

ONESOURCE™ CERTIFICATE MANAGER

RELEASE NOTES

VERSION 2.2.4.0

Document Version 6

© 2024 Thomson Reuters. All rights reserved. Republication or redistribution of Thomson Reuters content, including by framing or similar means, is prohibited without the prior written consent of Thomson Reuters. Thomson Reuters and the Kinesis logo are trademarks of Thomson Reuters and its affiliated companies. [More information can be found here.](#)

In compliance with the license agreements for the Open Source Libraries leveraged by Thomson Reuters, our customers can obtain copies of these libraries by contacting Customer Support at <https://tax.thomsonreuters.com/support/onesource/customer-center/>.

DOCUMENT HISTORY

VERSION NUMBER	VERSION DATE	SUMMARY
1	November 15, 2021	Initial publication.
2	December 20, 2021	Added 2.2.1.0 Release Notes.
3	January 12, 2022	Added the 2.2.1.1 Release Notes.
4	April 21, 2022	Added the 2.2.2.0 Release Notes.
5	November 27, 2023	Added information about the revised ONESOURCE Certificate Manager Original support timelines, the important announcement regarding ONESOURCE Determination Original, and the 2.2.3.0 Release Notes.
6	July 8, 2024	Added the 2.2.4.0 Release Notes.

TABLE OF CONTENTS

Important Announcement Regarding ONESOURCE Determination Original	1
Discover the Power of ONESOURCE Determination Enterprise	1
Resources Supporting Your Upgrade to ONESOURCE Determination Enterprise	1
ONESOURCE Certificate Manager Original Support Timelines	3
Certificate Manager 2.2.4.0 Release Notes	4
Release Highlights	4
New Features	4
Addressed Issues	4
System Security Updates – Vulnerabilities found in CM jar files (984883,1038038,1038045,1097768,1205263, 1205276, 952534, 952558, 952559, 952560, 952561, 1031513)	4
TCM Forms Issues (1182928)	5
Report is not able to export in excel format for CM Application (1221041)	5
TCM -2.2.3.0 version issues (1248321)	5
User is unable to preview certificate image while creating the certificate, seeing broken image (1251550, 1156482)	5
Certificate Image not visible for certificate (1031654, 1026122)	5
Known Issues	6
Incorrect Page Initiation text on the Customer and Certificate page	6
Certificate Manager 2.2.3.0 Release Notes	7
Release Highlights	7
New Features	7
Addressed Issues	7
Unable to Login to the Certificate Manager Application when Using ONESOURCE Determination Version 5.13.12.0 (Bug 930350)	7
Certificate Manager-Original - Certificate Manager Upgrade to Spring 5.3.29 (Bug 952726)	7
Enable the Unit Test Cases Working for Certificate Manager (Bug 956929)	7
System Security Updates - Vulnerabilities Found in Certificate Manager JAR Files (731552, 733767, 733803, 733868, 733915, 733934, 736701, 772094, 772127, 828988, 916571, 921736, 930350, 952726 and 956929)	8
Known Issues	8
Certificate Manager 2.2.2.0 Release Notes	9
Release Highlights	9

New Features	9
Encrypt Data Source Credentials Using AES-256 (CMC-3239)	9
Upgraded Spring4Shell Library (CM-3292)	9
Addressed Issues	9
Unable to Use Same Customer Number for Two Companies (CM-3262)	9
Unable to Extract a Certificate Report with Has Image Column in Microsoft SQL Server (CM-2917)	10
Known Issues	10
Certificate Manager 2.2.1.1 Release Notes	11
Release Highlights	11
New Features	11
New Amazon Corretto Version Supported (CM-3134)	11
Logback-core and Logback-classic Versions Upgraded (CM-3277)	11
Addressed Issues	11
Known Issues	11
Certificate Manager 2.2.1.0 Release Notes	13
Release Highlights	13
New Features	13
New Operating System Versions Supported (CM-3143)	13
New Microsoft SQL Server Versions Supported (CM-3143 and CM-3172)	14
New JBoss Versions Supported (CM-3143)	14
New Java Versions Supported (CM-3143)	14
Addressed Issues	14
Known Issues	15
Certificate Manager 2.2.0.0 Release Notes	17
Release Highlights	17
New Features	17
Display Active and Available Authorities in Certificate Manager (CM-3200 and CM-3220)	17
Display Customer Number in View/Edit Certificate Page (CM-3201)	17
Addressed Issues	18
Certificate Manager Creating Duplicate Records in ONESOURCE Determination (CM-3251)	18
Limited Use Criteria Not Reflected in ONESOURCE Determination (CM-3249)	18
Incorrect Synched Flag in ONESOURCE Determination for Limited Use Certificates (CM-3248)	18
Basic Certificate Template Not Selectable for Armed Forces (CM-3148)	18
Certificate Manager Data Source MSSQL Tomcat Line Endings (CM-3145)	18

System Security Updates - Outdated Third Party Libraries (CM-3211 , CM-3212 , CM-3213 , CM-3214 , CM-3215 , CM-3216)	19
Known Issues	19
Download the Software	21

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 30, 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 ONESOURCE Determination Original on 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.

ONESOURCE CERTIFICATE MANAGER ORIGINAL SUPPORT TIMELINES

Revised ONESOURCE Certificate Manager Original support timelines as of February 2023 include:

CERTIFICATE MANAGER VERSION	RELEASE DATE	MAINSTREAM SUPPORT EXPIRATION	EXTENDED SUPPORT EXPIRATION
2.1.1.3	April 2019	April 2021	April 2023
2.1.1.4	June 2020	June 2022	June 2024
2.1.1.5	July 2020	July 2022	July 2024
2.1.1.6	August 2020	August 2022	August 2024
2.2.x.x	December 2021	June 2025	June 2026



Customers will no longer be able to download unsupported versions of Certificate Manager Original from the [Indirect Tax Customer Center](#) after extended support has expired.

For details and to assess the impact on your business, see our [FAQ document](#) (sign in to the ONESOURCE Indirect Tax Help and Support page required).

CERTIFICATE MANAGER 2.2.4.0 RELEASE NOTES

See [ONESOURCE Certificate Manager Original Support Timelines \(page 3\)](#) for important information regarding the latest revisions to the ONESOURCE Certificate Manager Original support timelines.

RELEASE HIGHLIGHTS

Certificate Manager 2.2.4.0 introduces the addressed issues listed below.

NEW FEATURES

There are no new features in this release.

ADDRESSED ISSUES

The topics below describe addressed issues in this release.

System Security Updates – Vulnerabilities found in CM jar files (984883,1038038,1038045,1097768, 1205263, 1205276, 952534, 952558, 952559, 952560, 952561, 1031513)

The following list includes the high-level security system vulnerabilities that are resolved in this upgrade:

- CM Very High Flaw: very high flaw in angular jar
- CM Original - High Vulnerability found in logback-classic-1.2.10.jar.
- CM Original - High Vulnerability in logback-core-1.2.10.jar
- CM Original - 2 Medium vulnerabilities in commons-compress-1.21.jar
- CM Original - 1 High Vulnerability in examples.php file
- CM Original - 1 High Vulnerability in json.php file

- CM Original - 3 High Vulnerabilities in angular 1.2.16
- CM Original - Medium Vulnerabilities in jQuery jar
- CM Original - Medium Vulnerabilities in bootstrap jar
- CM Original - 2 Medium Vulnerabilities in jQuery Ui
- CM Original - Medium Vulnerabilities in data tables
- Apache cxf upgrade 3.3.11 and xmlsec 2.1.6.

TCM Forms Issues (1182928)

An issue was reported, while uploading latest content to TCM, system was throwing an error as '*Form Import has failed*'. As a part of this release this issue has been fixed.

Report is not able to export in excel format for CM Application (1221041)

As a part of this release, we have fixed this issue, so that Reports can be exported in excel format.

TCM -2.2.3.0 version issues (1248321)

An installation issue was reported for TCM 2.2.3.0 version, system was throwing an error post installation of UI, users were unable to login. As a part of this release, this has been fixed.

User is unable to preview certificate image while creating the certificate, seeing broken image (1251550, 1156482)

As a part of this release, a fix has been done so that while uploading the image user should not see any error message. Also, the user should see the uploaded image preview after completion of the upload process.

Certificate Image not visible for certificate (1031654, 1026122)

An issue was reported where the user is not able to see the preview after successfully editing the certificate. This has been addressed as part of this release.

KNOWN ISSUES

The topics below describe known issues in this release.

Incorrect Page Initiation text on the Customer and Certificate page

A temporary issue is occurring for few users where users are not seeing the correct page counts at the Page Initiation text. Clearing the cache and incognito mode is advised in this situation. This is going to be addressed in upcoming releases.

CERTIFICATE MANAGER 2.2.3.0 RELEASE NOTES

See [ONESOURCE Certificate Manager Original Support Timelines \(page 3\)](#) for important information regarding the latest revisions to the ONESOURCE Certificate Manager Original support timelines.

RELEASE HIGHLIGHTS

Certificate Manager 2.2.3.0 introduces the addressed issues listed below.

NEW FEATURES

There are no new features in this release.

ADDRESSED ISSUES

The topics below describe addressed issues in this release.

Unable to Login to the Certificate Manager Application when Using ONESOURCE Determination Version 5.13.12.0 (Bug 930350)

You can now successfully login to the Certificate Manager application when using ONESOURCE Determination version 5.13.12.0 and Certificate Manager version 2.2.3.0.

Certificate Manager-Original - Certificate Manager Upgrade to Spring 5.3.29 (Bug 952726)

In the Certificate Manager application, a Spring upgrade to version 5.3.29 was completed because commercial support for Spring version 5.2.x is ending by 2023.

Enable the Unit Test Cases Working for Certificate Manager (Bug 956929)

The unit test cases for Certificate Manager in GO-CD were fixed.

System Security Updates - Vulnerabilities Found in Certificate Manager JAR Files (731552, 733767, 733803, 733868, 733915, 733934, 736701, 772094, 772127, 828988, 916571, 921736, 930350, 952726 and 956929)

The following list includes the high-level security system vulnerabilities that are resolved in this upgrade:

- CM Very High Flaw: very high flaw in velocity-1.7.jar
- CM 2.2.2.0 - High flaw in commons-compress-1.19.jar
- CM 2.2.2.0 - High flaw in jackson-databind-2.12.2.jar
- CM 2.2.2.0 - High flaw in xmlsec-2.1.6.jar
- CM 2.2.2.0 - High flaw in woodstox-core-5.1.0.jar
- CM 2.2.20 - High flaw in hibernate-core-5.4.22.Final.jar
- CM v.2.0 - jackson-databind-2.12.2 affected with multiple high vulnerabilities
- CM Original - High vulnerability in cxf-rt-transport-http-3.3.11.jar
- CM Original - Critical vulnerability in cxf-core-3.3.11.jar
- CM 2.2.2.0 - Medium flaw in hibernate-validator-5.0.3.Final.jar
- CM Original - High vulnerability in guava-30.1-jre.jar

KNOWN ISSUES

There are no known issues in this release.

CERTIFICATE MANAGER 2.2.2.0 RELEASE NOTES

See [ONESOURCE Certificate Manager Original Support Timelines \(page 3\)](#) for important information regarding the latest revisions to the ONESOURCE Certificate Manager Original support timelines.

RELEASE HIGHLIGHTS

Certificate Manager 2.2.2.0 introduces the features and addressed issues listed below.

NEW FEATURES

The topics below describe features added with this release.

Encrypt Data Source Credentials Using AES-256 (CMC-3239)

If you require Tomcat data source credentials to be encrypted, Certificate Manager now provides the additional option. All of the **Tax Certificate Manager Data Source**, **User Management Data Source** and **Content Management Data Source** username and password credentials can now be encrypted using a utility that encodes the username and password using the AES-256 mechanism. For details, click [here](#) to access the related guides.

Upgraded Spring4Shell Library (CM-3292)

The Spring4Shell library in Certificate Manager is now upgraded to 5.2.21 version.

ADDRESSED ISSUES

The topics below describe addressed issues in this release.

Unable to Use Same Customer Number for Two Companies (CM-3262)

An issue was identified in Certificate Manager where two different customers with same customer number were not correctly attached to the appropriate company. This issue is now resolved.

Unable to Extract a Certificate Report with Has Image Column in Microsoft SQL Server (CM-2917)

An issue was reported in Certificate Manager for customers using Microsoft SQL Server. When the **Has Image** column was used in a Certificate report, the report could not be extracted. This issue is now fixed. Certificate reports can be extracted in Excel, CSV and Microsoft SQL Server.

KNOWN ISSUES

There are no known issues in this release.

CERTIFICATE MANAGER 2.2.1.1 RELEASE NOTES

See [ONESOURCE Certificate Manager Original Support Timelines \(page 3\)](#) for important information regarding the latest revisions to the ONESOURCE Certificate Manager Original support timelines.

RELEASE HIGHLIGHTS

Certificate Manager 2.2.1.1 introduces the features listed below.

NEW FEATURES

The topics below describe features added with this release.

New Amazon Corretto Version Supported (CM-3134)

Certificate Manager 2.2.1.1 now supports the Amazon Corretto Open JDK 11 Java version.

See the *ONESOURCE Indirect Tax Certificate Manager 2.2.x.x Documentation and Platform Support* knowledge base article for details related to the supported platforms.

Logback-core and Logback-classic Versions Upgraded (CM-3277)

In Certificate Manager, the Logback-core and Logback-classic libraries are now upgraded to the 1.2.10 version.

ADDRESSED ISSUES

There are no addressed issues in this release.

KNOWN ISSUES

There are no known issues in this release.

CERTIFICATE MANAGER 2.2.1.0 RELEASE NOTES

See [ONESOURCE Certificate Manager Original Support Timelines \(page 3\)](#) for important information regarding the latest revisions to the ONESOURCE Certificate Manager Original support timelines.

RELEASE HIGHLIGHTS

Certificate Manager 2.2.1.0 introduces the features listed below.

NEW FEATURES

The topics below describe features added with this release.

New Operating System Versions Supported (CM-3143)

Certificate Manager 2.2.1.0 now supports the following operating system versions:

- Microsoft Windows 2016
- Microsoft Windows 2019
- Oracle Linux 7.8, 7.9, 8.2, 8.3
- Red Hat Enterprise Linux (RHEL) Server Edition 7.5, 7.6, 7.7, 7.8, 7.9, 8.2, 8.3

See the *ONESOURCE Indirect Tax Certificate Manager 2.2.x.x Documentation and Platform Support* knowledge base article for details related to the supported platforms.



- Oracle Linux 7.1 and 7.2 are not supported with this version of Certificate Manager. They are being considered for support in a future version based on need.
- Red Hat Enterprise Linux (RHEL) Server Edition 6.5, 7.1 and 7.2 are not supported with this version of Certificate Manager. They are being considered for support in a future version based on need.

New Microsoft SQL Server Versions Supported (CM-3143 and CM-3172)

Certificate Manager 2.2.1.0 now supports the following database versions:

- Microsoft SQL Server 2016 SP2
- Microsoft SQL Server 2019

See the *ONESOURCE Indirect Tax Certificate Manager 2.2.x.x Documentation and Platform Support* knowledge base article for details related to the supported platforms.

New JBoss Versions Supported (CM-3143)

Certificate Manager 2.2.1.0 now supports the following versions of the Application Servers:

- JBoss 7.1, 7.2, 7.3, 7.4 Enterprise Edition
- Apache Tomcat 8.5.x

See the *ONESOURCE Indirect Tax Certificate Manager 2.2.x.x Documentation and Platform Support* knowledge base article for details related to the supported platforms.

New Java Versions Supported (CM-3143)

Certificate Manager 2.2.1.0 now supports the following Java versions:

- Oracle Java 10
- Oracle Java 11

See the *ONESOURCE Indirect Tax Certificate Manager 2.2.x.x Documentation and Platform Support* knowledge base article for details related to the supported platforms.



Amazon Corretto 11 will not be supported with this Java version for Certificate Manager 2.2.1.0, but will be considered in a future version based on need.

ADDRESSED ISSUES

There are no addressed issues in this release.

KNOWN ISSUES

There are no known issues in this release.

CERTIFICATE MANAGER 2.2.0.0 RELEASE NOTES

See [ONESOURCE Certificate Manager Original Support Timelines \(page 3\)](#) for important information regarding the latest revisions to the ONESOURCE Certificate Manager Original support timelines.

RELEASE HIGHLIGHTS

Certificate Manager 2.2.0.0 includes addressed issues and introduces the features listed below.

NEW FEATURES

The topics below describe features added with this release.

Display Active and Available Authorities in Certificate Manager (CM-3200 and CM-3220)

Under the **Authority** column (**Country > State > Authority Type**) in the **Certificate Jurisdiction** section of a certificate, all of the active authorities that are tied to a zone now display. This is consistent with how the authorities are displayed in ONESOURCE Determination.



To deactivate an authority, click **Menu > Tax Data > Authorities > Advanced Configuration**, select the authority, click the **Options** tab then set the value for **Turn Off Authority** to **Yes**.

Display Customer Number in View/Edit Certificate Page (CM-3201)

The customer number now displays with the customer name when View/Edit Certificate page. Either the customer name or the customer number can be edited. If the customer number is edited, the customer name is updated (and vice versa).

ADDRESSED ISSUES

Certificate Manager Creating Duplicate Records in ONESOURCE Determination (CM-3251)

An issue was identified with updating a certificate to include limited use criteria was resulting in creation of a duplicate certificate in ONESOURCE Determination. This issue is now fixed.

Limited Use Criteria Not Reflected in ONESOURCE Determination (CM-3249)

While adding or modifying the limited use criteria of a certificate record, the updated data was not showing in ONESOURCE Determination even though the record was synchronized to ONESOURCE Determination. This issue is now fixed.

Incorrect Synched Flag in ONESOURCE Determination for Limited Use Certificates (CM-3248)

An issue was identified where the **Synched** flag showed a failure for a certificate record with limited use criteria even when the certificate was successfully synchronized to ONESOURCE Determination. This issue is now fixed.

Basic Certificate Template Not Selectable for Armed Forces (CM-3148)

Selecting any of the armed forces as a certificate issuer state did not display a form for selection. This issue is now fixed. The Basic Certificate is now available as a form that can be selected for any one of armed forces states.

Certificate Manager Data Source MSSQL Tomcat Line Endings (CM-3145)

Data in the **certificate-manager-data-source-mssql-tomcat.txt** file in the **tomcat** folder under **...\\Docs\\application-server-files\\tomcat\\conf** did not align correctly when the file was opened in Notepad. This issue is now fixed. The contents of this file are formatted correctly when opened in Notepad.

System Security Updates - Outdated Third Party Libraries (CM-3211 , CM-3212 , CM-3213 , CM-3214 , CM-3215 , CM-3216)

Addressed some high and medium level security system vulnerabilities that were identified in the following third party libraries used by the application:

- jackson-databind-2.7.3.jar
- jackson-mapper-asl-1.9.13.jar
- cxf-rt-transport-http-3.1.0.jar
- cxf-rt-rs-extension-providers-3.1.0.jar
- poi-3.12.jar
- poi-ooxml-3.12.jar
- logback-classic-1.1.2.jar
- logback-core-1.1.2.jar
- commons-collections-3.2.1.jar
- DOM4J-1.6.1.JAR

KNOWN ISSUES

There are no known issues in this release.

DOWNLOAD THE SOFTWARE

To download and install the software, get the *N/A* file from the Indirect Tax Customer Center:

1. Open the Indirect Tax Customer Center at <https://customercenter.sabrix.com/>.
2. Log on using the username and password provided by Customer Support.
3. Find Certificate Manager in the **Available Products** list, and verify that **Installed Version** is set to **None**.
4. Select **Download** for Certificate Manager.
5. Save the file.
6. Unzip the *N/A* file.