



# **TIBCO ActiveMatrix® Service Grid**

## **Security Guidelines**

Version 3.4.3 | February 2025

# Contents

---

<b>Contents</b> .....	<b>2</b>
<b>Introduction</b> .....	<b>3</b>
<b>Secure Communication Channels for Various Components</b> .....	<b>4</b>
Enable Secure Communication Channels by Using Command-Line Scripts .....	7
<b>Trust Stores</b> .....	<b>8</b>
<b>Unlimited Jurisdiction Files</b> .....	<b>9</b>
Installing Unlimited Jurisdiction Files .....	9
<b>TIBCO Credential Service</b> .....	<b>10</b>
<b>Other Recommendations for Running the ActiveMatrix Enterprise Securely</b>	<b>11</b>
Passwords .....	11
Internal and External ActiveMatrix Administrator Communication .....	12
Disable OSGi Console When Not Required or Not in Use .....	12
<b>TIBCO Documentation and Support Services</b> .....	<b>13</b>
<b>Legal and Third-Party Notices</b> .....	<b>15</b>

# Introduction

---

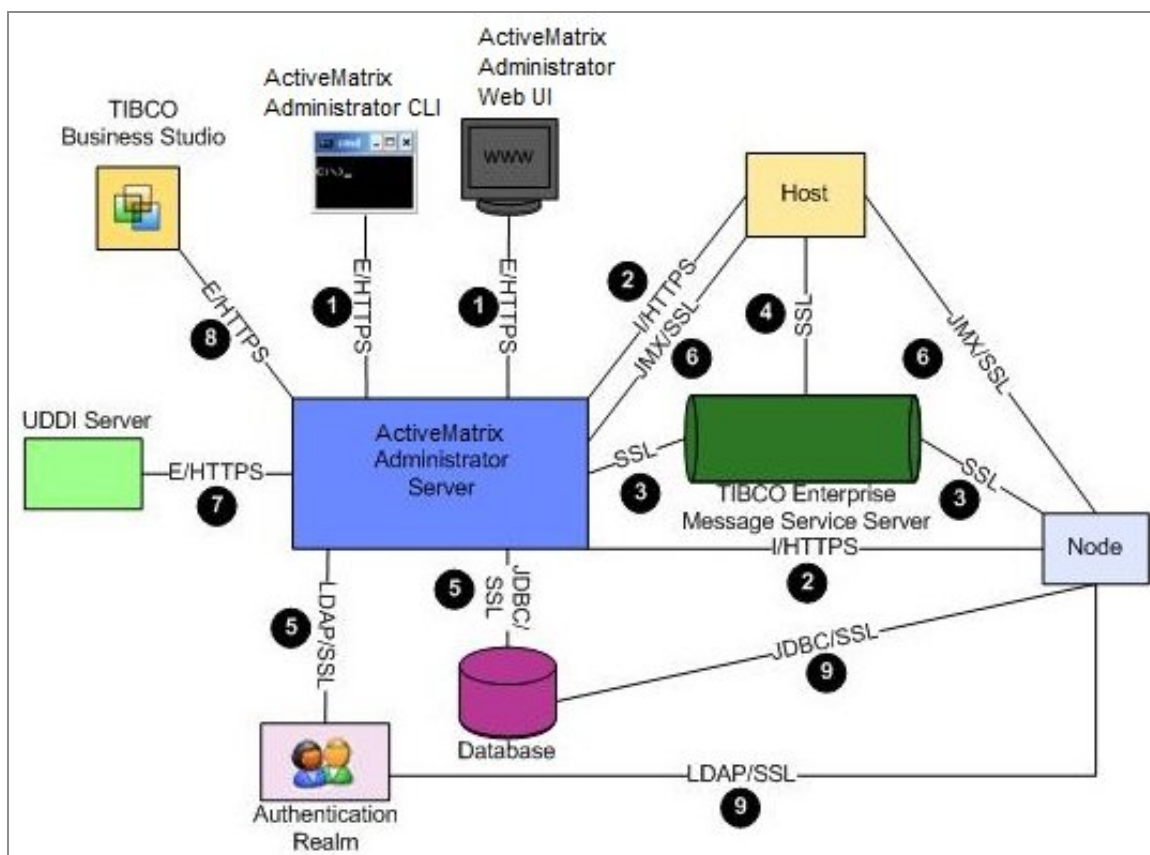
This document describes guidelines to ensure security within the various components TIBCO ActiveMatrix® Service Grid and the channels of communication between them. It also provides additional security-related guidance and recommendations for other aspects of internal and external communication. In particular,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

For information about how to upgrade third-party components and postinstallation activities, see *TIBCO ActiveMatrix® Service Grid Installation and Configuration*.

# Secure Communication Channels for Various Components

ActiveMatrix® Service Grid is partitioned across many components. You can secure the corresponding communication channels during the initial configuration (while configuring the ActiveMatrix Service Grid setup using the TIBCO Configuration Tool) or secure them later (using the ActiveMatrix Administrator GUI).

ActiveMatrix Service Grid components communicate with each other and with third-party applications over several communication protocols. The following diagram illustrates the components and communication protocols.



By default, some communication channels are not secure but they can be secured by configuring the channels to use the Secure Sockets Layer (SSL) protocol.

You can specify the SSL configuration of the communication channels at different times in the lifecycle of component deployment. The following tables list the entities that can be configured using the TIBCO Configuration Tool, ActiveMatrix Administrator UI and CLI, and TIBCO Business Studio™ - BPM Edition. The tables also list the entities that can be upgraded, downgraded, or updated using the TIBCO Configuration Tool, ActiveMatrix Administrator UI and CLI, and TIBCO Business Studio - BPM Edition. The key column in the table refers to the numbers in the diagram.

Key	Channel	Initial Configuration	Upgrade, Downgrade, or Change Configuration
1	Administrator server (external HTTP port) - Web and CLI clients	When creating the Administrator server in the TIBCO Configuration Tool.	Upgrade or downgrade: Administrator CLI  Change SSL configuration: Administrator CLI
2	Administrator server (internal HTTP port) - hosts and nodes	When creating the Administrator server in the TIBCO Configuration Tool.	Upgrade or downgrade: Administrator web UI or CLI  Change SSL configuration: Administrator web UI or CLI
3	Administrator server - Enterprise Message Service server  (Notification Server and Messaging Bus)	When creating the Administrator server in the TIBCO Configuration Tool.	Upgrade or downgrade: Administrator web UI or CLI  Change SSL configuration: Administrator web UI or CLI

Key	Channel	Initial Configuration	Upgrade, Downgrade, or Change Configuration
4	TIBCO Host instance - TIBCO Enterprise Message Service	When creating the Administrator server or TIBCO Host instance in the TIBCO Configuration Tool.	Upgrade or downgrade: Administrator CLI  Change SSL configuration: Administrator CLI
5	Administrator server - external database and LDAP servers	When creating the Administrator server in TIBCO Configuration Tool.	Change SSL configuration: Administrator CLI
6	Administrator server - hosts and nodes (management)	When creating Administrator in the TIBCO Configuration Tool.	Upgrade: Administrator web UI or CLI  Change SSL configuration: Administrator CLI
7	Administrator -UDDI server	Manually import the UDDI server certificate into the Administrator server trust store using keytool.  Enable secure communication in Administrator web UI or CLI.	Same procedure as initial configuration
8	Administrator server (external HTTP port) - TIBCO Business Studio - BPM Edition	Administrator - When creating an Administrator server in TIBCO Configuration Tool.  TIBCO Business Studio - BPM Edition - When you connect to an administrator.	Administrator Upgrade or downgrade: Administrator CLI  Change SSL configuration: Administrator CLI

Key	Channel	Initial Configuration	Upgrade, Downgrade, or Change Configuration
9	Resource instances (JDBC, JMS, SMTP, LDAP, HTTP) - external servers	Administrator web UI or CLI	Administrator web UI or CLI

## Enable Secure Communication Channels by Using Command-Line Scripts

You can use CLI scripts to enable secure communication channels for the following:

- HTTP connector
- External database
- Database authentication realm
- LDAP authentication realm

For detailed steps, see *TIBCO ActiveMatrix® Service Grid Administration*.

# Trust Stores

---

A trust store is a keystore that contains trusted certificates. Each time you configure an external server connection for SSL, you create and configure a trust store for that connection.

You can create a trust store by:

- Using certificates imported from trusted servers.
- Uploading a keystore file.

For creating and configuring trust store keystores, see *TIBCO ActiveMatrix® Service Grid Administration*.



# Unlimited Jurisdiction Files

---

By default, Java vendors include a set of policy files that do not permit unlimited strength cryptography. The default set of policy files, typically, restricts usage of 192-bit AES and 256-bit AES. In countries exempt from these restrictions, an unlimited strength set of these policy files can be downloaded and installed.

## Installing Unlimited Jurisdiction Files

To install the unlimited strength policy files on nodes where key lengths for symmetric (bulk) ciphers are required, perform the following steps.

### Procedure

1. Download the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files from the JRE vendor.
2. Back up the files located in `TIBCO_HOME/tibcojre/jre_version/lib/security`.
3. Extract the files that you downloaded to `TIBCO_HOME/tibcojre/jre_version/lib/security/`.
4. Restart the node and the TIBCO Host instance.

# TIBCO Credential Service

---

The TIBCO Credential Service provides credentials that secure the management connections between the ActiveMatrix Administrator server, hosts, and nodes. The TIBCO Credential Service runs as a plug-in to the ActiveMatrix Administrator server.

The Credential Service acts as a certificate authority and creates a unique identity for each node and host. The Credential Service is automatically created when you create an ActiveMatrix Administrator server. For information on how to specify the properties of the TIBCO Credential Service, see the installation guide for your product.

# Other Recommendations for Running the ActiveMatrix Enterprise Securely

---

This section provides some recommendations to secure other aspects of communication when running the enterprise.

## Passwords

### Super-user or Root Password Selection

Specify a strong password for ActiveMatrix Administrator super-user or root user. Considering that a root user or super-user can perform all critical operations that can damage or destabilize the enterprise.

The password should ideally consist of:

- A minimum of eight characters
- Mix of uppercase and lower case characters
- Numbers
- Special characters

### Password Storage in the `remote.properties` File

ActiveMatrix Administrator command-line interface scripts communicate with the ActiveMatrix Administrator via the HTTP protocol. For this, the credentials (username and password) must be specified in the `remote.properties` file. Avoid storing the passwords as clear text in this file. Instead, use the obfuscation tool packaged with the product to obfuscate the password.

# Internal and External ActiveMatrix Administrator Communication

## Running the External Connector of the ActiveMatrix Administrator

We recommend that you:

- Run the external HTTP connector of the ActiveMatrix Administrator in the SSL-enabled mode. This connector serves as the web front end for the ActiveMatrix Administrator. (The default port is 8120.)
- Use your own SSL certificate obtained by a well-known certificate authority. If you update the SSL certificate, you must obtain the certificates used by ActiveMatrix Administrator CLI scripts. For information about how to update the `remote.properties` file of CLI scripts to provide client certificates, see *TIBCO ActiveMatrix® Service Grid Administration*.
- Configure the external HTTP connector to use the TLS 1.2 protocol. Starting with ActiveMatrix Service Grid 3.4.0, the TLS 1.2 protocol is enabled by default.

## Running the Internal Communication of the ActiveMatrix Administrator

Between ActiveMatrix enterprise entities, the communication is either via TCP or TIBCO EMS, and we recommend that both these modes of transport are secured via SSL.

## Disable OSGi Console When Not Required or Not in Use

As the ActiveMatrix Service Grid runtime nodes are OSGi-based, their state can be viewed by enabling the OSGi console. This console is exposed over the TIBCO Configuration Tool and is not authenticated. We strongly recommend that you disable the console if you see no use for it. By default, the console is disabled.

Starting with ActiveMatrix Service Grid 3.4.0, you can check whether the OSGi port of a specific node in an enterprise is enabled. To do this, use the Enterprise Status page in ActiveMatrix Administrator. For more information about the Enterprise Status page, see *TIBCO ActiveMatrix® Service Grid Administration*.

# TIBCO Documentation and Support Services

---

For information about this product, you can read the documentation, contact TIBCO Support, and join TIBCO Community.

## How to Access TIBCO Documentation

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

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

## Product-Specific Documentation

The documentation for this product is available on the [TIBCO ActiveMatrix® Service Grid Product Documentation](#) page.

## How to Contact Support for TIBCO Products

You can contact the Support team in the following ways:

- To access the Support Knowledge Base and getting personalized content about products you are interested in, visit our [product Support website](#).
- To create a Support case, you must have a valid maintenance or support contract with a Cloud Software Group entity. You also need a username and password to log in to the [product Support website](#). If you do not have a username, you can request one by clicking **Register** on the website.

## How to Join TIBCO Community

TIBCO Community is the official channel for TIBCO customers, partners, and employee subject matter experts to share and access their collective experience. TIBCO Community offers access to Q&A forums, product wikis, and best practices. It also offers access to extensions, adapters, solution accelerators, and tools that extend and enable customers to gain full value from TIBCO products. In addition, users can submit and vote on feature

requests from within the [TIBCO Ideas Portal](#). For a free registration, go to [TIBCO Community](#).

# Legal and Third-Party Notices

---

SOME CLOUD SOFTWARE GROUP, INC. (“CLOUD SG”) SOFTWARE AND CLOUD SERVICES EMBED, BUNDLE, OR OTHERWISE INCLUDE OTHER SOFTWARE, INCLUDING OTHER CLOUD SG SOFTWARE (COLLECTIVELY, “INCLUDED SOFTWARE”). USE OF INCLUDED SOFTWARE IS SOLELY TO ENABLE THE FUNCTIONALITY (OR PROVIDE LIMITED ADD-ON FUNCTIONALITY) OF THE LICENSED CLOUD SG SOFTWARE AND/OR CLOUD SERVICES. THE INCLUDED SOFTWARE IS NOT LICENSED TO BE USED OR ACCESSED BY ANY OTHER CLOUD SG SOFTWARE AND/OR CLOUD SERVICES OR FOR ANY OTHER PURPOSE.

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

This document is subject to U.S. and international copyright laws and treaties. No part of this document may be reproduced in any form without the written authorization of Cloud Software Group, Inc.

TIBCO, the TIBCO logo, the TIBCO O logo, ActiveMatrix, Business Studio, Enterprise Message Service, and Hawk are either registered trademarks or trademarks of Cloud Software Group, Inc. in the United States and/or other countries.

All other product and company names and marks mentioned in this document are the property of their respective owners and are mentioned for identification purposes only. You acknowledge that all rights to these third party marks are the exclusive property of their respective owners. Please refer to Cloud SG’s Third Party Trademark Notices (<https://www.cloud.com/legal>) for more information.

This document includes fonts that are licensed under the SIL Open Font License, Version 1.1, which is available at: <https://scripts.sil.org/OFL>

Copyright (c) Paul D. Hunt, with Reserved Font Name Source Sans Pro and Source Code Pro.

Cloud SG software may be available on multiple operating systems. However, not all operating system platforms for a specific software version are released at the same time. See the “readme” file for the availability of a specific version of Cloud SG software on a specific operating system platform.

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

THIS DOCUMENT COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN; THESE CHANGES WILL BE INCORPORATED IN NEW EDITIONS OF THIS DOCUMENT. CLOUD SG MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT(S), THE PROGRAM(S), AND/OR THE SERVICES DESCRIBED IN THIS DOCUMENT AT ANY TIME WITHOUT NOTICE.

THE CONTENTS OF THIS DOCUMENT MAY BE MODIFIED AND/OR QUALIFIED, DIRECTLY OR INDIRECTLY, BY OTHER DOCUMENTATION WHICH ACCOMPANIES THIS SOFTWARE, INCLUDING BUT NOT LIMITED TO ANY RELEASE NOTES AND "README" FILES.

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

Copyright © 2010-2025. Cloud Software Group, Inc. All Rights Reserved.