This command replaces the copy of the EMS server configuration file that is stored in the working directory with the file it retrieves from the EMS server.</p>
	Revert	<p>Undo modifications and stop editing.</p> <ul style="list-style-type: none"> <li>Discard undeployed modifications; display the current EMS server configuration.</li> <li>Release the lock.</li> </ul>
	Save	<p>Save modifications to the working directory.</p> <p>Note that the Central Administration web interface frequently auto-saves your modifications to the working directory. This command lets you force a save.</p>
	Download	<p>Download the server's JSON configuration file.</p> <p>Note that the download icon is only available from the JSON Source page.</p>

Table 5 Manipulating Items Icons







Icon	Name	Description
	Add	Add or define a new item.
	Delete	Delete an item.
	View	View more details.
	Duplicate	Make a copy of an item (as a starting point for defining a similar item).

Table 5 Manipulating Items Icons

Icon	Name	Description
	Rename	Change the name of the item.
	Undo	Undo the previous modification.

Index Pages

Index pages present a list of the items that are defined for a page. For example, Server List page includes an index of servers that are defined in the Central Administration server. Similarly, the Queues properties page offers an index of queues that are defined for the EMS server. To view details about any item in the list, click the item name.

For more information, see [Using Index Pages on page 40](#).

## Chapter 4      **Using Central Administration**

This chapter describes the steps needed to add servers to Central Administration and make and deploy configuration changes.

### Topics

---

- [Adding EMS Servers to Central Administration, page 34](#)
- [Viewing the Server Configuration, page 37](#)
- [Locking the Server, page 38](#)
- [Editing Server Configurations, page 39](#)
- [Deploying Configurations, page 42](#)
- [Refreshing the Server Configuration, page 48](#)
- [Monitoring Servers, page 49](#)

## Adding EMS Servers to Central Administration

---

This section describes the steps needed to add a running server to Central Administration, duplicate an existing server, or remove an EMS server from Central Administration.

### Add a Server

To add a running, JSON-configured `tibemsd` to Central Administration:

1. Open the Central Administration web interface. For details, see [Accessing the Central Administration Web Interface on page 26](#).
2. Navigate to the main **Server List** page in Central Administration by clicking the **Servers** link.
3. In the filter box, enter a name to identify the server. For example, `server1`. The server name entered here is used only in Central Administration and must be unique.

Names can only contain letters, digits, dashes and underscores. Spaces are not allowed.

4. Click **Create**.
5. In the box that appears, enter the URL on which the Central Administration server will connect to the EMS server. For example, `tcp://localhost:7222`.
6. Click **Add Server**.



The Central Administration server attempts to connect to the EMS server using the URL provided. After successfully connecting, the new server appears in the list of managed servers and can be accessed and configured through the web interface. The server configuration file is saved to the deployment archive.

### Duplicate an Existing Server

You can create and deploy a new EMS server by duplicating the configuration of an existing server. Duplicating a server can be used to clone a configuration, perform some changes, and deploy it to a different server. Duplicating a server is also the easiest method to change the name identifying the EMS server in the Central Administration server list. Simply provide the duplicate server with the desired name, and delete the source server after the duplication.

To duplicate an existing server:

1. Navigate to the main **Server List** page in Central Administration.

2. Locate the existing server that you wish to clone. You can quickly find the server by entering its name in the **Filter or Create** box.
3. Click the Options  icon.
4. Click the Duplicate  **Duplicate** option.
5. Enter an identifying name for the new server and click **Duplicate**.

The server name entered here is used only in Central Administration and must be unique.

Central Administration creates a copy of the server's JSON configuration file. This copy can then be edited and deployed.





The duplicate action creates an exact copy of the source EMS server configuration. All settings match the source file, including the Central Administration listen parameters. Deploying the new server without first editing these fields causes any configuration changes to be applied to the source server.

## Rename a Server Configuration

You can rename an existing EMS server configuration from the Server List page. This changes the name that is used to identify the server in Central Administration.

To rename a server:

1. Navigate to the main **Server List** page in Central Administration.
2. Locate the server. You can quickly find the server by entering its current name in the **Filter or Create** box.
3. Click the Options  icon.
4. Click the Rename  **Rename** option.
5. Enter a new name for the server and click **Rename**.

The server name entered here is used only in Central Administration and must be unique.



## Remove a Server from Central Administration

You can also remove an EMS server from Central Administration by deleting it from the Server List page. This removes the EMS server configuration file from Central Administration.



Removing an EMS server from Central Administration does not stop or otherwise change the running EMS server. The EMS server continues operating outside of Central Administration.

To remove a sever from Central Administration:

1. Navigate to the main **Server List** page.
2. Locate the existing server that you wish to remove. You can quickly find the server by entering its name in the **Filter or Create** box.
3. Click the Options  icon.
4. Click the Delete  **Delete** option.
5. In the confirmation dialog that opens, click **Delete** to remove the server or **Cancel** to leave the server in Central Administration.

When you click Delete, the server is removed from Central Administration.

## Viewing the Server Configuration

---

When JAAS is not configured in Central Administration, all users access the web interface using the same administrative credentials. As a result, if a user locks and edits the configuration, any other user can see and modify the edited configuration.


If JAAS is configured, all users can view the current configuration settings for an EMS server, although only administrators can edit the server's settings. If a configuration is locked, only the user with the lock sees the changes in progress. All other users see the current "snapshot" of the deployed EMS server.

## Locking the Server

---

In order to prevent conflicts, an administrator must obtain a lock on an EMS server before it can be edited. Only administrators may lock and edit servers. Guest users have view privileges only.

To lock a server:

1. Navigate to the [Server Overview Page](#) for the selected EMS server.
2. Click the Lock & Edit  command icon.

You may now make changes to the EMS server configuration.

### Lock Conflicts

If you attempt to lock an EMS server that has already been locked by another user, the Lock Conflict page appears.

- **Break the Lock**

Clicking this option removes any edits made by the current lock owner and reverts the file to the configuration current in the deployment archive.

- **Take the Lock**


Clicking this option retains edits made by the current lock owner, but transfers the lock to you.

To leave the lock in place with the current lock owner, click **Cancel Lock** to return to the server overview page.

### Revert — Release a Lock

If you have locked an EMS server, you can release the lock using the Revert icon. This command discards all your configuration edits and releases the lock.

To discard your edits and release the lock:

1. Navigate to the [Server Overview Page](#), or any properties page for the server.
2. Click the Revert  command icon.
3. In the dialog box that appears, click **Yes** to discard your configuration changes or **No** to cancel the action and keep the lock.



Releasing a lock without first deploying configuration changes causes Central Administration to discard all edits.



## Editing Server Configurations

---

To make edits to the EMS server configuration using Central Administration, you must have administrative privileges.

- If JAAS authentication is enabled, administrative users are determined by the JAAS authentication module. See [Configuring JAAS Authentication on page 20](#) for details.
- If JAAS is not configured, all users have administrative privileges.

Users without administrative privileges can view configuration settings, but may not make changes.

### Overview of Editing Process



The EMS server configuration stored in the working directory can be out-of-sync with the running configuration. This happens when the EMS server's configuration changed as a result of direct edits to the JSON configuration file, programming API calls, or commands issued through the administration tool. The Refresh command directs the Central Administration server to update its snapshot of the EMS server. See [Refreshing the Server Configuration on page 48](#) for more information.

To edit the configuration of an EMS server:













1. Navigate to the [Server Overview Page](#) for the EMS server you wish to edit.
2. Obtain the lock for the server. See [Locking the Server on page 38](#) for more information.
3. Make the desired edits to the configuration settings from the server properties pages. These pages are described in [Chapter 5, Properties Pages](#).
4. Review the Validation Results to locate and correct any errors in the configuration. For details, see [Validation on page 58](#).
5. Deploy the new configuration. For details, see [Deploying Configurations on page 42](#).

## Using Index Pages

Index pages are gateways to EMS server properties pages. These pages list the item definitions for a entity category. For example, there is a topics index page that lists all topics defined for the EMS server:

Server List / Server1 / Topics

Create

Name ↑	
business.inventory	 
business.orders	 
sales.>	 
sales.customers	 
sales.customers.prospective	 
sales.orders	 

6 of 6 filtered from 6 item(s).

This section describes features common to all index pages.

### Viewing an Item

To view an item in the list, click its name.

### Filtering the List

To view a subset of the items, type characters in the **Filter** or **Create** field. The list narrows to display only those items that contain the character sequence in their names.

Filters accept standard Java regular expressions using standard JavaScript regular expressions (we present a subset of the details in [Table 6](#)).

Table 6 Filtering Lists — Regular Expression Semantics

Syntax	Description
JavaScript Regular Expression Filtering	
. (dot)	Match any single character.


Table 6 Filtering Lists — Regular Expression Semantics

Syntax	Description
* (star)	Match zero or more instances of the preceding element.
+ (plus)	Match one or more instances of the preceding element.
\w	Match any word character.
[chars]	Match any single instance of the characters within square brackets.

### Creating a New Item

To create a new item, type its name in the **Filter or Create** field, then click the **Create** button or type the Enter key. The new item is created, and the relevant properties page opens. (This operation is available only when you own the lock for the EMS server; see [Locking the Server on page 38](#))

### Duplicating an Item

To duplicate a definition (as a starting point for defining a similar item) click the **Duplicate**  icon. The browser immediately displays the duplicate item in the relevant properties page for editing. (This operation is available only when you own the lock for the EMS server.)

### Deleting a Item

To delete a definition, click the **Delete** icon  corresponding to the definition. (This operation is available only when you own the lock for the EMS server.)

# Deploying Configurations

Central Administration enables users to quickly update all modified servers by deploying all servers for which the user owns the lock with one action. In other words, the deploy action deploys every EMS server locked by the current user.



The Central Administration server does not automatically update its configuration snapshot for an EMS server. If configuration changes were made directly to the EMS server, such as through API calls, you should refresh the server configuration in Central Administration before deploying. See [Refreshing the Server Configuration on page 48](#) for details.

**Permission Requirements** To deploy, the current user must have administrative credentials for each EMS server in the deployment. If you do not have adequate permissions to modify an EMS server, the deployment of that server fails.


If the user who owns the lock does not have the necessary permissions to deploy the changes, another user with administrative permissions can take the lock and deploy. See [Take the Lock on page 38](#).



**Deployment Errors** Deployment of an EMS server fails if the Central Administration encounters any errors while connecting to and updating the server. Errors include:

- Failure to connect to the EMS server.
- Inadequate permissions for the user initiating the deployment.
- Invalid settings in the new EMS server configuration.
- The configuration currently held by the EMS server was modified either through the Administration Tool or the Admin API.

Each deployment can affect a number of EMS servers, but there is no dependency between the servers. That is, some EMS servers may deploy correctly while some fail. Those servers that did not deploy can attempt redeployment later. The server lock file remains in its edited state.

**Deployment Results** Following a deployment, you can check its status in the deployment log. Review the status of each server:

-  Deployment succeeded.
  - The server accepted the changes.
  - All changes have been activated.

-  Deployment succeeded. Restart required.
  - The server accepted the changes.
  - The server requires a restart to activate the changes.
-  Deployment failed.
  - The server rejected the changes.
  - Central Administration could not connect to the server.

Because deployment succeeds or fails for each EMS server individually, deployment results may differ for each server. If deployment to an EMS server fails, that server remains locked and editable by the user.



### Fault Tolerant Configurations

When a server that is a member of a fault-tolerant pair requires a restart, both servers must be restarted to activate the change. When the active server of the fault tolerant pair is shut down, the standby server does not reinitialize its properties (such as listens, heartbeats, timeouts, and so on) during activation. It does reinitialize objects such as queues, topics, factories, routes, and so on. It also takes into account the addition, deletion, or modification of stores of type File Store.

The correct sequence when a deployment requires a restart is to:

1. Shutdown the active server.
2. Let the standby fully activate.
3. Restart the server shutdown in [step 1](#).
4. Let the restarted server reach the standby state.
5. Shutdown the server activated in [step 2](#).
6. Let the standby fully activate.
7. Restart the server shutdown in [step 5](#).


If restart can wait until a period when the servers can both remain offline for the recovery period, shutdown both servers and restart them simultaneously. In the particular case of the addition or deletion of stores of type File Store, only steps 1 to 3 are necessary.

## Deploy All Locked Servers



The deploy action deploys not only the selected server, but all servers for which the current user holds the lock. For example, if you have the lock on five servers, all five servers are updated when the deploy command is issued.

To deploy configuration changes made to EMS servers:


1. Navigate to the [Server Overview Page](#), or any properties page for an EMS server.
2. Click the Deploy  command icon.
3. In the dialog box that appears, enter an identifying name for the deployment. This name is used in the deployment archive, and will help you identify this deployment when you view its log, or should you need to redeploy at a future date.

By default, the deployment name is the date and time of the deployment: *year-month-day-hour-minute-second-millisecond*. For example, 2012-09-08-17-11-06-73 indicates a deployment on September 8, 2012 at 5:11:06:73 in the afternoon.

4. Click **Deploy**. If you wish to continue editing, click Cancel.

Once Deploy is clicked, the Central Administration server:

- deploys the working copy of the JSON configuration file to the EMS server,
- updates the deployment archive with the new current configuration,
- releases the lock on the EMS server, and
- opens the Deployments page.

5. To view details about the deployment, including any errors, click the View  icon next to the deployment name.

If some cases, the EMS server requires a restart before the configuration changes take effect. If such cases, the server deployment log notes this requirement.



6. If required, restart the EMS server. This task cannot be completed using the Central Administration web interface.

## Redeploy a Previous Configuration

If a deployment fails, you can easily roll back to a successful earlier deployment.



Only successful deployments can be redeployed. Any EMS servers that failed in the initial deployment are excluded from a redeployment. If only some of the EMS servers included in a deployment were successfully deployed, only those EMS servers are redeployed. If the initial deployment was wholly unsuccessful—none of the EMS servers deployed—the deployment is unavailable for redeployment.

1. Navigate to the Deployments page.
2. Locate the deployment that you wish to redeploy in the Recent Deployments list.
3. Click the Redeploy  icon.
4. Click **Yes** to redeploy this version of the configuration, or **No** to retain the current configuration.
5. To view details about the deployment, including any errors, click the View  icon next to the deployment name.

If some cases, an EMS server requires a restart before the configuration changes take effect. If such cases, the server deployment log notes this requirement.

6. If required, restart the EMS servers. This task cannot be completed using the Central Administration web interface.

The Central Administration server reverts all EMS servers deployed in the selected previous deployment.





Redeploying updates the EMS server but does not affect the working directory or lock file. As a result, the working copy and lock files in Central Administration are out of sync with the running EMS server.

This allows you to retain the configuration changes made prior to the redeploy. To obtain the current configuration, refresh the EMS server configuration. See [Refreshing the Server Configuration on page 48](#) for details.

## Review the Deployment Logs

A record of all deployments is maintained on the [Deployments Page](#). A log is kept for each deployment, showing providing useful details about the deployment.

To review a deployment record:

1. Navigate to the Deployments page.
2. Locate the deployment in the Recent Deployments list.
3. Click the View  icon next to the deployment name to view a summary of the deployment.
4. Click the arrow  next to the server name in the Deployment Server Log section.
5. To view the full log, click **Full server deployment log available here**. The full log includes all details about the deployment, including:
  - Configuration changes made.
  - Status of each edit made to the server.

If the deployment was redeployed, each server log for each deployment is separated by a line of hash marks: #####.



It is best to regularly review your Recent Deployment list and delete records for deployments that are insignificant and unlikely to be redeployed. This practice ensures that the list is not over-crowded, and that essential deployment records can be easily located.

### When the EMS Server Configuration was Modified Locally

If changes were made directly to the EMS server configuration using the Administration Tool or the Admin API and the corresponding configuration in Central Administration was not refreshed, you receive the following error when you attempt a deployment:

The deployment was rejected due to local changes

If this occurs, you can view the differences between the base configuration stored in Central Administration and the one held by the running EMS server, as well as between the base configuration and the configuration with the latest edits saved in the lock file that resulted in a rejected deployment. From there, you can choose which configuration to keep. This functionality is available through the **Actions** drop-down menu on the server deployment log page. Note that this menu is available only for deployments that have been rejected due to local changes.



You can choose the following actions from the Actions menu:

- View changes made in the EMS server since the last refresh. This action shows differences between the base configuration stored in Central Administration and the one held by the EMS server.
- View changes made in Central Administration since the last refresh. This action shows differences between the base configuration stored in Central Administration and the configuration with the latest edits saved in the lock file, which resulted in a rejected deployment.
- Refresh the Central Administration configuration with this server's configuration. This action discards all changes you've made in Central Administration.



If the configuration is locked, this action affects both the lock file stored in the working directory and the base configuration. Any changes you have made in Central Administration since locking the file are lost.


- Overwrite the EMS server configuration with Central Administration's configuration. This action forces the Central Administration deployment, and disregards local changes in the EMS server. You will lose changes made in the EMS server.

See [Refreshing the Server Configuration on page 48](#) for more information on updating Central Administration with changes made to an EMS server using the Administration Tool, API calls, or by directly editing the configuration file.

### Delete a Deployment Record

If desired, you can remove a failed or otherwise unwanted deployment from the Recent Deployments list. Once a deployment is deleted, you no longer have access to its logs, and cannot redeploy it.

To delete a deployment record:

1. Navigate to the Deployments page.
2. Locate the deployment that you wish to remove from the Recent Deployments list.
3. Click the Delete  icon.
4. Click **Yes** to the deployment record, or **No** to cancel and keep the record.



## Refreshing the Server Configuration

---

The Central Administration server does not automatically detect configuration changes made directly to the EMS server. That is, if changes have been made to the server configuration using the Administration Tool, API calls, or by directly editing the configuration file, the Central Administration server must be instructed to retrieve these changes from the server.

You can instruct the Central Administration server to connect to the EMS server and retrieve its current configuration. This configuration replaces the JSON configuration file stored for the server in the working directory.

To obtain the current configuration settings from a running EMS server:

1. If the server is locked, discard any changes and stop editing. If you own the lock, click the Revert  icon to discard your changes and stop editing. If another user has the lock, you may wish to break the lock. See [Break the Lock](#) for details.
2. On the Server List page, locate the server in the list of managed servers.
3. Click the  Refresh icon.
4. In the dialog box that opens, click **Yes** to update the configuration from the EMS server, or **No** to cancel.



To ensure that Central Administration has the latest EMS server configuration settings, always refresh before editing a server.

## Monitoring Servers

---

The monitoring feature, available from the Server overview page, allows you to interact with and view statistics related to a live EMS server. Statistics and details available through this interface reflect the monitoring and tracing settings configured for the server, as described in Chapter 17, *Monitoring Server Activity* in the *TIBCO Enterprise Message Service User's Guide*.



Because monitoring interacts with a live server, some monitoring activities can impact server performance.

- |               |  |
|---------------|--|
| Query Results | On any monitoring page, you can refine the results by entering a name in the Query field. Use partial names or patterns to limit the records shown. The Query field supports * and > patterns.   |
| Sort Results  | <p>You can change the sort order of the displayed records by clicking any of the column heading for any of the displayed fields.</p> <p>Clicking a header performs a local sort on the data already retrieved by the browser. It does not refresh the query.</p> |

### Temporary Server Tracing Options

You can configure temporary client tracing options for a server. These options remain active until changed, or until the server is restarted.

To configure client tracing options:

1. Navigate to the desired Server overview page.
2. Select the **Monitor** option.
3. Select the **Server** category.
4. From the Manage Server tab, select **Client Tracing...**
5. Select the desired Output Target and Filter Type, then click **Set Options**.

These options remain active until changed, or until the server is restarted. For details about the available target and filter types, see `client_trace` parameter.

## Monitor Destination Activity

Monitoring activities that report on destinations, including topics, queues and durables, can place a heavy burden on the EMS server. To minimize any negative impact on performance, a limit is placed on the number of entries that the server reviews.

If the EMS server has more than 200 destinations in the particular results screen, no data is immediately returned. Instead, you must use the query tools to refine the monitoring results:

- **Destination Name Filter** In the Query box, enter a destination name or partial name with pattern. This field supports the standard \* and > patterns.

If query results are already visible on the page, entering text in the Query box immediately filters those results. A server-side query is performed only after the **Query** button is clicked.

- **Order** Choose an order preference from this drop-down box. For example, you can choose to order results by name, subscriber count, size, or several other criterion. If you choose to order based on a numeric field, destinations with the largest value are returned first. That is, Central Administration determines the results by collecting the records with the greatest value for the specified field.
- **Retrieve Count** This tool allows you to control the number of results that are returned. The options available are:
  - **Retrieve By Page** — (Available for topics and queues only.) Retrieves a page of 50 filtered but unsorted records at a time. Use the Next and Previous buttons to retrieve additional pages or return to a previously retrieved page of results. There is no limit on the number of pages that can be requested.
  - **Retrieve Default Count** — Retrieves matching records up to the default limit of 200 items.
  - **Retrieve Max Count** — Retrieves up to 5,000 matching records.
  - **Customize** — Select this option to input the number of records you would like to retrieve. Any integer from 1 to 5000 may be entered. Note that this custom value does not apply to the Retrieve By Page option, which always retrieves 50 records per page.

Click **Query** to retrieve the list of matching records.


Note that to rank the results, Central Administration has to read and process each element. As a result, these queries can put a heavy burden on the EMS server.

## Detail Pages

Central Administration presents query results in a table. In many cases, objects in the table are linked to detailed summary pages which show monitoring statistics and runtime configuration for the inspected object. For example, on the Consumer monitoring page, each consumer entry offers a link to the related consumer ID, connection ID, and destination.

In some cases, you will need to enable the `statistics` parameter and configure detailed statistics before the EMS server will collect the desired information. For details, see Detailed Statistics in the *TIBCO Enterprise Message Service User's Guide*.

### Manage Objects

These detail pages typically provide a **Manage** menu  **Manage**, which provides the ability to manage the specified object. For example, depending on the object you may be able to refresh the data, compact, purge, or delete the object.



These commands operate on a live EMS server and their execution is not reversible. In cases where the command purges or destroys, the data in question is lost forever.



## Chapter 5      **Properties Pages**

This chapter provides a reference to the EMS server properties pages accessed through the Central Administration web interface. Links to the *TIBCO Enterprise Message Service User's Guide* provide easy navigation to parameter descriptions and usage guidelines.

### Topics

---

- [Destinations, page 54](#)
- [Connections, page 55](#)
- [Server, page 57](#)
- [Security, page 60](#)

## Destinations

---

The properties pages in the Destinations category configure EMS server destinations.

### Topics

Use the index screen to access existing topics or create a new topic.

Restrictions and rules on topic names are described in Destination Name Syntax in the *TIBCO Enterprise Message Service User's Guide*.

The fields on the properties page for each topic configure its destination properties. Full descriptions and usage information for each property is available in the Destination Properties section of the *TIBCO Enterprise Message Service User's Guide*.

### Queues

Use the index screen to access existing queues or create a new queue.

Restrictions and rules on queue names are described in Destination Name Syntax in the *TIBCO Enterprise Message Service User's Guide*.

The fields on the properties page for each queue configure its destination properties. Full descriptions and usage information for each property is available in the Destination Properties section of the *TIBCO Enterprise Message Service User's Guide*.

### Durables

Use the index screen to access existing durable subscribers or create a new durable subscriber.

The fields on the Durable properties page correspond to the parameters in the `durables.conf` configuration file.

### Bridges

Use the index screen to access existing bridges or create a new bridge between destinations.

The fields on the Bridge properties page correspond to the parameters in the `bridges.conf` configuration file.



## Connections

---

The properties pages in the Connections category configure the connections between the EMS server and other servers, clients, and messaging systems.

### Transports

Enable or disable transports between the TIBCO Enterprise Message Service server and TIBCO FTL, TIBCO Rendezvous, and TIBCO SmartSockets by clicking the relevant checkboxes.



In order to enable a transport type, you must also set the **Module Path** field on the [Server Properties](#) page.

Transport configuration fields, including the Configured Transports index screen, are available only when transports are enabled.

#### FTL Transports

Check the **Enable FTL Transports** checkbox to enable these transport types, then use the Configured Transports index screen to edit or create a new FTL transport definition.

When adding or editing a transport definition in the Configured Transports index screen, the fields available on the Transport properties page change depending on the Transport Type selected. When FTL is selected for this field, the fields shown correspond to the relevant parameters in the `transports.conf` configuration file. See also the section on Transport Definitions in the *TIBCO Enterprise Message Service User's Guide*.

#### RV and RVCM Transports

Check the **Enable RV and RVCM Transports** checkbox to enable these transport types, then use the Configured Transports index screen to edit or create a new RV transport definition.

The fields available on the Transport properties page change depending on the Transport Type selected. When RV or RVCM are selected for this field, the fields shown correspond to the relevant parameters in the `transports.conf` configuration file. See also the section on Transport Definitions in the *TIBCO Enterprise Message Service User's Guide*.

## SmartSockets Transports

Check the **Enable SmartSockets Transports** checkbox to enable these transport types.

When adding or editing a transport definition in the Configured Transports index screen, the fields available on the Transport properties page change depending on the Transport Type selected. When SmartSockets is selected for this field, the fields shown correspond to the relevant parameters in the `transports.conf` configuration file. See also the section on Transport Definitions in the *TIBCO Enterprise Message Service User's Guide*.

The **SmartSockets Config Directory** field that appears corresponds to the related TIBCO FTL Transport Parameters setting in the `tibemsd.conf` configuration file.

## Factories

Use the index screen to access existing connection factory definitions or create a new connection factory.

The fields on the Factory properties page correspond to the parameters in the `factories.conf` configuration file.

## RVCM

Use the index screen to access existing TIBCO Rendezvous certified messaging (RVCM) listeners or create a new listener.

The fields on the RVCM Listener properties page correspond to the parameters in the `tibrvcml.conf` configuration file.

## Routes

Enable or disable routes using the **Enable Routing** checkbox. The route index screen is visible only when routes are enabled.

The fields on the Route properties page correspond to the parameters in the `routes.conf` configuration file.

# Server

The properties pages in the Server category configure the basic operation of the EMS server.

## Server Properties

The fields on the Server Properties page correspond to the parameters in the `tibemsd.conf` configuration file. The fields have been organized to mirror the parameter categorization given in the *TIBCO Enterprise Message Service User's Guide*, as shown here:

Heading	See Parameter Category
Global Parameters	Global System Parameters
Network Failure Detection	Detecting Network Connection Failure Parameters
Connection and Memory	Connection and Memory Parameters
Message Tracking	Message Tracking Parameters
DB Driver	Extensible Security Parameters
JVM Parameters	JVM Parameters
Advanced Properties	None. This interface should be used only with direction from TIBCO Support.

### FT Active

The FT Active radio button determines the `ft_active` parameter setting for the secondary server. The `ft_active` setting for the primary server is determined by the Secondary Listens URL settings in the main [Fault Tolerance](#) page.

### EMSCA Deployment Listens

The URLs entered here are used by the Central Administration server to communicate with the EMS server. If fault tolerance is configured, you must add two EMSCA Deployment Listens.

## Stores

Use the index screen to access existing store definitions or create a new store.

The fields on the Store properties page change depending on the store Type selected. Fields correspond to the parameters in the `stores.conf` configuration file.

For database store parameter definitions, see the section on Configuring Database Stores in the *TIBCO Enterprise Message Service User's Guide*.

## Fault Tolerance

The Fault Tolerance properties page determines the behavior of EMS servers in a fault tolerant pair. The fields on this page correspond to the Fault Tolerance Parameters parameters in the `tibemsd.conf` configuration file, and influence the behavior of both the primary and secondary servers in the pair.

Fault tolerant pairs share a single JSON configuration file. To configure the secondary EMS server, add a Secondary Listens URL for each URL on which the EMS server should listen in the event that it becomes active. Click the **FT Active** radio button next to the Secondary Listens URL that the primary server should use to check the secondary server heartbeat.



The FT Active radio button determines the `ft_active` parameter setting for the primary server. The `ft_active` setting for the secondary server is determined by the Primary Listens settings in the main [Server Properties](#) page.


For more information, see Configuring Fault Tolerance in Central Administration in the *TIBCO Enterprise Message Service User's Guide*.

## Trace/Log

The fields on the Tracing and Logging properties page correspond to the Tracing and Log File Parameters parameters in the `tibemsd.conf` configuration file.


## Validation

The Validation Results page shows a list of any validation errors in the current server configuration. Each time you edit a field, the Central Administration validates the revised server configuration and reports any errors in the Validation Results page. Immediate feedback is provided through the Validation Results link in the sidebar. The number of errors, if any are present in the server configuration, appears to the right of the link name.

A description of each validation issue is listed on the Validation Results page. Click the View  icon to navigate to the properties page where the issue is located.

## JSON Source

The JSON Source page displays a read-only copy of the server configuration file that is currently stored in the working directory. This file contains any edits that have been made but not yet deployed to the server.

If the source file is too large to display quickly, you are prompted to use the Download  icon instead. You can either left-click on that icon to display an unformatted version of the source or right-click on the icon to download and save the source as a JSON file.

## Security

---

The properties pages in the Security category configure access to the EMS server.

### Users

Use the index screen to access existing user definitions or create a new user.

The fields on the User properties page correspond to the parameters in the `users.conf` configuration file.

You can assign permissions to the user from the User properties page by adding Access Control Lists (ACLs) for individual destinations. This provides a very granular level of control. Use the Groups property page to assign the same set of permissions to a group of people.

Similarly, you can grant administrative privileges to the user by adding an Admin ACL on the User page. You can also add the user to a group with administrative privileges.



Users configured here are local, and apply only to the current EMS server. Users that are defined through JAAS or LDAP do not appear on these pages. To add permissions to externally sourced users (those configured through the JAAS module), use the ACLs page.

### Groups

Use the index screen to access existing group definitions or create a new group.

The fields on the Group properties page correspond to the parameters in the `groups.conf` configuration file.



Groups configured here are local, and apply only to the current EMS server. Groups that are defined through JAAS or LDAP do not appear on these pages. To add permissions to externally sourced groups (those configured through the JAAS module), use the ACLs page.

## ACLs

Use the index screen to access existing Access Control List (ACL) definitions or create a new ACL. The ACLs page provides access to both locally and externally sourced users and groups. That is, users and groups that are specific to this EMS server, and those that are configured through a JAAS or LDAP system.

The fields on the ACLs properties page correspond to the parameters in the `acl.conf` configuration file.

## LDAP

The fields on the LDAP properties page correspond to the LDAP Parameters parameters in the `tibemsd.conf` configuration file.

Also, refer to Chapter 8, Authentication and Permissions in the *TIBCO Enterprise Message Service User's Guide*.

## SSL

The fields on the SSL properties page correspond to the SSL Server Parameters parameters in the `tibemsd.conf` configuration file.

Also, refer to Chapter 18, Using the SSL Protocol in the *TIBCO Enterprise Message Service User's Guide*.





## Appendix A    **Converting Server Configuration Files to JSON**

The `tibemscnf2json` utility is provided to convert a set of text-based EMS server configuration files into a single JSON configuration file. This tool is available on platforms that support Central Administration. For a list of supported platforms, see the supported platforms list for Central Administration in the *TIBCO Enterprise Message Service Installation* guide.

When using the utility, keep in mind that:

- If there are any unsupported parameters in the source configuration file, the `tibemscnf2json` utility issues a warning but continues converting.

Review the *TIBCO Enterprise Message Service Release Notes* for details about any obsolete parameters that were removed from the current release.

- To convert a fault tolerant pair, use the `-secondaryconf` option to merge the two `tibemsd.conf` files of a fault tolerant pair of servers.

**Syntax**    To convert a EMS server configuration to JSON, use the command:

```
tibemscnf2json -conf source-file [-secondaryconf ft-source-file]
[-confencoding character-set-name] -json output-file | -console
```

where

- *source-file* is the path to the `tibemsd.conf` to be converted. Sub-file names and locations are derived from the content of the `tibemsd.conf` file. When converting servers in a fault tolerant pair, specify the configuration file for the primary server.
- *ft-source-file* is the path to the server configuration file for the second server in a fault tolerant pair. Specify this path with the `-secondaryconf` option to convert a fault tolerant pair.
- *character-set-name* is the name of the character set that was used to encode the *source-file* (and *ft-source-file*, if given). Any character encoding supported by the Java SE platform can be specified. Specify the encoding using the Canonical Name for `java.lang.API`.

When omitted, the expected encoding is UTF-8. Note that the output JSON file is always encoded with UTF-8.

- *output-file* is the name and location of the new JSON file. This file must have the `.json` extension. For example, `tibemsd.json`. If no path is specified, the file is created in the current working directory.
- Alternately, specify `-console` to display the JSON output to the screen rather than saving to file.

The `tibemscnf2json` utility converts the `.conf` file to a JSON-based configuration.

If `-json output-file` is specified, the file is created and saved in the location specified, or the current working directory if no path is given. You can then start the EMS server using the JSON configuration, and access the server through the Central Administration web interface.

### Convert a Fault Tolerant Pair

If a `-secondaryconf ft-source-file` is specified, the `tibemscnf2json` utility first converts the primary configuration to JSON, then uses the secondary configuration to complete the fault tolerant setup, deciding which one of the primary listen URLs must be marked as `FT Active` and adding extra secondary listen URLs, if any.

Note that the secondary configuration is used only for the purpose of completing the fault tolerant setup. With the only exception of the `logfile` property, any differences and discrepancies between the two initial sets of configuration files that are outside fault tolerance parameters are ignored.

# Index

## A

### ACLs

properties page [61](#)

### authentication

with JAAS [20](#)

### authorization

JAAS users [20](#)

## B

### benefits

of central administration [2](#)

### breadcrumbs [29](#)

### break a lock [38](#)

### bridges

properties page [54](#)

### browser

location of central administration [26](#)

## C

### central administration

add EMS server [34](#)

command line options [9](#)

deploy EMS server [42](#)

edit EMS server [39](#)

JAAS configuration [20](#)

JSON file [6](#)

location of web interface [26](#)

lock EMS server [38](#)

### navigation

navigating

central administration [25](#)

navigation tools [29](#)

overview [2](#)

properties pages [53](#)

remove EMS server [36](#)

requirements [2](#)

revert [38](#)

security [19, 60](#)

SSL configuration [21](#)

start server [9](#)

stop server [16](#)

structure [3](#)

supported browsers [2](#)

validation [58](#)

### central administration server command

deploy [30](#)

download [31](#)

lock [30](#)

refresh [31, 48](#)

revert [31](#)

save [31](#)

cipher suites [23](#)

command icons [30](#)

### command line options

central administration server [9](#)

### configure

EMS server in central administration [39](#)

- configuring
  - ACLs [61](#)
  - bridges [54](#)
  - connection factories [56](#)
  - durable subscribers [54](#)
  - fault tolerance [58](#)
  - groups [60](#)
  - LDAP [61](#)
  - queues [54](#)
  - routes [56](#)
  - RVCN [56](#)
  - SSL [61](#)
  - stores [58](#)
  - topics [54](#)
  - tracing and logging [58](#)
  - transports [55](#)
  - users [60](#)
- conflicts
  - lock [38](#)
- connection factories
  - properties page [56](#)
- connections
  - configuring in central administration [55](#)
- convert
  - to JSON [63](#)
- customer support [xvii](#)

## D

- deploy
  - command icon [30](#)
  - configurations [42](#)
  - logs [46](#)
  - redeploy [45](#)
- deployment directory [4](#)
- deployments page [29](#)
- destinations
  - configuring in central administration [54](#)
- download
  - command icon [31](#)
- duplicate
  - EMS server [34](#)

- durable subscribers
  - properties page [54](#)

## E

- edit
  - lock EMS server [30, 38](#)
- editing
  - in central administration [39](#)
- EMS Server
  - properties pages [57](#)
- EMS server
  - add to central administration [34](#)
  - delete from central administration [36](#)
  - deploy edits [42](#)
  - duplicate [34](#)
  - edit in central administration [39](#)
  - JSON source [59](#)
  - lock and edit [38](#)
  - managed servers page [27](#)
  - overview page [28](#)
  - refresh configuration [48](#)
  - revert edits [38](#)
  - validation [58](#)
- emsc-admin
  - JAAS user [20](#)
- emsc-guest
  - JAAS user [20](#)
- errors
  - validation [58](#)

## F

- factories
  - properties page [56](#)
- fault tolerance
  - properties page [58](#)
- filter or create [40](#)
- semantics [40](#)
- flow of information [4](#)

## G

- give up a lock [38](#)
- groups
  - properties page [60](#)
- GUI
  - central administration [25](#)

## H

- home page
  - EMS server [28](#)
- HTTPS [22](#)

## I

- icons [30](#)
  - command icons [30](#)
  - deploy [30](#)
  - download [31](#)
  - lock & edit [30](#)
  - manipulating items [31](#)
  - refresh [31](#), [48](#)
  - revert [31](#)
  - save [31](#)
- index page [40](#)
- information
  - flow [4](#)

## J

- JAAS
  - central administration configuration [20](#)
  - central administration users [20](#)
- JSON [6](#)
  - view source [59](#)

## L

- LDAP
  - properties page [61](#)
- location
  - central administration web interface [26](#)
- lock
  - conflicts [38](#)
  - lock & edit [30](#)
  - release [38](#)
  - the EMS server [38](#)
- lock file [4](#)
- logout [29](#)
- logs
  - deployment log [46](#)

## M

- managed servers page [27](#)
- manipulating items
  - icons [31](#)

## N

- navigation
  - filter or create [40](#)
  - sidebar [29](#)
  - tools [29](#)

## O

- options
  - central administration server [9](#)
- overview
  - central administration [2](#)

**P**

- properties pages [53](#)
  - ACLs [61](#)
  - bridges [54](#)
  - durable subscribers [54](#)
  - factories [56](#)
  - fault tolerance [58](#)
  - groups [60](#)
  - JSON source [59](#)
  - LDAP [61](#)
  - queues [54](#)
  - routes [56](#)
  - RVCN [56](#)
  - server properties [57](#)
  - SSL [61](#)
  - stores [58](#)
  - topics [54](#)
  - tracing and logging [58](#)
  - transports [55](#)
  - users [60](#)
  - validation [58](#)

**Q**

- queues
  - properties page [54](#)

**R**

- record
  - deployment log [46](#)
- redeploy [45](#)
- refresh
  - command icon [31](#)
  - update from EMS server [48](#)
- remove
  - EMS server from central administration [36](#)
- requirements
  - central administration [2](#)

- revert
  - command icon [31](#)
  - release a lock [38](#)
- routes
  - properties page [56](#)
- RVCN
  - properties page [56](#)

**S**

- save
  - command icon [31](#)
- security
  - central administration [19](#)
  - configuring in central administration [60](#)
  - considerations [19](#)
- semantics
  - filter or create [40](#)
- server overview page [28](#)
- servers
  - managed servers page [27](#)
- sidebar [29](#)
- SSL
  - central administration policy [14](#)
  - configuring in central administration [21](#)
  - properties page [61](#)
- start central administration server [9](#)
- stop central administration server [16](#)
- stores
  - properties page [58](#)
- structure
  - central administration [3](#)
- subscribers
  - configuring durable [54](#)
- support, contacting [xvii](#)
- supported browsers [2](#)

**T**

- take a lock [38](#)
- technical support [xvii](#)

- TIBCO\_HOME [xiv](#)
- tibemscat
  - start and stop [8](#)
- tibemscnf2json utility [63](#)
- tibemscd.conf
  - convert to JSON [63](#)
- tibemscd.json file [6](#)
- tools
  - navigation [29](#)
- topics
  - properties page [54](#)
- tracing and logging
  - properties page [58](#)
- transports
  - properties page [55](#)
- troubleshooting
  - validation [58](#)

## U

- update
  - refresh EMS server configuration [48](#)
- users
  - properties page [60](#)
- utility
  - tibemscnf2json [63](#)

## V

- validation [58](#)
- view
  - EMS server configuration [37](#)
  - JSON source [59](#)

## W

- web interface
  - central administration [25](#)
  - location of central administration [26](#)

- working directory [4](#)
  - location [9](#)