Oracle Hospitality Cruise Shipboard Property Management System

EONE Interface User Guide

Release 23.3
G39308-01
October 2025

Oracle Hospitality Cruise Shipboard Property Management System EONE Interface User Guide, Release 23.3

G39308-01

Contents

Preface

EONE is an interface that receives and helps process the Crew's master data, scheduled embarkation information, address details, emergency contact details, crew effects list, immigration data, and check-in / check-out request from the JD Edwards EONE (JDE E1) system.

Audience

This document is intended for project managers, application specialists, system administrators and users of Oracle Hospitality Cruise Shipboard Property Management System. (SPMS)

Customer Support

To contact Oracle Customer Support, access the Customer Support Portal at the following URL:

https://iccp.custhelp.com

When contacting Customer Support, please provide the following:

- Product version and program/module name
- Functional and technical description of the problem (include business impact)
- Detailed step-by-step instructions to re-create
- Exact error message received
- Screenshots of each step you take

Documentation

Oracle Hospitality product documentation is available on the Oracle Help Center at http://docs.oracle.com/en/industries/hospitality/cruise.html.

Revision History

Date	Description of Change
October 2025	Initial publication.

1

EONE Interface

The following section describes the parameters available to the EONE Interface, setup and usage of the EONE Interface, communication messages, and the use of keypair and certificate.

Parameters Settings

For the EONE Interface to work seamlessly, there are two parameter groups you must configure:

- **System Parameter-EONE:** This is set up in **OHC Administration, System Setup menu, Database Parameter menu**
- **Interface Parameter:** This is set up in **EONE Interface, Settings tab, EONE**

Table 1-1 Parameter Group EONE

PAR Name	PAR Value	Description
Backup Days	0	This parameter defines the number of days that older reservation records will be deleted. The default value is zero. You can also set this value in EONE Interface Parameter, 'Delete reservation Data older than'.

Setting up Message Queues

The following section guides you on how to create the incoming/outgoing message queue.

1. Ensure the Microsoft Message Queue (MSMQ) server features are turned on
2. Go to **Control Panel, Administration Tools,** and **Computer Management**
3. In Computer Management, expand the **Services and Applications** tree view and click **Message Queuing**
4. Right-click the **Private Queues** and select **New. Private Queue**
5. Enter the **Queue name** and select the **Transactional** checkbox
6. Click **OK** to save
7. Repeat steps 4 to 6 for the Outgoing Message Queue

Contingency Reason Code

A Contingency Reason Code is needed when you enable or disable the contingency mode. You can set this up in the OHC Administration module.

1. Log in to the OHC Administration module
2. Go to the **System Codes** option and select **EONE Enable Contingency Mode Reason Code** or the **EONE Disable Contingency Mode Reason Code**
3. Right-click the left pane of the Setup window and select **Add New**
4. Enter a **short code, description**, and **comments**. For example, COMM for Communication Issue
5. The **Enabled** checkbox is selected by default. Removing the check mark disables the code
6. Click **Apply** to save.
7. To enter more codes, repeat the above steps

Supported Message Type from JDE E1

The SPMS supports nine different types of messages from the JDE E1 system. They are listed below.

Table 1-2 Supported Message Type from JDE E1

Message Type	Description
CrewPrimaryManifest	This manifest is provided by the JDE E1 system and contains the master crew data. SPMS must receive the mandatory data before you can transfer other message types for the same crew. The JDE E1 system produces the employee/crew ID and it MUST be unique across all fleets JDE E1 must send a valid OPO_ID (from ship SPMS database). Messages with invalid ID received will not be processed and are returned with a failure message

Table 1-2 (Cont.) Supported Message Type from JDE E1

Message Type	Description
CrewScheduleChange	This message contains the crew's scheduled embarkation details, consisting of all the mandatory information for the embarkation process There are three (3) schedule types that SPMS accept: **SRA** • SPMS will ONLY cancel the reservation if the crew is under the expected list • SPMS will not perform any operation if the crew already checked-in/checked out • SPMS DOES NOT DELETE crew reservation physically from its database except during database maintenance via ADPI **SRON** • If the crew account is under the expected list, SPMS will update the expected sign-on date, sign-on port, expected sign-off date, expected sign-off port and other information in this message type into the SPMS database • If the crew has already checked-in, the system will not update the expected sign-on date and expected sign-on port. All other information in this message will be updated in the Crew record • If the crew already check-out, checked-out from SPMS, and there is no matching sign-on date, no changes will be made **SROF** • If the crew is under the expected list, all fields below will be updated; Expected Sign on date/port, Expected Sign off date/port • If the crew is already checked-in (sign-on), only the expected sign-off date/port will be updated when the sign-on date matches the actual check-in date of the crew member • If the crew is already checked-out from SPMS, it will be updated as a future reservation for the crew member if the previous same sign-on date data exist for this crew member
CrewSignOn	This is a crew check-in request from JDE E1 to SPMS to check-in the crew in reference.
CrewSignOff	This is a crew check out request from JDE E1 to SPMS to check out crew members.
CrewAddress	This message updates the crew's address details from JDE E1 to SPMS. Only the home address is updated.
CrewEffects	This message will add/append the effects belonging to the crew.

Table 1-2 (Cont.) Supported Message Type from JDE E1

Message Type	Description
CrewImmigration	Updates Immigration Data consisting of four types of data, the master Passport/travel document, Seaman Document data, and Brazilian and Mexican Visa information.
CrewAddressEmergency	This message updates the crew's emergency contact address details into SPMS.

Supported Message from SPMS to JDE E1

Table 1-3 Supported Message from SPMS to JDE E1

Message Type	Description
Success Message	EONE interface will send a successful message to JDE E1 when the message received is processed successfully.
Failure Message	A failure message is sent from the JDE E1 interface for any of the messages that it cannot process.
Contingency On/Off Message	A message is sent from the JDE E1 interface when the contingency mode changes.

Creating Shipboard Keypair and Certificate

The shipboard keypair is used for messages destined for the shipboard. The data sent from the shore system is encrypted with the shipboard public key and is decrypted by the ship system using a shipboard private key.

There are many ways to create a keypair and certificate. The following explanation describes creating a keypair with a self-signed certificate using the .NET 2.0 "**makecert.exe** utility, provided in MS .NET Framework 2.0 SDK. On one of the shipboard server nodes, the command to run is:

```
makecert -r -pe -n "CN= BizTalk Shipboard XX" –sr localmachine -ss My –sky
exchange
```

You are to replace the XX with the 2-digit shipcode.

You can also create the PFX file on any machine and import it into the local machine. See Exporting Shipboard Keypair and Importing Shipboard Keypair (Once Per Ship BIZ02 Engine) for steps to export/import a keypair.

There are other actions you can take with the makecert utility, including directly outputting the certificate to a file. However, generating a PFX file directly is not one of these functions. If you need to automate the entire process, the alternative is to create a pvk file with the "sv" tag along with the cer file, then use cert2spc to convert the .cer file to an spc file, and use "pvkimport –pfx" to merge the spc and pvk files into a PFX file.

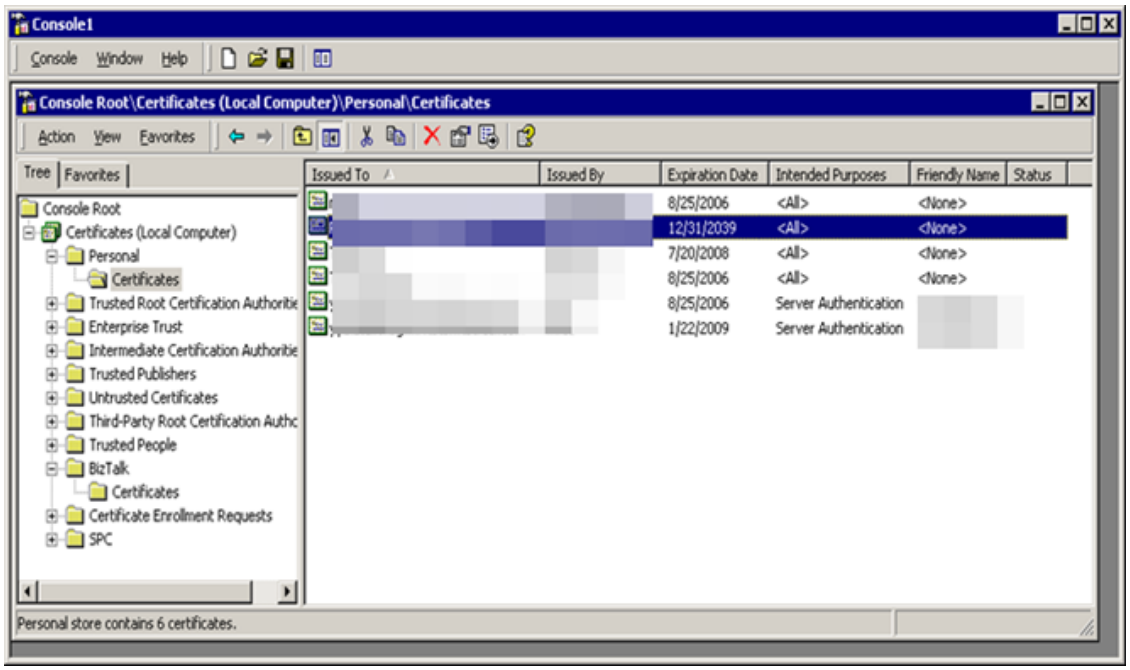
Below are the explanations of tags:

- -r – Creates a self-signed certificate, issuer will be the same as the CN

- -pe – Marks the private key as exportable when inserted into the OS Key Container
- -n – Specifies the X.500 standard subject certificate name
- -sr – The subject certificate store **location**. Options here are **localmachine** for machine-level keys, or **currentuser** (default) for the current user
- -ss – The subject certificate store **name**. Using “My” makes the certificate go into the “Personal”
- -sky – The subject keytype. This can be signature or exchange. If you are sending messages, this must be **exchange**

When opening the MMC for “Local Computer” certificates, you should see something similar to Figure 1–1 Console Root Window below. Notice the `Certificates (Local Computer) / Personal / Certificates` is showing the new certificate.

Figure 1-1 Console Root Window

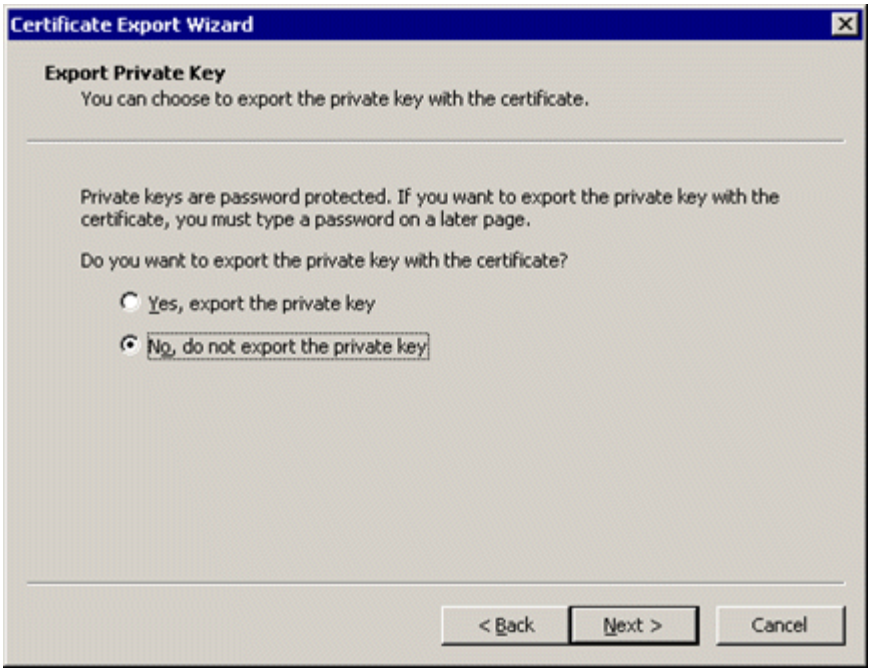


When opening up the details of the certificate, you can see at the bottom, “You have a private key that corresponds to this certificate.” This means the OS Key Container public/private keypair is associated with the certificate in the Certificate Store, and you can decrypt items as they come into this “BizTalk” Node.

Exporting Shipboard Certificate

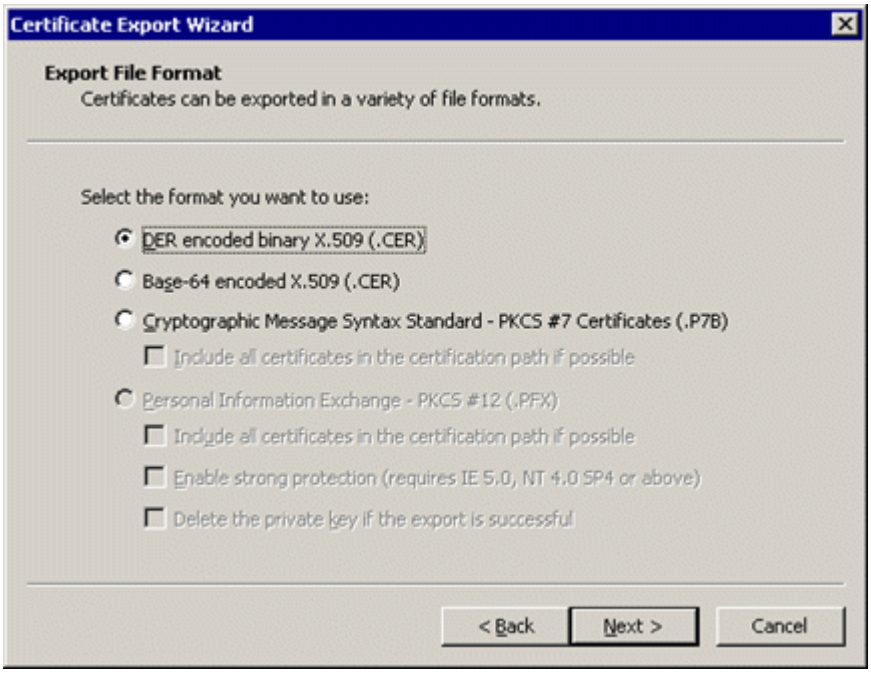
1. Expand the **Certificates (Local Computer),** then **Personal,** and then the **Certificate** folder
2. Right-click the certificate and select **All Task**, then **Export**
3. Within the wizard, select **NO Do not export the private key**, and click **Next**

Figure 1-2 Certificate Export Wizard —Export Private Key



4. Select the **DER encoded binary format** and click **Next**

Figure 1-3 Certificate Export Wizard —Export File Format



5. Save the output file to the file system as “BizTalk Shipboard XX” and click **Finish**. This creates the CER file

Exporting Shipboard Keypair

1. Right-click the certificate and select **All Task**, then select **Export**
2. Within the wizard, select **YES export the private key**, and click **Next**. See Certificate Export Wizard —Export Private Key
3. Select the PFX format (your only option). Leave strong protection enabled.
4. Enter the password, output the file to the file system as “BizTalk Shipboard xx,” and follow the steps to complete the creation. This creates the PFX file.

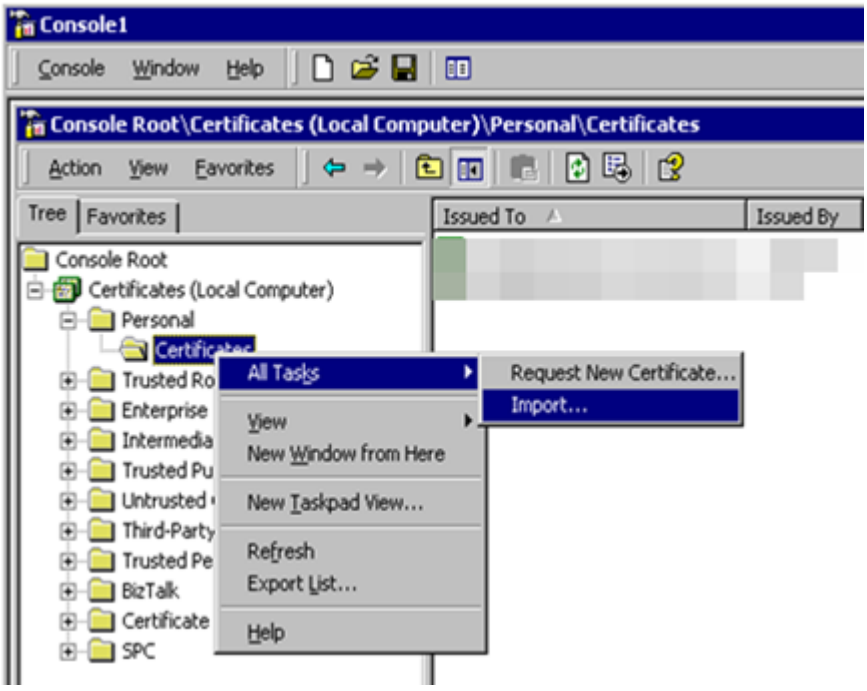
> **Note**
>
> This PFX file has the private key in it. Be careful about sharing the file access and make sure only appropriate people know the password.

Importing Shipboard Keypair (Once Per Ship BIZ02 Engine)

Perform the following on all Shipboard BizTalk nodes that will be running the BizTalk 2002 engine.

1. Copy the PFX file to the node you are working on
2. Right click the **Personal, Certificates** folder, select **All Tasks**, and then select **Import**

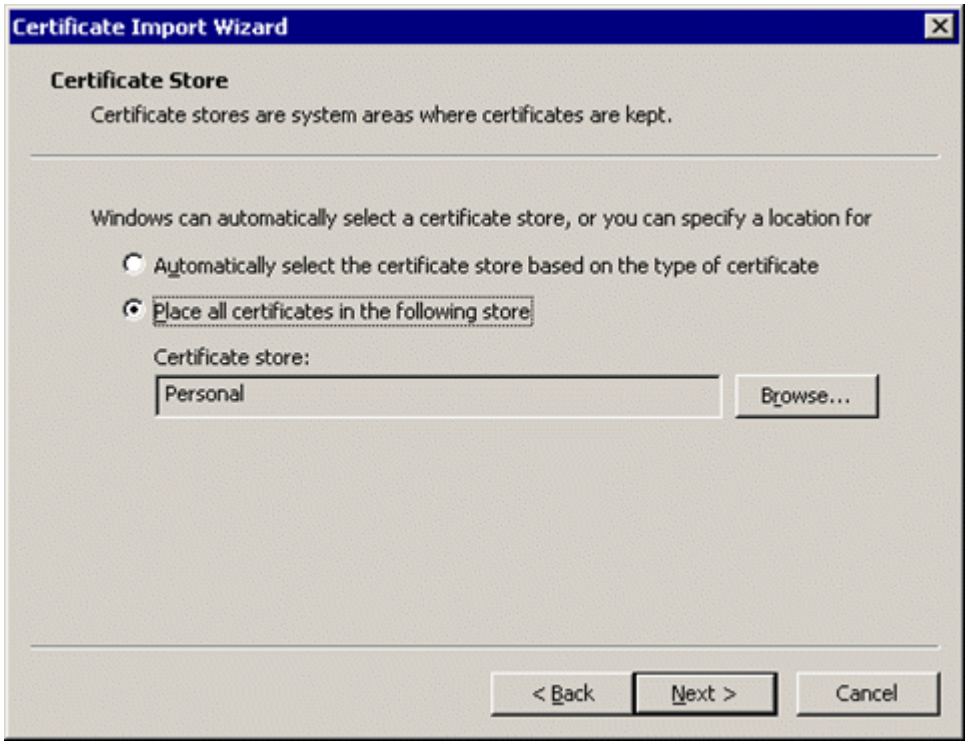
Figure 1-4 Certificate Container



3. When specifying the file to import, change the “Files of Type” to “Personal Information Exchange (*.pfx, *.p12)” and select the “BizTalk Shipboard xx.pfx” file
4. When prompted, enter the password and **do not select Mark this key as exportable.** This is to prevent the key from being exported and used elsewhere

5. Select the option **Place all certificates in the following store** and use the default **Personal** store.

Figure 1-5 Certificate Import Wizard — Certificate Store



6. Copy and paste the certificate to the **local computer, trusted root certification authorities folder** in the snap-in

> **Note**
>
> Do not forget to go back and do this step on all Shipboard BizTalk nodes that will be running a BizTalk 2002 Engine.

Importing Shipboard Certificate (Once Per Shore Node)

Perform the following on **all** Shoreside BizTalk nodes that will be running a BizTalk host.

1. Copy the CER file to the node you are working on
2. At the `Console Root\Certificates (Local Computer)`, right-click the **Other People** folder.
3. Select **All Tasks**, and then select **Import**
4. When specifying the file to import, change the **Files of Type** to **X.509 Certificate (*.cer;*.crt)** and select the **BizTalk Shipboard xx.cer file**
5. At the Certificate Import Wizard, select **Place all certificates in the following store**, and use the default **Other People** store, and then click **Next**
6. Copy and paste the certificate to the **local computer, trusted root certification authorities** folder in the snap-in