

ONESOURCE™ CERTIFICATE MANAGER

INSTALLATION GUIDE

ORACLE DATABASE AND TOMCAT

2.2.X.X

Document Version 2

COPYRIGHT NOTICE

© 2023 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	December 2021	Created first version for Certificate Manager 2.2.x.x.
2	April 22, 2022	Added steps for encrypting Tomcat data source credentials using the AES-256 standard.

TABLE OF CONTENTS

Introduction	1
Who Should Read This Guide?	1
Upgrade From Tax Certificate Manager 1.x	1
Architecture	1
Resources	4
Style Conventions	5
Tomcat Checklists	6
Prerequisites	6
Installation	6
Post-Installation Tasks	7
Prerequisites	9
Review System Requirements	9
Gather Administrative Information	9
Download the Software	10
Certificate Manager	10
Data File Integrator	11
Configure the Database	13
Set Database Initialization Parameters	13
Set Database Character Set	13
Get JDBC Driver	13
Create Tablespace and User	13
Configure Certificate Manager in Tomcat	15
Set JAVA_HOME	15
Configure JDBC	15
Configure Tomcat Logging	15
Configure Tomcat Initialization	16
Create Data Sources in Tomcat	17
Insert Data Source Snippets	17
Edit Tax Certificate Manager Data Source	17
Edit User Management Service Data Source	18
Edit Content Management Service Data Source	19
Encrypting Tomcat Data Source Credentials	20

Change Tomcat Ports	22
Deploy Certificate Manager Under Tomcat	23
Installer	23
Applications	24
Post-Installation Tasks	25
Certificate Manager	25
General Configuration	25
Email Configuration	27
Determination	28
Determination Roles	28
Determination Configuration Parameter	33
Additional Configurations	33
Data File Integrator	35

INTRODUCTION

Certificate Manager controls all aspects of the exemption certificate lifecycle and is tightly integrated with ONESOURCE Determination to reduce operating costs, mitigate risks, and increase tax accuracy.

This guide explains how to install Certificate Manager version 2.2.x.x at your business. For information about cloud installations of Certificate Manager, contact your sales representative.

WHO SHOULD READ THIS GUIDE?

The installation requires the coordination of people in various roles. If you are responsible for overseeing the installation, make this guide available to the following contributors:

- Database administrator
- Application server administrator
- IT administrator
- Tax professional

UPGRADE FROM TAX CERTIFICATE MANAGER 1.X

Certificate Manager 2.x is a new product offering that does not support a seamless, out-of-the-box upgrade path for existing Tax Certificate Manager 1.x implementations.

For more information about upgrading from Tax Certificate Manager 1.x to Certificate Manager 2.x, please contact ONESOURCE Professional Services or your account representative.

ARCHITECTURE

Before starting the installation, review selected architectural considerations and the system layout:

Workflow: Data flows only from Certificate Manager to Determination. Users change customer, contact, and certificate information in Certificate Manager—not directly in the Determination user interface.

User Accounts: Certificate Manager uses Determination users and roles.

Installation Environment:

Certificate Manager cannot be installed without access to an instance of Determination.

Certificate Manager cannot be installed in the same application server instance as Determination.

A best practice is to install Certificate Manager and Data File Integrator in separate application server instances.

If you have multiple ONESOURCE products on the same server, change ports to avoid conflicts.

Certificate Manager is composed of several applications (see below). The typical layout is to deploy all the applications in a single application server/web container instance. However, you can deploy the User Management Application or the Content Management Application in separate instances.

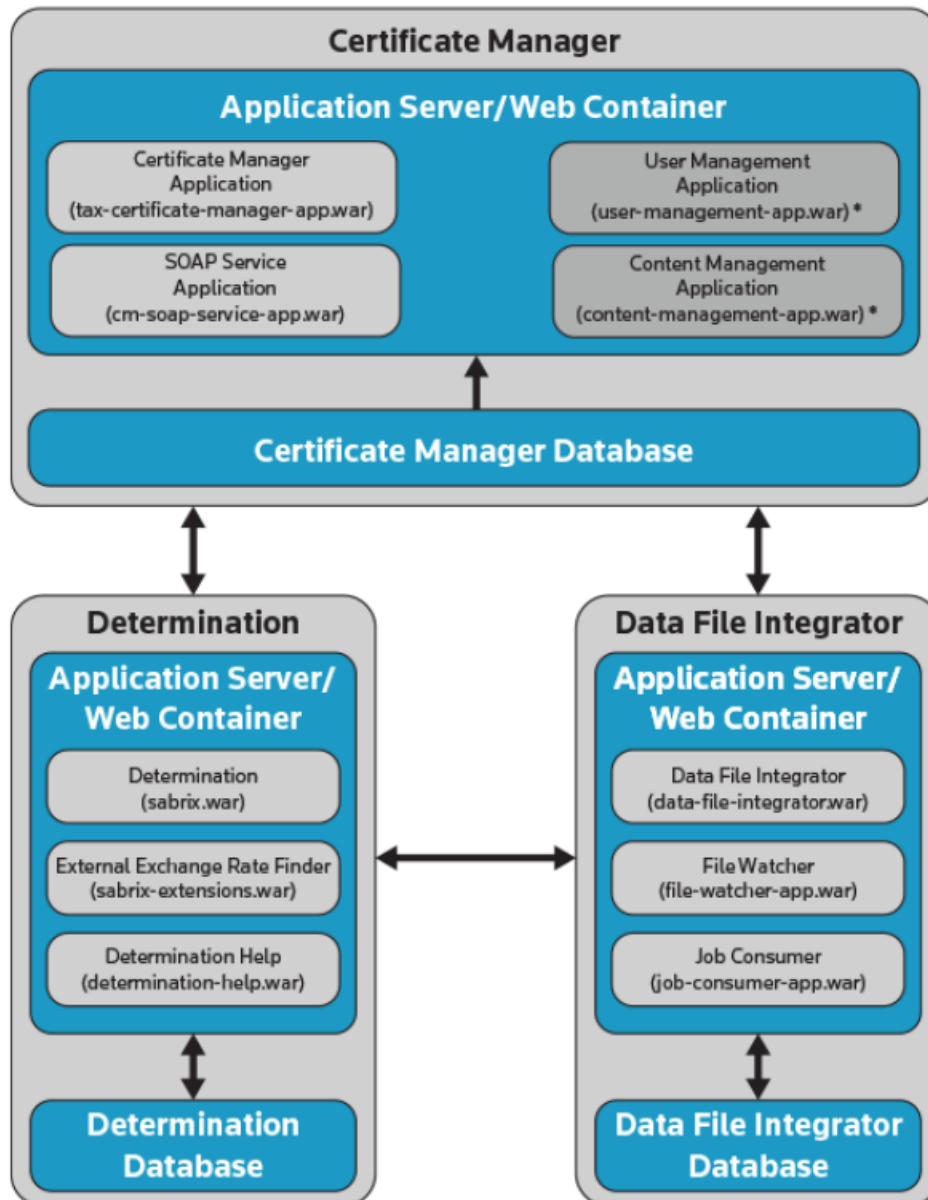
Certificate Manager Application (*tax-certificate-manager-app.war*)

SOAP Service Application (*cm-soap-service-app.war*)

User Management Application (*user-management-app.war*)

Content Management Application (*content-management-app.war*)

Typical Layout



* You can deploy this application in its own application server/web container instance.

RESOURCES

Several resources help you become familiar with ONESOURCE Indirect Tax Certificate Manager and master its features. Help is installed with the application. All documents are posted on the [ONESOURCE Customer Center](#). To locate documents specific to your application, enter the search term "Certificate Manager documentation."

CERTIFICATE MANAGER RESOURCES	
Resource	Description
Help	This Help system gives assistance within Certificate Manager. Use Help after Certificate Manager is installed and configured.
Installation Guide	This guide is intended for technical users and contains complete details about how to install and configure Certificate Manager.
Platform Support	This describes the combinations of operating systems, databases, and application servers on which Certificate Manager operates.
Product Support Lifecycle	This lists the end-of-life dates for products in the ONESOURCE Indirect Tax Suite.

Still can't find what you're looking for? Try these additional resources:

ONESOURCE RESOURCES	
Resource	Description
ONESOURCE Customer Center https://tax.thomsonreuters.com/support/onesource/customer-center/	Search for answers in the Knowledge Base, enter product support tickets, and track support ticket history for you and your organization.
Indirect Tax Customer Center https://customercenter.sabrix.com/	Download ONESOURCE Indirect Tax software.
Other ONESOURCE Indirect Tax Products and Services https://tax.thomsonreuters.com/products/brands/onesource/indirect-tax/	Browse descriptions of other ONESOURCE Indirect Tax products and services.

ONESOURCE RESOURCES	
Resource	Description
Documentation Feedback onesource.indirect.tax.fb@thomsonreuters.com	Send feedback about ONESOURCE Indirect Tax documentation.

STYLE CONVENTIONS

Thomson Reuters uses the following formatting throughout this guide:

Bold text indicates most user interface elements, such as:

- Data you are expected to enter, such as in a text field
- Pages, buttons, tabs, and field names
- Dialog boxes, drop-down lists, selections within lists, and check box titles
- Windows
- Menu items

Italic text indicates the following:

- File and folder names
- Java classes, PL/SQL objects and executable files
- Document titles

CAPITAL text indicates keyboard commands, such as ENTER, or database components.

`Courier` text indicates command-line input/output.

<brackets> indicate user entry. For example, <host> indicates you should replace the text and angle brackets with your server name.

Book titles are shown in italics and sections within a book are in quotation marks, such as “Starting the Installation” in the *ONESOURCE Indirect Tax Certificate Manager Installation Guide*.



This pencil symbol indicates suggestions or additional information.



This warning symbol indicates important text that you should review before proceeding.

↵ This carriage return symbol indicates that a single line of code is divided into multiple lines so you can read it. If you copy and paste code with these symbols, be sure to keep the code before and after the carriage return on the same line.

```
1  /* Some code snippets may
   have numbered lines with a gray background. */
2  /* If you copy lines from code snippets that include
   line numbers, be sure to remove those line numbers. */
```

TOMCAT CHECKLISTS

Use the checklists below to track your progress through the installation.

Prerequisites

PREREQUISITES	
Task	Complete?
Review System Requirements (page 9)	
Gather Administrative Information (page 9)	
Download the Software (page 10)	

Installation

TOMCAT CONFIGURATION	
Task	Complete?
Set Database Initialization Parameters (page 13)	
Set Database Character Set (page 13)	
Get JDBC Driver (page 13)	

TOMCAT CONFIGURATION	
Task	Complete?
Create Tablespace and User (page 13)	
Set JAVA_HOME (page 15)	
Configure JDBC (page 15)	
Configure Tomcat Logging (page 15)	
Configure Tomcat Initialization (page 16)	
Create Data Sources in Tomcat (page 17)	
Change Tomcat Ports (page 22)	
Configure Certificate Manager in Tomcat (page 15)	

Post-Installation Tasks

PREREQUISITES	
Task	Complete?
General Configuration (page 25)	
Email Configuration (page 27)	
Determination Roles (page 28)	
Determination Configuration Parameter (page 33)	
Additional Configurations (page 33)	
Data File Integrator (page 35)	

PREREQUISITES

Complete the following tasks before you install and configure Certificate Manager.

 Certificate Manager requires a working installation of Determination 5.6.2.4 or higher.

[Review System Requirements](#)

[Gather Administrative Information](#)

[Download the Software](#)

REVIEW SYSTEM REQUIREMENTS

ONESOURCE Certificate Manager has detailed requirements for the following:

- Computer hardware
- Operating system
- Database
- Application server/web container

To confirm you are using supported components, review platform support and product support lifecycle information listed in the [ONESOURCE Customer Center](#).

GATHER ADMINISTRATIVE INFORMATION

Before installing Certificate Manager, record your administrative information below:

TYPE	WHERE TO FIND	YOUR VALUES
Customer Center credentials	Thomson Reuters Customer Support	
Server name and port for your Certificate Manager database	Your Database Administrator (DBA)	

TYPE	WHERE TO FIND	YOUR VALUES
Service or instance name for your Certificate Manager database	Your DBA	
Administrative credentials for your Certificate Manager database	Your DBA	
Server name and port for your Determination database	Your DBA	
Service or instance name for your Determination database	Your DBA	
Tax user credentials for your Determination database (for example, SBXTAX)	Your DBA	
Server name and port for your Certificate Manager application server or web container	Your application server administrator	
Determination URL	Your Determination administrator	

DOWNLOAD THE SOFTWARE

Download Certificate Manager from the [ONESOURCE Customer Center](#). If you plan to do bulk uploads of customers and certificates, also download Data File Integrator.



To install Certificate Manager, you must use a version of Oracle Java that is appropriate to your application server. See the [ONESOURCE Customer Center](#) for additional information.

Certificate Manager

Download Certificate Manager and a ONESOURCE forms file.

1. Log on to Customer Center by entering the user name and password assigned by Customer Support.
2. Under **Available Products**, locate ONESOURCE Indirect Tax Certificate Manager.

3. For **Current Installed Version**, select **None**.
4. Click **Download**, and then save this file to a directory on the system hosting Certificate Manager or to a networked folder that can be accessed by that system.
5. Unzip the *ONESOURCEIDTCertificateManager_22xx.zip* file.
6. Back in the Customer Center, locate **Certificate Manager Forms Content** under **Available Products**.
7. For **Current Installed Version**, select **None**.
8. Click **Download**, and then save the forms .zip file to the same location as the Certificate Manager software.



Do not unzip the forms content file.

Data File Integrator



You can install Data File Integrator on the same computer as Certificate Manager, but it is best to keep them in separate application server instances. See the ONESOURCE Indirect Tax Data File Integrator Installation Guide for instructions about getting started.

1. Continue in the Customer Center and locate Data File Integrator under **Available Products**.
2. For **Current Installed Version**, select **None**.
3. Click **Download**, and then save this file to a directory on the system hosting Data File Integrator or to a networked folder that can be accessed by that system.
4. Unzip Data File Integrator in a separate directory from Certificate Manager.

CONFIGURE THE DATABASE

This guide covers the installation of Certificate Manager in the Oracle RDBMS. After you confirm that you are using the correct database version, review the following sections.

SET DATABASE INITIALIZATION PARAMETERS

Ensure that your database has appropriate initialization parameters before you start the Certificate Manager installation. Contact Oracle if you need assistance setting these parameters in your environment.

SET DATABASE CHARACTER SET

Configure the database to use a UTF8-compatible database character set. Optimize the handling of multi-byte characters by using the national character set AL16UTF16 (default). You need to either install or upgrade the database to meet these requirements.

GET JDBC DRIVER

Locate a Java 1.6 or 1.8 compliant Oracle JDBC driver appropriate for your database:

- ojdbc8.jar (Oracle Database 19c)
- ojdbc6.jar (Oracle Database 11g)

Make a note of the directory path and file name because you need it later in the installation.



JDBC drivers are usually packaged with the database or database client software. See [Oracle](#) for information about compatibility.

CREATE TABLESPACE AND USER

Certificate Manager requires an Oracle tablespace and user before you install the software. Use the .sql scripts in *Docs/database-creation-scripts/oracle* where you unzipped the Certificate Manager software.

These directions assume that you can connect to the database with SQL*Plus from where you unzipped the software. If you cannot, then move the following three files to a location where you can run them: *OracleSetup.sql*, *CreateOracleTablespaces.sql*, and *CreateOracleUsers.sql*.

1. Log on to SQL*Plus as a database user with administrative privileges.
2. Execute the following script in *Docs/database-creation-scripts/oracle*:
@OracleSetup.sql
3. To accept the default values in square brackets [], press ENTER, or type your own values:

SCRIPT PROMPT	DESCRIPTION
Enter CM Datafile Directory without trailing separator	Enter the location of the database datafile.
Enter CM Path Separator for this platform, either / or \	Enter the operating system path separator: "/" for UNIX or "\" for Microsoft Windows (without the quotation marks).
Enter CM Tablespace Name. Enter "none" or "NONE" to skip	Enter a tablespace name.  Only enter NONE or none to use an existing tablespace instead of a new tablespace.
Enter CM Tablespace Size. Enter M for megabytes or G for gigabytes	Adjust this medium-sized default value up or down depending on your installation requirements.
Enter CM user tablespace name	Enter a tablespace name.  If you do not want the default, choose a tablespace from the list above.
Enter CM user temporary tablespace name	Enter a temporary tablespace name.
Enter CM user to create	Enter a user name.
Enter CM user password	Enter a password.

4. When the script is complete, continue to the next section.

CONFIGURE CERTIFICATE MANAGER IN TOMCAT

When Tomcat is installed and ready for Certificate Manager configuration, complete the following:

[Set JAVA_HOME](#)

[Configure JDBC](#)

[Configure Tomcat Logging](#)

[Configure Tomcat Initialization](#)

[Create Data Sources](#)

[Change Tomcat Ports](#)

[Deploy Certificate Manager Under Tomcat](#)

SET JAVA_HOME

Ensure that you have a JAVA_HOME variable pointing to the Java installation directory.

CONFIGURE JDBC

You located a JDBC driver in the [Get JDBC Driver \(page 13\)](#) step. Insert that driver into the *lib* directory below *TOMCAT_HOME*.

CONFIGURE TOMCAT LOGGING

1. Go to following directory where you unzipped the Certificate Manager software:
Docs/application-server-files/tomcat/conf
2. Copy *logback.xml*.
3. Insert *logback.xml* into the directory *TOMCAT_HOME/conf*.

CONFIGURE TOMCAT INITIALIZATION

Insert the file *setenv* into Tomcat to allocate memory and set a log parameter. The file has these default settings:

JAVA OPTION	VALUE	DESCRIPTION
-Xms	512m	This is the recommended starting memory allocation in megabytes. Increase this value if your loads require more memory.
-Xmx	1024m	This is the recommended maximum memory allocation in megabytes. Increase this value if your loads require more memory.
-Dlogback.configurationFile=	../conf/logback.xml	Do not change this logging parameter.

- Go to the following directory where you unzipped the Certificate Manager software:
Docs/application-server-files/tomcat/bin
- Depending on your operating system, copy one of the following:
 - Unix/Linux: *setenv.sh*
 - Microsoft Windows: *setenv.bat*
- Go to the directory *TOMCAT_HOME/bin* and insert *setenv*.
- If you need to increase the memory settings because you anticipate large certificate loads, open *setenv* in a text editor.
- Change the values in **bold** below:

Unix/Linux:

```
JAVA_OPTS="-Xms512m -Xmx1024m -XX:MaxPermSize=1024m -Dlogback.configurationFile=../conf/logback.xml"
```

Microsoft Windows:

```
set "JAVA_OPTS=-Xms512m -Xmx1024m -Dlogback.configurationFile=../conf/logback.xml"
```

- Save and close *setenv*.

CREATE DATA SOURCES IN TOMCAT

Create data sources by inserting ONESOURCE snippets in *server.xml* and then editing the values.

Insert Data Source Snippets

1. Go to the following directory where you unzipped the Certificate Manager software:

Docs/application-server-files/tomcat/conf

2. Open *certificate-manager-data-source-mssql-tomcat.txt* in a text editor.
3. Copy all the data source snippets (the entire contents of the file).
4. Go to the directory *TOMCAT_HOME/conf*.
5. Open the file *server.xml* in a text editor.
6. In *server.xml*, insert the data source snippets immediately above the closing tag `</GlobalNamingResources>`.



Certificate Manager offers an option to encrypt the Tomcat data source username and password. In addition to the sections below, see [Encrypting Tomcat Data Source Credentials \(page 20\)](#) to encrypt the Tomcat data source credentials.

7. Remain in *server.xml* and complete the steps in the next sections for editing each data source.

[Edit Tax Certificate Manager Data Source \(page 17\)](#)

[Edit User Management Service Data Source \(page 18\)](#)

[Edit Content Management Service Data Source \(page 19\)](#)

Edit Tax Certificate Manager Data Source

In *server.xml*, find the `<Resource>` element that contains `jdbc/TaxCertificateManagerDataSource`.

```
<Resource name="jdbc/TaxCertificateManagerDataSource"
auth="Container"
type="javax.sql.DataSource"
username="user name"
password="password"
driverClassName="oracle.jdbc.driver.OracleDriver"
url="jdbc:oracle:thin:@//host:port/service"
validationQuery="select user from dual"
maxTotal="10"
maxIdle="4"/>
```

Change the values inside the `<Resource>` element that correspond to the elements in **jdbc/TaxCertificateManagerDataSource** as shown in the table below:

DATA SOURCE (JDBC/TAXCERTIFICATEMANAGERDATASOURCE)	
ELEMENT	DESCRIPTION
username=" user name "	Replace user name with the Certificate Manager database user name (for example, certmgr).
password=" password "	Replace password with the Certificate Manager database user password (for example, certmgr).
url="jdbc:oracle:thin:@ host:port/service "	Replace the following with values for your implementation: host: The name of the system hosting the Certificate Manager database. port: The Certificate Manager database port (default 1433). database: The name of the Certificate Manager database.  Use the following format for Oracle 11g: url="jdbc:oracle:thin:@host:port/service"

Save *server.xml*, and remain in the file to complete additional edits in the next section.

Edit User Management Service Data Source



This data source points to the Determination database, not to the Certificate Manager database.

In *server.xml*, find the `<Resource>` element that contains **jdbc/UserManagementServiceDataSource**.

```
<Resource name="jdbc/UserManagementServiceDataSource"
auth="Container"
type="javax.sql.DataSource"
username="user name"
password="password"
driverClassName="oracle.jdbc.driver.OracleDriver"
url="jdbc:oracle:thin:@//host:port/service"
validationQuery="select user from dual"
maxTotal="10"
maxIdle="4"/>
```

Change the values in the snippet that correspond to the elements in **jdbc/UserManagementServiceDataSource** as shown in the table below:

DATA SOURCE (JDBC/USERMANAGEMENTSERVICEDATASOURCE)	
ELEMENT	DESCRIPTION
username=" user name "	Replace user name with the user name of the Determination Tax schema (for example, sbtax).
password=" password "	Replace password with the password of the Determination Tax schema (for example, sbtax).
url="jdbc:oracle:thin:@// host:port/service "	Replace the following with values for your implementation: host: The name of the system hosting the Determination database. port: The Determination database port (default 1521). database: The name of your Oracle service.  Use the following format for Oracle 11g: url="jdbc:oracle:thin:@host:port/service"

Save *server.xml*, and remain in the file to complete additional edits in the next section.

Edit Content Management Service Data Source

 This data source points to the Determination database, not to the Certificate Manager database.

In *server.xml*, find the `<Resource>` element that contains **jdbc/ContentManagementServiceDataSource**.

```
<Resource name="jdbc/ContentManagementServiceDataSource"
auth="Container"
type="javax.sql.DataSource"
username="user name"
password="password"
driverClassName="oracle.jdbc.driver.OracleDriver"
url="jdbc:oracle:thin:@//host:port/service"
validationQuery="select user from dual"
maxTotal="10"
maxIdle="4"/>
```

Change the values in the snippet that correspond to the elements in **jdbc/ContentManagementServiceDataSource** as shown in the table below:

JDBC/CONTENTMANAGEMENTSERVICEDATASOURCE	
ELEMENT	DESCRIPTION
username=" user name "	Replace user name with the user name of the Determination Tax schema (for example, sbtax).
password=" password "	Replace password with the password of the Determination Tax schema (for example, sbtax).
url="jdbc:oracle:thin:@// host:port/service "	Replace the following with values for your implementation: host: The name of the system hosting the Determination database. port: The Determination database port (default 1521). database: The name of your Oracle service.  Use the following format for Oracle 11g: url="jdbc:oracle:thin:@host:port/service"

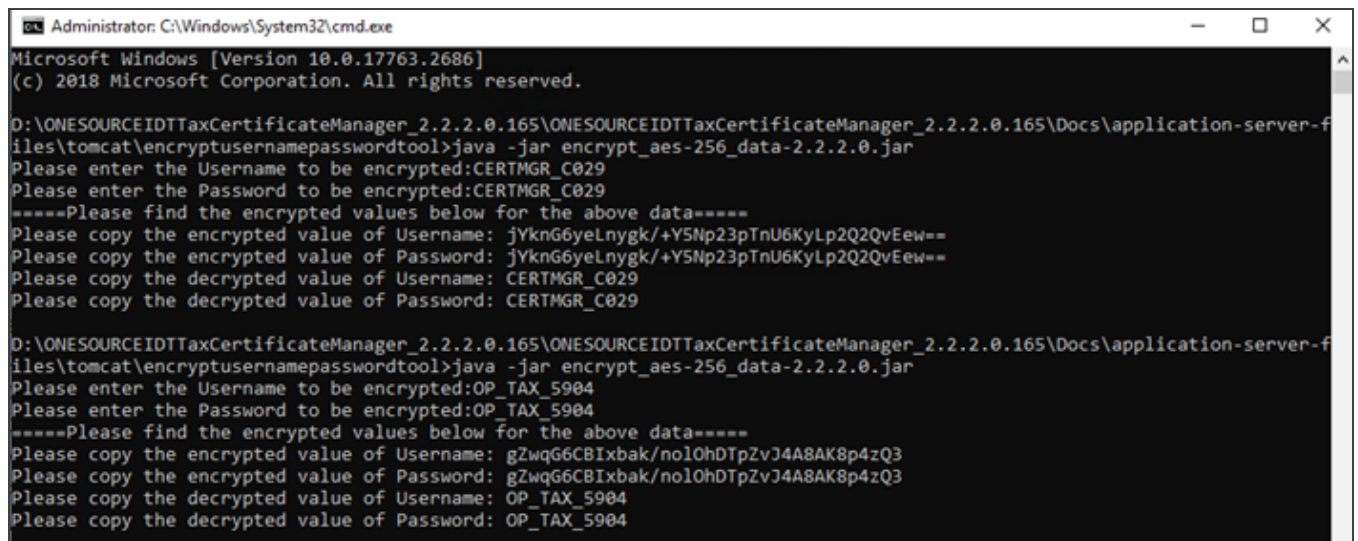
Save *standalone.xml*, and remain in the file to complete additional edits in the next section.

Encrypting Tomcat Data Source Credentials

The steps below take you through the process of encrypting Tomcat data source credentials for the Tax Certificate Manager Data Source, User Management Service Data Source and Content Management Service Data Source using the AES-256 standard. Encrypting Tomcat data source credentials is optional.

To encrypt Tomcat data source credentials:

1. Locate the `encrypt_aes-256_data-2.2.2.0.jar` file in the path `\Docs\application-server-files\tomcat\encryptusernamepasswordtool` where you unzipped the `ONESOURCEIDTTaxCertificateManager_2.2.2.x.x.zip` file. The `encrypt_aes-256_data-2.2.2.0.jar` file generates the encrypted value for the username and password text and uses AES-256 as the encoding mechanism.
2. Copy the `encrypt_aes-256_data-2.2.2.0.jar` file then paste it in `<TomcatBaseDirectory>\lib` folder.
3. Open the Command Prompt window.
4. Enter the following command, which will generate the encrypted values: `java -jar encrypt_aes-256_data-2.2.2.0.jar`. The following graphic shows an example:



```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.17763.2686]
(c) 2018 Microsoft Corporation. All rights reserved.

O:\ONESOURCEIDTTaxCertificateManager_2.2.2.0.165\ONESOURCEIDTTaxCertificateManager_2.2.2.0.165\Docs\application-server-f
iles\tomcat\encryptusernamepasswordtool>java -jar encrypt_aes-256_data-2.2.2.0.jar
Please enter the Username to be encrypted: CERTMGR_C029
Please enter the Password to be encrypted: CERTMGR_C029
=====Please find the encrypted values below for the above data=====
Please copy the encrypted value of Username: jYknG6yeLnygk/+Y5Np23pTnU6KyLp2Q2QvEew==
Please copy the encrypted value of Password: jYknG6yeLnygk/+Y5Np23pTnU6KyLp2Q2QvEew==
Please copy the decrypted value of Username: CERTMGR_C029
Please copy the decrypted value of Password: CERTMGR_C029

O:\ONESOURCEIDTTaxCertificateManager_2.2.2.0.165\ONESOURCEIDTTaxCertificateManager_2.2.2.0.165\Docs\application-server-f
iles\tomcat\encryptusernamepasswordtool>java -jar encrypt_aes-256_data-2.2.2.0.jar
Please enter the Username to be encrypted: OP_TAX_5904
Please enter the Password to be encrypted: OP_TAX_5904
=====Please find the encrypted values below for the above data=====
Please copy the encrypted value of Username: gZwqG6CBIXbak/nol0hDTpZvJ4A8AK8p4zQ3
Please copy the encrypted value of Password: gZwqG6CBIXbak/nol0hDTpZvJ4A8AK8p4zQ3
Please copy the decrypted value of Username: OP_TAX_5904
Please copy the decrypted value of Password: OP_TAX_5904
```

5. Update the `server.xml` file in `<TomcatBaseDirectory>\conf` by replacing the existing username and password in the `<Resource>` element with the encrypted username and password. In addition, add the following factory parameter:

```
factory="com.thomsonreuters.ositax.taxcertificatemanager.configuration.SecureT
omcatDataSourceImpl"
```

The following graphic shows the `<Resource>` element:

```

37 <GlobalNamingResources>
38   <!-- Editable user database that can also be used by
39        |   UserDatabaseRealm to authenticate users
40        |-->
41
42   <Resource name="UserDatabase" auth="Container"
43             type="org.apache.catalina.UserDatabase"
44             description="User database that can be updated and saved"
45             factory="org.apache.catalina.users.MemoryUserDatabaseFactory"
46             pathname="conf/tomcat-users.xml" />
47
48   <Resource
49     name="jdbc/TaxCertificateManagerDataSource"
50     auth="Container"
51     type="javax.sql.DataSource"
52     factory="com.thomsonreuters.ositax.taxcertificatemanager.configuration.SecureTomcatDataSourceImpl"
53     username="jYknG6yeLnygk/+Y5Np23pTnU6KyLp2Q2QvEew=="
54     password="jYknG6yeLnygk/+Y5Np23pTnU6KyLp2Q2QvEew=="
55     driverClassName="oracle.jdbc.driver.OracleDriver"
56     url="jdbc:oracle:thin:@c476dbmoradb.int.thomsonreuters.com:1522:ORCL"
57     validationQuery="select user from dual"
58     maxTotal="10"
59     maxIdle="4"/>
60
61   <Resource
62     name="jdbc/UserManagementServiceDataSource"
63     auth="Container"
64     type="javax.sql.DataSource"
65     factory="com.thomsonreuters.ositax.taxcertificatemanager.configuration.SecureTomcatDataSourceImpl"
66     username="gZwqG6CBixbak/nolOhDTpZvJ4A8AK8p4zQ3"
67     password="gZwqG6CBixbak/nolOhDTpZvJ4A8AK8p4zQ3"
68     driverClassName="oracle.jdbc.driver.OracleDriver"
69     url="jdbc:oracle:thin:@c476dbmoradb.int.thomsonreuters.com:1522:ORCL"
70     validationQuery="select user from dual"
71     maxTotal="10"
72     maxIdle="4"/>
73
74   <Resource
75     name="jdbc/ContentManagementServiceDataSource"
76     auth="Container"
77     type="javax.sql.DataSource"
78     factory="com.thomsonreuters.ositax.taxcertificatemanager.configuration.SecureTomcatDataSourceImpl"
79     username="gZwqG6CBixbak/nolOhDTpZvJ4A8AK8p4zQ3"
80     password="gZwqG6CBixbak/nolOhDTpZvJ4A8AK8p4zQ3"
81     driverClassName="oracle.jdbc.driver.OracleDriver"
82     url="jdbc:oracle:thin:@c476dbmoradb.int.thomsonreuters.com:1522:ORCL"
83     validationQuery="select user from dual"
84     maxTotal="10"
85     maxIdle="4"/>
86 </GlobalNamingResources>

```

CHANGE TOMCAT PORTS

If you are running other ONESOURCE products in separate Tomcat instances on the same server, change your ports for Certificate Manager to avoid conflicts.

For example, change all 8xxx ports to 9xxx in *server.xml*:

- 8080 becomes 9080
- 8005 becomes 9005

When you finish editing *server.xml*, save and close the file.

DEPLOY CERTIFICATE MANAGER UNDER TOMCAT

First, deploy the Certificate Manager installer, and then individually deploy the applications.

Installer

1. Stop Tomcat: In the *bin* directory under *TOMCAT_HOME*, execute the *shutdown* script:
 - Unix/Linux: *shutdown.sh*
 - Microsoft Windows: *shutdown.bat*
2. Go to the *WarFiles* directory where you unzipped the Certificate Manager software.
3. Copy *installer.war*, and then insert the file into *TOMCAT_HOME/webapps*.
4. Start Tomcat: In the *bin* directory under *TOMCAT_HOME*, execute the *startup* script:
 - Unix/Linux: *startup.sh*
 - Microsoft Windows: *startup.bat*
5. Open a browser, and then check the status at the installation URL (<http://<host>:<port>/installer>). The initial installation may take a few minutes and is finished when you see the notification **installer ok** in the browser window.
6. Stop Tomcat.
7. Remove the following from *TOMCAT_HOME/webapps*:
 - **File:** *TOMCAT_HOME/webapps/installer.war*
 - **Directory:** *TOMCAT_HOME/webapps/installer/*

Applications

1. Return to the *WarFiles* directory where you unzipped the Certificate Manager software.
2. Copy *cm-soap-service-app.war*, and then insert the file into *TOMCAT_HOME/webapps*.
3. Start Tomcat.
4. Wait until Tomcat creates the directory *webapps/cm-soap-service-app*.
5. From the *WarFiles* directory, copy the following files and insert them into *webapps*. Copy the files one at a time, waiting between each file for Tomcat to finish creating a new directory in *webapps*.

FILE	NEW TOMCAT DIRECTORY
<i>content-management-app.war</i>	<i>webapps/content-management-app</i>
<i>user-management-app.war</i>	<i>webapps/user-management-app</i>
<i>tax-certificate-manager-app.war</i>	<i>webapps/tax-certificate-manager-app</i>

6. Open a browser and go to the Certificate Manager **Login** page (<http://<host>:<port>/tax-certificate-manager-app>).
7. Log on to Certificate Manager using the built-in administrative user:
 - **User name:** `installer`
 - **Password:** `password`
8. Remain in Certificate Manager and then go to [Post-Installation Tasks](#).

POST-INSTALLATION TASKS

After you finish the application deployment, complete the tasks in the following sections:

[Certificate Manager \(page 25\)](#)

[Determination \(page 28\)](#)

[Additional Configurations \(page 33\)](#)

[Data File Integrator \(page 35\)](#)

CERTIFICATE MANAGER

The following configurations require you to be logged on to Certificate Manager. If you are logged on, continue with [General Configuration \(page 25\)](#).

If you have not logged on yet, complete the following:

1. Open a browser and go to the Certificate Manager logon page (<http://<host>:<port>/tax-certificate-manager-app>).
2. Log on to Certificate Manager using the built-in administrative user:
 - **User name:** installer
 - **Password:** password

General Configuration

On the **System Configuration** page, click **General Configuration**, and then complete the following settings that affect connectivity and validation:

FIELD	DESCRIPTION
Determination Base URL	Enter the URL of the Determination instance you want to connect to Certificate Manager. Use the following format: <a href="http://<host>:<port>/sabrix/services">http://<host>:<port>/sabrix/services

FIELD	DESCRIPTION
Connector Base URL	 Leave this field blank if you are doing a standard installation where all the services of Certificate Manager run in the same web container or application server instance. Connector Base URL is the location of the User Management Service that enables Certificate Manager users to use Determination roles. Only change this if you are doing a custom installation where you deploy <i>user-management-app.war</i> in a separate instance: http://<host>:<port>/user-management-app/services/
Content Service Base URL	 Leave this field blank if you are doing a standard installation where all the components of Certificate Manager run in the same web container or application server instance. Content Service Base URL is the location of the Content Management Service that provides tax content to Certificate Manager. If you are doing a custom installation where you deploy <i>content-management-app.war</i> in a separate instance, insert the URL for that instance using this format: http://<host>:<port>/content-management-app/services/contentManagementService/
Content Management Password	This password controls access to tax content information, such as lists of states.  You do not need to change this unless you want to change the default encrypted password. To change this password, see "Changing the Content Management Password" in the Help documentation.
Enable SOAP Logging	Select this option to add SOAP messages to Certificate Manager logs. Use this for troubleshooting SOAP connections to other software, such as to Determination.
Form Validation	Select Enable Form Validation if you want Certificate Manager to validate your entries for certificates.

FIELD	DESCRIPTION
Google Analytics	Select Enable Google Analytics to help Thomson Reuters improve your experience with Certificate Manager. Ensure that a port is open in your firewall that allows incoming and outgoing network traffic to the site google.com/analytics .

Email Configuration

Click **Email Configuration** to expand that section, and then complete the fields for sending notifications to your customers about their certificates.



If you are unsure about the correct email settings, insert dummy values and skip the email test.

1. Complete each of the fields in the following table:

FIELD	REQUIRED	DESCRIPTION
Host Name	Yes	Enter the name of the computer hosting your email server.
User Name	Yes	Enter the user name for the email account used to send notifications.
Sender Name	Yes	Enter the name of the sender of the email notification, for example, Avery Smith .
Email Server Port	Yes	Enter the number of the outgoing email port (SMTP).
Password	Yes	Enter the password for the email user.
Sender Email Address	Yes	Enter the email address of the sender; for example, avery@acme.com .

2. Click **Test email configurations**.
3. To test your configuration, enter a valid email address.
4. Click **Send**.
5. When you finish the email test, click **Save System Configuration** in the bottom left.

DETERMINATION

Complete the following configurations directly in Determination. Go to your instance (<http://<host>:<port>/sabrix>), and log on as a user with administrative privileges.

Determination Roles

Certificate Manager users log on using their Determination user names and passwords, but they use special roles for Certificate Manager. Complete the steps in the sections below for Certificate Manager roles.

Creating New Roles

 Skip this task if you are using Determination 5.7.0.0 or later.

Certificate Manager requires four new Determination roles shown in the following tables. Each table indicates the name, description, application, and permissions for the role. Instructions for adding each role are below the tables.

ROLE: CERTIFICATE MANAGER ADMIN				
DESCRIPTION: FULL ACCESS TO THE ENTIRE CERTIFICATE MANAGER APPLICATION AND REQUIRED DETERMINATION WEB SERVICES.				
Application	Create	Modify	Delete	View
Home				X
Display Error				X
Company Data				X
Change Password	X	X	X	X
Web Services				X
Web Services: Company Service	X	X	X	X
Web Services: Customer Service	X	X	X	X

ROLE: CERTIFICATE MANAGER ADMIN				
DESCRIPTION: FULL ACCESS TO THE ENTIRE CERTIFICATE MANAGER APPLICATION AND REQUIRED DETERMINATION WEB SERVICES.				
Application	Create	Modify	Delete	View
Web Services: Exemption Certificate Service	X	X	X	X
Web Services: User Service	X	X	X	X

ROLE: CERTIFICATE MANAGER SUPER USER				
DESCRIPTION: FULL ACCESS TO CERTIFICATE MANAGER AND REQUIRED DETERMINATION WEB SERVICES, WITH THE EXCEPTION OF CERTIFICATE MANAGER SYSTEM CONFIGURATION.				
Application	Create	Modify	Delete	View
Home				X
Display Error				X
Company Data				X
Change Password	X	X	X	X
System				X
Web Services				X
Web Services: Company Service	X	X	X	X
Web Services: Customer Service	X	X	X	X
Web Services: Exemption Certificate Service	X	X	X	X
Web Services: User Service	X	X	X	X

ROLE: CERTIFICATE MANAGER USER				
DESCRIPTION: PARTIAL ACCESS TO CERTIFICATE MANAGER FOR ADDING OR EDITING CUSTOMERS AND CERTIFICATES AND FOR RUNNING REPORTS.				
Application	Create	Modify	Delete	View
Home				X
Display Error				X
Company Data				X
Change Password	X	X	X	X
Web Services				X
Web Services: Company Service	X	X	X	X
Web Services: Customer Service	X	X	X	X
Web Services: Exemption Certificate Service	X	X	X	X
Web Services: User Service	X	X	X	X

ROLE: CERTIFICATE MANAGER VIEW ONLY				
DESCRIPTION: PARTIAL ACCESS TO CERTIFICATE MANAGER FOR SEARCHING CUSTOMERS, CONTACTS, OR CERTIFICATES; AND FOR RUNNING REPORTS.				
Application	Create	Modify	Delete	View
Home				X
Display Error				X
Company Data				X

ROLE: CERTIFICATE MANAGER VIEW ONLY				
DESCRIPTION: PARTIAL ACCESS TO CERTIFICATE MANAGER FOR SEARCHING CUSTOMERS, CONTACTS, OR CERTIFICATES; AND FOR RUNNING REPORTS.				
Application	Create	Modify	Delete	View
Change Password	X	X	X	X
Web Services				X
Web Services: Company Service				X
Web Services: Customer Service				X
Web Services: Exemption Certificate Service				X
Web Services: User Service				X

Refer to the four tables above as you complete the following steps to add each role:

1. Go to **Menu > System > Roles**.
2. Click **Actions > Add**.
3. In **Role**, enter the name from the first role table above: **Certificate Manager Admin**.



Role names are case sensitive.

4. In **Description**, enter the following from the first role table: **Full access to Certificate Manager and required Determination web services**.
5. Click **Submit**.
6. Select the boxes under **Create**, **Modify**, **Delete**, or **View** according to the permissions shown in the first role table above.
7. Click **Submit** when you finish selecting permissions.
8. Repeat steps 2 through 7 to create the three additional roles shown in the other three tables above.

9. When you finish, confirm you have the following roles and descriptions in Determination:

ROLE	DESCRIPTION
Certificate Manager Admin	Full access to the entire Certificate Manager application and required Determination Web Services.
Certificate Manager Super User	Full access to Certificate Manager and required Determination web services, with the exception of Certificate Manager system configuration.
Certificate Manager User	Partial access to Certificate Manager for adding or editing customers and certificates, and for running reports.
Certificate Manager View Only	Partial access to Certificate Manager for searching customers, contacts, or certificates, and for running reports.

Assigning the Certificate Manager Admin Role

Designate one of your Determination users as a Certificate Manager administrator to complete the remaining steps of the configuration.



Later, after you complete these initial configurations, you can grant Certificate Manager roles to additional Determination users.

1. Go to **Menu > System > Users**, and then click on the user to whom you want to assign the administrative role.
2. Click the **Roles** tab.
3. Click **Actions > Attach Role**.
4. Complete the fields listed in the User Roles table below:

FIELD	DESCRIPTION
Role	Select the role Certificate Manager Admin .
Company	Select a Determination company.
Start Date	Enter the date the role becomes active. Use the format MM/DD/YYYY; for example, 01/01/2021.

FIELD	DESCRIPTION
End Date	Enter the date the role becomes inactive (optional). Use the format MM/DD/YYYY; for example, 12/31/2021.
Is Cascading	Select if you want this user's role to apply to child companies.

- Click **Submit**.
- Remember the name of this Determination user because you will use it in [Additional Configurations \(page 33\)](#).
- Remain in Determination and continue to the next section.

Determination Configuration Parameter

 Skip this step if you are using Determination 5.6.x.

Determination versions 5.7.0.0 and later allow you to link directly to the Certificate Manager **Login** page:

- Log on to Determination.
- Go to **Menu > System > Configuration**.
- Click **Actions > Add**.
- Insert the following in the **Name** column: **CERTIFICATE_MANAGER_URL**.
- Insert the Certificate Manager URL in the **Value** column (for example, http://<host>:<port>/tax-certificate-manager-app).
- Click **Submit**.

ADDITIONAL CONFIGURATIONS

The basic installation of Certificate Manager is complete, but you need to make some additional configurations in Determination and Certificate Manager before you can use the software.

Determination

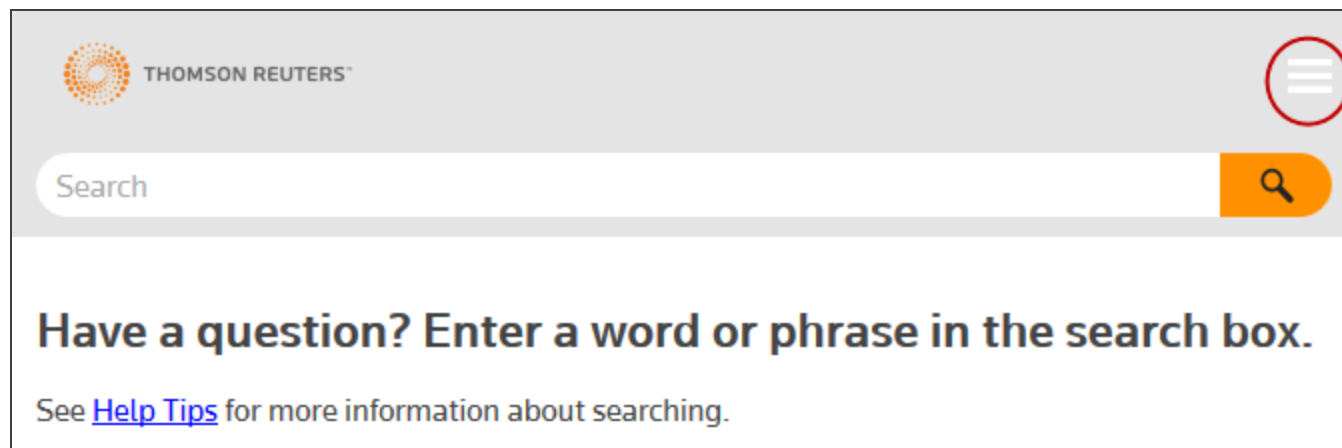
- Assign Certificate Manager roles to Determination users
- Configure certificate settings for companies in Determination

Certificate Manager

- Import forms
- Configure custom properties
- Configure default certificate status
- Configure exempt reasons
- Disable installer user

The instructions for these settings are in the Certificate Manager Help:

1. Log on to Certificate Manager using the Determination user who has the role **Certificate Manager Admin**.
2. In the upper-right corner of any page, click **Help**.
3. In the upper-right corner of Help, click the hamburger menu:

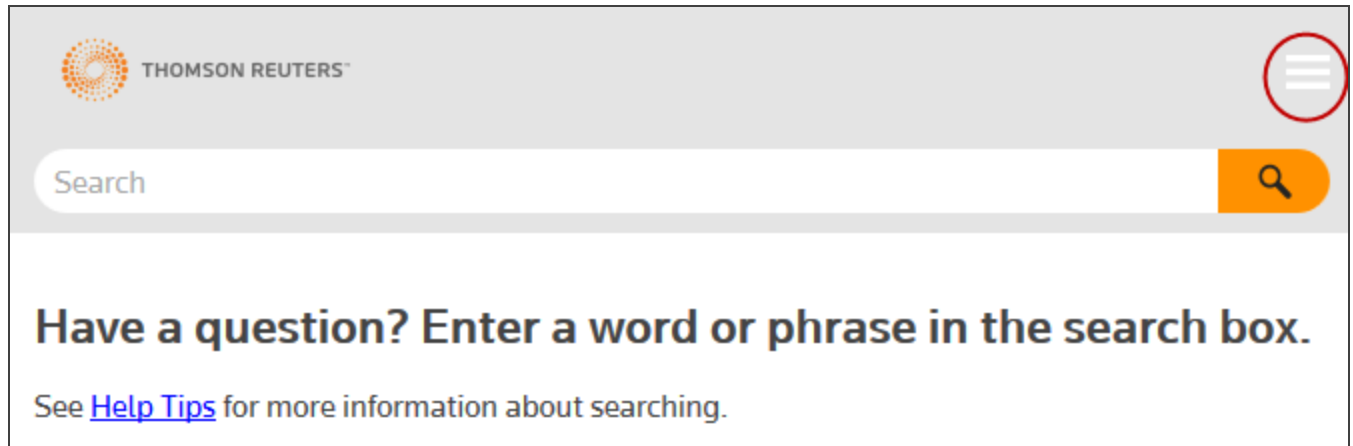


4. Go to **Introduction > Initial Configurations**.
5. Complete all the tasks in the **Initial Configurations** topic.

DATA FILE INTEGRATOR

If you plan to perform bulk uploads of customer and certificate data, see the overview topic about Data File Integrator in Certificate Manager Help:

1. In the upper-right corner, click the hamburger menu:



2. Go to **Supporting Software > Data File Integrator**.

Data File Integrator installation instructions are available in the [Knowledge Base](#).