



EUROPEAN COMMISSION

DIGIT
Connecting Europe Facility

CEF eSignature TLManager

Version 0.01

TLManager "Non-EU"¹- Release

¹ "Non-EU" designates the version of the application in contrast to the original version of TLManager. This version of the application is designed to Trusted Lists that are not pointed by the list of the lists (LOTL) published by the European Commission pursuant to Article 9 of eIDAS Regulation 910/2014.

Document Status:

Status
[Draft/Approved/Final]

Summary of Changes:

Version	Date	Created by	Short Description of Changes
0.01	14/01/2019		Creation

© European Union, 2018

Reuse of this document is authorised provided the source is acknowledged. The Commission's reuse policy is implemented by Commission Decision 2011/833/EU of 12 December 2011 on the reuse of Commission documents.

Table of Contents

1. INTRODUCTION	4
2. TLMANAGER INSTALLATION AND CONFIGURATION	5
2.1. PREREQUISITE	Error! Bookmark not defined.
2.2. DEPLOYMENT	5
2.3. MYSQL DATABASE CONFIGURATION	6
2.4. TOMCAT CONFIGURATION	6
2.5. TLMANAGER INSTALLATION	7
3. HOW TO	9
3.1. HOW TO START AND STOP THE APPLICATION	9
3.2. HOW TO USE YOUR OWN CAS SERVER AND USER LOGIN	9
3.3. HOW TO MANAGE USERS	10
3.4. HOW TO EDIT DRAFTS	10
3.5. HOW TO MANAGE DRAFTSTORES	11
3.6. HOW TO MANAGE SIGNING CERTIFICATES	11
3.7. HOW TO SIGN A TL	12
3.8. HOW TO ADD DATA PROPERTIES	13
3.9. HOW TO EDIT CHECKS	14
3.10. HOW TO CONFIGURE MONITORING JOBS	15
3.11. HOW TO START NEXU	15

1. INTRODUCTION

This version of TLManager is forked from TLManager 5.4. It provides more appropriate tools for Trusted Lists (TLs) that don't figure in the list of the lists (LOTL) published by the European Commission pursuant to Article 9 of eIDAS Regulation 910/2014. Therefore, constraints on the conformance and the signature of TLs are relaxed and some services as notifications, statistics and EU Trust Backbone have been removed.

This application allows the creation, the edition, the signature, the validation and the monitoring of TLs. These TLs follow a common template to provide information about trust services as defined under the ETSI TS 119 612 v2.1.1 standard.

This present document combines installation, configuration and user manuals of TLManager "Non-EU" version. While the next section on the installation and the configuration of the application is mostly technical, the other section is appropriate for both technical and business users.

2. TLMANAGER INSTALLATION AND CONFIGURATION

These next subsections present prerequisites steps to follow for the installation and the configuration of the web environment of the application.

2.1. PREREQUISITE

As a web application, TLManager needs the following software as a prerequisite:

- A Tomcat web server, to deploy TLManager;
- A MySQL database, to store data of the application;
- A Central Authentication Service (CAS), to manage registered access;
- Java 8 as JDK.

An existing Tomcat-MySQL-CAS environment can be reused, or a new one can be installed. As this application is a standard JEE application, please note that, with minor adjustments, other web servers, SQL databases, or CAS-based identity providers might be used as well.

① TLManager has been tested successfully with the following configurations:

	Environment 1	Environment 2
Operating System	Ubuntu 14.04.3 LTS	Windows 10 x64 Professional
Java	Oracle JRE 1.8.0_151-b12	Oracle JRE 1.8.0_191-b12
Apache Tomcat	8.0.33	9.0.0
MySQL	5.5.49	5.7.23

2.2. DEPLOYMENT

The zip file "TLManager Non-EU - Release 5.0.zip" contains 1 file and 3 folders, which will be used in the remainder of the document:

- *TLManager Non-EU - Release 5.0/lib*
- *TLManager Non-EU - Release 5.0/tlmanager-non-eu-config*
- *TLManager Non-EU - Release 5.0/webapps*
- *TLManager Non-EU - Release 5.0/migration-script.sql*

The following sections detail the deployment in 3 main steps:

- The database creation;
- The web server configuration;
- TLManager installation.

2.3. MYSQL DATABASE CONFIGURATION

Connect to the MySQL administration and create a new database named "tsl-noneu" using "utf8_general_ci" collation via the phpMyAdmin interface or using this command line:

```
CREATE DATABASE tsl-noneu DEFAULT CHARACTER SET utf8 DEFAULT COLLATE utf8_general_ci;
```



Figure 1: MySQL Administration

Then, import the SQL script "migration_script.sql" from the installation folder. Please note that the script is for a MySQL instance and should be adapted for other systems.

2.4. TOMCAT CONFIGURATION

Copy the folder "tlmanager-non-eu-config" found in the installation folder and paste it in your Tomcat installation folder.

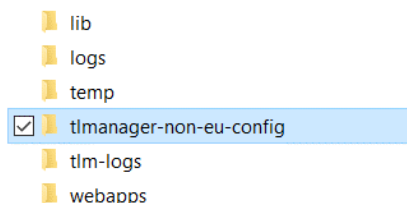


Figure 2: Tomcat folder

Copy the content found in the folder "TLManager Non-EU - Release 5.0\lib" in the "lib" folder of your Tomcat installation folder.

- *TLManager Non-EU - Release 5.0/lib/application-tlmanager-non-eu-custom.properties*
- *TLManager Non-EU - Release 5.0/lib/proxy.properties*
- *TLManager Non-EU - Release 5.0/lib/logback.xml*

Update both files to match with your web environment:

- *proxy.properties* (if necessary)

```
proxy.http.host=127.0.0.1
proxy.http.port=8008
proxy.http.user=
proxy.http.password=
proxy.http.enabled=false
proxy.http.exclude=

proxy.https.host=127.0.0.1
proxy.https.port=8008
proxy.https.user=
proxy.https.password=
proxy.https.enabled=false
proxy.https.exclude=
```

- *application-tlmanager-non-eu-custom.properties*

```
#CAS
casServerUrl=http://xxx.xxx.xxx.xxx:8080/cas-server-webapp-4.0.0
casServiceUrl=http:// xxx.xxx.xxx.xxx:8080/tl-manager-non-eu

#Database
jdbc.driverClassName=com.mysql.jdbc.Driver
jdbc.url=jdbc:mysql://localhost:3306/tsl-noneu
jdbc.username=<USERNAME>
jdbc.password=<PASSWORD>
```

where

- "xxx.xxx.xxx.xxx" should be the IP address of the corresponding server;
- <USERNAME> and <PASSWORD> should be updated with appropriate values.
 - o Be careful, those properties are case sensitive. White space at the end of value might produce database connection errors.

2.5. TLMANAGER INSTALLATION

Copy the 2 war files found in the folder "TLManager Non-EU - Release 5.0\webapps" and paste it in the "webapps" Tomcat folder.

- *TLManager Non-EU - Release 5.0/webapps/tl-manager-non-eu.war*
- *TLManager Non-EU - Release 5.0/webapps/cas-server-webapp-4.0.0.war*

Note: This last war file is the CAS server, delivered for convenience together with the application. Another CAS server can be used as an alternative.

Start the web server (See 3.1 HOW TO START AND STOP THE APPLICATION).

Once started, the application can be accessed via:
<http://xxx.xxx.xxx.xxx:8080/tl-manager-non-eu/> where "xxx.xxx.xxx.xxx" is the IP address of the server.

Next time you run the application, in the custom properties file, set the "hibernate.hbm2ddl.auto" property to "validate":

- *application-tlmanager-non-eu.properties*

```
#hibernate.hbm2ddl.auto=create  
hibernate.hbm2ddl.auto=validate
```


3. How to

This section shows how to correctly start and configure the application and provides guidance on how to create, edit and update drafts, draftstores, users and signatures.

3.1. HOW TO START AND STOP THE APPLICATION

To **start** your Tomcat webserver:

- Go to the "bin" folder of your Tomcat installation folder;
- Execute the start-up script;
- Optionally, verify in the log file that the server is starting. TLManager is accessible once the following line appears:

```
INFO [main] org.apache.catalina.startup.Catalina.start Server startup in ..... ms
```

For information purposes, here are 3 commands used to start the server on a Linux environment and to read the log file.

```
cd /opt/tomcat/bin
./startup.sh
tail -200f ../logs/catalina.out
```

To **stop** your Tomcat webserver:

- Go to the "bin" folder of your Tomcat installation folder;
- Execute the shutdown script;
- Optionally, verify in the log file that the server is stopping. As monitoring jobs are executed by TLManager, it may be possible that the shutdown script doesn't kill all the related processes. You may need to terminate those manually before restarting your server.

For information purposes, on a Linux environment, the "ps -ef" command displays all the running processes and the "kill" command followed by the process name terminates this process.

3.2. HOW TO USE YOUR OWN CAS SERVER AND USER LOGIN

In the *application-tlmanager-non-eu.properties* file (See 2.4 TOMCAT CONFIGURATION), modify the 2 following properties with the desired values and restart your webserver.

```
casServerUrl=https://xxxxxxxxxxxxxxxx
casServiceUrl=http://xxxxxxxxxxx:8080/tl-manager-non-eu
```

3.3. HOW TO MANAGE USERS

- You have an administrator set in the application.

Log in the application as administrator and choose "Users" in the management panel.

- You don't have an administrator set in the application.

Create an administrator directly in your database by adding a user in the "TL_USERS" table and attribute him the super administrator role (*role_id=1*) or the administrator role (*role_id=2*) in the "TL_USER_ROLE" table. You will now be able to log in as administrator and manage users directly in TLManager.

Administrator users have access to the "Management" and "My Drafts" panels while standard users only have access to the "My Drafts" panel.

All the users created in TLManager need to have at least one role defined. A user without any role will not be able to access the application.

Note: Every user created need to have a valid and authorized CAS account to access the application. Update *deployerConfigContext.xml* file in the *WEB-INF* folder of the CAS project deployed on your Tomcat. A "test" user is already configured with "password" as the password.

3.4. HOW TO EDIT DRAFTS

Drafts can be created or imported via the "My Drafts" panel which is accessible by any user with at least one role.

When creating an empty draft, if there are several countries registered in the properties (See 3.8 HOW TO ADD DATA PROPERTIES), you can choose in the drop-down list the territory of your Trusted List. Some fields in the *TL Information* of the created draft will be automatically set.



Figure 3: Creating an empty draft when several countries are available



Figure 4: Creating an empty draft when only one country is available

Importing a Trusted List from a local file is only possible if the *Version Identifier* of this file is "5" and if the *TSL Issuer* country is present in the data properties.

3.5. HOW TO MANAGE DRAFTSTORES

Draftstores are repositories where are located drafts. The identifier of your current draftstore can be found through the URL of your “My Drafts” page. By sharing this URL, you allow people to have access to your drafts. They will now be able to see, edit and delete these drafts.

When creating a new repository, a new draftstore will be created. If you want to be able to access your previous repository in the future, it is recommended to save the URL before proceeding. If you want to transfer some of your existing drafts to the newly created repository, you should export them beforehand, and import them in the new repository once created.

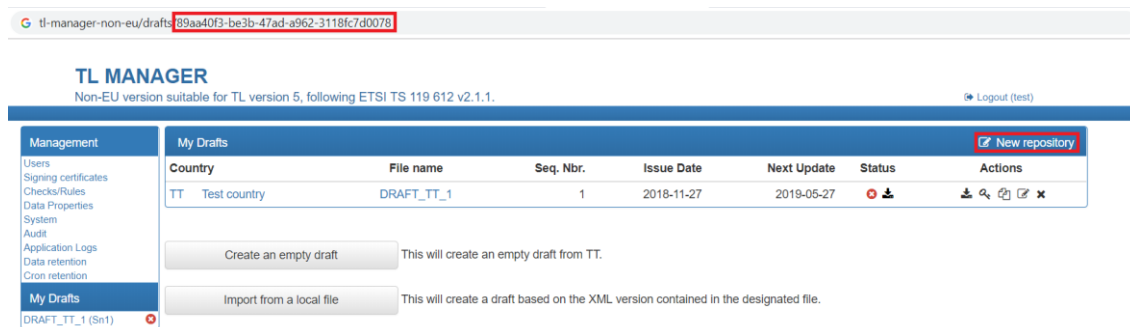


Figure 5: Locate draftstore ID and add a new draftstore

The identifiers of the draftstores can also be found in the “Data retention” management tab. From this page, draftstores and drafts can be deleted. Note that drafts can also be deleted from the “My Drafts” page (See 3.4 HOW TO EDIT DRAFTS).

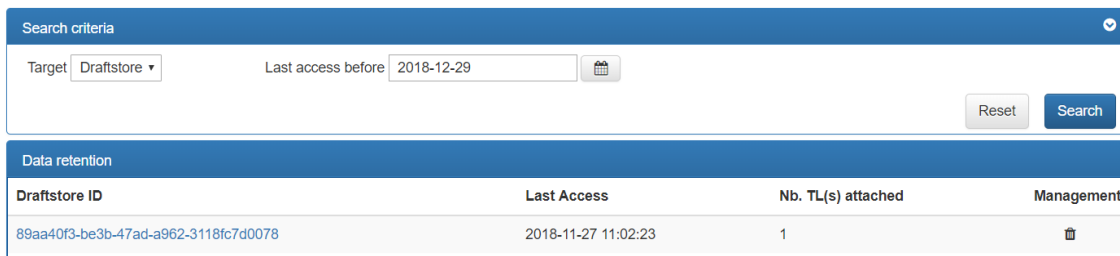


Figure 6: Manage draftstores in “Data retention” management tab

3.6. HOW TO MANAGE SIGNING CERTIFICATES

Signing certificates are the authorized certificates to sign Trusted Lists². When validating a signature, the certificate of the signature will be compared with the signing certificates declared as authorized and consider the signature as valid if a match is found.

² In fact, that is the private key linked to the certificate that will sign the Trusted List.

In order to manage these certificates, log in the application as “Administrator” user. (See 3.3 HOW TO MANAGE USERS) and select “Signing certificates” in the management panel.



Figure 7: Add a Signing Certificate

Adding a new certificate can be achieved in two ways:

- By importing a local certificate file;
- By copy-pasting a Base64 DER-Encoded certificate.

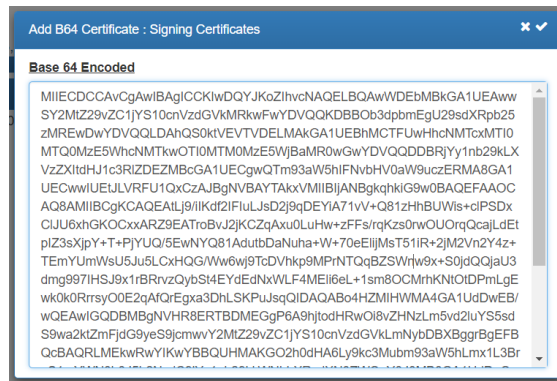


Figure 8: Copy paste of Base64 DER-Encoded certificate

3.7. HOW TO SIGN A TL

A Trusted List can be signed in two ways:

- A draft can be exported in XML format, be signed with any signature tool and the signed document can be imported again.
- A draft can be directly signed within TLManager using NexU (See 3.11 HOW TO START NEXU) via the “My Drafts” page or in the draft edition view.

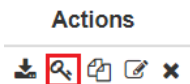


Figure 9: Sign button in “My Drafts” page



Figure 10: Sign button in draft edition view

If the status of your signature is “Indeterminate (NO_CERTIFICATE_CHAIN_FOUND)”, it means that the certificate used to sign is not present in the “Signing certificates” management tab (See 3.6 HOW TO MANAGE SIGNING CERTIFICATES).

3.8. HOW TO ADD DATA PROPERTIES

Data properties are used to check the conformance of the TL content and to populate dropdown lists while editing a draft. Adding these properties is an essential step to create and edit Trusted Lists. Some properties are provided as example within application. However, you should adapt these properties according to your needs. There are two ways to add a new property:

- (Recommended) As an administrator, using the “Data Properties” tab in the management panel;

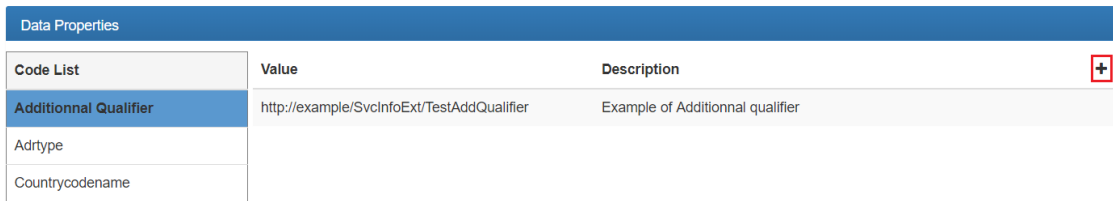


Figure 11: Adding a new property using the “Data Properties” tab


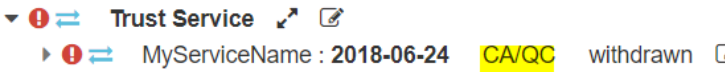
- Directly in the database via command lines or the phpMyAdmin interface.

```
INSERT INTO TL_PROPERTIES (PROPERTIES_ID, LABEL, DESCRIPTION, PROPERTIES_LIST_CODE)
VALUES(12, 'http://example/Svcstatus/status', 'Example of Service Status', 'SERVICE_STATUS');
```

Example of SQL query adding a new Service Status

Below are presented the different existing types of properties and their related fields:




Type	Related TL fields
Additional Qualifier	<i>Additional Service Information</i> in service extensions
Adrtype	<i>Electronic addresses</i> and <i>Distribution points</i>
Countrycodename	Each field requiring a territory. Note: When importing a Trusted List, its corresponding <i>SchemeTerritory</i> must be present in this type of properties.
Identifier Qualifier Type	<i>PolicySet</i> for qualifications extensions
Languages	Multi-languages fields (<i>Scheme name</i> , <i>Electronic addresses...</i>)
Mimetype	<i>Pointers to other TSL</i> for the <i>Mime Type</i> field
Qualifiers	<i>Qualifiers</i> in qualifications extensions
Service Previous Status	<i>Service status</i> in services history

Service Status	<i>Service status</i> for services and services history
Service Status Prefix	Used to shorten the <i>service status</i> to improve the readability of services  Figure 12: Service status once prefix has been removed
Service Types Identifiers	<i>Type Identifier</i> for services and services history
Service Types Prefix	Used to shorten the service <i>type identifier</i> to improve the readability of services  Figure 13: Service type once prefix has been removed
TL Communityrule	<i>Community Rule</i> in <i>SchemeInformation</i>
TL Status Determ Type	<i>Status Determination Approach</i> in <i>SchemeInformation</i>
TL Type	<i>TSL Type</i> in <i>SchemeInformation</i> and <i>TL Type</i> in <i>Pointers to other TSL</i>
TSL Tag Value	<i>TSL Tag</i> in <i>SchemeInformation</i>

A type will be displayed in the “Data properties” management tab only if this type contains at least one property. By default, the database is already populated with examples for each type.

3.9. HOW TO EDIT CHECKS

Checks which appear in the “Checks/Rules” management tab are the one present in the database. A severity is assigned to each check that change the type of icons displayed:

- ERROR: display  icon
- WARNING: display  icon
- INFO: display  icon
- IGNORE: don't display any icon

Even if the severity of a check is “IGNORE”, the check will still run in background. If you don't want a given check to run in the background, this check should be removed from the database.

3.10. HOW TO CONFIGURE MONITORING JOBS

TLManager includes monitoring features. When TLManager is deployed, 3 scheduled jobs have a scheduled execution:

- Check conformance process;
- Signature validation process;
- Retention process.

The Check conformance process runs a set of rules on each draft to verify its conformance according to ETSI TS 119 512 v2.1.1. By default, this job runs once a day, at 2 am.

The Signature validation process compares the signature of each draft with the certificates stored in the "Signing certificates" management tab. A signature is considered as valid if it is issued from a trusted "signing certificate" (See 3.6 HOW TO MANAGE SIGNING CERTIFICATES). By default, this job runs once a day, at 1 am.

The Retention process removes draftstores and trusted lists that have not been modified for a given time. By default, this job runs every first of the month at 0 am and removes data that has not been accessed within the last two months.

Default timings can be modified in the *application-tlmanager-non-eu.properties* file (See 2.4 TOMCAT CONFIGURATION):

```
#Checking TL conformity - every day @ 1AM
cron.signature.validation.job = 0 0 1 * * ?
#Verify TL signature - every day @ 2AM
cron.rules.validation.job = 0 0 2 * * ?
#every 1st of month @ 0AM
cron.retention.job = 0 0 0 1 1/1 ?
```

3.11. HOW TO START NEXU

Prerequisite: NexU is running on the local computer that is used to sign. If NexU is not running, the following information popup will be displayed when trying to sign a TL using TLManager.

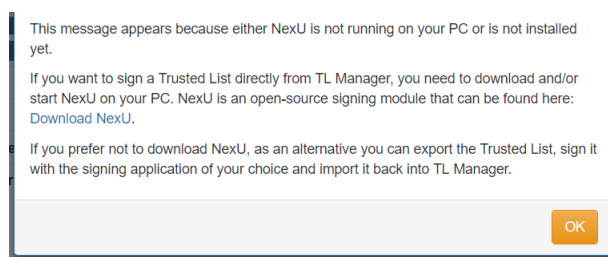


Figure 14: Signature popup when NexU is not running on the computer

If NexU is not present on your PC, please download it (version 1.10.5) at:

<http://lab.nowina.solutions/nexu-releases/nexu-bundle-1.10.5.zip> (the same link is provided in Figure 14).

Once downloaded, unzip the archive and run the "NexU-Startup.bat" file. Equivalent scripts can be implemented for another operating system. This will start NexU on your computer. When NexU is started, you should see a new icon through your OS system tray.

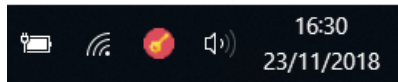


Figure 15: NexU icon in the Windows system tray

Restarting your computer will stop NexU. When you will later sign a document, make sure that NexU is running. You can either:

- Restart it manually by double-clicking on the start-up script. You may create a shortcut to this script on your desktop for convenience.
- Add it as a service so that NexU starts automatically at the start-up of your PC.

Note: The first time NexU is started, a certificate is installed in your OS certificate store. It is used to sign on HTTPS environment.