# TIBCO Hawk®

## Security Guide

Version 6.3.1 | November 2024

# Contents

# 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

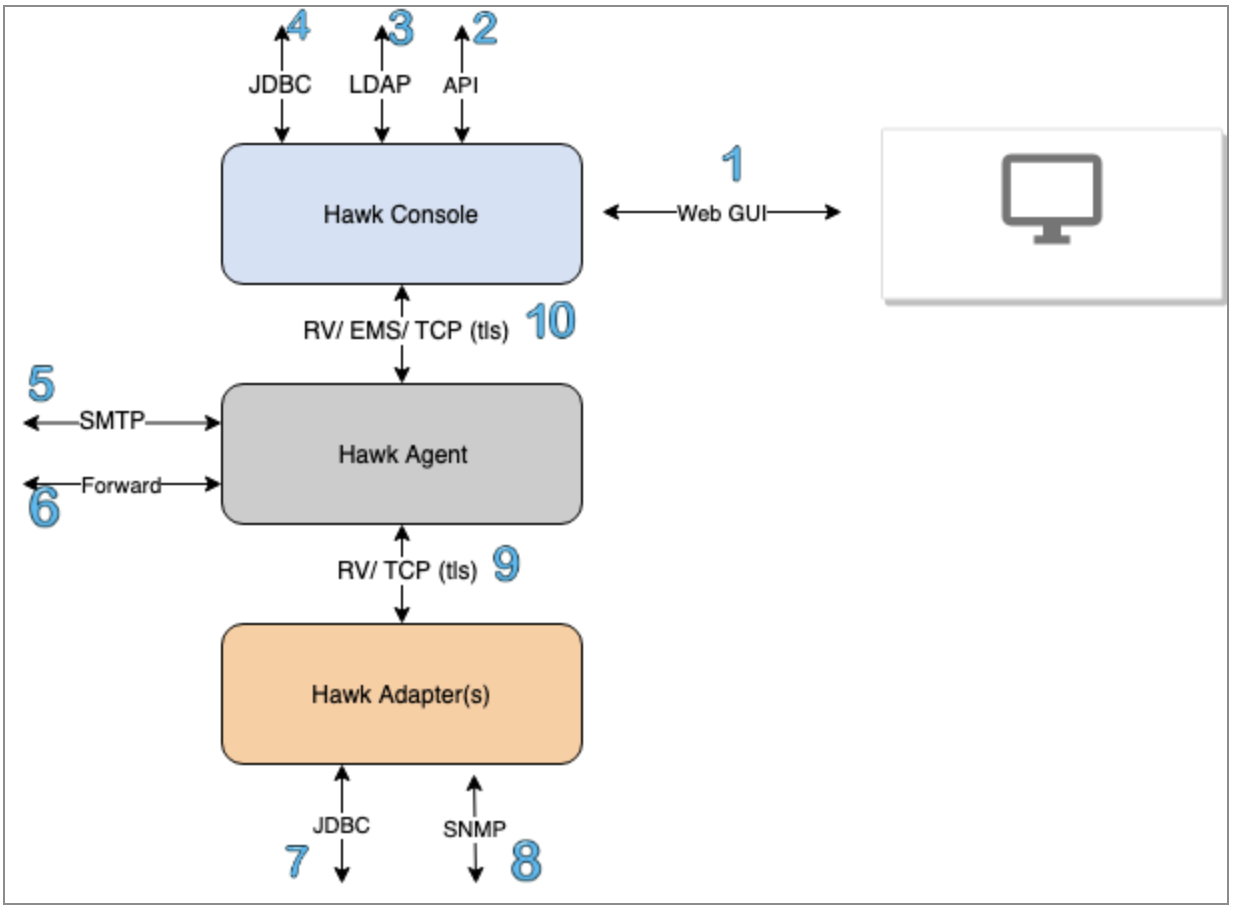
# Communication Channels and Their Security Configurations

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):<br>• Apache Ignite<br>• MySQL | Storing Hawk Alerts |
| | | JDBC (Event Service)<br>• IBM DB2<br>• Microsoft SQL Server<br>• Oracle<br>• Sybase | Storing Hawk Events and Alerts |
| 5 | SMTP | SMTP: TCP | Alerting |
| 6 | Forwarders<br>• Syslog<br>• ULDP | Syslog: UDP or TCP (TLS)<br>ULDP (TLS) | Data forwarding |
| 7 | JDBC | JDBC:<br>• Oracle<br>• Sybase<br>• Microsoft SQL | JDBC Adapter to monitor RDBMS databases, tables |
| 8 | SNMP | SNMP: UDP or TCP | SNMP Adapter |
| 9 | Hawk AMI Transport: | • TCP over TLS | TCP Transport offers TLS/ SSL |

| Key | Communication Channels | Connection | Description and References |
|---|---|---|---|
| | • TCP<br>• RV | • RV unsecured | support. For more information, see the *TIBCO Hawk Installation, Configuration, and Administration* guide. |
| 10 | Hawk Console API Transport:<br>• TCP<br>• EMS<br>• RV | • TCP over TLS<br>• EMS over SSL<br>• RV Unsecured | TCP Transport offers TLS/ SSL support. EMS transport offers SSL. For more information, see the *TIBCO Hawk Installation, Configuration, and Administration* 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



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.