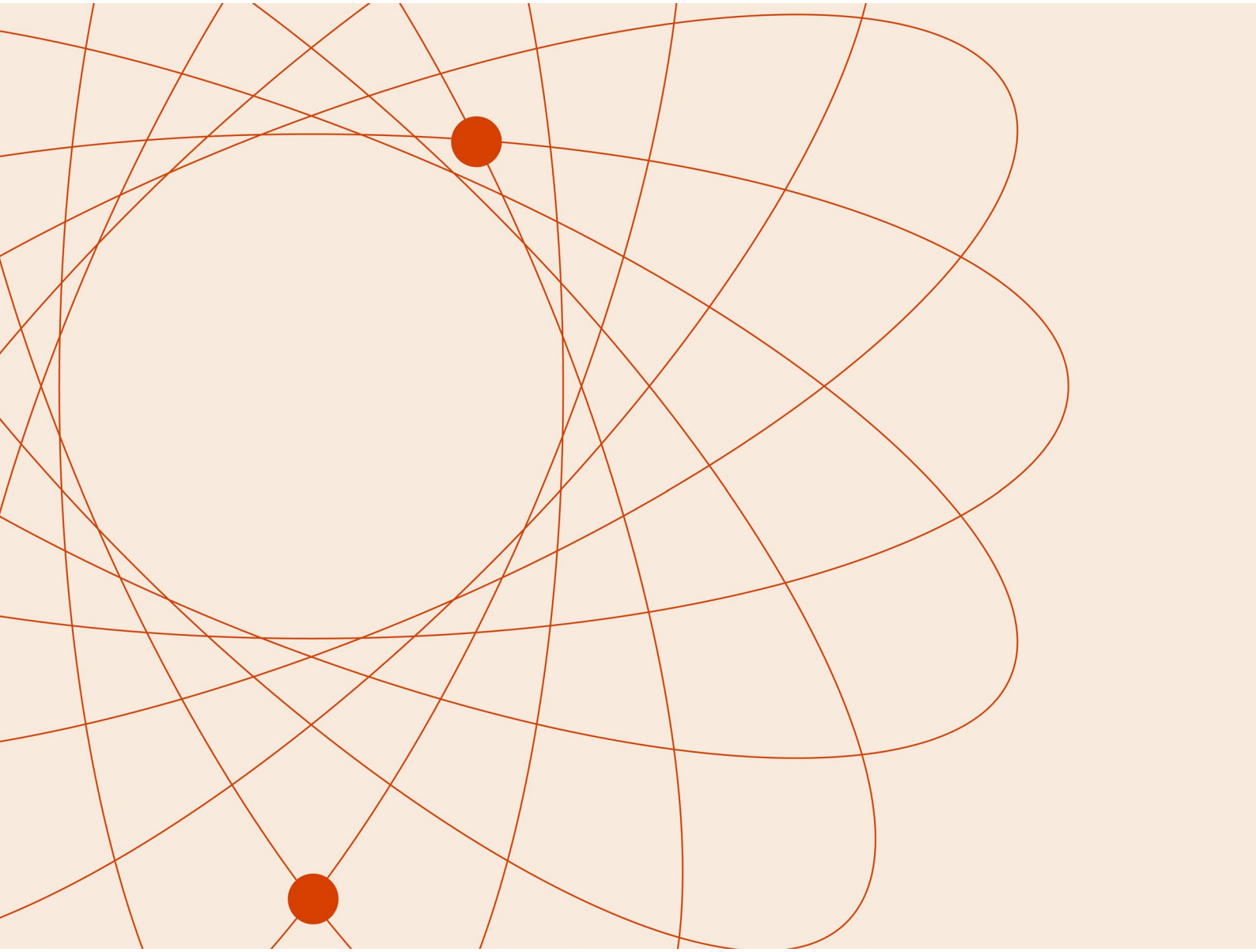
ONESOURCE INDIRECT TAX DETERMINATION

RELEASE NOTES

5.13.16.0



Contents

IMPORTANT ANNOUNCEMENT REGARDING ONESOURCE DETERMINATION ORIGINAL

After careful consideration, Thomson Reuters has made the strategic decision to discontinue our investment in the maintenance and support of ONESOURCE Determination Original and focus our resources on developing and enhancing ONESOURCE Determination Enterprise. Support for ONESOURCE Determination Original will officially end on **June 30th, 2026**. After this date, we will discontinue updates, security patches, and technical assistance for ONESOURCE Determination Original. (Please review the mainstream and extended support dates for the latest versions of Determination Original in the following page)

Discover The Power of ONESOURCE Determination Enterprise

Now is a great time to consider and plan for a move to ONESOURCE Determination Enterprise. Released in 2017, ONESOURCE Determination Enterprise is now used by hundreds of customers around the world. Its cloud-based and cloud-enabled (on-premises hybrid) deliver superior capabilities and performance than on-premises solutions, alleviate the heavy manual management burden and costs businesses often have when maintaining tax in-house.

Resources Supporting Your Upgrade to ONESOURCE Determination Enterprise

We understand that a solution upgrade requires time to plan and prepare. This is why Thomson Reuters created a specific upgrade procedure to facilitate this transition and ensure a seamless experience for you. Using advanced migration tools and with the support of experienced Thomson Reuters technical consultants, our goal is to make upgrading to ONESOURCE Determination Enterprise a seamless transition.

For more information and to get started, we recommend the following steps:

1. Review the ONESOURCE Determination Upgrade Frequently Asked Questions document.
2. Contact your Thomson Reuters Account or Client Success Executive who will guide you through the upgrade procedure and address any initial questions or concerns.
3. Register for our upcoming customer webinar: Discovering the Power of ONESOURCE Determination Enterprise (August 2, 2023). You'll learn more about the solution, its features, new benefits you can expect, and more about upgrading.

DETERMINATION 5.13.16.0 RELEASE NOTES

We are pleased to announce the latest release of Original Determination, featuring a major upgrade to Java 17. This release focuses on improving performance, security, and compatibility while introducing several enhancements and bug fixes.

JAVA 17 UPGRADE

We are please to announce the release of ONESOURCE Original Determination 5.13.16.0, includes several updates and improvements. Notably, this release upgrades our platform to Java 17, ensuring improved performance and security.

For a comprehensive overview of all the changes, enhancements, and platform support information, related to Java 17, please refer to our ONESOURCE Determination article in the Help and Support page.

NEW FEATURES

Minnesota Retail Delivery Fee Calculation (1704553)

A change has been implemented to the MN Retail Delivery Fee Authority to correctly trigger the fee when the total invoice gross amount exceeds $100 for eligible lines with specific commodity codes. Previously, the fee was only applied when an individual line exceeded $100, but now it will be applied to the entire invoice when the total gross amount of eligible lines meets the $100 threshold. This update ensures that customers in Minnesota will be charged the correct 50-cent fee for deliveries, providing a more accurate and fair billing experience.

Implementation for improving VAT invoice document rounding algorithm

We have implemented a standardized document rounding logic, using the current India logic as the base, for all countries excluding Brazil, Canada, and the USA. This new logic ensures consistent and accurate calculations across different countries. The key aspects of this logic are:

- For Italy and Turkey, pennies are adjusted to the highest value.
- For India, pennies are pitched for the absolute highest amounts.
- Separate pennies calculations and pitching are applied for Forward charge and Reverse charge scenarios.

Seller registration numbers enhancement for domestic sales transactions In South Africa (1362525)

We have enhanced our application to improve the handling of seller registration numbers for domestic sales transactions in South Africa. The system now recognizes both country-level and province-level registration numbers for sellers, providing greater flexibility and accuracy. When a correct registration number is provided at either the country or province level, and the transaction is a domestic sale (i.e., both the ship-from and ship-to locations are in South Africa), the system will return a Tax Type of 'S'.

Availability of new local currency for Curacao- Caribbean Guilder (1556817)

The system now includes the new currency code "XCG" for "Caribbean Guilder" for the countries of Curacao and Saint Maarten. The system has been updated to support this new currency, and testing has been implemented to verify its correct functioning.

Zimbabwe currency change – ZWG (1526527)

The currency code "ZWG" is now used consistently for Zimbabwe, aligning with the official ISO standard.

ADDRESSED ISSUES

Limitation of the system not being able to use an exemption in a graduated amount (1471367)

The system now correctly shows the Exempt tax block when the calculation type is 'Reverse from Tax' or 'Reverse from Total' and the Gross amount falls within any slab of the Graduated rate. The XML output will now accurately reflect the exempt amount, and the result page will display the correct gross amount. This update ensures that the application handles exemptions in graduated rates correctly and consistently.

Tax blocks unexpectedly suppressed (1167744)

We have resolved an issue where tax blocks were being suppressed unexpectedly when the company option "Exclude 0% Non-Recoverable Tax Block" was enabled and a line item had a rule applied that exempted a tax block. In this scenario, the exempt rule should not have suppressed the tax block. The issue was causing a "FAILED_TO_CALCULATE_TAX" response instead of returning the expected tax block. This fix ensures that exempt rules are handled correctly, and tax blocks are returned as expected, even when the "Exclude 0% Non-Recoverable Tax Block" option is enabled.

Lack of anti-automation mechanism (1102160)

We have implemented measures to prevent automated requests and ensure that password change requests originate from legitimate users. With this update, the application will now properly verify the authenticity of requests, preventing attackers from exploiting this vulnerability and reducing the risk of various types of attacks. This change enhances the overall security and integrity of our application, protecting our users' accounts and sensitive information.

Company level registration not getting assigned (1259318)

The tax engine now correctly applies the company-level registration setup for the 7 provinces in the UAE, allowing tax calls to Original Determination to proceed without errors. When a registration number is added to the Registrations setup, the tax engine picks up the registration number and uses it to generate taxes for domestic transactions within the UAE. The issue where the tax engine was not recognizing the registration number for UAE provinces has been addressed, ensuring that taxes are generated correctly for these regions.

Duplicated Texas State Sales Tax Rate (1270729)

The system now correctly triggers only one tax block for TX - State Sales/Use Tax with a rate of 6.25% for deliveries to Texas, including zip codes 77346, 77380, and 79938. The Company Option 'Evaluate US Custom Authorities past zone termination' no longer causes duplicate tax blocks for standard authorities like 'TX - State Sales/Use Tax'. This option only impacts custom authorities and does not affect standard authorities, ensuring accurate tax calculations for US domestic and

import/export scenarios, as well as international domestic and import/export scenarios. The system behaves as expected for various combinations of company options, zones, and custom authorities, and tax calculations are performed correctly without triggering duplicate tax blocks.

System Security Updates – critical / high / medium vulnerabilities (1730959, 1568890, 1262934, 1558269, 1558259, 1558164, 1558126, 1445616, 1421670, 754446, 1501904, 1501896, 1501897, 1501883, 1388410, 1501903, 1501899, 1501898, 1501895, 1501871, 1501879, 1567494, 1354684, 1252404, 1252408, 1303424, 1592384, 1240760, 351036)

We have addressed several critical, high, and medium security vulnerabilities to ensure the integrity and safety of our application. The following vulnerabilities have been resolved:

- Vulnerabilities in H2 database, Spring Web MVC, and Eclipse Jetty, which could have led to security threats such as Denial of Service (DoS)
- Path Traversal issues, which could have allowed unauthorized access to sensitive data
- SQL Injection vulnerabilities, which could have enabled attackers to execute malicious SQL code
- Deserialization of Untrusted Data vulnerabilities, which could have allowed attackers to execute arbitrary code
- Unsafe Reflection vulnerabilities, which could have enabled attackers to access and manipulate sensitive data
- Cross-site Scripting (XSS) vulnerabilities in multiple JavaScript libraries, which could have allowed attackers to inject malicious code into our application
- Vulnerabilities in various dependencies, including Oracle JDBC, YAML, Plexus Utils, JDOM, Java EL, Apache Maven, Apache XMLBeans, Spring Security, XStream, and Jackson Core.

By fixing these vulnerabilities, we have significantly enhanced the security posture of our application, protecting our customers' data and preventing potential exploits.

Penetration Test Vulnerabilities (1417295, 1417296, 1417288, 1417297, 1417291, 1413385, 1417249, 1413404, 1417261, 1417268, 1417254, 1417241, 1417255, 1417290, 1417285, 1417280)

We have addressed several security vulnerabilities identified during our annual Penetration Test, to ensure the integrity and safety of our application. The following issues have been resolved:

- Sensitive information, such as internal paths, admin usernames, internal services, operating system types, and internal IP addresses, were stored in cleartext within the source code and have been secured.
- Outdated versions of jQuery and Apache Tomcat, which had publicly known vulnerabilities, have been updated to prevent exploitation.
- Internal IP addresses were disclosed within the response headers of the server and have been removed to prevent attackers from obtaining information about the internal network structure.
- Vulnerabilities that allowed remote attackers to obtain internal IP addresses have been fixed to prevent further attacks.

- Error messages containing internal system information are no longer presented to users, preventing malicious users from exploiting this vulnerability to obtain sensitive information.
- The application is no longer vulnerable to persistent cross-site scripting (PXSS) attacks, which allowed client-side scripts to be injected into the application's input fields and stored in the data repository.
- The application's input validation mechanism has been improved to prevent malicious users from inserting code into the application's database.
- Sensitive information is no longer sent using the request URL, preventing malicious attackers from extracting the information from the browser's history mechanism.
- Reflected cross-site scripting (RXSS) vulnerabilities have been fixed to prevent attackers from embedding scripts into the output presented to users.
- Rate limiting has been enforced to prevent automated scripts from submitting high volumes of requests without restrictions.
- File upload validation checks have been implemented on the server-side to prevent malicious users from uploading malicious files.
- The application is no longer vulnerable to cross-site request forgery (CSRF) attacks, which allowed attackers to perform actions on behalf of authenticated users without their knowledge.
- Credentials are no longer sent using basic authentication, which can be easily decoded to reveal the username and password.
- Parameter tampering vulnerabilities have been fixed to prevent malicious users from accessing components of different companies without having the relevant permissions.
- Web services interfaces are no longer accessible through the Simple Object Access Protocol (SOAP) XML over HTTP, preventing anonymous attackers from obtaining access conventions and web services information.
- The server no longer discloses internal information, such as the web server version, type, and technology in use, within the response headers and error messages.
- The session ID cookie is now stored securely with the appropriate 'Secure' attribute, preventing attackers from capturing the session ID through man-in-the-middle (MITM) or cross-site scripting (XSS) attacks.

By addressing these security vulnerabilities, we have significantly enhanced the security posture of our application, protecting our customers' data and preventing potential exploits.

Porting ONESOURCE Original Determination 5.13.15.1 (1678734)

The latest version of DET, 5.13.16.0, now includes all the features and bug fixes from the previous release, 5.13.15.1. The ported features function correctly in the new version without introducing any new bugs.

Porting ONESOURCE Original Determination 5.13.14.1 (1678736)

The latest version of DET, 5.13.16.0, now includes all the features and bug fixes from the previous release, 5.13.14.1. The ported features function correctly in the new version without introducing any new bugs.