Oracle Hospitality Cruise Property Management

Border Control Installation and User Guide

Release 23.2
G36522-02
August 2025

Oracle Hospitality Cruise Property Management Border Control Installation and User Guide, Release 23.2

G36522-02

Contents

Preface

Part I Installing Cruise Property Management Border Control REST API/Web Application Server

1 Preparing Java Environment

Create Java Keystore for Cruise Property Management Border Control API/Apps Server 1

Generate a new Java Keystore using Java Keytool 2

Generate a Certificate Signing Request (CSR) using Java Keytool 3

Importing SSL/TLS Certificate to the Keystore 3

Create Key Pair for Cruise Property Management Border Control API Authentication 4

Generating a new Key Pair using JSON Web Key Generator 4

Generating Keystore and CSR File for EES System to System (S2S) Integration 5

Importing eu-LISA Certificate (.pem format) to Keystore File 6

Create Truststore (.p12) by Importing eu-LISA Certificate Chain (.pem) 6

2 Cruise Property Management Border Control

Uninstalling Cruise Property Management Border Control Database Updater 6

OHC Border Control Database Updater 6

Part II Getting Started

Part III Entry / Exit System

3 Setting Up EES

Configure EES Setup Details 1

Modifying EES Setup Details 2

4 Generating Request File

Creating Request File 1
Deleting Request File 3
Viewing Request File 3
Re-generating Request File 3

5 Processing Response File

Uploading and Processing Response File 1
Searching for Response File 1
Viewing Response File 1

6 Managing EES Response Status

Searching for Reservation Records 1
Deleting Reservation Record 1

7 Administration Module

Configure Nationality Groups 1
Configure Document Types 1
Configure Transport Identification Number 1
Configure Harbor Country 1
New User Definable Security Alert Setup 2

8 WPF Security Module

9 Advance Quick Check In Module

10 Management Module

Preface

Oracle Hospitality Cruise Property Management Border Control is an application that generates passenger manifests from the Oracle Hospitality Cruise Shipboard Property Management System. The generated passenger manifests can be uploaded/transferred to the relevant authorities for verification.

Oracle Hospitality Cruise Property Management Border Control version 23.2.0 introduces Entry/Exit System (EES), developed in accordance with eu-LISA authority requirements.

Purpose

This document provides instructions on how to install, and configure the Cruise Property Management Border Control and the use of EES application.

Audience

This document is intended for project managers, application specialists and users of Oracle Hospitality Property Management System.

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/.

Revision History

Table 1 Revision History

Date	Description of Change
August 2025	Initial publication. Address internal documentation bug HCSP-10953

Prerequisite and Compatibility

This minimum enterprise server operating system, and databases supported by the Property Management Border Control follows the same requirements as Cruise Shipboard Property Management System (SPMS).

The requirements for each server type and supported database versions are listed in Cruise Compatibility Matrix at the https://docs.oracle.com/en/industries/hospitality/cruise.html.

Prerequisite

Before you begin, review the Cruise Installation Guide for complete setup of Shipboard Property Management System (SPMS). Check out a copy of the guide for the respective version at https://docs.oracle.com/en/industries/hospitality/cruise.html.

Entry/Exit System (EES)

To ensure a compliant and successful EES implementation, it is mandatory that you engage directly with eu-LISA prior to starting any implementation activities. Please note that Oracle, as a service provider does not participate in this process. For comprehensive information and official procedures, please visit the eu-LISA website https://www.eulisa.europa.eu/activities/carriers

Part I

Installing Cruise Property Management Border Control REST API/Web Application Server

Prerequisites

- The Time zone on both the Web application server and API server must be the same. It is recommended that you use the database server time zone
- The minimum version of SPMS Database must be v8.0.22.3 or later. If you are running on version lower than the stated, upgrade the SPMS database version before continuing
- The Web application server and API server do not require IIS
- Java JDK version 17.0.4 and above is required
- In this document, we demonstrate generating JSON Web Keys (JWK) with a custom tool, but you can choose from many available options. Select a tool that meets your organization’s security and compliance requirements. Always update the tool, apply the latest security patches, and scan it for malware. Failing to use a secure tool may compromise your environment.
- The API and Web application access uses a Secure Socket Layer and Transport Layer Security (SSL/TLS) cryptographic protocol. You must set up a keystore (.jks format) that contains the private key and certificate
- The keystore must have the default option value as

  ```
  “-keyalg RSA -keysize 2048”
  ```
- A public (verify-jwk.json) and private key (sign-jwk.json) for setting up secure OAUTH. As an example, this document explains how to generate a public and private key

1

Preparing Java Environment

Before you install the Cruise Property Management Border Control Version 23.2 API / Web App server,

1. Ensure the JDK is installed
2. Ensure that you have a tool for manipulating certificates installed

Set JAVA_HOME or JRE_HOME variable

1. Search **Environment Variables** in the search box (next to the Windows start button) then click **Edit**
2. Click the **Environment Variables** button
3. Under System Variables, click **New**
4. In the **Variable Name** field, enter either of the following:
    - **JAVA_HOME** if you have the JDK (Java Development Kit) installed
    - **JRE_HOME** if you have the JRE (Java Runtime Environment) installed
5. Browse the Directory and select `“C:\Program Files\Java\[java version]”`
6. Click **OK** to apply the changes.

Setting the JAVA Path

1. Search **Environment Variables** and then click **Edit**
2. Click the **Environment Variables** button
3. Find the ‘Path’ from the **System Variable** and click **Edit** then **New**
4. Browse directory `“C:\Program Files\Java\[java version]\bin”`
5. Click **OK** to apply the changes.

Installation Process

Installation is a three-step process, where:

- **Step 1:** Create a Java keystore containing certificates purchased from a reputable Certificate Authority
- **Step 2:** Generate security keys for OAuth
- **Step 3:** Install the software

Create Java Keystore for Cruise Property Management Border Control API/Apps Server

Background

Java Keystore is needed to store private keys and certificates used by the Cruise Property Management Border Control API/Web App. A Java Keytool is used to create a Java Keystore, and is distributed as part of the Java JDK. Java Keystore files can be generated on any machine. They need not be on the same server where the SSL/TLS certificate will be installed.

Important: In this section, we use OpenSSL to demonstrate the process. You should select a certification manipulation tool that meets your organization's security policy.

Recommendations

It is recommended that you generate a new Keystore following the process outlined in this section. Installing a new certificate to an existing Keystore often ends in installation errors or the SSL/TLS certificate not working properly. Before you begin this process, backup and remove any old Keystores.

The act of generating a self-signed Digital Certificate to identify the Cruise Property Management Border Control API/Web application is not recommended for the production environment. It increases the risk of an unscrupulous party impersonating the Cruise Property Management Border Control API/Web App to steal sensitive information. However, for limited, non- production testing of Cruise Property Management Border Control API/Web application, you could use a self- signed certificate despite the increased security risk but do so at your own risk as this is not recommended.

Generate a new Java Keystore using Java Keytool

1. Navigate to the directory where you plan to manage your Keystore and SSL/TLS certificates
2. Run the following command:

   ```
   keytool -genkey -alias <ALIAS> -keyalg RSA -keysize 2048 -keystore
   <SITE_NAME>.jks –ext SAN=dns:<SITE_NAME>
   ```

3. In the command above, `<SITE_NAME>` is the name of the domain you want to secure with the SSL/TLS certificate. The command will generate the Keystore with the public and private key pair and a self-signed certificate for the server. `<ALIAS>` is the name for this newly generated entry in the Keystore
4. You will be prompted to create a password for the new Keystore
5. Enter the SSL/TLS certificate information for the self-signed certificate
   a. When prompted for the first and last name, enter the Fully Qualified Domain Name (FQDN) for the site you wish to secure with the SSL/TLS certificate. For example, `www.yourdomain.com` or `mail.yourdomain.com`. If the SSL/TLS certificate is a Domain wildcard type, the FQDN is `*.yourdomain.com`
   b. Enter the Common Name (CN), for example, The FQDN
   c. Enter the Organizational Unit (OU), for example, Cruise Operation
   d. Enter the Organization (O), for example, Cruise Company
   e. Enter the Locality (L), for example, Redwood City
   f. Enter the State or Province Name (S), for example, California
   g. Enter the Country Name (C), for example. US
   h. You will be prompted to verify all the information entered. Type 'y' or 'yes' to confirm
   i. Enter the Keystore password when prompt. The new Keystore file `<SITE_NAME>.jks` is now available in the current working directory

Generate a Certificate Signing Request (CSR) using Java Keytool

1. Navigate to the directory where the Keystore was generated earlier
2. Run the following command:

   ```
   keytool -certreq -alias <ALIAS> -file csr.txt -keystore <SITE_NAME>.jks –ext
   SAN=dns:<SITE_NAME>
   ```

3. In the command above, `<SITE_NAME>` is the name of the Keystore generated in earlier section, and `<ALIAS>` is the name of the entry in the Keystore that defined in earlier section. The CSR will manifest itself as an output file based on the certificate info entered earlier. You will also need to enter the Keystore password to proceed
4. The CSR output file is in the same working directory, for example, `<SITE_NAME>.txt`

Backing Up the Keystore

Save and back up the Keystore file to a safe, secure location.

Importing SSL/TLS Certificate to the Keystore

After receiving your SSL/TLS certificate from Certificate Admin, you must import the SSL/TLS Certificate file to the same Java Keystore under the same alias name (for example, alias server) used to generate your CSR. If you try to install the certificate to a different keystore or under a different alias, the import command will not work.

> **Note**
>
> Before importing the SSL/TLS certificate, ensure the certificate chain format is appropriate and valid. You can use OpenSSL tool to check on the validity as follows:
>
> ```
> openssl pkcs7 –print_certs –in <cert_name>.p7b
> ```

1. Navigate to the directory where the Keystore was generated earlier
2. Run this command:

   ```
   keytool -import -alias <ALIAS>-file <CERT_NAME>.p7b -<SITE_NAME>.jks
   ```

3. In the command above, `<CERT_NAME>` is the name of the SSL/TLS Certificate. `<SITE_NAME>` is the name of the Keystore generated in earlier section. `<ALIAS>` is the name of the entry in the Keystore that defined in earlier section
4. You will get a confirmation message that displays “Certificate reply was installed in keystore.” Type *‘y’* or *‘yes’* to proceed
5. This will load all the necessary certificates to the Keystore
6. The Keystore is now ready to be used by the Tomcat/Tomcat Embedded Server

Create Key Pair for Cruise Property Management Border Control API Authentication

Background

OAuth 2.0 is the user authorization mechanism used by Cruise Property Management Border Control API. It requires a generation of an asymmetric key pair to work. The asymmetric key pair is used to securely sign and read contents found in the Security token. Security of the API relies on the security token. API calls made without a valid Security token will be rejected. In detail, the security token contains a checksum. This checksum ensures that the token is not tampered with. The checksum is calculated by adding up the bytes in the security token and is signed by the private key. A third party can check the validity of a token by recalculating the checksum, decrypting the original checksum with the public key, and comparing the two. Any differences between the two checksum indicates that the token has been tampered with.

> **Note**
>
> We provide the process below as an example. You can use other certificate manipulation tools to generate the public and private keys. Whichever tool you use, ensure that you download them from a reliable source and that the downloaded tool is security checked, virus scanned, and checksum checked. Without such due diligence, you may compromise the security of your installation.

Generating a new Key Pair using JSON Web Key Generator

1. Go to https://mkjwk.org/ for the JSON Web Key generator tool
2. Select the **RSA** tab
3. Select the right **Key Size** in bits, required for RSA key types. Recommended size is 2048 and above
4. Select the **Key Use** as signature
5. Select the **Key ID** as specify and enter any string, for example sign-rsa
6. In the **ShowX.509**, select **No**
7. Copy the *Public Key* and *Public and Private Keypair Set* into a separate files with .json extension and save
8. Sample public and private keys are shown below.

   Sample Public key:

```
{
   "keys": [
       {
          "kty": "RSA",
          "e": "AQAB",
          "use": "sig",
          "kid": "sign-rsa",
          "alg": "RS256",
          "n": "g88SjdDsfdHd64fdf..."
      }
```

```
  ]
}
```

Sample Private key:

```
{
 "keys": [
   {
     "p": "5BjdvhhdGjjjdsUI...",
     "kty": "RSA",
     "q": "k-7TihGsdfjnjLLf8...",
     "d": "e4t4J7dfk7jddPo78...",
     "e": "AQAB",
     "use": "sig",
     "kid": "sign-rsa",
     "qi": "UlYwJ6Jsdfsdfc...",
     "dp": "CDz5rYYsdffffI1...",
     "alg": "RS256",
     "dq": "fBAEeUP98HHdf...",
     "n": "g88SjLLjsdf881IP..."
   }
  ]
}
```

Generating Keystore and CSR File for EES System to System (S2S) Integration

Background

The implementation of the EES S2S integration model is governed by mutual TLS (mTLS) requirements as mandated by eu-LISA. This ensures that both the carrier system and eu-LISA can authenticate and securely exchange data.

To comply with these requirements:

- The carrier operator must create a keystore file, generate and provide a CSR to eu-LISA. This CSR represents the identity of the system initiating the secure connection. The CSR will be used to obtain a private certificate issued by eu-LISA authority (CA),facilitating mutual authentication. See topic Generate a new Java Keystore using Java Keytool and Generate a Certificate Signing Request (CSR) using Java Keytool for further details
- The carrier operator must also submit the public IP address of the server or proxy hosting the Border Control API for whitelisting by eu-LISA, ensuring that only authorized endpoints can establish a connection to their platform.
- To Import private certificate obtained from eu-LISA. See Importing eu-LISA Certificate (.pem format) to Keystore File file section on the import process
- Create a truststore file (.p12 format) from the complete certificate chain (.pem format) received from eu-LISA with only the root certificate, and the intermediate certificate which can verify the eu-LISA server certificate for server authentication. See topic Create Truststore (.p12) by Importing eu-LISA Certificate Chain (.pem) on the create process

Importing eu-LISA Certificate (.pem format) to Keystore File

After receiving the private SSL certificate from eu-LISA, you must import the complete certificate chain (client private certificate along with the root certificate, and the intermediate certificate, if any) into the keystore file, for client authentication under the same alias name used to generate your CSR. For example, alias client.

If you try to install the certificate to a different keystore or under a different alias, the import command will not work.

1. Navigate to the directory where the Keystore was generated earlier
2. Run command: `keytool -importcert -alias <ALIAS> -file <CERT_NAME>.pem -keystore <SITE_NAME>.jks -storepass <PASSWORD>`
3. In the command above,
   - <ALIAS> is the name of the entry in the keystore that defined in earlier section
   - <CERT_NAME> is the name of the private certificate.
   - <SITE_NAME> is the name of the keystore generated in earlier section
   - <PASSWORD> is the password of the keystore file
4. Once the command is run, a confirmation message “Certificate reply was installed in keystore.” shall prompt. Type ‘y’ or ‘yes’ to proceed
5. This will load all the necessary certificates to the keystore file, and would be ready for use in S2S Integration

Create Truststore (.p12) by Importing eu-LISA Certificate Chain (.pem)

Private certificate received from eu-LISA contains the client certificate, root certificate, and the intermediate certificate, if any.

Since truststore only requires the root certificate and the intermediate certificate to validate the server certificate, create a new certificate chain (.pem format) from the certificate received from eu-LISA to include only root certificate, and the intermediate certificate if any.

To create,

1. Navigate to the directory where the new `.pem` file is created
2. Run command: `keytool -importcert -alias <ALIAS> -file <CERT_NAME>.pem -keystore <TRUST_STORE_NAME>.p12 -storepass <PASSWORD>`
3. In the command above,
   - <ALIAS> is the name of the entry in the keystore that defined in earlier section
   - <CERT_NAME> is the name of the new .pem file that includes the root certificate, and the intermediate certificate if any
   - <TRUST_STORE_NAME > is the name of the truststore file to be created from new .pem file
   - <PASSWORD> is the password of the truststore file to be created

2

Cruise Property Management Border Control

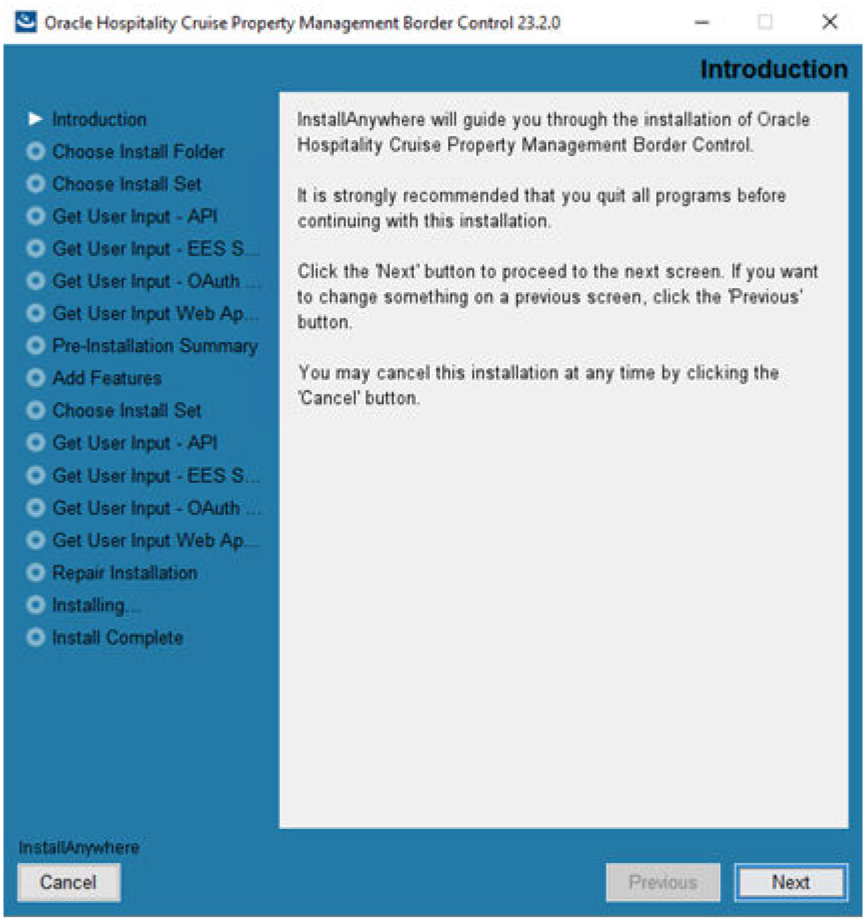
You can perform a custom installation or a typical installation. A custom installation allows you to exclude the products that you do not need. If you choose to perform a typical installation, you can still remove/disable the features that you do not need post installation.

The installation requires the user performing the installation to have an Administrator privilege.

Installing Cruise Property Management Border Control 23.2x

1. Log in as a Microsoft Windows Administrative user
2. Start the installation program by right-clicking the **CruiseBorderControl_23.2.0.exe** and select **Run as Administrator**

Figure 2-1 Cruise Property Management Border Control Installation Page



Oracle Hospitality Cruise Property Management Border Control 23.2.0
Introduction
▶ Introduction
○ Choose Install Folder
○ Choose Install Set
○ Get User Input - API
○ Get User Input - EES S...
○ Get User Input - OAuth ...
○ Get User Input Web Ap...
○ Pre-Installation Summary
○ Add Features
○ Choose Install Set
○ Get User Input - API
○ Get User Input - EES S...
○ Get User Input - OAuth ...
○ Get User Input Web Ap...
○ Repair Installation
○ Installing...
○ Install Complete
InstallAnywhere
Cancel
Previous
Next

InstallAnywhere will guide you through the installation of Oracle Hospitality Cruise Property Management Border Control.

It is strongly recommended that you quit all programs before continuing with this installation.

Click the 'Next' button to proceed to the next screen. If you want to change something on a previous screen, click the 'Previous' button.

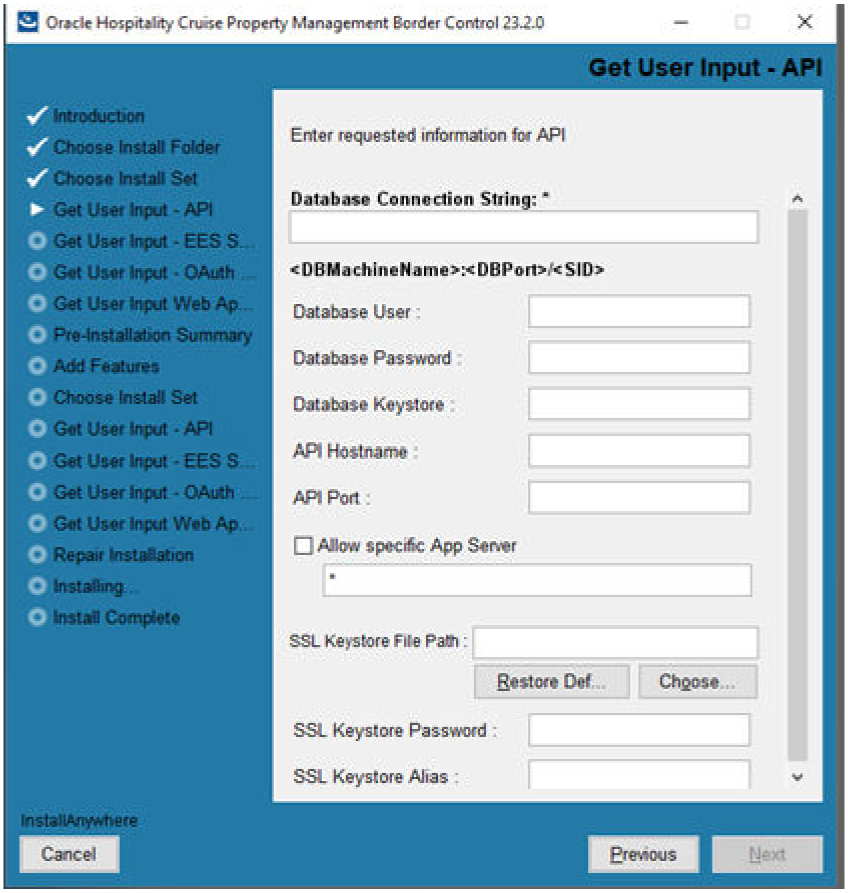
You may cancel this installation at any time by clicking the 'Cancel' button.

3. Click **Next** and navigate to the “Choose Install Folder”. The default folder is **“**`C:\`**”.**

   If you choose to install it in a folder different from the default, make sure you grant users the full folder permission so that the user can start the APIs or Apps

4. To grant the folder permission,
   1. Access the **Properties** dialog box
   2. Select the **Security** tab
   3. Click **Edit**
   4. In the Group or user name section, select the user(s) you wish to set **permissions** for
   5. In the Permissions section, use the checkboxes to select the right **permission level**
   6. Click **Apply**
   7. Click **OK**
5. Click **Next** and navigate to “Choose Install Set” and if you choose,
   - **Typical**, most common application will be installed. This option is recommended for most users
   - **Custom**, you can customize the features to be installed as either WebApp or API or both to install based on the requirement
6. Click **Next** to input the below fields:
   - **Database connection String:** `<DBMachineName>:<DBPort>/<SID>`
   - **Database User:** Database User
   - **Database Password:** Database Password
   - **Database Keystore:** DB Keystore’s password for database encryption. Minimum password length is 14 characters
   - **API Hostname:** API Server’s Hostname
   - **API Port:** API Server’s port number
   - **Allow specific App Servers:** Check to enable input of server machines with APP installed that are allowed to access the API. Uncheck if it applies to all servers
   - **SSL Keystore File Path:** Keystore file path which contain .jks file extension
   - **SSL Keystore Password:** Keystore password
   - **SSL Keystore Alias:** Private key/Alias used to generate the keystore

Figure 2-2 Cruise Property Management Border Control API Settings



Oracle Hospitality Cruise Property Management Border Control 23.2.0

Get User Input - API

- ✓ Introduction
- ✓ Choose Install Folder
- ✓ Choose Install Set
- ▶ Get User Input - API
- ○ Get User Input - EES S...
- ○ Get User Input - OAuth ...
- ○ Get User Input Web Ap...
- ○ Pre-Installation Summary
- ○ Add Features
- ○ Choose Install Set
- ○ Get User Input - API
- ○ Get User Input - EES S...
- ○ Get User Input - OAuth ...
- ○ Get User Input Web Ap...
- ○ Repair Installation
- ○ Installing...
- ○ Install Complete

Enter requested information for API

Database Connection String: *

<DBMachineName>:<DBPort>/<SID>

Database User :

Database Password :

Database Keystore :

API Hostname :

API Port :

□ Allow specific App Server

*

SSL Keystore File Path :

Restore Def... Choose...

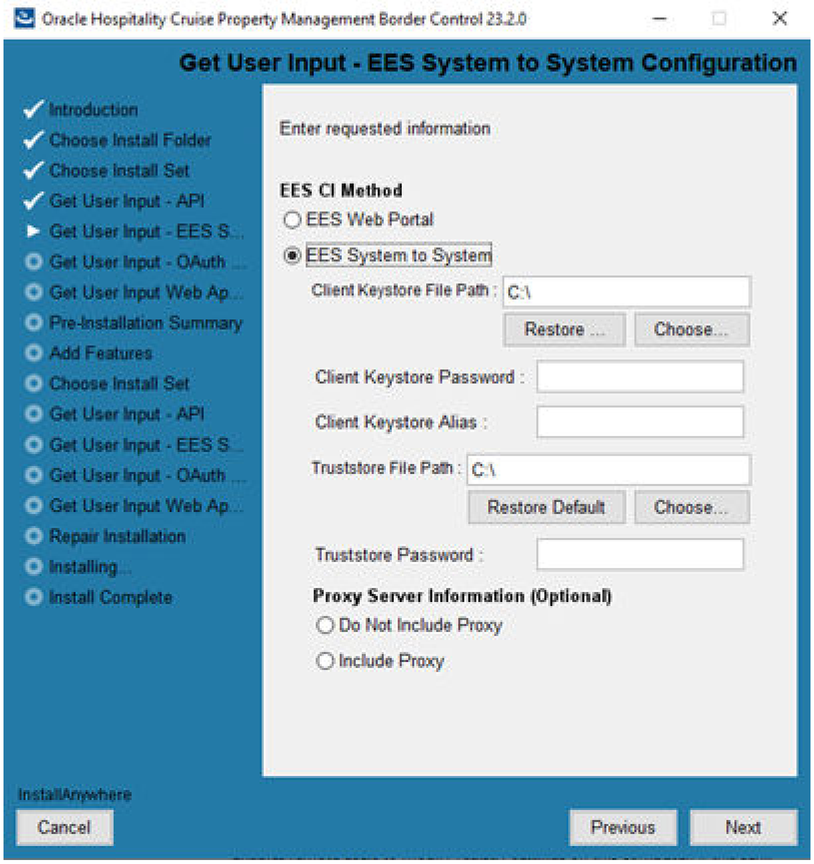
SSL Keystore Password :

SSL Keystore Alias :

7. Click **Next** to select the Carrier Interface (CI) method. The available CI method are:
   - **EES Web Portal -** if selected, this allows you to create a request file with CSV format, which has to be manually uploaded to EES web portal for processing the request file.
   - **EES System to System (S2S) -** if selected, the EES S2S Configuration details will appear. All fields are mandatory

   If no option is selected, the installer will default to EES Web Portal.

Figure 2-3   EES Installation - Get User Input



Oracle Hospitality Cruise Property Management Border Control 23.2.0

Get User Input - EES System to System Configuration

Enter requested information

EES CI Method

○ EES Web Portal

● EES System to System

Client Keystore File Path : C:\

Client Keystore Password :

Client Keystore Alias :

Truststore File Path : C:\

Truststore Password :

Proxy Server Information (Optional)

○ Do Not Include Proxy

○ Include Proxy

- **Client Keystore File Path:** Path to the keystore (.jks) file used for client communication
- **Client Keystore Password:** Password used to protect the keystore file
- **Client Keystore Alias:** Alias name for the key entry within the keystore
- **Truststore File Path:** Path to the truststore (.p12) file used to validate the remote certificate
- **Truststore password:** Password protecting the truststore file
- **Proxy Server Information (Optional)** - If a proxy is required for network communication, select **Include Proxy** and provide the following:
  - **Proxy Host:** Hostname or IP address of the proxy server
  - **Proxy Port:** Port number used by the proxy server

8. Click **Next** to input the OAuth Configuration settings' fields
   - **OAuth Public Key File:** OAuth public key file in .json file extension
   - **OAuth Private Key File:** OAuth private key file in .json file extension
9. Click **Next** to input the **Web Application** port
   - **WebApp Port**: Single instance of Border Control WebApp is supported. User need to choose an unused port for the installation

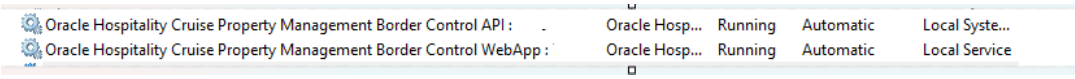
- **API Gateway**: By default, it is based on the API Hostname and port number defined in previous step. However, if the API is located at another server, user need to define the installed API server name
- **Keystore File Path:** If user has separate API server, then keystore file path has to be provided
- **Keystore Password**: Keystore file path for the API Gateway if it is different from the default API Server

10. Click **Next** for Pre-Installation Summary and verify that it is the desired set up
11. Click **Install** to begin installation

> **Note**
>
> For a better end user experience, at the end of the installation a `installer.properties` file containing all the configurations, encryption of passwords is created and added to folder where Border Control InstallAnywhere is placed
>
> The `installer.properties` file's content will be cleared once the InstallAnywhere application is triggered. If you would like to maintain the same configurations or information, please backup this file

12. API's configuration is stored in the `application.properties` file of the installed folder
13. At the end of the installation, the system creates two (2) new Windows Services; namely **Oracle Hospitality Cruise Property Management Border Control WebApp** and **Oracle Hospitality Cruise Property Management Border Control API**

Figure 2-4 Cruise Property Management Border Control Window Services



Oracle Hospitality Cruise Property Management Border Control API :	Oracle Hosp...	Running	Automatic	Local Syste...
Oracle Hospitality Cruise Property Management Border Control WebApp :	Oracle Hosp...	Running	Automatic	Local Service

14. The system will create a folder `Oracle Hospitality Cruise\ Border Control\v23.2` under the directory if it does not exist, and one or two (2) sub-folders - 'API', and/or 'WebApp', depending on the installation type

Uninstalling / Modifying Cruise Property Management Border Control 23.2.0

Any modification or uninstallation are performed through Windows Control Panel in a Maintenance mode. This would allow user to select the options to perform like add features, remove, or uninstall the product.

1. Start the installation program by right-clicking the **CruiseBorderControl 23.2.0.exe** and select **Run as Administrator**
2. If you have already installed the application, the Setup starts in Maintenance mode, allowing you to reinstall
    - **Add features:** InstallAnywhere will guide you through adding features to the installed set. By default, WebApp and API will be disabled if already installed
    - **Remove features:** InstallAnywhere will guide you through removing features of the installed product. You can *uncheck* the product features (WebApp / API) that need to uninstall. Checked features will remain installed

- **Uninstall Product:** InstallAnywhere will remove all the features that were installed during product installation including files, folders and windows services

Uninstalling Cruise Property Management Border Control Database Updater

Installer for Border Control DB Updater is not required from version 23.2.0. Instead, border control database can be directly updated using **OHC Border Control Database Updater.exe** without any dependencies. Therefore, you can uninstall the previous database updater (CruiseBorderControlDBUpdater_23.1.x.exe) from the Control Panel.

OHC Border Control Database Updater

Prerequisites

1. Microsoft .NET Framework 2.0, 3.5, and 4.8 features are enabled on the target machine
2. Oracle 19c Database client with ODAC is installed on the target machine. See topic **Oracle Database Client and ODAC Installation** in the **SPMS Installation Guide**

To complete the installation, you will need to run **OHC Border Control Database Updater** packaged with the Installation to update the database to latest Border Control requirements.

1. Double-click the **OHC Border Control Database Updater.exe** to launch the program
2. At the Welcome screen, click the **Next** button to navigate to the next screen
3. On the Database Connection screen, enter the **SPMS Database TNS name** and **Database Schema Password**
4. If the Database TNS name or Database Schema password is incorrect, you will receive an error message. Correct the information and retry
5. To validate the Database connection, click the **Test Connection** button
6. Click the **Next** button to proceed to the Options screen and select the mode to run
   - **Standard:** Updates the Database with the required changes
   - **Simulation:** Checks and generate a list of changes applicable to this version, but it will not run the update on the database
7. Click the **Next** button to confirm and proceed with the install
8. Click **Next** to start the process
9. The progress of the update is shown in the Status screen. When the update completes, click the **Next** button to continue
10. Once the database update completes, you will find a process log is saved in the Public Document folder "`C:\Users\Public\Document\Oracle Hospitality Cruise`". Alternatively, you can click the **Copy to Clipboard** button to save the file
11. Click the **Finish** button to exit

Part II

Getting Started

Launching the application

To launch the application from a desktop browser:

1. Open your browser. See Oracle Software Web Browser Support Policy
2. Enter the application URL, for example, `Https://<webapp_hostname>:<portno>`. See your system administrator to obtain the host name and port if you are do not already have it

Log in to the application

1. On the application page, enter your user name and password

   > **Note**
   >
   > The user name and password is same as SPMS and is case-sensitive

2. If you sign in with an incorrect user name, password or both, you will receive an error **'Invalid login. Please try again'** and the field color changes to red. The account will be locked for numbers of minutes after a few unsuccessful log ins. The lock of duration is based on the value defined in the parameter **Lockout Minutes**

   > **Note**
   >
   > The number of failed attempts is determined by the value set in SPMS parameter **System, Max Login**

3. Upon successful login, your user name and profile picture is will appear at the top right of the page, and it brings you to the Border Control page
4. To logout from the application, press the arrow down icon on the page and press the **Sign Out** button when shown. This brings you back to the login page
5. To access the application, you must have role access for Border Control. This access is managed in the Cruise Property Management System, Role Manager - Border Control User Group

   > **Note**
   >
   > The role access for Border Control application is only available with SPMS version 23.1.0 and above

Part III

Entry / Exit System

As a prerequisite, the European Travel Information and Authorisation System (ETIAS) will perform a detailed checked on each applicant to determine whether they are allowed to enter any Schengen Zone country. Therefore, cruise ships must submit their passengers and crew manifest for verification before departing from the harbor.

To facilitate this, the Entry/Exit System (EES) is used to generate the required EES data file for submission, and this can be done in two ways.

- **Web Portal (CSV)**: Export of required EES date file to .csv format and update to eu-LISA Web Portal
- **System to System (S2S)**: Submit the required EES date file directly to eu-LISA endpoint using REST API, System to System(S2S)

Once the EES processes the submission, a response files is generated.

- For Web Portal submission, download the response file from the eu-LISA Web portal and manually uploaded into SPMS, EES module to update each passenger's or crew's status
- For System to System, manual uploading of response file is no longer needed. The returned statuses are automatically updated in SPMS through the API endpoint

3 Setting Up EES

The **EES Setup** page allows you to configure all settings needed to integration SPMS with EES. Within the EES Setup, you can

- **Select the nationality groups** to include in EES submission
- **Exclude specific travel document types** from submission
- Configure the **Carrier Interface (CI) Method** in **System to Setup Setup**. This setting is mandatory and you must choose one of the interface option

> ⓘ **Note**
>
> Regardless of the selected CI Method, the configuration of **Nationality Groups** and **Travel Document Types** is needed to ensure smooth and accurate file submission. See Administration topic on how to configure them

Configure EES Setup Details

1. From the **Navigation** menu, select **Entry/Exit System** then the **EES Setup**
2. Enter the following mandatory fields
   - **Select Nationality Group To Include:** Select a nationality group with predefined nationalities
   - **Select Travel Document Type(s) To Exclude:** Allows you to add multiple selection of travel document types to be excluded needed for EES setup
3. You can add, remove or search for the codes with the below function
   - **Search:** The excluded travel document types appears when selecting the combo box. Entering the document name at the search text box field will filter the document type accordingly
   - **Add:** Select the combo box and then the excluded travel document type to added to the list. Continue to add multiple selection as required
   - **Remove:** Select the **X** icon from the combo box to remove the travel document type from list
4. To configure the CI setup details, select the **Carrier Interface Method** for request file submission and validation with EES. The options are:
   - **Web Portal (CSV)**
     This is the default option. Use this option if the S2S integration is not available or if you intend to manually upload the request file to the eu-LISA Web Portal. The request file is generated in CSV format
   - **System to System (S2S)**
     Select this option for communication using REST API. The request file is created in JSON format and submitted automatically, provided the below is registered with EES and configured

- Carrier ID
- Service Provider ID
- EES URL
  The Carrier ID and Service Provider ID must be the identifiers registered with eu-LISA, and the EES URL provided for communication with their production environment

5. Click the **Save** button. A confirmation message **Setup Completed** appear once the record is saved

Modifying EES Setup Details

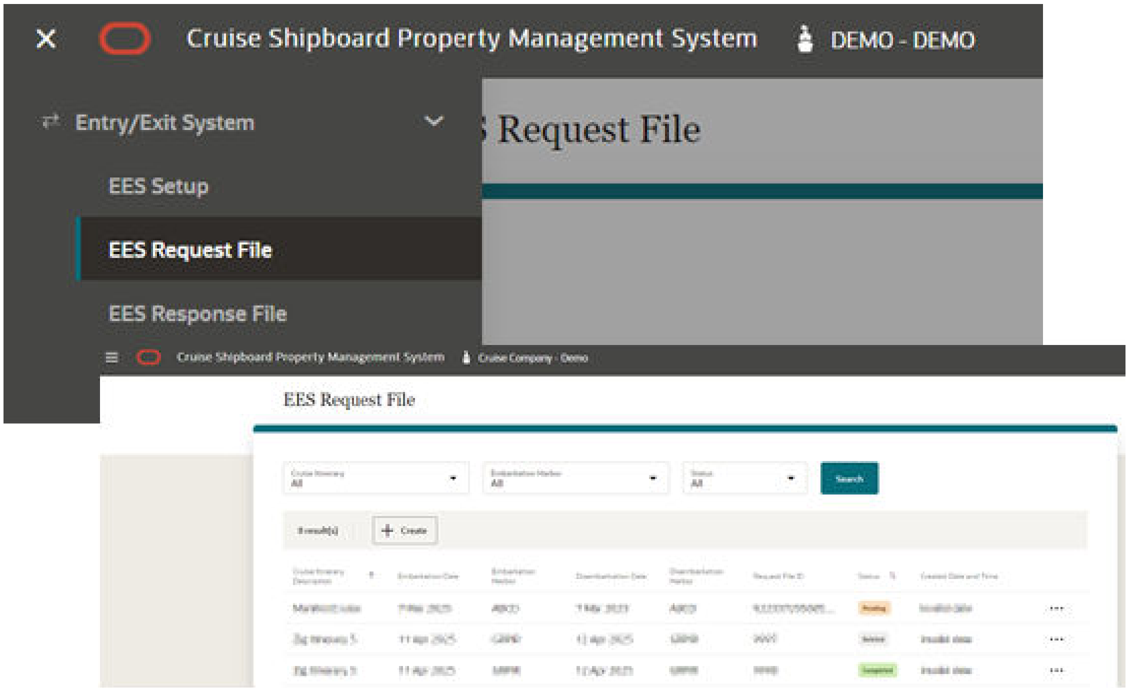
1. From the **Navigation** menu, select **Entry/Exit System**, and then **EES Setup**
2. In the EES Setup configuration page, the **Save** button is disabled
3. Editing any of the fields on the page will enable it. Click **Save** button to update the change.
   A confirmation message will appear when the setup is complete

4

Generating Request File

The EES Request File page allows you to view previously generated request files, and has an option to create a new request file for submission (reservation manifest) to EES for verification.

Figure 4-1 EES Request File Page



In the EES Request File page, all the records of previously generated EES request files are shown. You can search a record using one of the search filters - cruise itinerary, embarkation harbor and request file status.

In each of the request records, you can delete, re-generate and view based on the Request File status - Pending, Completed and Deleted.

- **View:** Applicable for status Pending, Deleted and Completed
- **Re-generate:** Only applicable for status that is *Pending* and CI method is Web Portal (CSV)
- **Delete:** Only applicable for status that is *Pending*

Creating Request File

There are two ways to create request file per EES application setup - Web Portal (CSV) and System to System (S2S), and below are the steps.

For CSV method,

1. From the **Navigation** menu, click **Entry/Exit System** then the **EES Request File**
2. Click **Create** button to open the Create Request File page
3. At the Create Request File screen, the reservation manifest listing will populate based on below selection criteria; modification of the manifest is not allowed as it is listed based on Embarkation Harbor:
   - **Profile Type:** a reservation filter by profile type, with possible options of guest and crew
   - **Cruise Itinerary:** current or future cruise itinerary record
   - **Embarkation Harbor:** the embarkation port with arrival date based on the selected Cruise Itinerary
4. Upon selecting the above criteria, the system auto fills the Embarkation and Disembarkation Date, Disembarkation Harbor and Time. Modification on these fields is not allow
5. Click the **Process** button to retrieve listing of guest manifest records meeting the selected criteria. The record shown would only consists of checked in reservation status with actual embarkation date matching the embarkation harbor date
6. You can also search the reservation record by entering these keywords: a surname, given name, stateroom number or folio number
7. A guest data is deemed as an error and is highlighted in red if the data is missing the following information - Folio number, Surname, Given Name, Date of Birth, Sex, Nationality, Travel Document Type, Travel Document Number, Travel Document Expiry Date and Travel Document Issued Country
8. The **Generate** option is disabled if the loaded information contain erroneous data. You need to correct all the erroneous reservation data in SPMS Desktop Application, and then refresh the manifest by clicking the **Process** button. If there are no error in the reloaded reservation data, the **Generate** button become enabled. You can also enable the button by deleting the erroneous data from the manifest, and then select the **Ellipsis** button followed by the **Delete** button
9. Click **Generate** button to generate the csv file. The generated filename format is according to the selected profile type:
   - Guest Profile type will be “EESReqYYMMDDHHMM00.csv
   - Crew Profile type will be CrewEESReqYYMMDDHHMM00.csv
10. The generated request file is saved to the user defined browser download location

For S2S method,

1. Repeat step 1 to 8 of **For CSV method**
2. Clicking **Generate** button in S2S configuration will create the request file in JSON format and it will not be downloaded. Instead, it will redirect you to *Request file* page, listing the newly created requests with status *pending*
3. Once the request file is created successfully, it will be processed automatically by Border Control application EES S2S integration by connecting to eu-LISA endpoint
4. When the request is processed successfully, the status will be updated to *Completed*, along with individual records status updated to the appropriate EES status received from eu-LISA
5. If there is an error occurs while processing the request file, then the status of the file will show '*Error*', with specific error messages returned by eu-LISA shown in the Error

Message column. To view the all the request records with error status, click the **Status Filter** and select the error status

6. Request file with error status will not be re-processed. User *must* delete the request file, resolve all errors and recreate a new file with the same data. You *cannot* recreate the request file with the same data if you have not delete the earlier file. See Deleting Request File topic for detailed steps on how to delete a request file.

Deleting Request File

1. On the EES Request File Listing page, select the request file record to delete and then the **Ellipsis** button
2. Click **Delete** button. At the confirmation message ‘Delete EES request?’, clicking **Cancel** will close the dialog box and **Delete** will flag the request file as Deleted
3. Once the Request File is flagged as deleted, the reservation manifest in this Request File will automatically flagged as deleted. To regenerate, see topic Creating Request File
4. Deleting a *Completed* or *Deleted* status request file is not permissible

Viewing Request File

1. From the **Navigation** menu, select **Entry/Exit System** and then **EES Request File**
2. On the EES Request File Listing page, select the request file record and then the **Ellipsis** button
3. Click **View** button to open View Request File page
4. There are two sections on this page:
   - **Cruise Itinerary:** Section shows the cruise itinerary details, request file ID and request file status
   - **Request File Record(s):** Section shows the guest details records

Re-generating Request File

The Re-generate File option re-creates the same EES Request File with the exact data from the selected File ID. This option is only available to CI method - Web Portal (CSV) and request file status is pending.

1. From the **Navigation** menu, select **Entry/Exit System** and then **EES Request File**
2. On the EES Request File Listing page, select the request file record and then the **Ellipsis** button
3. Click **Re-generate** to open the View Request File page and then the **Re-generate File** button to proceed

5

Processing Response File

After EES System verified the uploaded request file, they will return the guest manifest records with an updated status (OK, NA, NOK EES, NOK ETIAS), and provide a response file in CSV format. The response file is downloadable from EES System, after which you can upload it to Entry/Exit System application for processing following the below steps.

Uploading and Processing Response File

1. From the **Navigation** menu, select **Entry/Exit System**, and then **EES Response File**
2. Click **Process** button to open the Process Response File page
3. From the Add response file(s) section, use the drag and drop action to upload one or more downloaded response file (csv format) for processing
4. The selected response file appears on the page. Click the **X** icon to remove unwanted response files
5. The **Process** button is enabled once the response file is uploaded. Click **Process** button to proceed and a dialog box with message ‘Processing of file(s) may take some time” appears. Clicking **Cancel** button will close the dialog box and the **Process** button will proceed
6. Once the file is processed successfully, a confirmation message ‘Response file(s) processed’ appears and records of generated EES response files with ‘completed’ status is shown on the list
7. If the user uploads an invalid file format, file not found in local computer or uploading response files that are already processed, an alert message ‘Some of the file(s) failed to process. Please review the file(s) and add again to process’ appears. You need to select the **X** icon to delete the invalid files or re-upload the response file for processing
8. If the CI method is S2S the **Process** button will not be visible as the response is auto-generated when EES processes the request

Searching for Response File

In the EES Response File page, the records shown in the listing section are the processed EES response files. You can search a record using one of the search filters - cruise itinerary, embarkation harbor and file id

1. From the **Navigation** menu, select **Entry/Exit System**, and then **EES Response File**
2. Perform a search using search filters Cruise itinerary, Embarkation Harbor or File ID
3. Clicking the **Search** button will bring up all the EES response file records that matches the search criteria

Viewing Response File

1. From the **Navigation** menu, select **Entry/Exit System** and then **EES Response File**

2. On the EES Response File Listing page, select the desired record and then the **Ellipsis** button
3. Click **View** button to open View Response File page
4. There are three sections on this page:
    - **Cruise Itinerary:** Section shows the cruise itinerary details
    - **Response File:** Section shows response file id, processed response file name and processed date and time
    - **Response File Record(s):** Section shows reservation details records with EES status

6

Managing EES Response Status

This module allows you to search for processed reservation records in EES response file. The **Delete** option enables the removal of processed records regardless of its status, and allow you to include them in a new EES request file.

Searching for Reservation Records

1. From the **Navigation** menu, select **EES Entry/Exit System**, and then **Manage EES Response Status**
2. Perform search for reservation record using search filters Cruise itinerary, Embarkation Harbor, EES Response Status, First Name, Last Name, Stateroom or Folio Number
3. Click **Search** button. The reservation records matching the search criteria will appear on Manage EES Response Status listing

Deleting Reservation Record

1. At the Manage EES Response Status Listing page, select the reservation records regardless of its EES status that you want to delete and click the **Ellipsis** button
2. Click **Delete** button. A confirmation message ‘Delete [Last Name][First Name] from the EES verification? Deleting this reservation record, the reservation EES Status will be removed.’ appears
3. Clicking the **Cancel** button will close the dialog box and the **Delete** button will proceed to remove this reservation record from the listing
4. Click **Delete** button. A confirmation message **Record Deleted** appears, removing the selected reservation records from the listing

7

Administration Module

Below are the setup that is required to be configured in the OHC Administration module before setting up the EES Setup page.

Configure Nationality Groups

1. This setup will be used at the **EES Setup** option under the **Select Nationality Group To Include** option
2. From the **Administration** menu, select **System Codes** then the **Nationality Groups**
3. Right-click and select **Add Nationality Group** option to create a new record
4. Enter the description field and assign the Non-European nationality code to the Nationality Codes section. Click **Apply** to save the entry

Configure Document Types

1. This setup is used at the **EES Setup** option under the **Select Travel Document Types(s) To Exclude** option
2. From the **Administration** menu, select **System Codes** then the **Document Types**
3. Right-click and select the **Add Document Types** option to create a new record

Configure Transport Identification Number

1. The Transport Identification number is one of the required fields needed by the EES request file. Therefore, the carrier operator would need to define the transport identification number on each cruise itinerary
2. From the **Administration** menu, select **System Setup** then the **System Cruise Setup**
3. Select the setup Cruise and enter the transport identification number in the **Itinerary ID** field
4. Click **Apply** to save the changes

Configure Harbor Country

Each of the harbor records used in Cruise Itineraries would need to be configured and assigned to a country in the **Country** field in the **Harbor Setup** screen. The information is needed in the Country of Arrival request file for EES to validate the reservation's first and last port of entry into EU Country, and determine if it requires a double entry visa.

1. From the **Administration** menu, select **System Setup** then the **Harbor Setup**
2. Select the **Harbor** and define the country in the **Country** field
3. Click **Apply** to save the change. This will append the selected country code and description to the **Comments** field

Note

Do not manually edit or change the country code from the **Comment field**. Doing so will create an incorrect country code and causes the generation of the EES request to fail. Any changes to the country code should be done from the Country field itself.

New User Definable Security Alert Setup

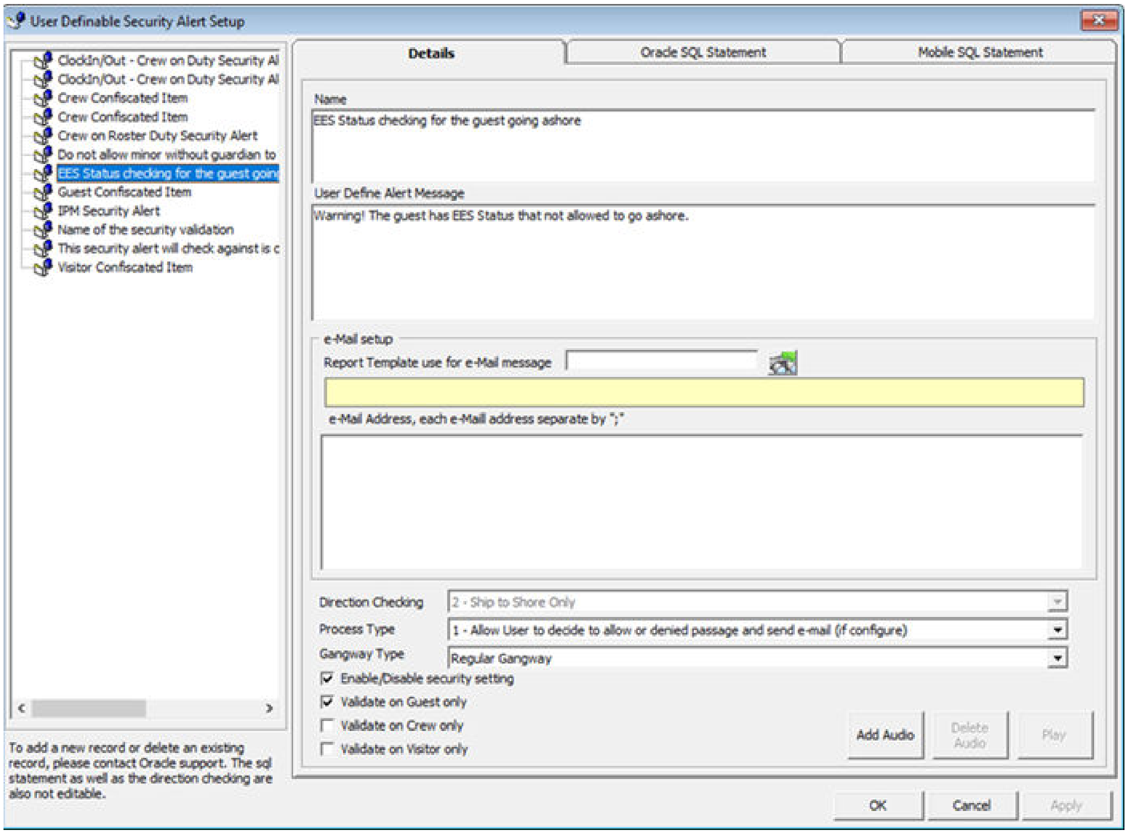
In the **Administration, Security Setup, User Definable Security Alert Setup**, you will find the **EES Status checking for the guest going ashore**, allowing you to configure an alert for use in the Gangway Security module.

Once setup, the security alert will check the arrival guest's harbor country for the following European countries:

- AX - Åland Islands
- AT – Austria
- BE – Belgium
- BG – Bulgaria
- IC - Canary Islands
- HR – Croatia
- CY – Cyprus
- CZ - Czech Republic
- DK – Denmark
- EE – Estonia
- FI – Finland
- FR – France
- GF - French Guiana
- DE – Germany
- GI – Gibraltar
- GR – Greece
- GP – Guadeloupe
- HU – Hungary
- IE – Ireland
- IT – Italy
- LV – Latvia
- LT – Lithuania
- LU – Luxembourg
- MT – Malta
- MQ – Martinique
- YT – Mayotte
- NL – Netherlands

- PL – Poland
- PT – Portugal
- RE – Réunion
- RO – Romania
- MF - Saint Martin (French Part)
- SK - Slovakia (Slovak Republic)
- SI – Slovenia
- ES – Spain
- SE - Sweden

Figure 7-1 User Definable Security Alert Setup



User Definable Security Alert Setup

- ClockIn/Out - Crew on Duty Security Al
- ClockIn/Out - Crew on Duty Security Al
- Crew Confiscated Item
- Crew Confiscated Item
- Crew on Roster Duty Security Alert
- Do not allow minor without guardian to
- EES Status checking for the guest going
- Guest Confiscated Item
- IPM Security Alert
- Name of the security validation
- This security alert will check against is c
- Visitor Confiscated Item

To add a new record or delete an existing record, please contact Oracle support. The sql statement as well as the direction checking are also not editable.

Name: EES Status checking for the guest going ashore

User Define Alert Message: Warning! The guest has EES Status that not allowed to go ashore.

e-Mail setup

Report Template use for e-Mail message:

e-Mail Address, each e-Mail address separate by ";"

Direction Checking: 2 - Ship to Shore Only

Process Type: 1 - Allow User to decide to allow or denied passage and send e-mail (if configure)

Gangway Type: Regular Gangway

☑ Enable/Disable security setting

☑ Validate on Guest only

☐ Validate on Crew only

☐ Validate on Visitor only

8 WPF Security Module

You will need to configure the same alert in WPF Security module for the guest movement from ship to ashore. This is only applicable to *Guest type*.

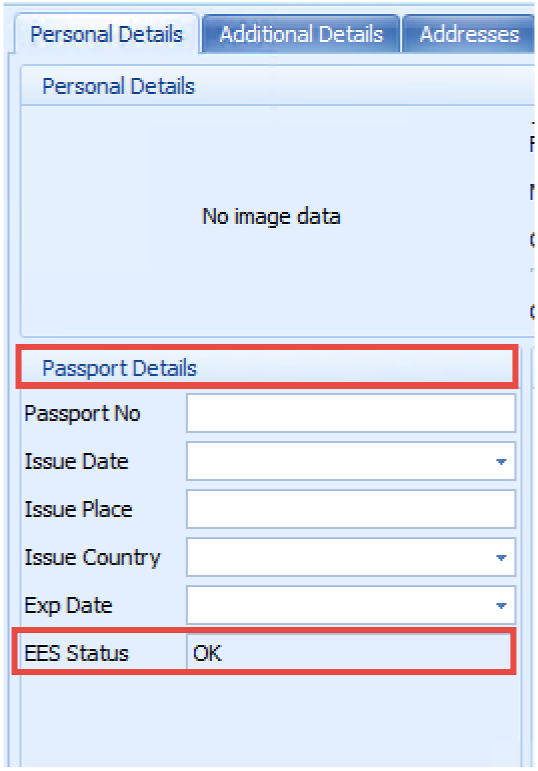
You are required to define the Arrival Harbor Country in **Administration module, System Cruise Setup**.

Once set up, an alert will be triggered when the guest’s EES response status is either NOK EES or NOKETIAS, and the Arrival Harbor Country matches the country defined in the security alert.

9 Advance Quick Check In Module

A new field EES Status is added to Advance Quick Check In (from SPMS v20.3 and above) and you will find it in Passport Details section. You can customize to have the field appear in different tabs using the drag and drop action and this would require the parameter **Quick Check in, Customize QCI** enabled.

Figure 9-1 Advance Quick Check In



Passport No

Issue Date

Issue Place

Issue Country

Exp Date

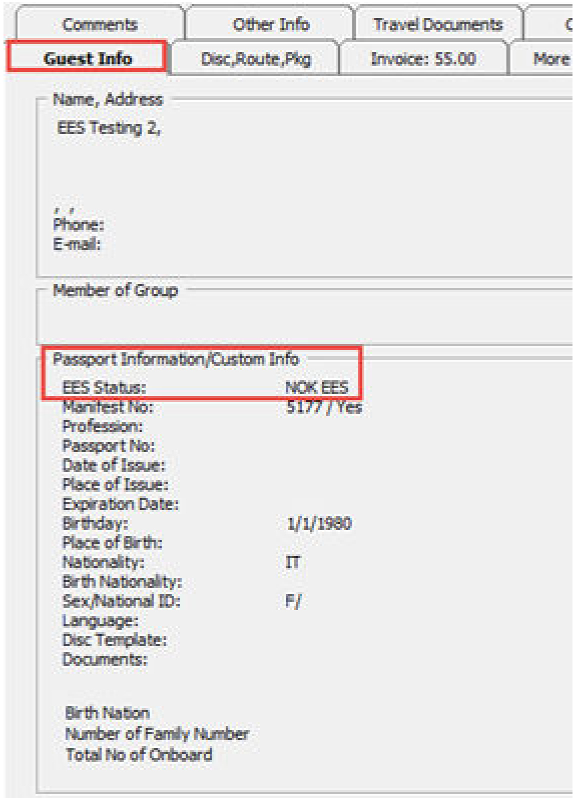
EES Status OK

10

Management Module

Like Advance Quick Check In, a new field is also added in Management module, Cashier, Guest Handling (from SPMS v20.3 and above). This field is located at the **Guest Info** tab, and under the **Passport Information/Custom Info** section and is a view only mode, showing the response status received from EES.

This field is also available in **Expected, Check-In, Check-Out, Cancelled and No-Show** tabs.



Name, Address

EES Testing 2,

, ,
Phone:
E-mail:

Member of Group

Passport Information/Custom Info

EES Status:	NOK EES
Manifest No:	5177 / Yes
Profession:	
Passport No:	
Date of Issue:	
Place of Issue:	
Expiration Date:	
Birthday:	1/1/1980
Place of Birth:	
Nationality:	IT
Birth Nationality:	
Sex/National ID:	F/
Language:	
Disc Template:	
Documents:	

Birth Nation
Number of Family Number
Total No of Onboard

You can also add the EES Status field in `Guest Info.html` for the status to display.