ORIGINATOR: TAXUD/A4	ISSUE DATE: 12/11/2010	VERSION: 5.00-EN

SUBJECT:

TARIC3 Administration Manual

DOCUMENT HISTORY

EDI.	REV.	DATE	DESCRIPTION	ACTION	PAGES
0	01	22/09/2008	Initial version	Insert	All
0	10	04/06/2009	SFR	Update	4.2.2
1	00	07/07/2009	Implementation of review comments. Sent for acceptance.	Update	As required
1	10	09/09/2009	Sent for Review.	-	-
2	00	30/09/2009	Implementation of review comments. Sent for Acceptance	Update	As requested
2	01	30/10/2009	Minor updates.	Update	Section 4.1 and 4.2
2	10	16/04/2010	Sent for Review.	-	-
3	00	18/05/2010	Sent for Acceptance.	Update	As requested
3	10	08/06/2010	Sent for Review.	-	-
4	00	22/06/2010	Sent for Acceptance.	-	-
4	01	26/10/2010	Removing of the Quota2 configuration (QTM156) Sent for Internal Review.	Update Delete	4.1, 4.1.6, 4.2.2, 4.2.4, 4.3.1 4.1.5, 4.1.8, 4.2.6
4	10	29/10/2010	Sent for Review.	-	-

5	00	12/11/2010	Sent for Acceptance.	-	-

TABLE OF CONTENTS

LIST OF TABLES

1. INTRODUCTION

1.1. Objective of this document

This document describes the administration procedures for the TARIC3 application. The basics of the administration procedures are shared by all new customs applications of the Directorate General Taxation and Customs Union (DG TAXUD).

1.2. Intended audience

This document is intended for people responsible for the administration of the different customs applications at DG TAXUD that use the BEA WebLogic application server infrastructure. The administration of the TARIC3 application is treated in this document.

1.3. Structure of this document

Chapter 2 contains a general description of all the administration procedures. Chapter 3 describes the prerequisites. Finally, chapter 4 describes the administration procedures in detail.

1.4. Abbreviations and acronyms

CCN	Common Communication Network
CCN/TC	CCN Technical Center
CSI	Common Service Interface
DDS	Data Dissemination System
DG	Directorate General
EJB	Enterprise Java Bean
HTTP	HyperText Transfer Protocol
ISO	International Organization for Standardization
JEE	Java Enterprise Edition
JMS	Java Messaging Service
JVM	Java Virtual Machine
TARIC	TARif Intégré Communautaire
TAXUD	Taxation and Customs Union
URL	Uniform Resource Locator
WLS	WebLogic Server

XML   eXtensible Markup Language

1.5. Reference documents

[CSI-INS-001]   "CSI Bridge Installation and Administration Guide", ref.
                          CSI-INS-001, 1.02

[UM-INS-001]   "UM Installation and Administration Guide", ref. UM-
                          INS-001, 1.02

[UM-USG]   "UM User Guide", ref. UM-USG-001, 1.00

[TARIC3-IPR]   "TARIC3 Installation Procedure Manual", ref. TARIC3-
                          IPR, 3.00

1.6. Applicable documents

None.

2. OVERVIEW

This chapter contains a general description of the administration procedures. The basic procedures are very similar for all applications that use the BEA WLS. The aim of this overview is to provide the reader with a global view of the administration procedures and the tools used.

The BEA WLS has been chosen as the platform to host the new implementations of the DG TAXUD customs applications. WLS is an implementation of Java Enterprise Edition 5 (JEE5). The customs applications have as common requirement to keep information in a persistent storage. All persistent data is stored in an Oracle 10 (10.2.0.3) relational database.

The administration of the application itself consists of:

1. Modification of the application deployment descriptors;

2. Security management;

3. CSI queue transfer configuration;

4. Translation management;

5. Loading reference data;

6. Configuration of schedule tasks;

7. Trace facility configuration;

8. JMS message queues facilities;

9. Adding new country;

10. Backup consideration.

3. ADMINISTRATION PREREQUISITES

Refer to chapter "Installation prerequisites" in [TARIC3-IPR] for details about the prerequisites for the administration of the application.

Please refer to the "WebLogic Server Administration Guide" for detailed information on the administration of the WLS environment. A number of administration aspects are independent from the application itself, and the associated decisions are up to the administrator of the system. These aspects are out of the scope of this document.

4. ADMINISTRATION

This chapter contains a detailed description of each administration procedure.

4.1. TARIC3 application and module deployment descriptors

The `s_taric3_<release_number>.ear` archive contains the business logic implementation and the presentation logic implementation for the TARIC3 application. It contains a number of J2EE modules which have to be deployed in the correct servers. The following table contains an enumeration of the J2EE modules present in the archive. For each of these modules it is indicated to which server they are assigned (targets).

J2EE module	Admin server	TARIC3 server
g_demco_ejb	No	Yes
g_demco_management	No	Yes
g_demco_batch_frontend_ejb	No	Yes
s_taric3_ejb	No	Yes
s_taric3_ui	No	Yes
s_taric3_ug_war	No	Yes
s_taric3_ob_ug_war	No	Yes
s_taric3_ib_ug_war	No	Yes
s_taric3_mu_ug_war	No	Yes
s_taric3_rep_ug_war	No	Yes
s_taric3_pub_ug_war	No	Yes

Table 1. Deployment of J2EE modules

The deployment descriptors of the different modules may be updated if necessary.

4.1.1. *Modification of a deployment descriptor*

To modify a deployment descriptor, please apply the following procedure.

1. Explode the enterprise application archives.

The following enterprise application archives must be deployed in the managed server that hosts the TARIC3 application.

s_taric3-<release_number>.ear

To be able to do this, <u>the administrative server must be running</u>. The deployment is done using an exploded distribution of the application archive. To generate that exploded distribution, execute the following command:

```
$ ./configure explode
```

A directory `s_taric3-<release_number>.ear` containing the exploded distribution will be created in the `<GROUP>/app/taric3/exploded` directory of the runtime environment.

Some values in the deployment descriptors are replaced during this operation by values taken in the `runtime.properties` file (see section "Application runtime environment" of [TARIC3-IPR]).

Note that the original (non-exploded) J2EE archive `s_taric3-<release_number>.ear` can be found in the `<GROUP>/app/taric3/j2ee_archives` directory.

2. Modify the deployment descriptors.

The deployment descriptors can be edited (with a text editor like VI) from the `exploded` directory.

For example the deployment descriptors for the g_demco_ejb module can be found in the directory `<GROUP>/app/taric3/exploded/s_taric3-<release_number>.ear/g_demco_ejb-x.x.jar/META-INF`.

3. Deploy the application.

The deployment of the application is done with the command:

```
$ ./configure server deploy
```

This command will deploy the application in the WLS `<APP_SERVER>`.

Another way is to do this from the WebLogic console interface.

Before doing a deployment, please delete or undeploy the current application (via WebLogic console interface).

4.1.2. g_demco_ejb

The default deployment descriptor **does require** adaptations for the correct functioning of the module <u>especially if the application must run in test mode</u>. The server needs to be restarted once changes are done.

This module implements a set of generic logic used by the TARIC3 application. This includes the TARIC3 integration with the CSI Bridge, the asynchronous message handling and the business logic controller among others.

The following environment entries for the *Configuration* bean have to be configured with the correct value:

ccnbridge-server-url: The URL of the Weblogic server in which the ccnbridge is deployed for the domain (e.g. *[Removed]*); if the CSI Bridge is running on the TARIC3 server, the operator may specify "local" for this environment entry. This parameter will be set to the value specified for the variable CCNBRIDGE_SERVER_URL in the `runtime.properties` file during the `./configure explode` step.

When necessary, the TARIC3 reports are executed in a new JVM that runs outside of the WLS. It is possible to configure the arguments passed to that JVM.

JVMArgs: represents the arguments passed to the JVM that creates the reports; in production the maximum heap and the stack size must be correctly configured (advice "*-noclassgc -Xmx2048m -XX:MaxPermSize=128m -Xss4m").*

The value of some environment entries of the *Configuration* bean may have to be changed. These are paths to a directory where temporary files will be stored and automatically removed by the system[1] when they will not be necessary anymore. ***Note that the default path for temporary files should be modified to avoid write conflicts between different environment/applications***:

FileSystemAsyncQueryTemp represents a path on a disk where asynchronous query temporary files will be stored (default is `<GROUP>/app/taric3/tmp/async-query-tmp`);

FileSystemLog represents a path on a disk where the messages will be dumped (if *DumpMessageOnReception* or *DumpAppMessageOnReception* is true) (default is `<GROUP>/app/taric3/tmp/message-dump`);

FileSystemBinaryTemp represents a path where binary files will be temporarily saved by the web application. In a clustered environment, this directory must be accessible from every server running the web application (default is `<GROUP>/app/taric3/tmp/web-tmp`);

FileSystemXEPTemp represents a path on a disk where XEP temporary files will be stored (default is `<GROUP>/app/taric3/tmp/xep-tmp`);

g.demco.batch.tmpdir represents a path on a disk where the batch temporary files will be stored (default is `<GROUP>/app/taric3/tmp/batch`);

Beware that the user running the instance of WLS must have sufficient access rights to read/write/delete files in the specified directories.

The message dump facility can be enabled/disabled at two levels by altering the value of the *DumpMessageOnReception* and *DumpAppMessageOnReception* environment entries to 'true' or 'false' for the *Configuration* bean.

If 'true', *DumpMessageOnReception* will dump the complete asynchronous input and output messages;

If 'true', *DumpAppMessageOnReception* will dump every business action received and sent by the controller coming from the *MessageHandler* or the Web interface;

4.1.3. g_demco_management

The default deployment descriptor does not require any adaptation for the correct functioning of the module.

This module is implementing the security management for the TARIC3 application.

---

[1] It is not required that the directories exist at installation time. The system will create them when needed.

4.1.4. g_demco_batch_frontend_ejb

The default deployment descriptor does not require any adaptation for the correct functioning of the module.

This module is implementing the presentation services for the batch and reporting tasks of the TARIC3 application.

4.1.5. s_taric3_ejb module

The default deployment descriptor does not require any adaptation for the correct functioning of the module.

This module is implementing the business for the TARIC3 applications and provides an access point for requests made from the swing client.

4.1.6. s_taric3_ui module

The default deployment descriptor does not require any adaptation for the correct functioning of the module.

This module is implementing the presentation logic for the TARIC3 applications.

4.1.7. s_taric3_ug_war module

The default deployment descriptor does not require any adaptation for the correct functioning of the module.

This module is implementing the user guide for the TARIC3 CDCO application.

4.1.8. s_taric3_ob_ug_war module

The default deployment descriptor does not require any adaptation for the correct functioning of the module.

This module is implementing the user guide for the TARIC3 Output Bridge.

4.1.9. s_taric3_ib_ug_war module

The default deployment descriptor does not require any adaptation for the correct functioning of the module.

This module is implementing the user guide for the TARIC3 Input Bridge.

4.1.10. s_taric3_mu_ug_war module

The default deployment descriptor does not require any adaptation for the correct functioning of the module.

This module is implementing the user guide for the TARIC3 Mass updates.

4.1.11. s_taric3_rep_ug_war module

The default deployment descriptor does not require any adaptation for the correct functioning of the module.

This module is implementing the user guide for the TARIC3 Reports.

4.1.12. s_taric3_pub_ug_war module

The default deployment descriptor does not require any adaptation for the correct functioning of the module.

This module is implementing the user guide for the TARIC3 Publication.

4.2. Security management

4.2.1. Configuration of the security using the User Management module

With User Management module, it is possible to automatically create the security environment of the application. This is done using some pre-configured files containing all the security information required to run the application. The User Management Web Interface application may also be used to manage WebLogic users and groups. See the User Management application documentation for detailed information (see [UM-USG]).

The User Management application must be properly configured, deployed and running to execute the following step.

To create the security environment, go in the directory `<GROUP>/app/taric3/bin` and execute the following command:

```
$ ./loadsecurity <User> <Password>
```

Where `<User>` and `<Password>` define an existing WebLogic user member of the groups TAXUD, security-manager, security-all (see [UM-INS-001]).

This command will create all WebLogic groups, users and associations required for the TARIC3 application.

4.2.2. WLS user management

The provided deployment descriptors assume that the following WLS groups exist in the domain:

Group	Purpose
taric3-consultation	All members of this group can consult TARIC3 data.
taric3-management	All members of this group can manage TARIC3 data.
taric3-batch	All members of this group can create TARIC3 reports.

Table 2. WebLogic security groups

Using these group assignments it is possible to give a user the correct role by a limited number of group assignments.

4.2.3. Asynchronous processing

To support the asynchronous processing of messages, some surrogate2 groups and users are automatically created.

The following group is created:

wls.user.async: Every surrogate user created to perform asynchronous queries is member of this group. The purpose of the group is to mark these users.

4.2.4. CCN user mapping

The following WLS groups representing CCN profiles have to be created. Note that the <mode> must be replaced by the name of the CCN mode written in lowercase. For production mode, <mode> is empty and the first dash is removed. For other mode, please use the corresponding infix for the appropriate environment:

Group	Purpose
ccn.taric3-management-*<mode>*-prf.taric3	Represents the CCN users that can manage TARIC3 data.

Table 3. CCN profiles' groups

The following group memberships are needed for the correct functioning:

Group	Member
taric3-management	ccn.taric3-management-*<mode>*-prf.taric3
TAXUD	*[Removed]*
taric3-management	*[Removed]*

Table 4. CCN groups mapping

In order to be able to perform the data dependent verifications and therefore only allow an administration to manage its own information, the CCN group representing the CCN site has to be assigned to the correct WLS country group. Please contact the CCN/TC to get the correct site ID's for all administrations.

The following table gives three examples:

Group	Member
Country-BE	ccn.site.cust.be (exact name known by CCN/TC)
Country-FR	ccn.site.cust.fr (exact name known by CCN/TC)
Country-XY	ccn.site.cust.xy (exact name known by CCN/TC)

Table 5. Country groups mapping

Note that for testing purposes, the DG TAXUD site must be assigned to a particular country. The CCN group representing the Commission's CCN site is *[Removed]*.

---

2 Created by the system whenever required. Group assignments will be kept in sync with the real user by the system.

4.2.5. *TARIC3 batch user*

The TARIC3 batch jobs need to run under the specific WLS user *[Removed]*. This user must be created (if not done yet) and assigned to the following groups:

User	Member of group
[Removed]	taric3-batch

Table 6. TARIC3 batch user

4.2.6. *Input bridge system user*

The Input Bridge requires the existence of the user '*[Removed]*'.

This user must be created (if not done yet) and assigned to the following groups:

User	Member of group
[Removed]	taric3-consultation, taric3-management

Table 7. Input Bridge system user

4.3. Translation management

4.3.1. *Batch mode*

This mode uses data files to load a batch of translations. Certain commands (located in the TARIC3 application bin directory) are used to configure these components. The administrator should execute these commands from within that directory. The TARIC3 hosting server must be running for this. The administrator must load the definition of the translation items once by executing the following command:

```
$ ./loaddictionary
```

Each time an administrator wants to load or alter the translations for a particular module and a particular language this command can be used. The available arguments are:

module: the module name (TARIC3);

language: ISO code of the language (lowercase);

translationFile: The file containing the translations.

The following commands load all the available translations for the given language:

```
$ ./loadtranslation TARIC3 xx \
        ../data/translations/TARIC3_XX.properties
```

As an example, the following command will load the English translations of TARIC3.

```
$ ./loadtranslation TARIC3 en /tmp/TARIC3_EN.properties
```

They must be executed for the following pairs of attributes (note that the translation files must be present, if some files are not present, skip the processing for the given language):

Value of xx	Value of XX

Value of xx	Value of XX
bg	BG
cs	CS
da	DA
de	DE
el	EL
en	EN
es	ES
et	ET
fi	FI
fr	FR
hu	HU
it	IT
lt	LT
lv	LV
mt	MT
nl	NL
pl	PL
pt	PT
ro	RO
sk	SK
sl	SL
sv	SV

Table 8. Loading of translations

Loading of the translations used by the reports is performed in a similar way:

```
$ ./loadtranslation TARIC3 xx \
        ../data/translations/TARIC3_report_XX.properties
```

The following command unloads the available translations to the specified file for a given module and a given language (note that this command produces a file in which the translation resources are not sorted as in the original files provided by the development/help desk/TAXUD teams):

```
$ ./unloadtranslation <module> <language_code> \
        <output_file>
```

As an example, the following command will unload the English translations of the TARIC3 module to the /tmp/TARIC3_EN.properties file:

```
$ ./unloadtranslation TARIC3 en
/tmp/TARIC3_EN.properties
```

4.4. Configuration of scheduled tasks

4.4.1. Overview of scheduled tasks

Some tasks should be scheduled in the TARIC3 application on a regular and automatic basis. This concerns:

The cleaning of successful task results.

The scheduling of the above tasks can be handled by the batch environment and more specifically performed by dedicated job generators.

Ensure that the security environment of the TARIC3 application (see section 4.2) is configured before going to the next sections.

4.4.2. Security consideration

The TARIC3 tasks described in this chapter need to be run under a WebLogic user assigned to the following groups:

User	Member of group
[Removed]	– TAXUD

Table 9. Security considerations for the scheduled tasks

4.4.3. Cleaning of successful tasks

A task generator must be configured to clean-up the results of the tasks that have been successfully executed at regular intervals. It is proposed to clean-up at least the successful "Index Rebuild" tasks and the "Cleaning Tasks" themselves. Note that the clean-up of any other executed job can be configured.

To do this:

In the user interface, select "Task management" and then "New Task Generator."

The following properties must be configured (the proposed values may be modified):

Properties	Values
Task Generator Name	Cleaning Task
Schedule Descriptor	It is advised to run the cleaning task each day: 45 21 * * *
Exclusion Period	No exclusion period.

Table 10. Cleaning scheduled task

4.5. Trace facility configuration

The *g_demco_ejb* module contains a facility to dump all incoming and outgoing XML messages into the file system. A WebLogic log entry is written containing a reference to the applicable files.

In order to control the message tracing facility, the operator can enable/disable the message dump facility at two levels by altering the value environment entries of the *Configuration* bean. Setting *DumpMessageOnReception* environment entry to 'true' will dump the complete asynchronous input and output messages. Setting *DumpAppMessageOnReception* environment entry to 'true' will dump every business action received and sent by the business logic controller (in relation to the system-to-system interface or the web interface).

See section 4.1.2 to know the configured location where the trace files are generated.

4.6. JMS message queue facilities

There is a set of utilities to put messages on the input queue and to retrieve messages from the output and error queue.

4.6.1. Put a message on the TARIC3 input queue

An operator can put a message on the input queue using the following command:

```
$ ./taric3/bin/sendmessage –user <wls-user-name>
  -password <password> -fileToSend <filename>
```

Where the meaning of the parameters is the following:

<wls-user-name>: The user used to put the message on the queue. The message will be processed using this identity;

<password>: The password for the given user;

<filename>: The file containing the message to send.

Note that the envelope ID entry in the message must be unique for each message.

4.6.2. Get all output messages

An operator can consume all messages available on the output queue using the following command:

```
$ ./taric3/bin/consumemessages –user <wls-user-name>
  -password <password>
```

Where the meaning of the parameters is the following:

<wls-user-name>: The user used to get the messages from the queue;

<password>: The password for the given user.

4.6.3. Get all critical error messages

An operator can consume all messages available on the output queue using the following command:

```
$ ./taric3/bin/consumeerrors –user <wls-user-name>
  -password <password>
```

Where the meaning of the parameters is the following:

<wls-user-name>: The user used to get the messages from the queue;

<password>: The password for the given user.

4.7. Addition of a new country

The addition of a new country can be performed as follow:

Update the deployment descriptor ejb-jar.xml of the g_demco_management module, environment entry "validIsoCodes", add the country code.

Update the deployment descriptor ejb-jar.xml of the g_demco_management module, add a security-role-ref element with the new country-code as in the example here under (for Austria).

```
<security-role-ref>

  <description>Austria</description>

  <role-name>AT</role-name>

  <role-link>AT</role-link>

</security-role-ref>
```

Update the deployment descriptor ejb-jar.xml of the g_demco_management module; add a security-role element with the new country-code as in the example here under (for Austria).

```
<security-role>

  <description>Austria</description>

  <role-name>AT</role-name>

</security-role>
```

Update the deployment descriptor weblogic-ejb-jar.xml of the g_demco_management module; add a security-role-assignment element with the new country-code as in the example here under (for Austria).

```
<security-role-assignment>

  <role-name>AT</role-name>

  <principal-name>Country-AT</principal-name>

</security-role-assignment>
```

Update the deployment descriptor ejb-jar.xml of the g_demco_ejb module, environment entry "Organisations", add the new organisation to the list.

Update the deployment descriptor ejb-jar.xml of the g_demco_ejb module, add a security-role-ref element with the new country-code as in the example here under (for Austria).

```
<security-role-ref>
```

```
<description>Austria</description>

<role-name>AT</role-name>

<role-link>AT</role-link>

</security-role-ref>
```

Update the deployment descriptor ejb-jar.xml of the g_demco_ejb module; add a security-role element with the new country-code as in the example here under (for Austria).

```
<security-role>

<description>Austria</description>

<role-name>AT</role-name>

</security-role>
```

Update the deployment descriptor weblogic-ejb-jar.xml of the g_demco_ejb module; add a security-role-assignment element with the new country-code as in the example here under (for Austria).

```
<security-role-assignment>

<role-name>AT</role-name>

<principal-name>Country-AT</principal-name>

</security-role-assignment>
```

Create a WebLogic group (via the WebLogic console) for the new country as in the example Country-AT (for Austria).

The operator may have to update the User Management application to be able to create a user being member of that new country.

Update the deployment descriptor ejb-jar.xml of the g_demco_management module, environment entry "validIsoCodes", add the country code.

Update the deployment descriptor ejb-jar.xml of the g_demco_management module; add a security-role-ref element with the new country-code as in the example here under (for Austria).

```
<security-role-ref>

<description>Austria</description>
```

```
    <role-name>AT</role-name>

    <role-link>AT</role-link>

   </security-role-ref>
```

Update the deployment descriptor ejb-jar.xml of the g_demco_management module; add a security-role element with the new country-code as in the example here under (for Austria).

```
  <security-role>

   <description>Austria</description>

   <role-name>AT</role-name>

  </security-role>
```

Update the deployment descriptor weblogic-ejb-jar.xml of the g_demco_management module; add a security-role-assignment element with the new country-code as in the example here under (for Austria).

```
<security-role-assignment>

<role-name>AT</role-name>

<principal-name>Country-AT</principal-name>

</security-role-assignment>
```

The check on the countries is done via TARIC. The country must be a member of the country group 1010 in the TARIC application.

4.8. Backup considerations

All persistent data information related to the TARIC3 application are stored in the database schema. So, a backup of the TARIC3 database schema has to be done on a daily basis.