QAD GTTE Release Notes

GTTE v20.7 Patch #10

September 2026

Contents

1. Introduction.....3
2. New Features and Enhancements.....4
    2.1. Web UI.....4
    2.2. Oracle Transportation Management Integration.....5
    2.3. Carrier Activation Self Service Portal (CASP).....6
3. Security Updates.....7
4. Resolved Issues.....8
    4.1. Web UI.....8
    4.2. DEM.....8
5. Integration Updates.....9
    5.1. DEM.....9
6. Documentation Updates.....10
    6.1. Information on Prior Releases.....10
7. Contact Information and Support.....11

1. Introduction

QAD is pleased to announce the availability of GTTE v20.7 Patch #10. This patch delivers new features and enhancements, along with cumulative fixes and security updates. Upgrading to this patch is strongly recommended.

Install GTTE base version 20.7 before applying this patch.

This patch supports the following component versions:

Component	Version
Web UI	13.0.9-0
Highway	14.0.0-4
CD Subscriber	10.0.1-0
Configserver	14.0.0-6
DEM	15.0.5-0
Documents	15.0.1-0
EFM	15.0.0-34
EFM Bridge	1.0.1-2
Eureka	15.0.0-7
Exports	15.0.0-8
FBAP	15.0.0-13
Foundation	14.0.0-32
Gateway	15.0.0-8
Imports	13.2.2-0
Shipping	15.0.0-11
Sidecar	7.0.0-6
TE	15.0.4-0

2. New Features and Enhancements

This section summarizes the general updates and module-specific enhancements delivered in this patch release.

2.1. Web UI

2.1.1. Inquiry Screen - Carrier Tracking URL Enhancements

The carrier tracking link feature on the View Shipment screen now supports more complex tracking URLs.

Previously, the Tracking Site system value for a carrier only supported a single tracking number placeholder when building the tracking URL. This prevents direct links to carriers that require additional parameters — such as postal codes, consignment numbers, or reference fields — in their tracking URLs.

Administrators can now configure tracking URLs with multiple placeholders, enabling support for a broader range of carriers and URL formats. When a user clicks the tracking number link in the Packages tab of the Shipment Line Details panel, the system automatically replaces each placeholder with the corresponding shipment field value.

To configure: Update the Tracking Site system value for the relevant carrier to include the additional placeholders required by that carrier's tracking URL.

2.1.2. Inquiry Screen - Display of End of Day Batch Number

The View Shipment screen now displays the End of Day (EOD) Batch Number for each shipment in the main shipment grid.

The EOD Batch Number identifies the manifest batch the shipment was grouped into, based on its carrier and packing location.

Note: The EOD Batch Number is a display-only field and cannot be used as a search filter.

2.1.3. Inquiry Screen - DEM Tracking Update

The Carrier Tracking button on the View Shipment screen now displays live delivery status from the Delivery Exception Management (DEM) Delivery API. Previously, this button redirected users to the legacy Package Exception Management (PEM) screen.

When a user clicks Carrier Tracking, an inline panel opens showing:

- A Packages grid listing all packages on the shipment
- Delivery status from DEM, including shipment direction (Inbound or Outbound)
- Tracking history and comments from the DEM delivery record

For shipments with multiple packages, delivery status is retrieved using the first available tracking number. If no DEM delivery record exists for the shipment, the panel displays a message indicating that tracking information is not currently available.

2.1.4. End of Day Manifest Screen – Allow Resend of Package Level Detail Data

A new Reset Sent Flag button has been added to the End of Day (EOD) Manifest screen. Support Analysts and System Administrators can use this button to trigger a resend of Package Level Detail (PLD) files directly from the screen, without raising a support ticket or running manual database queries.

Clicking the button resets both the Sent flag and the PLD Created flag for the selected batch, allowing the file to be regenerated and resent through the existing EOD process.

The following safeguards apply:

- If the selected batch has already been sent, a confirmation dialog is displayed before any action is taken.
- If the selected batch has not yet been sent, an informational message is displayed and no action is taken.

2.1.5. End of Day Manifest Screen – Toolbar Reorganization and Access Controls

The End of Day (EOD) Manifest screen toolbar has been reorganized and several buttons renamed to make their purpose clearer. Visibility of sensitive actions is now restricted to authorized users only.

The following changes have been made:

- **Create New Batch** — The Create button has been renamed to Create New Batch, moved to the top row of the toolbar, and now displays a tooltip when hovered over. Visibility of this button is managed by your system administrator.
- **Run Batch Action** — The Run button has been renamed to Run Batch Action.
- **Reset Sent Flag** — This button is only visible to authorized users, as determined by your system administrator. When triggered, the reset clears both the Sent flag and the Package Level Detail (PLD) Created flag, ensuring the file can be fully regenerated in all deployment environments.

2.2. Oracle Transportation Management Integration

The connector between Oracle Transportation Management (OTM) and QAD GTTE has been extended beyond rating to now support full parcel shipment execution. The connector is a shared service that works across all clients and environments.

The following capabilities are now available:

- **Rating** — OTM continues to send shipment requests to the connector, which rates them through the carrier network and returns available carrier and service options to OTM. This behavior is unchanged.

- **Shipment Execution** — OTM can now create, ship, void, and reprint parcel shipments through the same connector. After a shipment is successfully processed, OTM receives the shipment reference, tracking number, and shipping label in return. Void and reprint operations use the same shipment reference.
- **Multi-Environment Support** — The connector now resolves environment settings automatically, allowing the same deployment to run across multiple environments without requiring configuration changes for each.

2.3. Carrier Activation Self Service Portal (CASP)

The Carrier Activation Self Service screen has been updated with the following improvements:

- The request form now includes additional fields: Zone Skip Details, Returns Required, Integration Type (Transportation Execution or Delivery Exception Management), API/EDI credentials, and IOSSN (Import One-Stop Shop Number) for EU regulatory compliance.
- A comment section is now available on submitted requests, allowing customers to communicate directly with the QAD carrier activation team and receive updates.
- When a request is submitted, the QAD carrier activation team is notified automatically.

3. Security Updates

QAD GTTE v20.7 Patch #10 addresses the following security vulnerabilities and hardening improvements. Apply this patch to address all listed vulnerabilities.

- **Spring Platform Upgrade** — The Spring Framework, Spring Security, Spring Data, and related Spring libraries have been updated to their latest secure versions. This resolves vulnerabilities that could allow attackers to bypass authorization controls, traverse file directories, impersonate authenticated users, exhaust system resources, or disrupt service availability.
- **Apache ActiveMQ Upgrade** — Apache ActiveMQ has been updated to resolve vulnerabilities that could allow attackers to inject malicious code, access sensitive information, or disrupt message processing through invalid input.
- **Netty Network Library Upgrade** — Netty has been updated to resolve vulnerabilities that could allow attackers to smuggle malicious HTTP requests, amplify data traffic, or exhaust system resources through crafted network requests.
- **Jackson Data Library Upgrade** — The Jackson data processing library has been updated to resolve vulnerabilities that could allow attackers to overload the system by sending specially crafted data.
- **BouncyCastle Cryptographic Library Upgrade** — The BouncyCastle cryptographic library has been updated to resolve vulnerabilities that could expose the system to timing-based attacks, allow the use of weak cryptographic algorithms, or cause the system to stop responding.
- **SSL Certificate Host Verification Fix** — Resolved a vulnerability where the system did not verify that an SSL certificate belonged to the server it was connecting to. An attacker could have exploited this to intercept encrypted communications by presenting a certificate from a different domain.
- **Sensitive Information in HTTP Response Cache** — Resolved a vulnerability in Spring Security where sensitive information could be retained in cached HTTP response headers, potentially allowing unauthorized access or information disclosure to other users.
- **Cryptographic Signature Verification Fix** — Resolved a vulnerability where an attacker could bypass signature checks by submitting an empty signature, causing the system to accept an unauthenticated message as valid and allowing impersonation of a trusted sender.
- **Template Injection Fix** — Resolved a vulnerability in the Thymeleaf templating engine where an attacker could inject malicious expressions during page rendering to execute unauthorized actions on the server.
- **Improper Authentication Fix** — Resolved a vulnerability in the embedded web server where a flaw in the DIGEST authentication process allowed any unknown username to be accepted, bypassing access controls entirely.
- **Information Exposure Fix** — Resolved a vulnerability in the BIRT reporting component where a flaw in how data was processed during report generation could allow an attacker to expose sensitive server-side information or trigger unauthorized class loading.

4. Resolved Issues

This section summarizes the issues addressed in this release. These fixes enhance system stability, improve user experience, and resolve specific problems reported by users or identified internally. For clarity, each issue includes a brief description.

4.1. Web UI

- **US Military Postal Code Validation** — Resolved an issue where valid US military postal codes in the DPO AE range were incorrectly rejected with an invalid postal code error during Desktop Shipping.
- **Memory Leak Fix** — Resolved a memory leak that caused the application to run out of memory and become unavailable under normal usage conditions.
- **Date Filter Validation** — Resolved an issue on the View Shipments screen where the Transaction Date and Despatch Date filters allowed an end date earlier than the start date to be entered without displaying a validation error.

4.2. DEM

- **Carrier Tracking Link Fix** — Resolved an issue where clicking the carrier tracking link on a delivery opened a broken URL.
- **POSTI Carrier Tracking Status Fix** — Resolved an issue where delivery statuses for the POSTI carrier were not displaying correctly in the Tracking History section of the Deliveries screen.
- **Supplier Wizard Preview Fix** — Resolved an issue in the Supplier Wizard where the Preview screen did not open correctly for certain supplier types.

5. Integration Updates

This section outlines key updates to integration functionality introduced in QAD GTTE v20.7 Patch #10. Reviewing these changes will help you understand their impact on the overall integration landscape, ensure a smooth transition, and support the efficient adoption of enhanced integration capabilities.

5.1. DEM

To support greater connectivity, the following DEM supplier integrations were added or enhanced in this patch:

DANX Carousel	Carousel	API (Tracking Number) A new tracking API integration is now supported.
GEODIS	Geodis EDI	Updated to map the tracking number through the URL on the STS segment.

6. Documentation Updates

The documentation for QAD GTTE has been updated to reflect the latest features and enhancements included in this release. For complete and up-to-date information, including new topics, revised procedures, and the latest user guides, refer to the QAD GTTE Online Help and QAD Document Library.

6.1. Information on Prior Releases

The QAD Document Library provides access to user guides, training materials, release documentation, and other resources for current and prior release

7. Contact Information and Support

You can contact the QAD Support team for assistance with QAD GTTE. The team is available to help with troubleshooting, technical guidance, and product-related questions.

- Support Portal**:** https://www.qad.com/global-support-resources
- Immediate Assistance: For urgent issues or production system outages, contact your nearest QAD support location: https://projects.qad.com/plugins/servlet/desk/category/contact-support
- General Inquiries: For questions about QAD products and services not related to support, call +1 805 566 6100 or visit www.qad.com.