

# TIBCO Cloud Integration Security Overview

---

## Certification and Compliance

TIBCO Cloud Integration iPaaS has been certified by independent auditors to meet the following requirements:

- SOC1 Type II and SOC 2 Type II Compliance
- ISO/IEC 27001:2013
- PCI/DSS Data Security Standard
- Health Insurance Portability and Accountability Act (HIPAA)\*

*\*TIBCO can enter into a business associate agreement (BAA) to address HIPAA. Please contact your account executive or customer success representative for details on a BAA or any other certifications.*

## European Union General Data Protection Regulation (GDPR)

TIBCO's GDPR posture:  
[www.cloud.com/trust-center](http://www.cloud.com/trust-center)

## Privacy Statement

TIBCO Privacy Policy:  
[www.cloud.com/trust-center/privacy](http://www.cloud.com/trust-center/privacy)

Within the TIBCO Cloud Integration platform, security is our highest priority. 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 TIBCO infrastructure security, on the data center security standards provided by our infrastructure providers, and on the connections into the TIBCO Cloud environment. Every customer's data is encrypted and logically separated to ensure it is secure and only available to them.

## TIBCO Cloud Integration Overview

---

TIBCO Cloud Integration secure, best-in-class integration platform as a service (iPaaS) is 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 that power the service.

## TIBCO Cloud Integration App Types

Several types of applications can be created using the TIBCO Cloud Integration iPaaS, including:

### Connect Apps

These apps require zero code and are configured completely in the Web UI. Connect apps can be used to connect SaaS and other systems using connectors. This type of app runs on a Windows service agent either in the TIBCO Cloud environment or deployed locally to avoid opening firewall rules for direct access to local systems. The services are isolated.

When deployed locally, the agents run the integration processes locally. The agent will retrieve compiled instructions from the cloud. Telemetry, status details, and execution details are securely pushed to the TIBCO Cloud environment to display in the UI or access via the API. Controls exist to restrict any error data from being sent to the cloud to keep sensitive data on the local environment.

## Integrate Apps

These are TIBCO BusinessWorks apps developed using the Eclipse-based integrated development environment (IDE), which provides a visual drag-and-drop interface that can handle complex app and data integration scenarios using a variety of TIBCO BusinessWorks plug-ins. The TIBCO BusinessWorks IDE uses a secure mechanism to push locally developed apps to TIBCO Cloud resources directly from the IDE, or a Command Line Interface (CLI) and be used. Access to APIs, which are consumed in the TIBCO Cloud environment, are available from the IDE while debugging applications. TIBCO BusinessWorks apps are deployed inside a Docker container where the isolation of the apps is ensured by the TIBCO Cloud infrastructure security layer. See the section on Hybrid Agent for connectivity options.

## Develop Apps

These are TIBCO Flogo apps based on the open source Project Flogo (flogo.io) framework. Develop apps are discrete event-driven microservices that are designed natively for real-time event/streaming integration patterns in the Web UI. TIBCO created Flogo Connectors that can be used in addition to open source contributions. This type of app is deployed inside a Docker container where the isolation of the applications is ensured by the TIBCO Cloud infrastructure security layer. See the section on Hybrid Agent for connectivity options.

## Node.js Apps

Node.js apps can be deployed in the TIBCO Cloud environment. These apps are deployed inside a Docker container where the isolation of the applications is ensured by the TIBCO Cloud infrastructure security layer. See the section on Hybrid Agent for connectivity options.

## TIBCO Cloud Integration Services

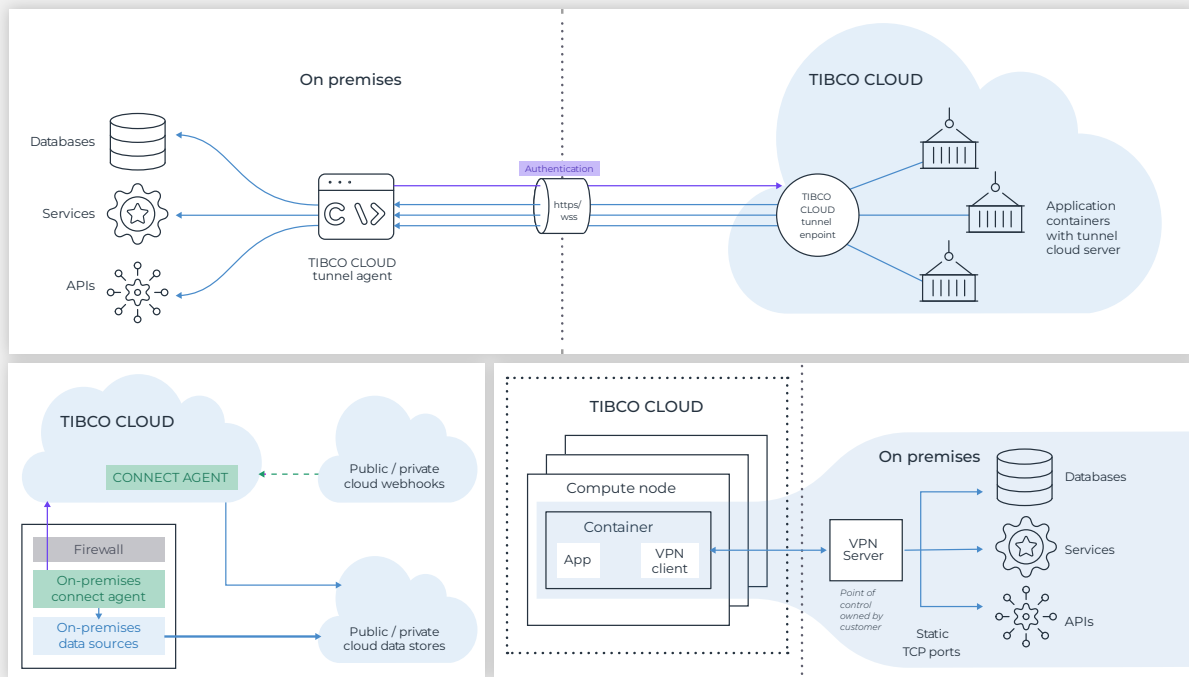
The TIBCO Cloud Integration iPaaS uses a combination of standard cloud services offered by hosting providers (Amazon, Microsoft, etc.) to provide security, load balancing, segmentation, and high-availability.

# TIBCO Cloud Integration Architecture

## Region and Data Center Availability

The TIBCO Cloud Integration platform is available on Amazon Web Services and Microsoft Azure.

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



*Connect, Integrate, Develop and Node.js Deployment Overview*

## Compute Layer

Applications (Integrate, Develop, and Node.js) created by customers run in individual Linux Docker containers in the compute layer. This ensures that end-user application code that is deployed does not interact in any way with other end user applications. It also ensures that end-user application code does not interact with any TIBCO Cloud Integration microservices.

## Runtime Processing/Deployment

Containers are used for Integrate, Develop, Node.js, and Mock capabilities. Depending on the license, these can be run on TIBCO Cloud infrastructure or in the hosting environment of your choice. If hosted in the TIBCO Cloud environment, customers can use the VPN or Hybrid Agent to establish connectivity with on-premises systems, apps and data stores.

TIBCO Cloud infrastructure supports Integrate, Develop, and Node.js apps on seamless upgrade paths. When one of these apps is upgraded, the new app version is started up before the old version is stopped, providing for zero downtime.

The Connect Agent provides runtime processing for Connect applications. This can be either deployed in the TIBCO Cloud environment as a Connect Cloud Agent, or downloaded to run the application locally. These agents can accomplish both cloud-to-ground and cloud-to-cloud.

## Application Scalability/Availability

TIBCO Cloud infrastructure has been designed with scalability as a core focus. It is a multi-tenant platform with customers logically separated. It limits OS access (CPU, disk, memory) to user apps through Docker security and configuration.

The TIBCO Cloud Integration Develop, Integrate, and Node.js apps can have multiple instances running simultaneously for automated load balancing. Having multiple instances running supports increased capacity and high availability.

Connect apps run on a TIBCO Cloud Agent and are monitored and managed by TIBCO.

## High Availability

Integrate, Develop, and Node.js applications are executed in an availability zone that is automatically selected based on available resources. TIBCO will automatically switch apps to a new zone if the original zone goes down or stops reporting status. Apps are scaled across multiple zones for high availability and to ensure that the load is distributed evenly by the system.

## Integration Lifecycle Management

The TIBCO Cloud Integration iPaaS provides tools to simplify lifecycle management by creating logical segmentation between teams that manage different phases of the integration lifecycle, such as development, quality assurance, user acceptance, and production.

## Child Organizations

Child Organizations provide a logical boundary or container where your apps and any associated configuration information resides. In your TIBCO Cloud Integration subscription you are granted access to your top-level or parent organization. At that point, you can choose how to organize the next level of your organization by generating several child organizations. Details on this process can be found here:

<https://support.tibco.com/s/article/App-Lifecycle-in-TIBCO-Cloud-Integration-TCI>

## Security

---

TIBCO maintains a company-wide information security management system and control program that includes security policies, standards, and procedures based on ISO/IEC 27001:2013.

### Identity and Access Management

All users of the TIBCO Cloud Integration iPaaS must log in to the TIBCO Cloud environment by using their federated credentials to enable user authentication and role-based access management. TIBCO Cloud Integration software defaults to using TIBCO accounts for authenticating users. Alternatively, customers can configure external identity providers (a SAML 2.0 compliant provider, Google, LDAP, or JWT-based OAuth for OEMs).

- Authentication via a web browser is done using SAML 2.0 Web SSO Profile.
- Authentication via the command line interface (CLI) is done using OAuth 2.0 password flow.
- TIBCO Cloud Integration software 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 log in again if no activity is detected for that session.
- A 24-hour forced login; if a user stays active for 24 hours, a new login is forced.
- Single sign-on for all TIBCO web properties.
- Single sign-off for all TIBCO web properties.
- Default Transport Layer Security is TLS 1.2 for all communication.

The TIBCO Cloud Integration iPaaS provides a centralized location to manage all integrations in one place. Child organizations can be created for logical separations between teams using the platform. This restricts user access only to organizations that are relevant to their business role. Additionally, all users must be assigned a role to ensure all employees have the correct permissions levels.

Roles are assigned at the organization level (either child or parent), which allows fine-grained control over team member access and permission level in each organization.

User Roles:

- **Organization owner:** Administrator at organization level can invite users to join the organization and domains, and manage roles at domain level.
- **Team member:** Any user who is invited by organization owners to join their organization.
- **Team administrator:** Administrator at domain level; can manage roles only at domain level.
- **Read-only:** Read-only permissions.

App developers can be assigned to Integrate, Develop, and Node.js apps that gives them control over a particular app. Other team members can see the developer's work, but cannot make updates. History and other tracking details are provided to users.

## TIBCO VPN Support

You can configure a virtual private network (VPN) client within TIBCO Cloud Integration software to connect to a VPN server within your network, with the exception of Connect Apps. This enables Integrate, Develop, and Node.js apps hosted in TIBCO Cloud Integration system to connect to services running on-premises in your network using the VPN. Your on-premises services such as JDBC, FTP, and JMS could then be used by TIBCO Cloud Integration apps. It does not require exposing your database or service as a public internet service, so there are no open ports on your side.

VPN connectivity supports Cisco AnyConnect SSL VPNs (using the Cisco AnyConnect protocol) and Juniper SSL VPNs (using the Juniper Network Connect protocol). For more details, see Prerequisites.

## TIBCO Cloud Integration Hybrid Agent

The TIBCO Cloud Integration Hybrid Agent is a lightweight program that you run locally to facilitate communication between on-premises apps and TIBCO Cloud Integration. With the Hybrid Agent, you can:

- Establish tunnel connections to apps running on TIBCO Cloud Integration. In TIBCO Cloud Integration, you can configure an app to use the tunnel to connect to on-premises resources like a database server, a JMS server, or a REST server.
- Stream logs directly from a TIBCO Cloud Integration app container.
- Securely communicate information on registered remote apps, such as monitoring statistics, app status, and other app details. Remote apps are displayed in TIBCO Cloud Integration on the Apps list. You can see and monitor your remote apps the same way as your cloud apps.

You can configure your Integrate, Develop, or Node.js app within TIBCO Cloud Integration software to connect to a TIBCO Cloud Integration Hybrid Agent running within your network. This enables you to connect apps hosted in TIBCO Cloud Integration environment to services running on-premises.

Using the TIBCO Cloud Integration Hybrid Agent, your on-premises services such as JDBC, FTP, JMS, could then be used by TIBCO Cloud Integration apps. It does not require exposing your database or service as a public internet service, so there are no open ports on your side.

The TIBCO Cloud Integration Hybrid Agent consists of a downloadable client that is executed on-premises. The client can be executed on the command line and establishes a tunnel connection to a given app running on the TIBCO Cloud Integration iPaaS. On TIBCO Cloud Integration software, you can configure apps to use the tunnel to connect to these on-premises applications.

TIBCO Cloud Integration Hybrid Agent uses the secure WebSocket protocol (WSS on top of TLS) as the transport layer between on-premises resources and TIBCO Cloud resources. The connection is initiated over HTTPS/WSS using TLS encryption. Once established, TIBCO Cloud Integration Hybrid Agent uses an additional protocol on top of a secure WebSocket connection, ensuring that the caller is authenticated.

The TIBCO Cloud Integration Hybrid Agent is designed to support both high availability and fault tolerance.

## Application Endpoint Security

The ingress traffic is separated between apps and TIBCO services thereby isolating app endpoint traffic from TIBCO Cloud Integration software. All communication to the app service endpoints flows through HTTPS port 443. Data in transit is encrypted using TLS. TLS 1.2 is fully supported and is used to do key negotiation over EC/RSA and SHA-2. Clients may choose AES 256 bit encryption. Note that for wider acceptability, ciphers with both AES 128 and AES 256 are supported. Clients may choose to negotiate only stronger AES 256 ciphers. A reverse proxy acts as a load balancer when multiple instances of the same app are running.

## Whitelisting Requirements

- Details for the whitelisting requirements on Connect apps can be found [here](#).
- Details on whitelisting requirements for Integrate, Develop, and Node.js apps can be found [here](#).

## CI/CD Processes/Change Management

Implement change management controls via seamless connectivity to your preferred version control system by using a combination of CLI tools and RESTful APIs. You can also integrate with systems like Jenkins, Maven, etc.

## App Monitoring

In-application monitoring details are available, but in addition to that, customers can use a combination of the TIBCO Cloud Command Line Interface or RESTful APIs to access logs that capture details. This is a perfect choice when using TIBCO Cloud Integration software in combination with other log and monitoring tools or SIEM software.

## Connector/Plug-in Security

A connector/plug-in is compiled code that enables data transformation to different systems. Connectors are available from the Marketplace within TIBCO Cloud Integration software and installed on the agent. TIBCO BusinessWorks plug-ins are available via a download eDelivery portal hosted by TIBCO.

Connectors and plug-ins are thoroughly tested and validated, which includes static code analysis and other review measures, to ensure they meet our strict security standards. Furthermore, any connectors/plug-ins provided by TIBCO have undergone validation and QA testing, and are directly supported by TIBCO. Our connectors use secure authentication methods configured by the end user, which is provided by the application API.

## Connect Agent Security

Data transmitted by the Connect Agent to TIBCO Cloud API endpoints occurs using TLS 1.2 or higher. All data stored locally on the agent is encrypted.

## Data Storage and Encryption

---

### Data Stored in the TIBCO Cloud Environment

The TIBCO Cloud environment will store customer data in a multi-tenant data repository. Sensitive data is encrypted at rest.

Data at rest is encrypted using AES 256. The encrypted key is transported or stored encrypted using RSA 2048 with SHA-2.

### Data Retention Policy

TIBCO regularly backs up service systems for customers to ensure adequate recovery capabilities. Backups are appropriately protected to make sure only authorized individuals are able to access the protected data, including but not limited to encryption of data stored off-site in electronic media and appropriate classification and protection of hard copy records. If not separately backed up, TIBCO secures any files containing protected data against unauthorized access in accordance with the terms of the agreement until the backup tapes are recycled or properly destroyed so that the information on them cannot be read or reconstructed.

The TIBCO Cloud Integration iPaaS stores transactional information for up to 45 days, after which 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. Diagnostic and other log data is kept for up to 365 days. Log data, such as API logs, does not include personally identifiable information but does include audit information such as IP addresses, user names, dates/times, and the list of API calls made. These logs are retained for 60 days.

In the case of the Connect On-Premises Agent, you have control over any source record error information that is sent to the Cloud. This information is only used for the reprocessing of a transaction. If you do not want this stored in TIBCO, and you are using an on-premises agent, you can disable this feature.

### Data Persistence

TIBCO Cloud Integration software does not store any app data unless designed by the customer's integration flow, except in the case of Connect apps.

Connect apps automatically track execution runs, which includes status, details on records processed, and more. Customers can control whether any source record error information is sent back to the cloud when using an on-premises Connect Agent. This information is only used for the reprocessing of a record. If you do not want this stored in TIBCO Cloud software and you are using a Connect on-premises agent, you can disable this feature by going to your security settings. Customers can also create their own error handling process, regardless of cloud or on-premises agent and store or ignore that failed data in a location of their choosing.

Logs for all app types are accessed via the user interface. With Integrate and Develop apps, users can also use the TIBCO Cloud Integration Command Line Interface (CLI). Additional information can be implemented by the user and recorded in these logs.

Metadata related to connections is cached either in the browser or stored on TIBCO Cloud infrastructure.

## Password Encryption Security

Passwords used to connect to other systems are handled in two ways.

For Integrate, Develop, and Node.js apps, the password is captured before the app is deployed into a container. Password property is handled by a privacy service which is part of TIBCO Cloud infrastructure.

Connect apps use a centralized data store with encrypted details for the connection properties. Before these details are transferred over secure channels, they are encrypted with a tenant specific key, then stored in an encrypted format. When the app is deployed, the password(s) are decrypted and made available to the customer app. This method ensures customer information is only accessible through their app.

### User Data Security

- TLS 1.2 or higher is required for any inbound traffic to the TIBCO Cloud environment.
- Use of HTTPS/TLS only and configured for use of high-grade ciphers.
- 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.

## Secure Software Development Lifecycle Practices

We continuously test security to ensure our environment stays secure after every release. 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.

TIBCO is addressing the secure development lifecycle by adding security-related activities to our existing product lifecycle (PLC) development process. This approach helps ensure that security development activities, such as security risk analysis, code review, static code analysis, and penetration testing, are an integral part of the development effort. The objective is to discover and reduce vulnerabilities early by effectively building security into the development process.

# TIBCO DevSecOps

---

## Security Review

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

## Vulnerability Testing

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

- Blind SQL Injection
- Broken Authentication & Session Management
- Cross-site Scripting
- Insecure Direct Object Reference
- Use of Components with Known Vulnerabilities
- Cross-site Request Forgery
- Sensitive Data Exposure
- Security Misconfigurations
- Missing Function Level Access
- Unvalidated Redirects and Forwards

## Access Control

All apps that are created by customers on the TIBCO Cloud Integration platform can only be managed by the single sign-on service provided by the TIBCO Cloud environment. Transport level security for user apps is ensured by the TIBCO Cloud Infrastructure security layer. All apps on the TIBCO Cloud Integration platform are deployed either inside a Docker container where the isolation of the apps is ensured by the TIBCO Cloud Infrastructure security layer, or by using isolated services in the case of Connect apps.

## TIBCO Secure Software Development Lifecycle

TIBCO has policies that guide our software development lifecycle (SDLC). They include peer reviews, static code analysis, and both manual and automated QA processes. In addition, 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. Supervised access is given to production systems only as needed and only to specific sections.

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 the use of standard accepted configurations. We use Microsoft's Guide to Server Hardening as a baseline for our imaging.

All employees are required to complete and comply with mandatory security training.

### **Data Center Security**

TIBCO Cloud Integration infrastructure is hosted exclusively in AWS and Microsoft Azure. TIBCO Cloud Integration software is deployed globally in multiple independent data centers across the US, EU, and APAC. A complete list of data centers can be found in the TIBCO Cloud Integration Documentation Center.

### **Status/Trust Site**

Publicly accessible status reporting can be found [here](#).

### **Software Release Policy**

TIBCO has a stringent software release policy. Notifications on pending releases are updated on the public status site prior to the release where possible. Urgent or critical releases may bypass this notification if deemed required; however, the release will be documented.

### **Security Incident Response**

TIBCO has an incident response policy and plan. The policy ensures that 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, our policy establishes responsibility and accountability for all steps in the process of addressing information from security incidents.

### **Business Continuity and Disaster Recovery**

The TIBCO Business Continuity Plan (BCP) maintains continuity of critical business operations and availability of critical business services during a disruptive event and provides predetermined guidelines, procedures, and information to effectively and efficiently manage an unexpected disaster or business disruption.

TIBCO has a full Disaster Recovery (DR) plan, including two defined disaster recovery sites to support TIBCO Cloud Integration software. This plan has been accepted as part of our SOC 2 compliance by a third-party auditor. We test and update the plan annually, if the underlying technology or vendors change, or as needed.

The TIBCO DR plan includes procedures for responding to emergencies (natural disasters such as fire, earthquakes, or hurricanes, or other disasters such as sabotage, virus, and terrorism), and includes: (i) descriptions of roles and responsibilities: identifying key individuals and the recovery team responsible for implementing recovery actions; (ii) data backup plans, providing for periodic backups of data from database systems that can be used to reconstruct data; (iii) contingency plans and disaster recovery guides that will be followed by members of the recovery team before, during, and after an unplanned disruptive event in order to minimize downtime and data loss; and (iv) procedures for annual testing and evaluating the Contingency and Disaster Recovery Guide including documenting the tests in writing.

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 Cloud Integration software.

TIBCO's Recovery Point Objective (RPO) is 24 hours, Recovery Time Objective (RTO) is eight hours. (Runtime traffic is handled directly and not part of the backup.) In addition, we perform a disaster rehearsal twice a year.

## TIBCO Support Service Levels

The TIBCO Cloud environment has dedicated technical support available by phone, email, or web as well as free online technical resources. [For details please take a look at the terms.](#)



**TIBCO Software**  
a business unit of  
Cloud Software Group, Inc.

4980 Great America Pkwy  
Santa Clara, CA 95054  
[www.tibco.com](http://www.tibco.com)

TIBCO, a business unit of Cloud Software Group, has helped global enterprises solve their most complex business challenges for more than 25 years. The TIBCO Platform delivers industrial-strength solutions that meet the highest performance, throughput, reliability, and scalability needs while offering the widest range of technology and deployment options to deliver real-time data where it's needed most. Learn how TIBCO solves its customers' mission-critical software needs at [www.tibco.com](http://www.tibco.com).

©2021–24, Cloud Software Group. All rights reserved. TIBCO, the TIBCO logo, and Enterprise Message Service are trademarks or registered trademarks of Cloud Software Group, or its subsidiaries in the United States and/or other countries. ApacheHadoop, HBase, Hive, Impala, and Subversion are trademarks of The Apache Software Foundation in the United States and/or other countries. All other product and company names and marks in this document are the property of their respective owners and mentioned for identification purposes only.

01Aug2024