



TIBCO Hawk®

Security Guide

Version 6.3.1 | November 2024

Contents

Contents	2
Introduction	3
Secure Communication Channels	4
Data Ingest and Ingress	4
Data Egress	4
Communication Channels and Their Security Configurations	5
Other Recommendations for Running TIBCO Hawk Securely	9
General Security Environment	9
Selection of Passwords	9
Data Center Placement	10
Backups	10
TIBCO Documentation and Support Services	11
Legal and Third-Party Notices	13

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

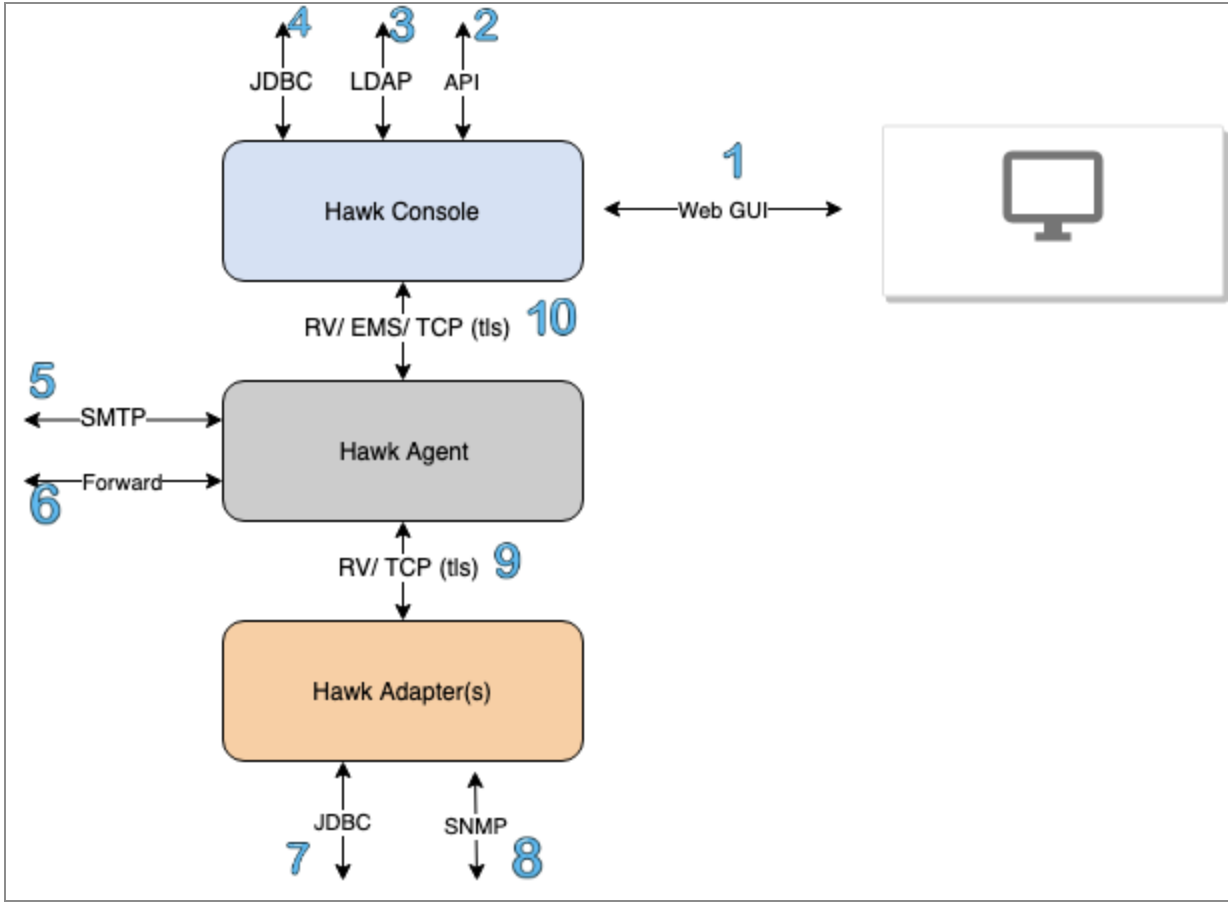
Communication Channels and Their Security Configurations

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
1	Web GUI	HTTPS	User Interface
2	API: RESTful	HTTPS	OpenAPI
3	LDAP Authentication	LDAP/S	User Authentication

Key	Communication Channels	Connection	Description and References
4	JDBC	JDBC (Hawk Console): <ul style="list-style-type: none"> • Apache Ignite • MySQL JDBC (Event Service) <ul style="list-style-type: none"> • IBM DB2 • Microsoft SQL Server • Oracle • Sybase 	Storing Hawk Alerts Storing Hawk Events and Alerts
5	SMTP	SMTP: TCP	Alerting
6	Forwarders <ul style="list-style-type: none"> • Syslog • ULDP 	Syslog: UDP or TCP (TLS) ULDP (TLS)	Data forwarding
7	JDBC	JDBC: <ul style="list-style-type: none"> • Oracle • Sybase • Microsoft SQL 	JDBC Adapter to monitor RDBMS databases, tables
8	SNMP	SNMP: UDP or TCP	SNMP Adapter
9	Hawk AMI Transport:	<ul style="list-style-type: none"> • TCP over TLS 	TCP Transport offers TLS/ SSL

Key	Communication Channels	Connection	Description and References
	<ul style="list-style-type: none"> TCP RV 	<ul style="list-style-type: none"> RV unsecured 	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.



Note

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.

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 Hawk® 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, Hawk, LogLogic, Rendezvous, Administrator, and BusinessWorks 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.cloud.com/legal>.

Copyright © 1996-2024. Cloud Software Group, Inc. All Rights Reserved.