TIBCO SCRIBE ® ONLINE SECURITY

This document provides an overview of security for TIBCO Scribe ® Online

© TIBCO® Software Inc. All rights reserved.

INTRODUCTION

TIBCO Scribe ® Online is a leading integration platform as a service (iPaaS) from TIBCO® Software Inc. It has a multi-tenant architecture that scales by distributing workloads across *Agents* that belong to each tenant. The cloud handles administrative tasks such as user management, connection management, integration design, scheduling, and monitoring. Agents carry out instructions they receive from the cloud, handling integration jobs and reporting results back to the cloud.

The platform uses C*onnectors* to communicate with specific applications, databases and file systems. Connectors address the specifics of each type of endpoint, including authentication, discovery of metadata, query formation, and target operations.

A comprehensive security model encompasses all aspects of the platform. The user interface, Agents, and third-party applications communicate with the cloud through secure channels. Connectors can be configured to use secure protocols to communicate with the APIs for the respective applications. Credentials are stored in encrypted containers and IP safe lists restrict access to specific tenants.

TIBCO Scribe ® Online adheres to the Trust Service Principles required for the Service Organization Control (SOC) 2 Report.

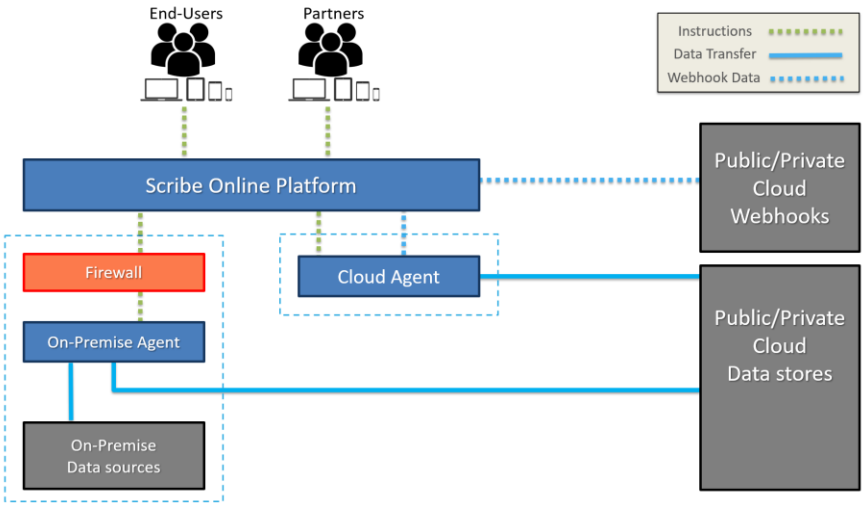
DETAILED OVERVIEW

The TIBCO Scribe ® Online production environment incorporates the highest security techniques and procedures. TIBCO ® has reviewed and adheres to the strict security guidelines in conjunction with SOC II compliance.

TIBCO® Software Inc. customers and prospects (under NDA) can request a copy of the SOC II report.

INFRASTRUCTURE OVERVIEW

TIBCO ® uses AWS for the core application and utilizes Microsoft's Azure Service Bus to facilitate near real-time communication with Agents.



Data transmitted to the TIBCO Scribe ® Online API end-points occurs over SSL / HTTPS connections. This ensures that communications from a TIBCO Scribe ® Online Agent to the cloud (https://agent.scribesoft.com), our

© TIBCO® Software Inc. All rights reserved. Other trademarks are the property of their respective owners

application server (https://app.scribesoft.com), or our API servers (https://api.scribesoft.com) is secure. We validate our endpoints using SSL Labs (see our A+ rating at Validate SSL). All business logic is governed at the API level. Further, we also "double encrypt" application credentials to mitigate man-in-the-middle attacks.

Other security precautions taken, but not limited to:

- Implemented patterns and practices to comply with SOC II since 2017.
- SOC II Certification as of 2018.
- Employs AES-managed encryption methods for storage of all sensitive data such as passwords and data at rest.
- All systems are behind a pair of Firewalls.
- Firewalls exists between public and private networks isolating access to Database servers.
- All sensitive communications between the client and the Web servers are encrypted via SSL.
- Password security: Passwords must be at least 8 characters consisting of at least one alpha and one numeric.
- Rigorous procedures and safeguards are in place to protect SSL and encryption keys.
- Routine vulnerability scans and penetration tests are performed by an outside vendor.
- Internal security scans are done every quarter or each release, whichever is sooner.
- We use a variety of systems to detect intrusions which includes, but is not limited to, the services offered by AWS.
- A process is in place to review system logs for anomalies and archives those logs.
- Regular Operating System security patches are applied.
- Virus protection system on all servers and the virus profiles are updated regularly.
- There is a strict policy of session timeouts of 120 minutes for all applications.

AGENT

Integration job processing happens on the Agent. Agents are responsible for carrying out the execution of the jobs and operate on compiled code which prevents hacking or code injection. Data does not flow through the TIBCO Scribe ® Online Platform directly; the Agent is responsible for connecting directly to any source or target system using a Connector. There are two varieties of Agents: those located in our Cloud or those downloaded and installed on local machines which is called an On-Premise Agent.

The configuration and design data are located in our US Data Center. Agents retrieve instructions from the Platform by initiating RESTful API calls and by attaching themselves to our Azure service bus. Because of this, they need to have at least port 443 available, but if real-time telemetry data is desired, we strongly suggest allowing additional ports. Details on whitelisting requirements can be found in the TIBCO Scribe ® Online Help.

EVENT PROCESSING

TIBCO Scribe ® Online can provide hosted end-points to receive messages from other systems which initiate integration processes. For example, when a record is updated in another system, it triggers a simple web service message that is received by TIBCO Scribe ® Online which, in turn, triggers off other integration processes.

These endpoints are hosted in our US datacenter and require SSL. Using a unique access token, users can update the URL to disable previously-given access. Additional security can be managed within the map using design

© TIBCO® Software Inc. All rights reserved. Other trademarks are the property of their respective owners

techniques. When the message is received is it directly relayed using the Service Bus to the Agent. The message is recorded in a database table and purged within 24 hours.

CONNECTOR

A Connector is compiled code which enables the data transformation to different systems. These are downloaded from our Marketplace and installed on the Agent. Connectors which are available in our Marketplace have undergone security certification, static code analysis, and other review measures to ensure they meet our strict security standards. Further, any Connectors provided by TIBCO ® have undergone further validation and QA testing, and are directly supported by TIBCO® Software Inc. Our Connectors use the secure authentication method as configured by the end-user which is provided by the application API.

CONTROLLING ROW FAILURE DATA

When a job runs, data on the status of the job is sent up to the Cloud so users can see real-time progress. The only time the contents of the job are returned to the Cloud is when an error occurs, so the details can be viewed and debugged. This option of returning the data to the Cloud can be controlled under security settings. If enabled, no source data is returned to the cloud. This option is only applicable when running an On-Premise Agent. Users may still initiate a reprocess of a message which directs the Agent to use the stored source data held locally to send. In this case no information is retransmitted to the TIBCO Scribe ® Online Cloud.

TEMPORARY DATA STORAGE

There are only two ways which source data is stored to the Platform from the Agent:

- When a failure occurs; however, there is a configuration at the Organizational level to restrict this, so that no data leaves the Agent and is not relayed to the Platform. This is locally stored Agent data is automatically purged after 45 days. Data is encrypted within our Blob Storage.

- User initiating a request within the Application to Preview or Debug a map, which sends a request to the Agent to send the data for the user. This is automatically purged after 24 hours.

DATA RETENTION POLICY

TIBCO Scribe ® Online stores error information for 45 days, after which that data is purged from the system. That data includes the error code and message, as well as a copy of the source data tied to that error for re-processing. If you would not like this stored in TIBCO Scribe ® Online, and you are using an On-Premise Agent, you can disable this feature by going to your security settings within the TIBCO Scribe ® Online organization to restrict the Source Data being moved to our Cloud.

DATA CENTER ASSIGNMENT

When an organization is created on TIBCO Scribe ® Online you can define which data center is to be assigned. This is both from a security and a performance standpoint. You can find a listing of our current data centers on our website. Cloud Agents are hosted by TIBCO ® and are located based on the data center. If the Agent is sending failed information for source rows, that detail is stored regionally in that data center.

© TIBCO® Software Inc. All rights reserved. Other trademarks are the property of their respective owners

TIBCO Scribe ® Online can provide end-points to receive data which triggers a Map to execute. These end-points are located based on the data center assigned to the Agent. Communication between the end-point and the Agent is direct, meaning it is geographically isolated and would not leave that datacenter.

You can find information on data centers and locations in TIBCO Scribe ® Online Help - Data Center Listing.

TIBCO SCRIBE ® ONLINE RELEASE TYPES

TIBCO Scribe ® Online has different types of releases that are associated with the Integration Platform. For each release type the following sections define the nature of the release, define what impact should be expected, and provide notification timing.

- TIBCO Scribe ® Online Platform, Application, and Agent Updates
- TIBCO Scribe ® Online Connector Update
- TIBCO Scribe ® Online Connector Release
- 3rd Party Connector Release/Update

TIBCO SCRIBE ® ONLINE PLATFORM, APPLICATION, OR AGENT UPDATES

TIBCO ® periodically releases updates to the TIBCO Scribe ® Online Platform, Application, and/or Agents, allowing us to add new capabilities and address issues found over time. These releases generally occur Friday evenings, US Eastern Time, to reduce any impact on system users. TIBCO ® issues a notification on our Trust Site two weeks before these updates are released, with a brief description or link to release notes with information about what is included.

In the course of normal software support and development, TIBCO ® will issue what we refer to as a "Hotfix". Hotfixes are typically issued to address a specific customer situation found in the field. Agent updates usually include a rollup of these fixes in the next version being released to make them generally available.

During the two-week notice period given for the Production release, we update our Sandbox environment to allow Customers to preview the new version prior to it being released. Unless otherwise stated, you should not need to update Solution/Maps since we strive to maintain compatibility. Customers are welcome to sign up for a Sandbox account at TIBCO Scribe ® Online DevPortal under Getting Started.

When the Production update begins, TIBCO ® posts a notice on the Trust Site letting everyone know that the release has begun. As soon as the update is complete, TIBCO ® updates the Trust Site with a notification stating that the update is complete.

The impact to system users is that the UI may become unavailable for a short time during the update. There is no impact to running integrations. TIBCO Scribe ® Online Agents do not perform an update while they are processing data; instead, they complete any running integrations and, when they are in an idle state, restart to complete the upgrade process.

Note: You may contact TIBCO Scribe ® Support before an Agent update and request that you be excluded. Once we release the Agent update, your Solutions remain in a Read-Only state until they are moved to an updated Agent. This allows you to manually move the Solutions to an upgraded Agent. This option is not available for those Solutions running on Cloud Agents. This must be requested prior to each release and be done 24 hours before the scheduled release.

© TIBCO® Software Inc. All rights reserved. Other trademarks are the property of their respective owners

TIBCO SCRIBE ® ONLINE CONNECTOR UPDATE

Connectors run on TIBCO Scribe ® Online Agents and handle the communication between third-party systems. Connectors created by TIBCO® Software Inc. undergo periodic updates to add new features, address changes to the endpoint API, or to address issues found over time. These Connector updates only occur for those Organizations that have installed the Connector from the Marketplace.

In the course of normal software support and development, TIBCO ® will issue what we refer to as a "Hotfix". Hotfixes are typically issued to address a specific customer situation found in the field. Connector updates usually include a rollup of these fixes in the next version being released to make them generally available.

TIBCO ® strives to issue update notifications on our Trust Site two weeks before these updates with a brief description or link to release notes with information about what is included. During the two-week notice period given for the Connector Update, we update our Sandbox environment to allow Customers to preview the new version prior to it being released. In the case of a critical issue or update we may need to shorten this timeframe.

TIBCO Scribe ® Online Agents do not perform an update while they are processing data; instead, they complete any running integrations, and when they are in an idle state they restart to complete the Connector upgrade process.

Note: You may contact TIBCO Scribe ® Support before a Connector update and request that you be excluded. This must be requested prior to each Connector release and be done 24 hours before the scheduled release.

TIBCO SCRIBE ® ONLINE CONNECTOR RELEASE

Connectivity to new applications is always being added and can be seen inside the Marketplace. When TIBCO ® releases a new Connector to the platform there is no impact to existing users. For any TIBCO Scribe ® Online Connector, there is a Success Community posting specific to that Connector and a new help file topic in the online help. There is no system notification via email for new Connectors on the platform.

3RD PARTY CONNECTOR RELEASE/UPDATE

Technology partners can create their own Connectors to be deployed on the TIBCO Scribe ® Online platform. For these partners, TIBCO ® provides some guidelines to make initial deployment and ongoing maintenance a smooth process. TIBCO ® does not notify users of any updates to the TIBCO Scribe ® Online Integration Platform for 3rd Party Connector Releases or Updates and relies solely on the partner to manage the notification of their customers.

TIBCO SCRIBE ® ONLINE SECURITY

BROWSER SECURITY

Standard testing for TIBCO Scribe ® Online includes only the last two versions of the following supported browsers:

- Microsoft Internet Explorer
- Mozilla Firefox
- Google Chrome
- Safari

All communication is done using SSL except for SignalR notifications.

© TIBCO® Software Inc. All rights reserved. Other trademarks are the property of their respective owners

We have implemented SignalR to provide real-time notifications to browsers and do not use SSL however these notifications do not contain sensitive information. You can find additional information on this technology at Microsoft - Introduction to SignalR.

APPLICATION SECURITY

TIBCO Scribe ® Online employs a unique model to user security. The model requires a TIBCO Scribe ® Online Admin user for a specific organization to invite other TIBCO Scribe ® Online users into that one organization. Without that invitation, there can be no access to the organization details, both from the UI or from the API.

TIBCO ® also allows you to define your own security rules, where you can restrict access to your organization's endpoint (for both Event-Based Integration as well as API access) to a defined IP range. You are in control of this from within the TIBCO Scribe ® Online UI, with separate approved zones for both the API and Event endpoints.

There is also the option to restrict the download of Agent logs.

AGENT SECURITY

Agents carry out the processing instructions. All data transformations happen in memory. Credentials and other security details are encrypted on the Agent.

DATABASE SECURITY

All customer Connection credentials are encrypted using Microsoft AES-256 bit encryption at rest and in motion. Passwords have an additional layer of encryption at rest.

Backups are performed using native database tools. Backups are compressed and encrypted when backed up locally. The backup is then uploaded up to Geo-Replicated cloud storage service via an encrypted connection. Database backups have a 45-day retention period.

INFRASTRUCTURE SECURITY

TIBCO Scribe ® Online's production infrastructure is hosted in exclusively in AWS and Microsoft Azure.

TIBCO® Software Inc. requires all visitors to be logged and escorted at all times. All external doors are key card locked. Only TIBCO ® Employees and authorized contractors or building management have access to the TIBCO ® facilities. The IT Data Room is safeguarded by key-card access which permits only authorized IT personnel into the room. This access is logged in the door management system. TIBCO ® also uses a 3rd party data center for disaster recovery purposes where key internal records are duplicated at that off-site data center. That data center only allows designated employees; visitors are not permitted. All office entry / exit doors and the IT room are monitored by security cameras. All entry / exit doors are monitored by a third-party security company.

EMPLOYEE SECURITY

All employees have annual IT security awareness training where they are required to read, acknowledge, and agree to the IT Security policy. New hires with the company are required to have a background check as a condition of employment.

© TIBCO® Software Inc. All rights reserved. Other trademarks are the property of their respective owners

All employees which have or could be granted access to production data have undergone a security background check prior to getting access. There is a clear division of access between development and DevOps and only supervised provisional access is granted to development as required.

SOFTWARE DEVELOPMENT POLICY

TIBCO ® has policies in place which guide our Software Development Life Cycle (SDLC). This includes peer reviews, static code analysis, and both manual and automated QA processes. On top of that, we routinely run performance testing on any new or updated software to ensure the highest quality.

There is a clear division between DevOps and development. Only as needed is supervised access given to production systems, and only for what is needed.

All changes are logged in our Source Code Repository. Additionally, out-of-band database changes are monitored by using a third-party tool from stories generated in our development management system. We also monitor the active directory for changes.

We leverage standard deployment tools to provision our servers. This ensures auditability and use of standard accepted configurations. We use Microsoft's guide to server hardening as a baseline for our images. We subscribe to the server hardening tactics recommended at Microsoft - Baseline Server Hardening Recommendations.

SECURITY INCIDENT RESPONSE

TIBCO ® has in place an incident response policy and plan. The policy ensures that information security incidents are identified, contained, investigated, and remedied. There is also a process for documentation, appropriate reporting internally and externally, and communication so that organizational learning occurs. Finally, it establishes responsibility and accountability for all steps in the process of addressing information security incidents.

This Policy applies to any computing or data storing devices owned or managed by TIBCO® Software Inc. that experience a Security Incident. It also applies to any computing or data storing device, regardless of ownership, which is used to store Protected Personal Data, or which, if lost, stolen, or compromised, and based on its privileged access, could lead to the unauthorized disclosure of Protected Personal Data.

TIBCO® Software Inc. has a TIBCO ® Privacy Policy which can be found at Privacy Policy.

DISASTER RECOVERY PLAN

TIBCO ® has a full Disaster Recovery plan in place. This plan has been accepted as part of our SOC 2 compliance by a third-party auditor. We test and update the plan annually or if the underlying technology or vendors change, and simply as needed.

For the TIBCO Scribe ® Online application, we leverage services hosted by underpinning contracts from Microsoft and Amazon. We leverage their resilient services wherever possible to enable automatically redundant features to support TIBCO Scribe ® Online. We have defined two disaster recovery sites to support TIBCO Scribe ® Online.

We have designated local alternate recovery facilities in the event of a local disaster that impacts our office. If necessary, we can share the summary DR plan under NDA, please contact scribesales@tibco.com for more details.

© TIBCO® Software Inc. All rights reserved. Other trademarks are the property of their respective owners

REFERENCE MATERIAL

- TIBCO ®'s Privacy Policy is located at: https://www.tibco.com/company/privacy.
- Trust and Uptime site for TIBCO Scribe ® Online is located at: https://trust.scribesoft.com/.
- TIBCO Scribe ® Online Data Center Locations: https://help.scribesoft.com/scribe/en/index.htm#sol/general/data_centers.htm
- TIBCO Scribe ® Online System Requirements: https://help.scribesoft.com/scribe/en/index.htm#sol/general/requirements.htm
- TIBCO Scribe ® Online Help: https://help.scribesoft.com/scribe/en/index.htm
- TIBCO Scribe ® Online DevPortal: https://dev.scribesoft.com
- For inquiries, please open a support case by visiting our community at: https://success.scribesoft.com.
- For sales related and general inquiries please contact your designated Account Manager or visit our website at https://www.scribesoft.com.

FAQ

ENCRYPTION

Q: **Is your solution's client authentication communication encrypted? If so, what type of encryption does it use?**

A: Yes. TIBCO Scribe ® Online uses a standard web browser as a client, and authentication communications are encrypted with the HTTPS (SSL) protocol.

Q: **Are the data transferred between the client and the application encrypted?**

A: Yes. All communication between the web browser client and the TIBCO Scribe ® Online servers in the cloud are encrypted using HTTPS.

Q: **Are the data encrypted when stored?**

A: Passwords are encrypted at the Agent level and source data is encrypted on the TIBCO Scribe ® Online cloud at rest. We have additional layers of encryption using other algorithms that vary depending on the storage location.

Q: **What security compliances do you adhere to?**

A: The TIBCO Scribe ® Online cloud runs in AWS, which provides our access to the design and management studio of the product. The way the TIBCO Scribe ® Online Agent architecture is built, if security is a concern you can run the data via a local Agent, in which case none of your data is processed via the TIBCO Scribe ® Online cloud. If you do decide to use a cloud Agent, they are hosted in Amazon AWS on TIBCO Scribe ® Online run and managed virtual machines. See other questions on HIPPA/PCI/GDPR.

AUTHENTICATION

Q: **What type(s) of authentication method(s) does your solution use to authenticate users?**

A: TIBCO Scribe ® Online authenticates its users using Microsoft's ASP.NET Membership provider. We use the option to store passwords only as hash codes.

Q: **What type of user access control is supported?**

A: TIBCO Scribe ® Online supports individual user access control, and each user account can be associated with one or more organizations. There are two permission levels, administrator and user, and an account can have different permissions in different organizations.

© TIBCO® Software Inc. All rights reserved. Other trademarks are the property of their respective owners

MISCELLANEOUS

Q: **Does the solution or application require that it be hosted on-premises or off-premises?**

A: TIBCO Scribe ® Online provides a cloud-based environment for managing connections, defining integration maps, scheduling jobs, and monitoring results. It uses an Agent to perform the actual integration work which is either deployed in the TIBCO Scribe ® Online cloud or on-premise.

Q: **Where is the TIBCO Scribe ® Online data center?**

A: The core application is hosted in AWS and Microsoft Azure. Customer can choose which geo-located AWS data center location to run cloud Agents from.

Q: **When using an online Agent syncing data between two online applications, where will that data reside?**

A: When a TIBCO Scribe ® Online Agent is processing data, that data is neither persisted to the Agent nor to our cloud database with one exception. If in trying to write data to the target connection the data fails to process, for example due to violation of some constraint in the target system, that row of data from the source is optionally persisted to our cloud database, in the case of using an On-Premise agent. If enabled, the data is stored encrypted.

TIBCO Scribe ® Online offers a security setting for each organization which prevents the Agent from sending up source record data to TIBCO Scribe ® Online. Users can still reprocess records as the details are kept a local Agent level.

Q: **How are credentials stored securely?**

A: Connection credentials are used in three circumstances: A) when testing a connection; B) when saving connections to our cloud database; and C) when processing data when an Agent is running a solution.

A. When a user tests a connection, the credentials are passed to the Agent using SSL encryption. We also add a basic level of encryption to the password so that even in test and development environments passwords are never transmitted as plain text.
B. When a user saves a connection, credentials are persisted in the cloud database using an AES algorithm and a 256-bit key. The implementation of the AES algorithm uses standard .NET code and follows the best practices for this type of encryption. The key is generated using a .NET library method, again following standard .NET code best practices.
C. TIBCO Scribe ® Online Agents store an encrypted copy of credentials in a local database. This encryption also uses an AES algorithm and a 256-bit key. The Agent does not save the key locally. It requests the encryption key via an SSL-encrypted web service call whenever it needs to use encrypted credentials.

Q: **What ports need to be open on our firewall for an On-Premise Agent to work properly?**

A: TIBCO Scribe ® Online makes use of the Azure Service Bus. If your on-premise Agent is unable to communicate with the TIBCO Scribe ® Online cloud, configure your firewall to allow the following:

- Outgoing TCP communication on TCP ports 5671, 5672, and 9350 to 9354
- Outbound HTTPS connection to Port 443

Additional information about this topic can be found in the TIBCO Scribe ® Online – Help under On-Premise Agent Requirements.

Q: **How do your cloud Agents communicate?**

A: TIBCO Scribe ® Online's Cloud Agents are hosted in Amazon AWS data centers. Each data center has two IP addresses that you must whitelist if you want to allow secure communication from our Cloud Agents to your on-premise systems.

For a current list of IP addresses for each data center, see the Whitelisting Requirements.

Q: **What are the system requirements for On-Premise Agents?**

© TIBCO® Software Inc. All rights reserved. Other trademarks are the property of their respective owners

A: The requirements can be found in our Online Help file topic On-Premise Agent Requirements.

CERTIFICATIONS

Q: **Is TIBCO Scribe ® Online HIPPA or PCI Compliant?**

A: Like many other software products, based on the implementation of TIBCO Scribe ® Online, we have found customers can adhere to provisions under HIPPA and PCI. Examples of this include storing data locally on an On-Premise Agent, restricting source data, and separation of duties and access to production and test organizations. Please contact us for more information on recommendations based on your specific requirements.

Q: **What about GDPR?**

A: TIBCO Scribe ® Online is compatible with GDPR. It moves data between business systems and does not normally store the data. The exception relates to record errors. When TIBCO Scribe ® Online encounters an error while moving a record, it stores a temporary copy of the record in case you want to reprocess the record later. While it is possible for a consumer's personally identifiable information to appear in a failed record, TIBCO ® removes this data automatically after a set time period, ensuring that your business will not retain a copy in the integration software.

© TIBCO® Software Inc. All rights reserved. Other trademarks are the property of their respective owners