sendflex
TECHNOLOGY

transtream

# Ship Anywhere. From Anywhere.

## Technical Overview

sales@sendflex.com 508.786.1919 www.sendflex.com

# Transtream Apps Automate Transportation Processes, from Purchase to Payment

## Introduction

Transtream is a scalable enterprise-class transportation platform. While this document is focused on Transtream Cloud, the platform can be deployed on-premise or accessed from our multi-tenant cloud environment. Transtream delivers a suite of secure browser-based transportation capabilities across the corporate network or Internet to a workstation or mobile device including:

Transtream Warehouse: Automate high performance parcel and freight shipping, print and apply labeling, and material handling controls within production shipping environments.

Transtream Store: Make it easy and convenient to ship from low volume stores, depots or parts distribution centers.

Transtream Office: Make it easy to control departmental expenditures by providing employees with the ability to manage addresses, create labels at their desktop or print authorization forms to be processed in the mailroom.

Transtream Widgets: Add carrier delivery service selection to shopping carts and build customer loyalty by providing a simplified returns process with Transtream widgets embedded within your site.

Opdimizer: Instantly determine the most costeffective and efficient way to pack orders using our cartonization engine, Opdimizer. Reduce unexpected dimensional weight charges by selecting the best cartons every time.

Composer: Modify Transtream's award winning apps to fit your organization's workflows and business rules. Composer is a drag-and-drop design studio that provides the flexibility to change as your business needs change.

Integration: Use our integration and mapping tools, APIs, and SDK to automate data exchange with enterprise systems. HubCapp is our Internet of Things (IoT) technology that connects Transtream cloud apps to on-premise systems and devices, and widgets within your web pages.

## KEY FEATURES

### Scalability

Transtream scales both horizontally and vertically, employing a stateless architecture that allows it to simply scale using standard load balancing options.

### Audit

With the focus on security, Transtream undergoes third party assessments and penetration testing to ensure your data stays safe.

### Network Security

Application tiers are isolated from data tiers to ensure no direct access to your data is possible without going through one of our applications.

### Data Privacy

Credentials of any type are stored as hashed values ensuring security of information. In addition, Transtream uses HTTPS for data in transit and can utilize standard Microsoft SQL Server options for encrypting data at rest.

### Data Center Security

Transtream Cloud is deployed in IBM's data center(s), providing one of the most secure and stable environments, so you can be sure to keep your business functioning.

### Single Sign-On

Transtream utilizes an in-house built Pierbridge Identity Provider (IdP) which provides authentication as a service to the product. It is capable of single sign-on with multiple clients and apps and allows to federate authentication to third party IDPs. The new IdP supports the following protocols: OpenID Connect, OAuth2 and SAML 2.0.

# Architecture

Transtream is an SOA platform built on standard .Net and IIS technology and is comprised of four Web Service components:

Composer is the presentation layer component of the platform that renders all applications to users. In addition, it provides Composer Designer, enabling drag-and-drop tools to compose application and widget workflows, business rules, and applies user access rights.

Logistics Server is the application layer component of the platform that manages transportation functions, connectivity to carriers and logistics service providers for automating rating, shipping, labeling, tracking, and other transportation and logistics functions.

Data Engine enables Transtream to connect and communicate in real-time with disparate systems, databases, applications, and other enterprise data sources.

HubCapp extends Transtream's connectivity to web pages, REST end points, local data sources such as databases or files, and local devices such as scales, thermal printers, meters, and mobile devices. HubCapp also provides secure page-topage communication when embedding Transtream widgets into your site(s) or application(s).

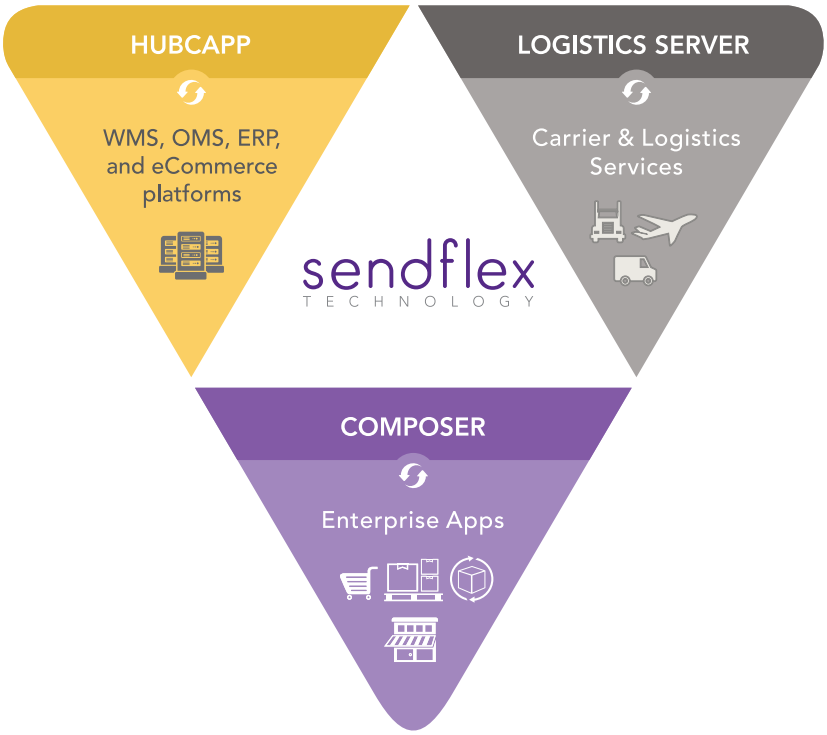
Transtream is accessed on almost any device using a standard web browser, whether on a PC, Mac or mobile device. There are several authentication options available, but in all cases a user is authenticated and is then able to access applications and functions for which they are authorized. Users are provided access to any Transtream application that the assigned user or group has been given permission to access, including links to data sources and devices. Transtream is stateless and therefore no persistent connection is established. In addition, no executables or plug-ins are loaded into the browser, but depending on the configuration and functions enabled in the application(s) an executable/application may be loaded on the workstation for the purposes of printing to thermal printers, reading a scale or accessing meters.

## Software Design

### Secure Architecture

Transtream's service-oriented architecture is designed to ensure robust and secure operation while integrating seamlessly and in real-time with a company's existing network and security infrastructure, including IIS.

Transtream software undergoes rigorous penetration testing throughout the product development lifecycle. In addition, regularly scheduled secure coding workshops and penetration tests are conducted by third parties to ensure total data security.



# SOA, Web Services

## API'S

Transtream provides an XML interface that allows customers and third-party developers to perform transportation functions, such as ship, rate, route, and void. To ensure connectivity to the many disparate platforms we encounter in customer environments, Transtream's interface is a simple HTTP(s) post of an XML document which results in an XML response message to the requestor. In addition to the functions noted above, there are many more, including but not limited to cartonization, rate shopping, time in transit, etc.

In addition, an API is also available for administrative functions, allowing for other applications to execute configuration tasks that would otherwise be done using Transtream's administrative application(s). The functions included allow you to add users, locations, carrier accounts, output configurations, and much more.

## Integration Options

Transtream's extensible architecture provides for options from the simplest integration, to the most complex. As noted above, there are standard APIs for systems and developers who wish to integrate transportation functions within their applications. In addition, Transtream can perform real-time integration to other systems. One of the simplest being direct database connectivity for SQL Server, MYSQL, Oracle and others, making for quick and easy integration to databases. Pre-built connectors to other systems like NetSuite, Prophet21 and Epicor allow for out-of-thebox integration to these systems. When these options aren't sufficient, implementation resources can create custom connectors that plug into the platform in the same way as our standard options. This makes for almost limitless options for integration.

Our HubCapp technology makes this, and more, possible whether Transtream is deployed on-premise or hosted in the cloud. Further, it expands the capabilities allowing for integration to data that might be local on a user's workstation (i.e. Excel spreadsheet) or devices such as scales, dimensioning hardware, and thermal printers.Further, it expands the capabilities allowing for integration to data that might be on a local workstation (i.e. Excel spreadsheet) or devices such as scales, dimensioning hardware, and thermal printers.

# Development

## Agile

To remain in compliance with carriers' constant requirements evolutions, we follow the Agile development process to exceed what our partners and customers expect. Scheduling development sprints and releases as needed to stay compliant, building on capabilities to continually add value for our customers. The transportation industry is constantly changing/evolving and therefore we must ensure we have constant review and prioritization of requests and changes that feed the development process.

## Release Schedules

Transtream's versioning is based on a Version.Revision. Patch numbering scheme. Patches are released as needed to correct any issues found within the software. Revisions are generally released at least once per quarter, but often monthly as carriers dictate changes. Revisions roll up the patches that were released in between the last revision and the current one, and provide small feature enhancements or additions to the platform. Versions are reserved for major initiatives and happen maybe once or twice per year depending on the scope of functionality being planned in a particular year.

## Maintenance Windows

Our multi-tenant cloud environment is architected to allow us to gradually update customer tenants. When updates are required, we announce maintenance windows at least 30 days ahead of time and schedule them for off hours (normally between a Saturday morning and Sunday evening) and for only the amount of time necessary to perform the update. We also look to avoid using a maintenance window during busy season(s) for our customers to ensure there is no impact to their businesses.

# Secure Environment

All or some of Transtream components can be deployed on-premise or within our highly secured, redundant Transtream Cloud environment. Transtream Cloud supports both multi-tenant and private cloud solutions, allowing customers to choose the option that best meets their corporate requirements.

## Facilities

Our Transtream Cloud environment is deployed at IBM Softlayer facilities. The primary platform is deployed in the Dallas, TX data center, and the secondary data center is located on the outskirts of Washington DC. Physical access to Transtream Cloud servers is restricted and servers are installed within locked cages, which are monitored by cameras 24/7 within the mirrored IBM Softlayer facilities. Remote/system access to these environments is also strictly limited with all access centrally managed to ensure no unauthorized access.

## Network

Our Transtream Cloud implementation utilizes multi-layer perimeter security, provided by a firewall between the load balancer and the application server(s) as well as network separation of the application servers from the back-end databases. This ensures segmentation of components and data, protecting customer information from unauthorized access.

## Platform

Transtream Cloud runs on Windows Server 2016 and MS SQL Server 2017 with the latest security patches installed. Servers have been penetration tested, and system logs are continuously audited for suspicious activity.

## Administration

Transtream Cloud servers are administered over a secure VPN connection to our Dallas and Washington DC facilities by a limited number of Pierbridge employees. This group of authorized administrators is kept small and is strictly managed to ensure no unnecessary employees have access.

VPN supports authenticated and encrypted remote login access by our staff. An intermediate server handles and authenticates all connections, thereby avoiding open ports and ensuring very tight access control.

## Scalable and Reliable

The Transtream Cloud infrastructure is both robust and secure. Redundant routers, switches, server clusters, and backup systems are used to ensure high availability. Transtream's stateless architecture allows for scalability and reliability using standard load balancers. The load balancers transparently distribute incoming requests among Transtream Cloud servers, with each request routed based on system availability to ensure consistent responses for our customers.

## Separate Databases

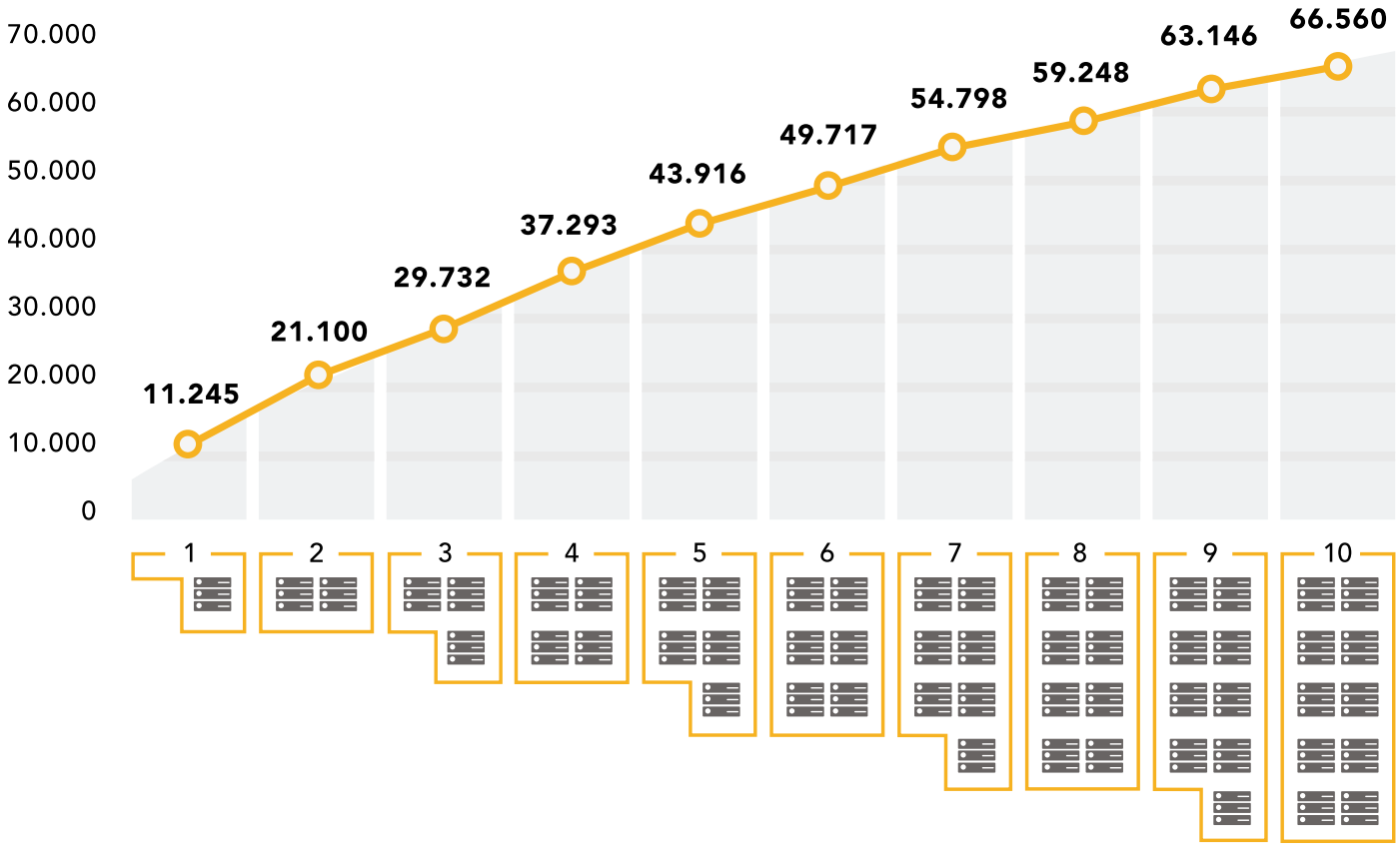
Data for each Transtream Cloud tenant (customer) is stored in a separate database to eliminate the possibility of confidential data disclosure across tenants. This architecture, along with other technology configurations, ensures isolation of customer data and processes.

# Performance

Transtream is comprised of a combination of web services; each web service can run independently as a node or can form part of a distributed node set to provide greater availability in the event of hardware failure. Network load balancing is used to enable multiple nodes to run from a single service URL, delivering greater resilience in the event of node failure and improved transactional throughput. SQL Clustering and Availability Groups are used to achieve the same effect for the application databases. A SQL cluster in the primary data center is mirrored in the secondary data center using the configured availability groups so that should the primary data center fail for any reason, all transactional and configuration data are safe and accessed by application servers to keep customers running.

## Throughput

Throughput for a particular customer will vary based on network connections/latency between our customers' networks and the Transtream cloud environment. The architecture is designed to ensure that the system responds to requests as quickly as possible, normally within a second or less depending also on response times from carrier APIs.




## SLA's

Transtream delivers up to 99.99% availability across the platform, excluding maintenance windows.

# Reporting

## Standard Reports

Transtream provides a number of standard reports. These include:

- Shipment detail by carrier
- Shipment summary by carrier
- Shipment detail by customer
- Shipment summary by customer
- Package detail by carrier
- Package summary by carrier
- Package detail by customer
- Package summary by customer
- Carrier tracking/delivery reports
- Shipment detail by cost center
- Shipment summary by cost center

## Report Tools

All standard reports are created using Active Reports. The reports are delivered in both the Administrative and User Applications, with access configured by role, user and/or group (profile). As needed to meet customer requirements, reports can be customized using Active Reports designer. In addition, new reports can be created, reporting on any of the data stored within the platform.

# Security Overview

This paper primarily focuses on application-specific features and configuration settings related to Transtream's overall security strategy, which includes a combination of technical infrastructure controls and a strong security framework. Our defense-in-depth strategy includes security policies and procedures, infrastructure controls, monitoring, and secure application development and architectures.

To ensure the highest level of data protection, Transtream's IT infrastructure includes a host of enhancements. All production servers use hardened Windows operating systems; additional measures include centralized logging and alerting, intrusion detection, network access control, anti-virus/anti-malware, and host-based firewalls. The core production servers are further protected by load balancers.

The application development lifecycle was also designed with an emphasis on information security. Every Transtream developer is trained on secure coding techniques, and every feature requires a security review to be released into production. Both internal staff and third-party security experts regularly perform security assessments.

Transtream provides strong defense-in-depth strategies and technologies to protect our customers' data. We also provide applicationspecific features and settings to further protect your Transtream deployment. You can ensure the ultimate security with a combination of your own securityrelated configuration settings and Transtream's features, policies, and technologies.

## User Authentication

Transtream confidentiality between the browser client and server builds on the strong foundation provided by authentication. Authentication verifies the identity of every party from the Transtream browser and server. Access controls further ensure that only authenticated parties can gain access to authorized applications and resources.

Transtream utilizes cookies as part of authentication process and these have been implemented as recommended by the best practices.

## Encryption

All Web-site connections are protected using HTTPS with TLS 1.2 with a minimum of 256-bit symmetric encryption and a 1024-bit authenticated key agreement. The Transtream server is authenticated with an X.509 digital certificate. The administrator authenticates by username/password.

Hashing techniques are used to ensure that sensitive data – logins and passwords – are never sent or stored in plain text.

Using standard SQL Server encryption tools, data at rest can be configured to meet customer security requirements. This is delivered as an option for customers that need/want it; primarily to ensure consideration of performance impact to encrypting and decrypting data as part of each transaction.

## Firewall Friendly

Transtream is firewall friendly. It generates only outgoing HTTP(s) to ports 80, 443 and/or 8200. Because most firewalls are already configured to permit outgoing Web traffic, administrators do not have to bypass or be concerned about compromising the corporate firewall to implement secure remote access with Transtream.

## Password Settings

With the new IdP, the password and security settings have been moved to the new IdP component. This allows for a stricter security policies e.g Minimum password length of eight and mandatory use of at least one special character, capital letter and a number in a password. For single sign on configurations, such as SAML, credentials are maintained by the respective external IdP database and no password information is stored within the Pierbridge IdP database.

## Session Settings

Several settings can be used to place restrictions on active user sessions. These include configuring the idle session timeout, locking sessions to the IP address used at login, and requiring secure (HTTPS) connections. Many of the default settings can be modified to improve security.

## Login and Authentication Settings

By default, all users can log in to Transtream from any IP address at any time of day, subject to the restrictions of the Identity Confirmation feature described below.

## Single Sign-on Options

With the use of the new IdP for authentication, the following features are enabled alongside with this integration such as allowing self-registration, reset of the password and support of email-as-username for login to the product along with usual username as before. To improve customization and user account management Transtream supports the following:

- Federated Authentication: Federated authentication directs Transtream to use the Security Assertion Markup Language (SAML) for user authentication.

## Data Privacy

We understand the importance of keeping enterprise data private, including personal data. Transtream has a very strong privacy policy that prohibits unauthorized disclosure of personal or corporate information to unauthorized 3rd parties.

To deliver transportation services, Transtream must collect certain user information, including first/last name, email address and account level passwords, where applicable. Unless expressly authorized, Transtream will not disclose this confidential information to any third party or use this information in any manner other than to deliver agreed services. With its users' express consent, Transtream sends service update messages to its designated users at the email addresses they provided when requesting the service.

### Profiles

A profile is similar to a role in many enterprise applications, except that each user must have one profile and cannot have more than one profile. Every profile includes one or more permissions that define what a user is authorized to do within Transtream. In addition to detailed permissions, a profile defines the default access privileges to standard and custom objects, such as address books, carrier accounts, applications, transportation functions, and more.

Since profiles are the first step in determining data and application access rights, they should be reviewed closely. If custom profiles have been used, each profile should be examined to determine which privileges are included and which users have been assigned to the profile.

### Roles

Roles within Transtream do not completely relate to the traditional concept of a role in Role-Based Access Control (RBAC). Instead, a role in Transtream is more closely tied to a collection of authorizations assigned to each user configured with the specific profile.

To properly use role-based authorization, an accurate organization-based role hierarchy should be defined and all users assigned to a role.

## Compliance & Audit Features

The Transtream platform provides several types of logs for monitoring activities and transactions across the different components. All the logging features can be viewed by your Transtream administrator, including:

Full Transaction Logging – All successful transactions are stored in the database, and failed transactions are recorded in the logs and saved for 60 days. Transaction logging provides a drill down to each step within the transaction lifecycle to provide diagnostics capabilities.

## Summary

Data security is a mindset, and it is very much in evidence with the design of the Transtream platform, operational processes, and implementation within a secure hosted environment. That's why hundreds of the largest enterprises across financial services, healthcare, retail, and manufacturing trust Transtream to preserve data integrity and customer privacy in all points of the transportation management process.

sendflex
TECHNOLOGY

sales@sendflex.com 508.786.1919 www.sendflex.com