

Java TD Installation  
Oracle FLEXCUBE Universal Banking  
Release 14.7.2.0.0  
Part No. F87755-01  
[November] [2023]



---

# Table of Contents

<b>1. JAVA TD INSTALLATION .....</b>	<b>1-1</b>
1.1 INTRODUCTION.....	1-1
1.2 PREREQUISITES .....	1-1
1.3 SERVER SETUP.....	1-1
1.4 WAR DEPLOYMENT AFTER BUILD .....	1-3
1.5 ORDER OF SERVER START .....	1-4
<b>2. TD MAINTENANCE IN FCUBS .....</b>	<b>2-1</b>
2.1 REQUIRED MAINTENANCE FOR JAVA TD.....	2-1
2.2 SCHEDULER JOB FOR TRIGGERING TD EOD IN FCUBS .....	2-3
<b>3. SSL SETUP WITH SELF SIGNED CERTIFICATE.....</b>	<b>3-1</b>
<b>4. TD END OF DAY BATCHES .....</b>	<b>4-1</b>

---

---

# 1. Java TD Installation

## 1.1 Introduction

This document lists steps to configure Application Server for JAVA TD Integration with FCUBS.

## 1.2 Prerequisites

Java TD installation requires a Weblogic domain.

Note: In the following sections, 10.10.10.10 IP address and 1010 port are used as an example. Please use valid IP and Port of corresponding server.

Java IC Installation is mandatory for TD.

## 1.3 Server Setup

Java TD Setup includes two sets of services:

1. **INFRA Services:** There are two services under this category.
  - a. **Discovery Service:** This service is required for Java TD Services Registration. On start-up all Java TD services will be registered with Discovery Service. The registered services can make inter service calls by making use of Discovery Service.

**Service Name: plato-discovery-services-6.0.0.war**
  - b. **Config Service:** All the configuration related details will be stored in a database table (table name: PROPERTIES). Config service provides the required configuration details for the corresponding Java TD Services during service start up.

**Service Name: plato-config-services-6.0.0.war**

**Note:** INFRA services are common for IC and TD. If already deployed for IC, deployment shouldn't be done for TD again. Further in the document, INFRA services related setup and deployment can be skipped if already done for IC.

2. **Java TD Services:** These Services are Java TD Functional Services. E.g.: Maturity Service, Deposit service, Maturity Calc Service etc.

INFRA services and Java TD Services must be deployed on two separate Managed Servers (Any name can be given to Managed Servers).

1. **ConfigServer:** In this managed server, INFRA Services should be deployed (plato-discovery-services-5.0.0.war and plato-config-services-5.0.0.war).
2. **JavaTDServer:** In this managed server, all the Java TD services should be deployed.
3. **JavalCServer:** In this managed server, all the Java IC services should be deployed.

For More Details on Installing IC Services, please refer Java IC Installation Document.

Following Data Sources have to be created for INFRA and Java TD Services:

Data Source JNDI Name	Type	Targets
<b>jdbc/OBIC</b>	Non-XA Datasource	JavalCServer
<b>jdbc/PLATO</b>	Non-XA Datasource	JavaTDServer, ConfigServer
<b>jdbc/PLATOBATCH</b>	Non-XA Datasource	JavaTDServer
<b>jdbc/FCUBS</b>	Non-XA Datasource	JavaTDServer

Below line must be included in setDomainEnv.cmd or setDomainEnv.sh of the Weblogic domain:

**For Linux Server:**

```
JAVA_OPTIONS="${JAVA_OPTIONS} ${JAVA_PROPERTIES} -Dflyway.enabled=false -  
Dspring.flyway.enabled=false -Dplato.services.config.uri=http://<config-server-ip>:<config-  
server-port> -Dplato.service.logging.path=<Debug Path where Logs are to be written>" -  
Dserver.id=<server id>
```

```
export JAVA_OPTIONS
```

E.g.:

```
JAVA_OPTIONS="${JAVA_OPTIONS} ${JAVA_PROPERTIES} -Dflyway.enabled=false -  
Dspring.flyway.enabled=false -Dplato.services.config.uri=http://10.10.10.10:1010 -  
Dplato.service.logging.path=/mnt/FC144/TDLogs" -Dserver.id=1
```

```
export JAVA_OPTIONS
```

**For Windows Server:**

```
set JAVA_OPTIONS=%JAVA_OPTIONS% %JAVA_PROPERTIES% -  
Dplato.services.config.uri=http://<config-server-ip> :<config-server-port> -Dflyway.enabled=false -  
Dspring.flyway.enabled=false -Dplato.service.logging.path=<Debug Path where Logs are to be  
written> -Dserver.id=<server id>
```

E.g.:

```
set JAVA_OPTIONS=%JAVA_OPTIONS% %JAVA_PROPERTIES% -Dflyway.enabled=false -  
Dspring.flyway.enabled=false -Dplato.services.config.uri=http://whf00bir:9005 -  
Dplato.service.logging.path=D:/TDLogs -Dserver.id=1
```

server id parameter should be a number used to uniquely identify an application instance. If only one deployment of a service is present then this value has to be set to 1. In case of multiple deployment, number from 1 to the number of instances can be assigned to the server where deployment is done.

Alternatively, if the parameters are to be set specific to a Managed Server where Services are deployed, then these properties can be set in Servers->Managed Server->Server Start in the argument section. Note: It will be useful only if Node-Manager is used to start managed servers.

<b>BEA Home:</b>	<input type="text"/>	The BEA home directory (path on the machine running Node Manager) to use when starting this server. <a href="#">More Info...</a>
<b>Root Directory:</b>	<input type="text"/>	The directory that this server uses as its root directory. This directory must be on the computer that hosts Node Manager. If you do not specify a Root Directory value, the domain directory is used by default. <a href="#">More Info...</a>
<b>Class Path:</b>	<input type="text"/>	The classpath (path on the machine running Node Manager) to use when starting this server. <a href="#">More Info...</a>
<b>Arguments:</b>	<pre>-Dflyway.enabled=false -Dspring.flyway.enabled=false - Dplato.services.config.uri=http://10.10.10.10:1010 - Dplato.service.logging.path=D:/ICLogs -Dserver.id=1</pre>	The arguments to use when starting this server. <a href="#">More Info...</a>
<b>Security Policy File:</b>	<input type="text"/>	The security policy file (directory and filename on the machine running Node Manager) to use when starting this server. <a href="#">More Info...</a>
<b>User Name:</b>	<input type="text"/>	The user name to use when booting this server. <a href="#">More Info...</a>
<b>Password:</b>	<input type="password"/>	The password of the username used to boot the server and perform server health monitoring. <a href="#">More Info...</a>
<b>Confirm Password:</b>	<input type="password"/>	
<input type="button" value="Save"/>		

## 1.4 WAR Deployment after Build

As part of FCUBS EAR build, in addition to FCUBS EAR, Java TD wars and Java TD INFRA wars will get copied into the destination location.

Below are the locations where the wars will be copied after build:

- FCUBS Application EAR and All Adapter EARs:** Available in the destination folder.
- INFRA Service WARs:** plato-discovery-services-6.0.0.war and plato-config-services-6.0.0.war will be available in the destination folder.  
Deploy all the INFRA Service WARs in **ConfigServer**.
- Java TD Service WARs:** All the Java TD Service WARs will be copied in "TD" folder under the destination folder.  
Deploy all the Java TD Service WARs in **JavaTDServer**.

4. **Java IC Service WARs:** All the Java IC Service WARs will be copied in “IC” folder under the destination folder.

Deploy all the Java IC Service WARs are in **JavaICServer**

## 1.5 **Order of Server Start**

After deployment or server restart, services have to be started in following sequence:

- a. plato-config-service
- b. plato-discovery-service
- c. Java IC Services
- d. Java TD Services

When servers are restarted, ensure to start **ConfigServer** first and then then **JavaTDServer**.

On every restart of **ConfigServer**, plato-discovery-service must be stopped and started. This is required as Discovery requires properties entries for self-registration to be picked from plato-config-service.

In order to check if all the services have started, below discovery URL can be checked:

<http://<config-server-ip>:<config-server-port>/plato-discovery-service>

E.g.:

<http://10.10.10.10:1010/plato-discovery-service>

All the deployed Java TD Services should get listed in the service discovery URL.

## 2. TD Maintenance in FCUBS

### 2.1 Required Maintenance for Java TD

Below maintenances are required in FCUBS

#### 1. Properties Maintenance (CSDPROPM):

- a. Launch the screen and query for entry present in LOV for Reference Number:

- b. Unlock the screen, Select All for “Update Service Details” and update the Service URL and Service Port as below:

Key	Value
plato.services.eureka.uri eureka.client.serviceUrl.defaultZone	<a href="http://&lt;discovery-service-ip&gt;:&lt;discovery-port&gt;/plato-discovery-service/eureka">http://&lt;discovery-service-ip&gt;:&lt;discovery-port&gt;/plato-discovery-service/eureka</a>
server.port and plato.services.entityservices.port	Managed Server port where the service is deployed

#### Note:

- a. Above properties are to be updated for all INFRA and Java TD Services.
  - b. If SSL setup is required for calls through discovery, below properties are to be updated: (This step is not mandatory)
    - i. server.port: Update to SSL Port of the managed server where service is deployed.
    - ii. plato.services.entityservices.port: Update to SSL Port of the managed server where service is deployed.
    - iii. isSslEnabled: Value has to be set to true.
    - iv. apiProtocol: Value has to be changed to https.
  - c. If step b has been followed for SSL Setup and if services are deployed on different servers, please follow section 3 (SSL Setup with Self Signed Certificate, Scenario2) for ssl handshake between obic-interest-batch-service managed server and other services managed server.
2. External Service Maintenance (IFDEXSER):

Prior to this step, user must maintain external system “FCJAVA” in CODSORCE screen.

User has to query for External System “FCJAVA” in IFDEXSER and following details have to be modified:

- a. Rest Service IP: The server IP where **fcubs-co-batch-services.war** has been deployed.
- b. Rest Service Port: The Managed Server port where **fcubs-co-batch-services.war** has been deployed.

If SSL is enabled in FCUBS properties file,

- c. Update Rest Service Port to SSL port of the managed server where **fcubs-co-batch-services.war** has been deployed.
- d. SSL configuration has to be done as per steps mentioned in section 3 (SSL Setup with Self Signed Certificate, Scenario1).
- e. External User: User ID of the Flexcube user FCUBSUSER is used for invoking the Java TD Services.

The screenshot shows the 'External Service Maintenance' form. It includes fields for External System, External System Type (set to Default), External System AppID, External User, Read Time Out (In Seconds), Connection Time Out (In Seconds), Retry Count, Archival Days, and a Rest Service Secured toggle switch. Below the form is a table with columns: Type, Service Name, WS Endpoint URL, Rest Service Context, Rest Service IP, Rest Service Port, and Rest Service Pattern. The table is currently empty, displaying 'No data to display.' Buttons for Audit, Exit, and Save are located at the bottom right.

### 3. IC Param Maintenance (ICDPARAM):

Launch the screen and unlock and modify the parameters.

The screenshot shows the 'Interest Charges Parameters' form. It features an 'Unlock' button at the top left. Below is a table with columns 'Parameter' and 'Param Value'. The table contains three rows: ADAPTER\_CALL\_TYPE with value 5, DB\_ACNTG\_COMMIT\_FREQ with value 510, and DB\_ACNTG\_FETCH\_SIZE with value 2000. A 'Change Log' button is at the bottom left, and 'Audit' and 'Exit' buttons are at the bottom right. The page indicator shows 'Page 1 of 1 (1-13 of 13 items)'.

Parameter	Param Value
ADAPTER_CALL_TYPE	5
DB_ACNTG_COMMIT_FREQ	510
DB_ACNTG_FETCH_SIZE	2000



Below are the parameters which can be configured as per requirement:

PARAM_NAME	PARAM_VAL	Description
JAVA_BATCH_SLEEP_TIME	5	Sleep time in seconds to verify the status of Java TD service submitted
SKIP_OBTD_ACNTG_ERR	0	<b>O</b> -Mark the accounting failures and complete the EOC batch, <b>E</b> - Fails the EOC batch when getting any accounting failures.
TD_JOB_SLEEP_TIMER	30	Sleep time to check the status of TD parallel streams - Conventional TD
JAVA_RETRY_COUNT	150	Maximum retry count to fail the EOC batch when the submitted java service is not picked up by scheduler
LOG_PATH	/tmp/OBTDLog	Log Path where the TD Service-related logs are to be written.
RESOLVE_MAX_TRY_WITHOUT_FAIL	5	Maximum retry to obtain account lock for resolution
TD_MULTI_DEST_AHOF	N	If Accounting Handoff is required for Multiple Source Systems, this flag must be marked Y. If N, it will be posted to single source.

4. PLATO\_LOGGER\_PARAM\_CONFIG has to be updated with the log path for IC logs corresponding to LOG\_PATH param value.
5. After the above maintenances, restart FCUBS Application and all the servers in the order mentioned in the section [1.5 Order of Server Start](#).

## 2.2 Scheduler Job for Triggering TD EOD in FCUBS

A new Scheduler Job “FCEODJ\_BATCH” has been introduced in order to trigger TD EOD in Flexcube. After the above maintenances are done, resume FCEODJ\_BATCH Job from SMSJOBRR screen before triggering FCUBS EOD:

The screenshot shows the 'Job Details' screen in the SMSJOBRR application. At the top, there are options for 'Search', 'Advanced Search', and 'Reset'. A 'Records per page' dropdown is set to 15. Below this is a search filter section titled 'Search (Case Sensitive)' with input fields for Job Name, Job Group, State, Next Fire Time, and Scheduler. The search results section shows a table with columns for Job Name, Job Group, State, Next Fire Time, Scheduler, and Error. The table is currently empty, with the message 'No data to display.' at the bottom. At the very bottom of the screen, there are 'Pause' and 'Resume' buttons.

**Note:**

1. FCEODJ\_BATCH Job Scheduler interval is set by default as 5 seconds and shouldn't be maintained lesser than 5 seconds.
2. FCEODJ\_BATCH Job has been released with start-up mode as Manual. Hence after every deployment of FCUBS application or restart of server, the job needs to be manually scheduled.
3. Before triggering UBS EOD job kindly ensure that FCEODJ\_BATCH Job is running.

---

### 3. SSL Setup with Self Signed Certificate

Please follow this section for below configurations:

**Scenario1:** If SSL is enabled for FCUBS Application, the call to fcubs-co-batch-services will be in SSL mode. This requires SSL Configuration to be done in both the FCUBS Server and the OBIC Server.

**Scenario2:** If SSL is to be enabled for calls through discovery service and services are deployed on different managed server. SSL handshake would be required between obic-interest-batch-service managed server and other services managed server.

SSL Configuration can be done with Self Signed Certificate in non-production environment only. Since SSL Handshake would be required between the two servers, below steps can be followed in order to setup self signed SSL Setup:

1. Run the below command to create keystore for each of the servers.  
To create keystore for FCUBS and OBIC server, below command has to be run. This will create keystore in the specified path:

```
keytool -genkey -keystore /path/to/keystore/server1.jks -alias  
<server1_cert_alias> -dname "CN=<server1_server_host>,OU=<organization>" -  
keyalg "RSA" -sigalg "SHA256withRSA" -keysize 2048 -validity <noOfDays>
```

```
keytool -genkey -keystore /path/to/keystore/server2.jks -alias  
<server2_cert_alias> -dname "CN=<server2_server_host>,OU=<organization>" -  
keyalg "RSA" -sigalg "SHA256withRSA" -keysize 2048 -validity <noOfDays>
```

In the above commands server1 and server2 has been used to indicate two servers involved in handshake.

For Scenario1, server1 is the server where scheduler application is deployed and server2 is the server where obic-interest-batch-services is deployed.

For Scenario2, server1 is the server where obic-interest-batch-services is deployed and server2 is each of the managed server where IC services are deployed. If SSL Configuration is already done for obic-interest-batch-services server, then Keystore need not be created again and only step involving certificate import to trust needs to be done.

<server1\_cert\_alias> Any alias name can be provided here. Alias name shouldn't be repeated.

<server2\_cert\_alias> Any alias name can be provided here. Alias name shouldn't be repeated.

<organization> has to be replaced with the organization code.

<noOfDays> has to be replaced with validity days of the certificate.

<server1\_server\_host> ip of the server1 can be mentioned here.

<server2\_server\_host> ip of the server2 can be mentioned here.

User will be prompted to enter password while running the above command. The same passphrase has to be entered in the further steps.

2. Configuring SSL in Weblogic server. This step has to be repeated for both the servers. Check "SSL Listen Port Enabled" Flag and enter SSL Listen Port

<b>Name:</b>	OBICServer	An alphanumeric name for this server instance. <a href="#">More Info...</a>
<b>Template:</b>	(No value specified) <a href="#">Change</a>	The template used to configure this server. <a href="#">More Info...</a>
<b>Machine:</b>	Machine-0	The WebLogic Server host computer (machine) on which this server is meant to run. <a href="#">More Info...</a>
<b>Cluster:</b>	(Stand-Alone)	The cluster, or group of WebLogic Server instances, to which this server belongs. <a href="#">More Info...</a>
<b>Listen Address:</b>		The IP address or DNS name this server uses to listen for incoming connections. For example, enter 12.34.5.67 or mymachine, respectively. <a href="#">More Info...</a>
<input checked="" type="checkbox"/> <b>Listen Port Enabled</b>		Specifies whether this server can be reached through the default plain-text (non-SSL) listen port. <a href="#">More Info...</a>
<b>Listen Port:</b>	8030	The default TCP port that this server uses to listen for regular (non-SSL) incoming connections. <a href="#">More Info...</a>
<input checked="" type="checkbox"/> <b>SSL Listen Port Enabled</b>		Indicates whether the server can be reached through the default SSL listen port. <a href="#">More Info...</a>
<b>SSL Listen Port:</b>	8031	The TCP/IP port at which this server listens for SSL connection requests. <a href="#">More Info...</a>
<input type="checkbox"/> <b>Client Cert Proxy Enabled</b>		Specifies whether the HttpClusterServlet proxies the client certificate in a special header. <a href="#">More Info...</a>
<b>Java Compiler:</b>	javac	The Java compiler to use for all applications hosted on this server that need to compile Java code. <a href="#">More Info...</a>
<b>Diagnostic Volume:</b>	Low	Specifies the volume of diagnostic data that is automatically produced by WebLogic Server at run time. Note that the WLDLF diagnostic volume setting does not affect explicitly configured diagnostic modules. For example, this controls the volume of events generated for Flight Recorder. <a href="#">More Info...</a>
<b>Default Datasource:</b>		The JNDI name of a system resource data source used to override the default datasource. <a href="#">More Info...</a>
<a href="#">Advanced</a>		
<a href="#">Save</a>		

Switch to Keystores tab and follow below steps:

- a. Change Keystores option to "Custom Identity and Java Standard Trust"
- b. For Custom Identity Keystore, enter the keystore file path.
- c. For Custom Identity Keystore Type, enter JKS.
- d. For Custom Identity Keystore Passphrase and Confirm Custom Identity Keystore Passphrase, enter the passphrase entered when creating keystore.
- e. For Java Standard Trust Keystore Passphrase and Confirm Java Standard Trust Keystore Passphrase, enter passphrase as "changeit".

[Save](#)

Keystores ensure the secure storage and management of private keys and trusted certificate authorities (CAs). This page lets you view and define various keystore configurations. These settings help you to manage the security of message transmissions.

**Keystores:** Custom Identity and Java Standard Trust [Change](#) Which configuration rules should be used for finding the server's identity and trust keystores? [More Info...](#)

— Identity —

**Custom Identity Keystore:**  The source of the identity keystore. For a JKS keystore, the source is the path and file name. For an Oracle Key Store Service (KSS) keystore, the source is the KSS URI. [More Info...](#)

**Custom Identity Keystore Type:**  The type of the keystore. Generally, this is JKS. If using the Oracle Key Store Service, this would beKSS [More Info...](#)

**Custom Identity Keystore Passphrase:**  The encrypted custom identity keystore's passphrase. If empty or null, then the keystore will be opened without a passphrase. [More Info...](#)

**Confirm Custom Identity Keystore Passphrase:**

— Trust —

**Java Standard Trust Keystore:**  The location of the java standard trust keystore. [More Info...](#)

**Java Standard Trust Keystore Type:**  The type of the java standard trust keystore. Generally, this is JKS. [More Info...](#)

**Java Standard Trust Keystore Passphrase:**  The password for the Java Standard Trust keystore. This password is defined when the keystore is created. [More Info...](#)

**Confirm Java Standard Trust Keystore Passphrase:**

[Save](#)

3. In SSL tab, do the below changes:
  - a. Enter Private Key Alias as entered while creating keystore.
  - b. For Private Key Passphrase and Confirm Private Key Passphrase, enter the passphrase entered when creating keystore.

**Configuration** Protocols Logging Debug Monitoring Control Deployments Services Security Notes

General Cluster Services Keystores **SSL** Federation Services Deployment Migration Tuning Overload Concurrency Health Monitoring Server Start Web Services Coherence

[Save](#)

This page lets you view and define various Secure Sockets Layer (SSL) settings for this server instance. These settings help you to manage the security of message transmissions.

**Identity and Trust Locations:** Keystores [Change](#) Indicates where SSL should find the server's identity (certificate and private key) as well as the server's trust (trusted CAs). [More Info...](#)

— Identity —

**Private Key Location:** from Custom Identity Keystore The keystore attribute that defines the location of the private key file. [More Info...](#)

**Private Key Alias:**  The keystore attribute that defines the string alias used to store and retrieve the server's private key. [More Info...](#)

**Private Key Passphrase:**  The keystore attribute that defines the passphrase used to retrieve the server's private key. [More Info...](#)

**Confirm Private Key Passphrase:**

**Certificate Location:** from Custom Identity Keystore The keystore attribute that defines the location of the trusted certificate. [More Info...](#)

— Trust —

**Trusted Certificate Authorities:** from Java Standard Trust Keystore The keystore attribute that defines the location of the certificate authorities. [More Info...](#)

— Advanced —

[Save](#)

Click "Advanced" block in the SSL Tab and set Hostname Verification to "None"

Advanced		Info...
<b>Hostname Verification:</b>	<input type="text" value="None"/>	Specifies whether to ignore the installed implementation of theweblogic.security.SSL.HostnameVerifier interface (when this server is acting as a client to another application server). <a href="#">More Info...</a>
<b>Custom Hostname Verifier:</b>	<input type="text"/>	The name of the class that implements theweblogic.security.SSL.HostnameVerifier interface. <a href="#">More Info...</a>
<b>Export Key Lifespan:</b>	<input type="text" value="500"/>	Indicates the number of times WebLogic Server can use an exportable key between a domestic server and an exportable client before generating a new key. The more secure you want WebLogic Server to be, the fewer times the key should be used before generating a new key. <a href="#">More Info...</a>
<input type="checkbox"/> <b>Use Server Certs</b>		Sets whether the client should use the server certificates/key as the client identity when initiating an outbound connection over https. <a href="#">More Info...</a>
<b>Two Way Client Cert Behavior:</b>	<input type="text" value="Client Certs Not Requested"/>	The form of SSL that should be used. <a href="#">More Info...</a>
<b>Cert Authenticator:</b>	<input type="text"/>	The name of the Java class that implements theweblogic.security.acl.CertAuthenticator class, which is deprecated in this release of WebLogic Server. This field is for Compatibility security only, and is only used when the Realm Adapter Authentication provider is configured. <a href="#">More Info...</a>

- Run below command for each of the servers to extract certificate from the corresponding keystores:

```
keytool -export -v -alias <server1_cert_alias> -file
/path/to/cert/server1.cer -keystore /path/to/keystore/server1.jks
```

```
keytool -export -v -alias <server2_cert_alias> -file
/path/to/cert/server2.cer -keystore /path/to/keystore/server2.jks
```

<server1\_cert\_alias> Any alias name can be provided here. Alias name shouldn't be repeated.

<server2\_cert\_alias> Any alias name can be provided here. Alias name shouldn't be repeated.

- Since SSL Handshake will be done between server1 and server2, the extracted certificate from the keystore of both the servers are to be imported into Trust Store of the corresponding servers. In step 2, since Java Standard Trust has been selected as the Trust store, corresponding certificates are to be imported into Java Standard Trust of the server. server1 Certificate has to be imported into server2 Java Standard Trust and server2 certificate has to be imported into server1 Java Standard Trust in order for the SSL Handshake to be successful.

Below command has to be run to import the certificate in to Java Standard Trust store "cacerts" file in the path mentioned in the "Java Standard Trust Keystore" path taken by weblogic in Step 2 for both the servers.

```
keytool -import -v -trustcacerts -alias <server1_cert_alias> -file
/path/to/cert/server1.cer -keystore /path/to/jdk/jre/lib/security/cacerts
```

```
keytool -import -v -trustcacerts -alias <obic_cert_alias> -file
/path/to/cert/obic.cer -keystore /path/to/jdk/jre/lib/security/cacerts
```

<server1\_cert\_alias> Any alias name can be provided here. As a practice, we can set hostname of the server1 server.

<server2\_cert\_alias> Any alias name can be provided here. As a practice, we can set hostname of the server2 server.

For Java Standard Trust Keystore, default password will be "changeit"

## 4. TD End of Day Batches

Following batches must be maintained for TD processing.

For End OF Transaction Input stage following batches must be maintained in the given order.

Other batches of EOC in this stage should have sequence number less than TD batch sequence number (below listed TD batches should be after all non TD batches).

EOC Group	Batch Name	Module	Frequency	Maintenance order
End OF Transaction Input	ACBCUTOF	AC	D	1
End OF Transaction Input	ICBCUTOF	IC	D	2
End OF Transaction Input	ICJRPBAT	IC	D	3
End OF Transaction Input	ICBRESOL	IC	D	4
End OF Transaction Input	TDJEOD	TD	D	5
End OF Transaction Input	ICBEOD	IC	D	6
End OF Transaction Input	ICJACPST	IC	D	7
End OF Transaction Input	DABHOFF	AC	D	8

No Other batch should be configured in between the above batches and all the batches of EOC in End OF Transaction Input stage should be of lower sequence number. As part of EOTI, TDJBOD is to be configured post ICBT batch.

For Beginning of the day stage following batches to be maintained in the given order. Other batches of EOC in this stage should have a sequence number less than these batches.

EOC Group	Batch Name	Module	Frequency	Maintenance order
Beginning of the Day	ICJBOD	IC	D	1
Beginning of the Day	ICJDUCOL	IC	D	2



Beginning of the Day	TDJBOD	TD	D	3
Beginning of the Day	DABHOFF	AC	D	4
Beginning of the Day	TDJPBOD	IC	D	5



Java TD Installation  
[November] [2023]  
Version 14.7.2.0.0

Oracle Financial Services Software Limited  
Oracle Park  
Off Western Express Highway  
Goregaon (East)  
Mumbai, Maharashtra 400 063  
India

Worldwide Inquiries:  
Phone: +91 22 6718 3000  
Fax: +91 22 6718 3001  
<https://www.oracle.com/industries/financial-services/index.html>

Copyright © [2007], [2023], Oracle and/or its affiliates. All rights reserved.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

**U.S. GOVERNMENT END USERS:** Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate failsafe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

This software or hardware and documentation may provide access to or information on content, products and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.