



TIBCO Hawk[®]

Security Guidelines

*Software Release 6.2
September 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, the TIBCO O logo, TIB, Information Bus, ActiveMatrix BusinessWorks, Enterprise Message Service, Hawk, Rendezvous, TIBCO Administrator, TIBCO Designer, and TIBCO Runtime Agent 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 Corporation 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. 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.

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 © 2019. TIBCO Software Inc. All Rights Reserved.

Contents

Preface	iv
Related Documentation	v
TIBCO Hawk Documentation	v
Other TIBCO Product Documentation	vi
Typographical Conventions	vii
TIBCO Product Documentation and Support Services	ix
How to Access TIBCO Documentation	ix
How to Contact TIBCO Support	ix
How to Join TIBCO Community	ix
Chapter 1 Introduction	1
Chapter 2 Secure Communication Channels	2
Data Ingest and Ingress	2
Data Egress	2
Communication Channels and Their Security Configurations	3
Chapter 3 Other Recommendations for Running TIBCO Hawk Securely	6
General Security Environment	6
Selection of Passwords	6
Data Center Placement	7
Backups	7

Preface

This guide describes the security guidelines for TIBCO Hawk.

Topics

- [Related Documentation, page v](#)
- [Typographical Conventions, page vii](#)
- [TIBCO Product Documentation and Support Services, page ix](#)

Related Documentation

This section lists documentation resources you may find useful.

TIBCO Hawk Documentation

The following documents form the TIBCO Hawk documentation set:

- *TIBCO Hawk 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.
- *TIBCO Hawk Concepts*: This manual includes basic descriptions of TIBCO Hawk concepts.
- *TIBCO Hawk Installation, Configuration, and Administration*: Read this book first. It contains step-by-step instructions for installing TIBCO Hawk software on various operating system platforms. It also describes how to configure the software for specific applications, once it is installed. An installation FAQ is included.
- *TIBCO Hawk Microagent Reference*: A reference to the microagents and methods used by a TIBCO Hawk Agent for system and application monitoring.
- *TIBCO Hawk WebConsole User's Guide*: This manual includes complete instructions for using TIBCO Hawk WebConsole.
- *TIBCO Hawk Programmer's Guide*: All programmers should read this manual. It contains detailed descriptions of Application Management Interface (AMI), Application Programming Interface (API) concepts, and the TIBCO Hawk security framework and its classes. It also contains detailed descriptions of each class and method for the following APIs:
 - AMI API
 - Java, C++ and C API
 - Console API
 - Java API
 - Configuration Object API
 - Java API

Programmers should refer to the appropriate language reference sections for the AMI API details. The TIBCO Hawk Application Management Interface (AMI) exposes internal application methods to TIBCO Hawk.

- *TIBCO Hawk Plug-in Reference Guide*: Contains details about the Enterprise Message Service, Messaging and JVM microagents methods that are used to administer and monitor the TIBCO Enterprise Message Service server.
- *TIBCO Hawk Plug-ins for TIBCO Administrator*: Contains detailed descriptions of the TIBCO Hawk plug-ins accessed via TIBCO Administrator.
- *TIBCO Hawk HTTP Adapter User's Guide*: Contains information about performing discovery, monitoring of agent status, monitoring of agent alerts, method invocation, method subscription, and many more activities on TIBCO Hawk and third-party products.
- *TIBCO Hawk Admin Agent Guide*: Contains basic configuration details for TIBCO Hawk Admin Agent and complete instructions for using the web interface of TIBCO Enterprise Administrator for TIBCO Hawk.
- *TIBCO Hawk Security Guide*: Provides guidelines to ensure security within the components of TIBCO Hawk and within the communication channels between the components.

Other TIBCO Product Documentation

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

- TIBCO® Enterprise Administrator
- TIBCO ActiveSpaces®
- TIBCO Rendezvous®
- TIBCO Enterprise Message Service™

Typographical Conventions

The following typographical conventions are used in this manual.

Table 1 General Typographical Conventions

Convention	Use
<i>ENV_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"> • Name Identifies the installation environment. This name is referenced in documentation as <i>ENV_NAME</i>. On Microsoft Windows, the name is appended to the name of Windows services created by the installer and is a component of the path to the product shortcut in the Windows Start > All Programs menu. • Path The folder into which the product is installed. This folder is referenced in documentation as <i>TIBCO_HOME</i>. <p>TIBCO Hawk installs into a directory within a <i>TIBCO_HOME</i>. This directory is referenced in documentation as <i>HAWK_HOME</i>. The default value of <i>HAWK_HOME</i> depends on the operating system. For example on Windows systems, the default value is <code>C:\tibco\hawk\6.0</code>.</p> <p>A TIBCO Hawk configuration folder stores configuration data generated by TIBCO Hawk. Configuration data can include sample scripts, session data, configured binaries, logs, and so on. This folder is referenced in documentation as <i>CONFIG_FOLDER</i>. For example, on Windows systems, the default value is <code>C:\ProgramData\tibco\cfgmgt\hawk</code>.</p>
<i>TIBCO_HOME</i>	
<i>HAWK_HOME</i>	
<i>CONFIG_FOLDER</i>	
code font	<p>Code font identifies commands, code examples, filenames, pathnames, and output displayed in a command window. For example:</p> <p>Use <code>MyCommand</code> to start the foo process.</p>

Table 1 General Typographical Conventions (Cont'd)

Convention	Use
bold code font	<p>Bold code font is used in the following ways:</p> <ul style="list-style-type: none"> • In procedures, to indicate what a user types. For example: Type admin. • In large code samples, to indicate the parts of the sample that are of particular interest. • In command syntax, to indicate the default parameter for a command. For example, if no parameter is specified, MyCommand is enabled: MyCommand [enable disable]
<i>italic font</i>	<p>Italic font is used in the following ways:</p> <ul style="list-style-type: none"> • To indicate a document title. For example: See <i>TIBCO BusinessWorks Concepts</i>. • To introduce new terms. For example: A portal page may contain several portlets. <i>Portlets</i> are mini-applications that run in a portal. • To indicate a variable in a command or code syntax that you must replace. For example: MyCommand <i>pathname</i>
Key combinations	<p>Key name separated by a plus sign indicate keys pressed simultaneously. For example: Ctrl+C.</p> <p>Key names separated by a comma and space indicate keys pressed one after the other. For example: Esc, Ctrl+Q.</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.

TIBCO Product 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 TIBCO Product Documentation website mainly in the 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>.

Documentation for TIBCO Hawk is available on the [TIBCO Hawk Product Documentation](#) page.

How to Contact TIBCO Support

You can contact TIBCO Support in the following ways:

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

How to Join TIBCO Community

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

Chapter 1 **Introduction**

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

Secure Communication Channels

TIBCO Hawk is a distributed peer-to-peer monitoring and management framework. The Hawk Agents (deployed on each machine or node) monitor the OS, applications, and systems locally or remotely using Microagents. Most communication within the Hawk components (Hawk Agents, Microagents, and Hawk Console) is limited to data center services.

Data Ingest and Ingress

Ingest and ingress of data into Hawk is limited to the following modes:

- Web GUI
- Hawk Console REST API
- Hawk Console API
- Hawk AMI API

Data Egress

Data can be sent out from Hawk in the following ways:

- Alerts: SMTP, SNMP traps
- Actions: Invoking parameterized scripts
- Universal Collector Microagent

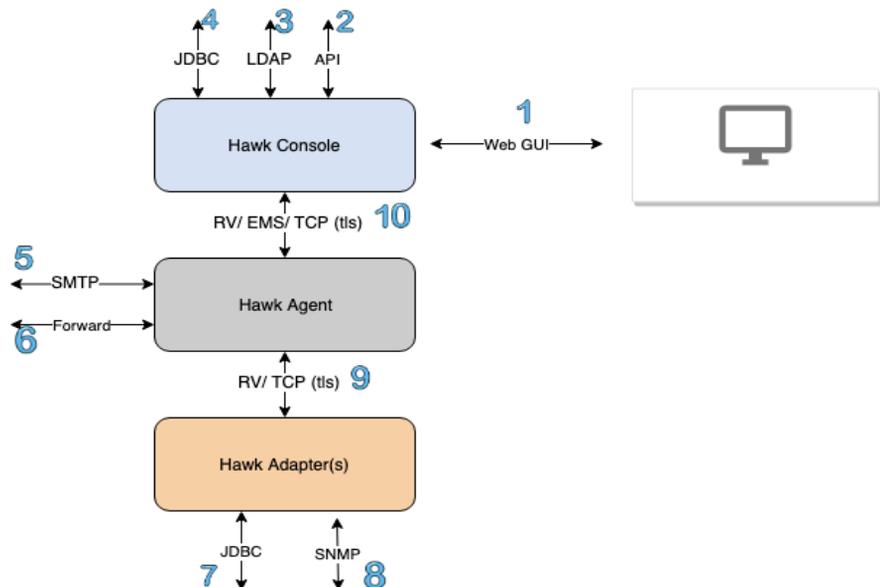
Communication Channels and Their Security Configurations

By default, some communication channels are not secure, but you can secure them by configuring channels and transports to use the Secure Socket Layer (SSL) or Transfer Layer Security (TLS) protocol. For information about how to configure a component for secure communication, see the *TIBCO Hawk Installation, Configuration, and Administration* guide.

For configuration information about specific Hawk Adapters and plug-ins, see the following documentation:

- TIBCO Hawk SNMP Adapter
- TIBCO Hawk Database Adapter
- TIBCO Hawk JMX Plugin

The following diagram illustrates the components and communication protocols in a typical Hawk deployment:



The following table describes the communication channels that can be configured, along with some references to more information, if applicable.

Key	Communication Channels	Connection	Description and References
8	SNMP	SNMP: UDP or TCP	SNMP Adapter
9	Hawk AMI Transport: <ul style="list-style-type: none"> • TCP • RV 	<ul style="list-style-type: none"> • TCP over TLS • RV unsecured 	TCP Transport offers TLS/ SSL support. For more information, see the <i>TIBCO Hawk Installation, Configuration, and Administration</i> guide.
10	Hawk Console API Transport: <ul style="list-style-type: none"> • TCP • EMS • RV 	<ul style="list-style-type: none"> • TCP over TLS • EMS over SSL • RV Unsecured 	TCP Transport offers TLS/ SSL support. EMS transport offers SSL. For more information, see the <i>TIBCO Hawk Installation, Configuration, and Administration</i> guide.

Other Recommendations for Running TIBCO Hawk Securely

This chapter provides some recommendations to secure other aspects of communication when using TIBCO Hawk.

General Security Environment

Hawk Agent(s) and Hawk Console: The operating system account for hosting the Hawk Agent or Hawk Microagent (HMA) and Hawk Console must be a super user account. Specify a strong password for the super user, which is heavily guarded and seldom used.

Hawk Console Users/ Clients: TIBCO recommends that the operating system and browsers used for accessing Hawk Console Web GUI or REST API must be properly maintained and secured according to security best practices.

To ensure secure (HTTPS) communication between Hawk Console and the GUI or REST API users, configure a valid X.509 certificate in Hawk Console. The certificate must be signed by a CA authority and recognized by the browsers used.

Selection of Passwords

Specify a strong password for the Hawk Console administrator accounts, considering that administrators perform all the critical operations. Weak administrator account passwords can result in security breach, resulting in severe damage and destabilization of the enterprise. The password must ideally consist of a minimum of eight characters, with a mix of uppercase and lowercase characters, numbers, and special characters. In the case of file-based authentication for Hawk Console, use the `tibhawkpassword` utility to obfuscate the passwords. You can use LDAP-based authentication for Hawk Console. In the LDAP-based authentication, the usernames and passwords are validated with a LDAP directory server.

Data Center Placement

The Hawk architecture assumes all the Hawk components are running on a trusted network, with access only from trusted computers and accounts. Consider the following security and data protection recommendations when deploying your data center (on-premises or on the cloud).

On-premises

When deploying Hawk components to the data center, keep Hawk components behind a firewall. This adds extra layers of security in protecting your data.

On the Cloud

When deploying Hawk components to the virtual data center, keep Hawk components behind a firewall.

Running your Hawk components in the same virtual private cloud (VPC) as your core services provides additional protection and better performance during data collection.



TIBCO recommends that you use TIBCO Hawk[®] Container Edition instead of deploying TIBCO Hawk on the Cloud.

Backups

You must export all backups (for configurations, rulebases, and so on) to a secure location to ensure quick recovery in case of a failure. Secure backup is necessary due to the sensitive nature of the files (for configurations, rulebases, and so on) that might be restored to production systems for recovery.