



TIBCO ActiveMatrix® Service Grid

Security Guidelines

*Software Release 3.4
April 2019*

Important Information

SOME TIBCO SOFTWARE EMBEDS OR BUNDLES OTHER TIBCO SOFTWARE. USE OF SUCH EMBEDDED OR BUNDLED TIBCO SOFTWARE IS SOLELY TO ENABLE THE FUNCTIONALITY (OR PROVIDE LIMITED ADD-ON FUNCTIONALITY) OF THE LICENSED TIBCO SOFTWARE. THE EMBEDDED OR BUNDLED SOFTWARE IS NOT LICENSED TO BE USED OR ACCESSED BY ANY OTHER TIBCO SOFTWARE OR FOR ANY OTHER PURPOSE.

USE OF TIBCO SOFTWARE AND THIS DOCUMENT IS SUBJECT TO THE TERMS AND CONDITIONS OF A LICENSE AGREEMENT FOUND IN EITHER A SEPARATELY EXECUTED SOFTWARE LICENSE AGREEMENT, OR, IF THERE IS NO SUCH SEPARATE AGREEMENT, THE CLICKWRAP END USER LICENSE AGREEMENT WHICH IS DISPLAYED DURING DOWNLOAD OR INSTALLATION OF THE SOFTWARE (AND WHICH IS DUPLICATED IN THE LICENSE FILE) OR IF THERE IS NO SUCH SOFTWARE LICENSE AGREEMENT OR CLICKWRAP END USER LICENSE AGREEMENT, THE LICENSE(S) LOCATED IN THE "LICENSE" FILE(S) OF THE SOFTWARE. USE OF THIS DOCUMENT IS SUBJECT TO THOSE TERMS AND CONDITIONS, AND YOUR USE HEREOF SHALL CONSTITUTE ACCEPTANCE OF AND AN AGREEMENT TO BE BOUND BY THE SAME.

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

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

TIBCO, the TIBCO logo, Two-Second Advantage, TIB, Information Bus, ActiveMatrix, Business Studio, Enterprise Message Service, Hawk, and Rendezvous are either registered trademarks or trademarks of TIBCO Software Inc. in the United States and/or other countries.

Java and all Java based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

All other product and company names and marks mentioned in this document are the property of their respective owners and are mentioned for identification purposes only.

This software may be available on multiple operating systems. However, not all operating system platforms for a specific software version are released at the same time. Please see the readme.txt file for the availability of this software version on a specific operating system platform.

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

THIS DOCUMENT COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN; THESE CHANGES WILL BE INCORPORATED IN NEW EDITIONS OF THIS DOCUMENT. TIBCO SOFTWARE INC. MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT(S) AND/OR THE PROGRAM(S) DESCRIBED IN THIS DOCUMENT AT ANY TIME.

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

This and other products of TIBCO Software Inc. may be covered by registered patents. Please refer to TIBCO's Virtual Patent Marking document (<https://www.tibco.com/patents>) for details.

Copyright © 2010-2019. TIBCO Software Inc. All Rights Reserved.

Contents

- TIBCO Documentation and Support Services5**
- Introduction 7**
- Secure Communication Channels for Various Components8**
 - Enable Secure Communication Channels by Using Command-Line Scripts 10
- Trust Stores 11**
- Unlimited Jurisdiction Files12**
 - Installing Unlimited Jurisdiction Files 12
- TIBCO Credential Service 13**
- Other Recommendations for Running the ActiveMatrix Enterprise Securely 14**
 - Passwords14
 - Internal and External ActiveMatrix Administrator Communication 14
 - Disable OSGi Console When Not Required or Not in Use14

TIBCO Documentation and Support Services

How to Access TIBCO Documentation

Documentation for TIBCO products is available on the TIBCO Product Documentation website, mainly in HTML and PDF formats.

The TIBCO Product Documentation website is updated frequently and is more current than any other documentation included with the product. To access the latest documentation, visit <https://docs.tibco.com>.

Product-Specific Documentation

Documentation for TIBCO ActiveMatrix® Service Grid is available on the <https://docs.tibco.com/products/tibco-activematrix-service-grid> page.

Use of the following features, installation profiles and development tools requires a TIBCO ActiveMatrix Service Grid license:



- TIBCO ActiveMatrix Policy Director Governance, TIBCO ActiveMatrix SPM Dashboard, and TIBCO ActiveMatrix SPM Runtime Server profiles; and
- TIBCO ActiveMatrix Service Grid development tools for Java, Webapp and Spring components.

Customers with only a TIBCO ActiveMatrix Service Bus license are not licensed to use these features, tools or profiles.

The following documents form the documentation set:

- *TIBCO ActiveMatrix Service Grid Concepts*: Read this manual before reading any other manual in the documentation set. This manual describes terminology and concepts of the platform. The other manuals in the documentation set assume you are familiar with the information in this manual.
- *TIBCO ActiveMatrix Service Grid Development Tutorials*: Read this manual for a step-by-step introduction to the process of creating, packaging, and running composites in TIBCO Business Studio.
- *TIBCO ActiveMatrix Service Grid Composite Development*: Read this manual to learn how to develop and package composites.
- *TIBCO ActiveMatrix Service Grid Java Component Development*: Read this manual to learn how to configure and implement Java components.
- *TIBCO ActiveMatrix Service Grid Mediation Component Development*: Read this manual to learn how to configure and implement Mediation components.
- *TIBCO ActiveMatrix Service Grid Mediation API Reference*: Read this manual to learn how to develop custom Mediation tasks.
- *TIBCO ActiveMatrix Service Grid Spring Component Development*: Read this manual to learn how to configure and implement Spring components.
- *TIBCO ActiveMatrix Service Grid WebApp Component Development*: Read this manual to learn how to configure and implement Web Application components.
- *TIBCO ActiveMatrix Service Grid REST Binding Development*: Read this manual to learn how to configure and implement REST components.
- *TIBCO ActiveMatrix Service Grid Administration Tutorials*: Read this manual for a step-by-step introduction to the process of creating and starting the runtime version of the product, starting TIBCO ActiveMatrix servers, and deploying applications to the runtime.
- *TIBCO ActiveMatrix Service Grid Administration*: Read this manual to learn how to manage the runtime and deploy and manage applications.

- *TIBCO ActiveMatrix Service Grid Hawk ActiveMatrix Plug-in*: Read this manual to learn about the Hawk plug-in and its optional configurations.
- *TIBCO ActiveMatrix Service Grid Policy Director Governance Custom Actions*: Read this manual to learn how you can configure and enforce policies for ActiveMatrix and external services hosted in third party containers, using TIBCO ActiveMatrix Policy Director Governance.
- *TIBCO ActiveMatrix Service Grid Service Performance Manager API Reference*: Read this manual to learn how to use the SPM APIs.
- *TIBCO ActiveMatrix Service Grid Error Codes*: Read this manual to know more about the error messages and how you could use them to troubleshoot a problem.
- *TIBCO ActiveMatrix Service Grid Installation and Configuration*: Read this manual to learn how to install and configure the software.
- *TIBCO ActiveMatrix Service Grid Security Guidelines*: Read this manual to learn more about security guidelines and recommendations for TIBCO ActiveMatrix Service Grid.
- *TIBCO ActiveMatrix Service Grid Release Notes*: Read this manual for a list of new and changed features, steps for migrating from a previous release, and lists of known issues and closed issues for the release.

How to Contact TIBCO Support

You can contact TIBCO Support in the following ways:

- For an overview of TIBCO Support, visit <http://www.tibco.com/services/support>.
- For accessing the Support Knowledge Base and getting personalized content about products you are interested in, visit the TIBCO Support portal at <https://support.tibco.com>.
- For creating a Support case, you must have a valid maintenance or support contract with TIBCO. You also need a user name and password to log in to <https://support.tibco.com>. If you do not have a user name, you can request one by clicking Register on the website.

How to Join TIBCO Community

TIBCO Community is the official channel for TIBCO customers, partners, and employee subject matter experts to share and access their collective experience. TIBCO Community offers access to Q&A forums, product wikis, and best practices. It also offers access to extensions, adapters, solution accelerators, and tools that extend and enable customers to gain full value from TIBCO products. In addition, users can submit and vote on feature requests from within the [TIBCO Ideas Portal](https://community.tibco.com). For a free registration, go to <https://community.tibco.com>.

Introduction

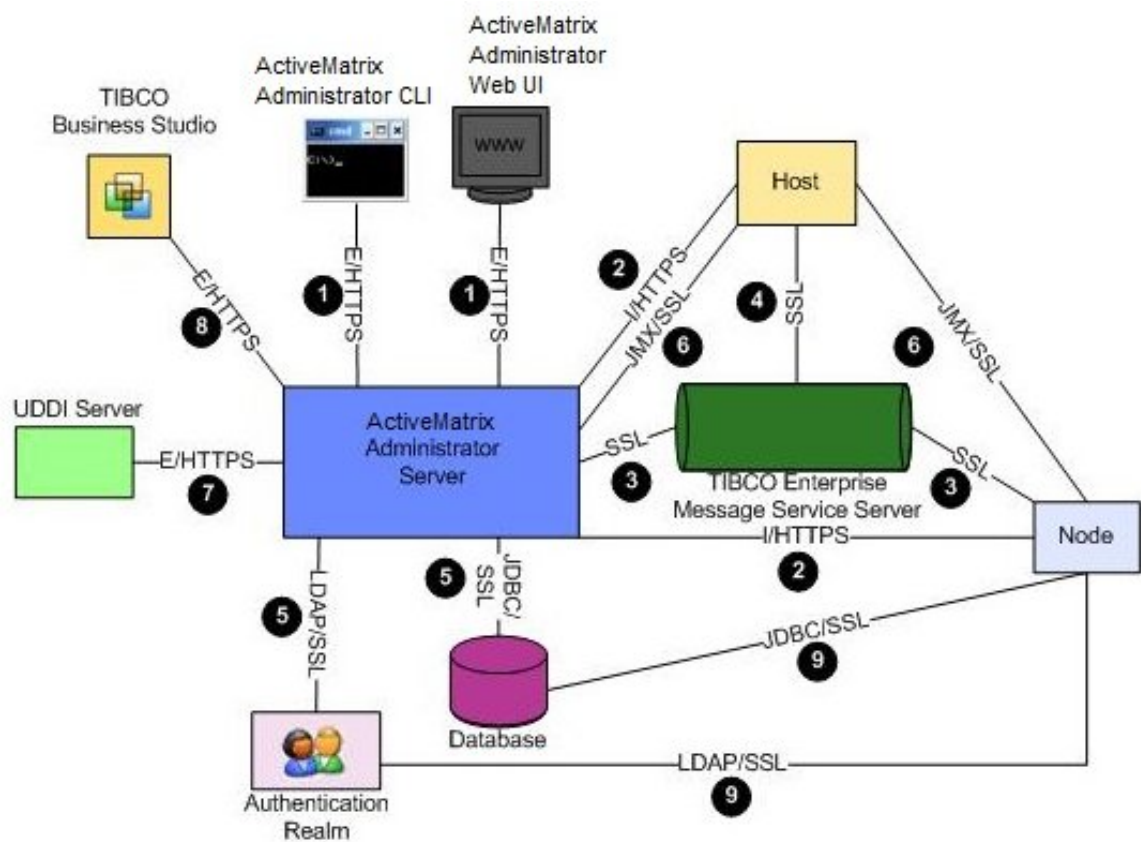
This document describes guidelines to ensure security within the various components of TIBCO ActiveMatrix Service Grid and the channels of communication between them. It also provides additional security-related guidance and recommendations for other aspects of internal and external communication. In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

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

ActiveMatrix 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. 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. The Key column in the tables 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 TIBCO Configuration Tool.	Upgrade or downgrade: Administrator CLI Change SSL configuration: Administrator CLI

Key	Channel	Initial Configuration	Upgrade, Downgrade, or Change Configuration
2	Administrator server (internal HTTP port) - hosts and nodes	When creating the Administrator server in 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 TIBCO Configuration Tool.	Upgrade or downgrade: Administrator web UI or CLI Change SSL configuration: Administrator web UI or CLI
4	TIBCO Host instance - TIBCO Enterprise Message Service	When creating the Administrator server or TIBCO Host instance in 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 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	Administrator - When creating Administrator server in TIBCO Configuration Tool. TIBCO Business Studio - When you connect to Administrator.	Administrator Upgrade or downgrade: Administrator CLI Change SSL configuration: Administrator CLI
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 HTTP connector, external database, database authentication realm, and 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 or by uploading a keystore file. Refer to *TIBCO ActiveMatrix Service Grid Administration* for creating and configuring Trust Store Keystores.

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 8 characters, with a mix of uppercase and lower case characters, numbers and special characters.

Password Storage in the `remote.properties` File

ActiveMatrix Administrator command-line Interface scripts communicate with the ActiveMatrix Administrator via 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 ActiveMatrix Administrator

We recommend that you:

- Run the external HTTP connector of ActiveMatrix Administrator in the SSL-enabled mode. This connector serves as the web front end for 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 TLSv1.2 protocol. Starting with ActiveMatrix Service Grid 3.4.0, the TLSv1.2 protocol is enabled by default.

Running the Internal Communication of 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 ActiveMatrix Runtime nodes are OSGi-based, their state can be viewed by enabling the OSGi console. This console is, currently, exposed over 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*.