TIBCO® Cloud Integration Security Overview

TIBCO Cloud Integration is secure, best-in-class Integration Platform as a Service (iPaaS) software offered in a multi-tenant SaaS environment with centralized management and administration. This document provides a detailed overview of the security framework, system design, and operational best practices powering the service.

TIBCO CLOUD INTEGRATION SECURITY

Security is the highest priority within TIBCO Cloud Integration. The product relies on the security best practices of our infrastructure providers, as well as on our own high standards.

This document contains information on the data center security standards providedby our infrastructure provider, on TIBCO infrastructure security, and on connections into the TIBCO cloud environment.

All customer data in flight is encrypted as is the logical separation between customers to ensure each customer's data is secure and only available to them.

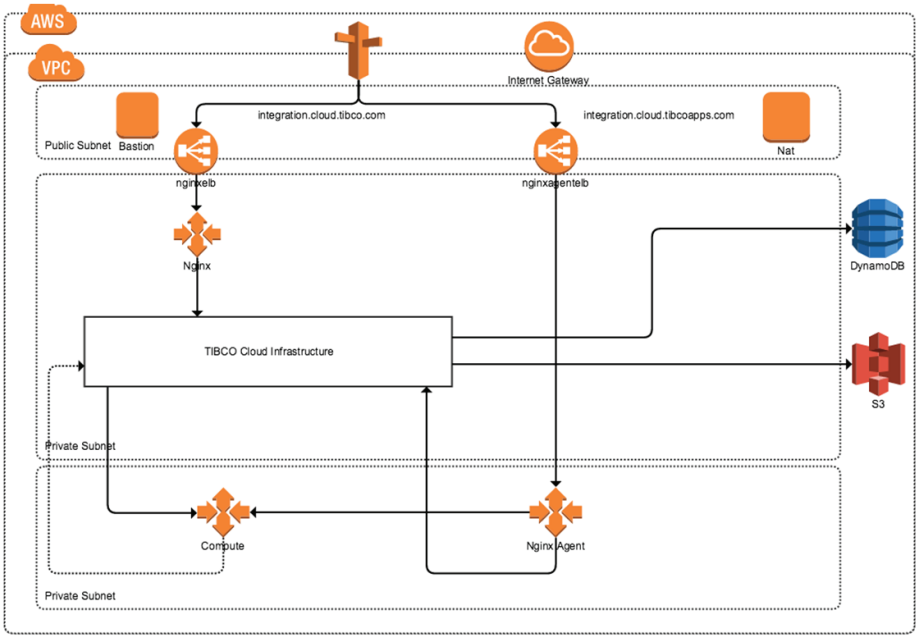
DATA CENTER SECURITY

The TIBCO Cloud Integration service runs on the Amazon Web Services (AWS) cloud platform and benefits from its world-class security features, technologies, and specifications as detailed in this document: Amazon Web Services – Overview of Security Processes

The TIBCO Cloud Integration platform adhers to the recommendations and best practices that are defined by Amazon in this document: Amazon Web Services – AWS Security Best Practices

INFRASTRUCTURE SECURITY

The following diagram provides an overview of TIBCO Cloud Integration network architecture.



VPC/NAT

TIBCO Cloud Integration uses AWS Virtual Private Cloud (VPC) with Class B (/16 Classless Inter-Domain Routing (CIDR).

The VPC uses private and public subnets. Each type of subnet is spread across three zones in an AWS region. End user applications and cloud infrastructure services run in different private subnets with no direct access from outside except through the Bastion host SSH port using SSH key access.

The VPC also uses a highly available Internet gateway and highly available network translation. There is Network Address Translation (NAT) in each zone with the ability to failover to a NAT in another zone.

SUBNETS

End user applications are run on an EC2 instance in a private subnet, isolating them from TIBCO Cloud Integration infrastructure services.

ELASTIC LOAD BALANCERS

All TIBCO Cloud Integration microservices are fronted by their own elastic load balancer (ELB). Transport level security is enabled for all ports exposed by the ELB.

Customer service endpoints deployed on the TIBCO Cloud Integration platform are fronted by their own ELB, thereby isolating them from other platform traffic. Transport level security is enabled for all ports exposed by the ELB. More information on ELB support for SSL and security groups can be found through these links:

Amazon Web Services – SSL Negotiation Configurations

Amazon Web Services – Configure Security Groups

SECURITY GROUPS

AWS security groups help control both inbound and outbound traffic. They provide logical grouping access in the VPC. It is easier to control traffic using security groups than IPs/CIDRs for access. Refer to the preceding link for more information on AWS support for security groups.

REVERSE PROXY

All TIBCO Cloud Integration microservices are fronted by an Nginx reverse proxy. Authentication and session management is enforced by the proxy. Transport Level Security (TLS) mutual authentication is terminated here for internal management services needing authorization.

Service endpoints of all applications deployed by customers are fronted by a separate Nginx reverse proxy thereby isolating application endpoint traffic from TIBCO Cloud Integration endpoint traffic. All communication to application service endpoints flows through HTTPS port 443. Reverse proxy also acts as a load balancer when multiple instances of the same application are running.

COMPUTE LAYER

All applications created by customers run in individual Docker containers on Amazon EC2 instances in the compute layer. This ensures that end user application code deployed to an EC2 instance does not interact in any way with other end user applications. It is also ensures that end user application code deployed to an EC2 instance does not interact with any TIBCO Cloud Integration microservices or with local Consul/Swarm daemons running on the host VM.

- Docker containers run with "--icc=false" to prevent network traffic between containers.
- IP routing table rules on EC2 instances prevent network traffic originating from Docker containers from reaching services running on the host VM.
- AWS security groups configured on the EC2 instance prevent network traffic originating from Docker containers from leaving the host VM.

PASSWORD ENCRYPTION SECURITY

TIBCO Cloud Integration does not store any application data until and unless designed by the customer in their integration flow. It only stores application configuration data such as passwords and secrets.

All secrets/passwords entered by end users are encrypted in the client(s) before being transferred over the wire. They are stored in the database in the encrypted format. When the customer application is deployed, the password(s) is decrypted and made available to the customer application.

This method ensures customer secrets are only accessible to their applications.

APPLICATION SECURITY

All applications that are created by customers on the TIBCO Cloud Integration platform can only be accessed by the Single Sign-on service provided by TIBCO Cloud. Transport level security for user applications is ensured by the TIBCO Cloud Infrastructure Security layer. For more detailed information, refer to sections VPC/NAT, Elastic Load Balancers, and Security Groups.

All applications on the TIBCO Cloud Integration platform are deployed inside a Docker container where the isolation of the applications is ensured by the TIBCO Cloud Infrastructure security layer. For more detailed information please refer to the sections Reverse Proxy and Compute Layer.

TIBCO Business Studio™ - Cloud Edition provides a secure way to push integration applications to the TIBCO Cloud Integration runtime. The security mechanisms that are used are similar to those described for the TIBCO Cloud - Command Line Interface in the section Session Security.

With TIBCO Business Studio - Cloud Edition, users have a rich set of policy features provided by TIBCO's ActiveMatrix BusinessWorks™ technology to ensure encryption, authentication, and confidentiality of the applications developed. Please refer to the section TIBCO Business Studio™ for detailed information. Applications built by users do not store data; users need to provision data storing in another way.

TIBCO Cloud infrastructure takes care of safeguarding secrets (e.g. passwords). Please refer to the section Infrastructure Security for more information on encryption of secrets.

SESSION MANAGEMENT

TIBCO Cloud integration uses TIBCO accounts for authenticating users.

- Authentication via a web browser is done using SAML 2.0 Web SSO Profile.
- Authentication via the command line interface is done using OAuth 2.0 password flow.
- TIBCO Cloud Integration issues a digitally signed JSON Web Token (JWT) containing the user profile data.
- A session is established between the browser or CLI and TIBCO Cloud Integration.

All sessions have the following characteristics:

- Inactivity timer of 30 minutes, which forces the user to login again if no activity is detected for that session.
- Twenty-four hour forced login. If a user stays active during 24 hours, a new login is forced.
- Single Sign-on for all TIBCO web properties.
- Single Sign-off for all TIBCO web properties.
- Transport Layer Security (TLS) is used for all communication.

ASSESSMENTS

To ensure that our environment stays secure after every release, we continuously test security. Using the Open Web Application Security Project (OWASP), TIBCO continuously updates the expected test results against emerging threats to ensure our servers remain running and our customers' data remains safe.

Customer's identity & authentication assessment

- Passwords are stored securely and managed separately by TIBCO IT.
- Signed SAML assertions or OAuth2 access tokens to convey identity; SSO pluggable.
- Cookies are secure and HttpOnly. Validity is increased by activity (30 is user friendly), but still capped for security (few days).
- All encryption keys are accessible only by TIBCO's CloudOps team.
- All operations logged and stored in separate machines.
- No PII in any URLs.

USER'S DATA SECURITY

- Use of HTTPS/TLS only and configured for use of high grade ciphers (grade A from http://ssllabs.com/).
- User apps are segregated from TIBCO infrastructure as well as from each other through VPC and other firewall settings.
- Clear protocols are in place for smooth upgrade procedures of key software parts allowing early and automatic software upgrades.
- User data is obfuscated so even limited TIBCO CloudOps personnel cannot access it.

TIBCO CLOUD INTEGRATION AVAILABILITY

TIBCO Cloud Integration has been designed with scalability as a core focus. It employs ELBs, auto scaling groups, and multiple instances of EC2 for running microservices with high availability and automatic scalability. It also limits OS access (CPU, disk, memory) to user apps through Docker security and configuration.

SECURITY REVIEW

TIBCO Cloud Integration has gone through internal security review using several tools, such as, IBM's AppScan and Tenable's Nessus.

VULNERABILITY TESTING

Common vulnerabilities testing includes test cases to find flaws in the TIBCO Cloud. OWASP top 10 vulnerabilities is the foundation for this vulnerability testing. A release does not go out without these items being tested and marked as completed:

NO.	OWASP TOP 10 (TEST TYPE)	TEST DETAILS
1	Injection	Blind SQL injection
2	Broken Authentication & Session Management	$5,000 Missing secure attribute in encrypted session (SSL) cookie

NO.	OWASP TOP 10 (TEST TYPE)	TEST DETAILS
3	Cross Site Scripting	Cross site scripting (reflected) Web browser XSS protection not enabled
4	Insecure Direct Object Reference	Hidden directory detected HTML comments sensitive information disclosure
5	Using Components with Known Vulnerabilities	Hidden directory detected HTML comments sensitive information disclosure
6	Cross Site Request Forgery	X-frame-options header not set X-content-type-options header missing Cross-domain JavaScript source file inclusion
7	Sensitive Data Exposure	Cacheable SSL page found HTML comments sensitive information disclosure Missing secure attribute in encrypted session (SSL) cookie Permanent cookie contains sensitive session information Query parameter in SSL request Application error disclosure Parameter tampering Password displayed as plain text

NO.	OWASP TOP 10 (TEST TYPE)	TEST DETAILS
8	Security Misconfigurations	Secure page includes mixed content, including scripts Buffer overflow Incomplete or no cache-control and pragma HTTP header set Cookie set without HttpOnly flag Password autocomplete in browser Cookie set without secure flag
9	Missing Function Level Access	UI show navigation to unauthorized functions Server side authentication or authorization checks missing Server side checks done that solely rely on information provided by the attacker
10	Unvalidated Redirects and Forwards	Redirect the request to a URL contained within untrusted input

TIBCO®

Global Headquarters
3307 Hillview Avenue
Palo Alto, CA 94304
+1 650-846-1000 TEL
+1 800-420-8450
+1 650-846-1005 FAX
www.tibco.com

TIBCO Software takes businesses to their digital destinations by interconnecting everything in real time and providing augmented intelligence for everyone, from business users to data scientists. This combination delivers faster answers, better decisions, and smarter actions. For nearly 20 years, thousands of businesses around the globe have relied on TIBCO technology to differentiate themselves through compelling customer experiences, optimized assets, and innovative new business models. Learn how TIBCO brings data alive at www.tibco.com.

01/30/17