Oracle® Hospitality Cruise Shipboard Property Management System

Entry/Exit System Installation and Configuration Guide

Release 23.0.1

F79496-03

September 2023

ORACLE®

Oracle Hospitality Cruise Shipboard Property Management System Entry/Exit System Installation and Configuration Guide, Release 23.0.1

F79496-03

Contents

6 Processing Response File

7 Managing EES Response Status

8 Administration Module

9 Advance Quick Check In Module

10 Management Module

11 WPF Security Module

Preface

The Entry/Exit System (EES) is a measure implemented by the European Union (EU) to register entry, exit and refuse entries of non-EU nationals crossing the external borders of EU Member States to strengthen and protect the external borders of the Schengen area.

Purpose

This document provides instructions on how to install and configure the EES on Oracle Hospitality Cruise Shipboard System.

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
April 2023	Initial publication.
August 2023	Updated new customer portal.
	Added annotation to Step 3: Install Cruise Border Control
	Added topics to Administration module

Table 1   (Cont.) Revision History

Date	Description of Change
September 2023	Removed Key Store File Path note and Shutdown Port note.

1

Prerequisite and Compatibility

This section describes the minimum requirement to operate the Entry/Exit System (EES) On-Premise.

Prerequisite

Before you begin, see the Cruise SPMS Installation Guides 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

Compatibility

SPMS version 20.1.3, 20.2.4 and 20.3.2.1 or later.

2

Installing Cruise SPMS 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:
  - 20.1.3 if the SPMS 20.1.x is installed or
  - 20.2.4 if SPMS 20.2.x is installed or
  - 20.3.2.1 if the SPMS 20.3.x is installed.
  - If you are running a lower version, 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.
- A tool for generating certificates. As an example, this document uses a custom tool for our internal team to generate Json web Key(JWK). Other tools are available. We recommend that you select a tool that suits your security requirements. Whichever tool you use, ensure that it is virus scanned and virus-free, up to date, and patch with the latest security fixes. Otherwise, you could compromise your environment.
- The API and Web application access uses a Secure Socket Layer and Transport Layer Security (SSL/TSL) 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 "`-alias server -keyalg RSA - keysize 2048`"
- The minimum PowerShell version required is 5.1.
- 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.
- Ensure that the 'Path' in the 'System Variable' (Environment variable) is entered like the following example: '`%SYSTEMROOT%\System32\WindowsPowerShell\v1.0\`'.

Preparing the Java Environment

Before you install the Cruise SPMS Border Control Version 23.0 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 select **Edit** to edit the system environment variable.

---

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 then select **Edit** to edit the system environment variable.

2. Click the **Environment Variables** button.

3. Find the 'Path' from the System Variable and click Edit then select **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

Step 1: Create the Java Keystore for Cruise SPMS Border Control API/Apps Server

Background

Java Keystore is required to store private keys and certificates used by the Cruise SPMS Border Control Version 23.0 API/Web App. A Java's Keytool is used to create a Java Keystore. Java's Keytool 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 SPMS Border Control API/Web app is not recommended for the production environment. It

increases the risk of an unscrupulous party impersonating the Cruise SPMS Border Control API/Web App to steal sensitive information. However, for limited, non- production testing of Cruise SPMS Border Control API/Web app, you could use a self- signed certificate despite the increased security risk. However, do so at your own risk: 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 server -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. When using a Domain wildcard certificate, do not include the asterisk (*) character in the SITE_NAME as the asterisk (*) character is not a valid Keytool command character. The command will generate the Keystore with the public and private key pair and a self-signed certificate for the server.

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 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 server -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. The CSR will manifest itself as an output file based on the Certificate Info you entered earlier. You will also need to enter the Keystore password to proceed.

4. The CSR output file is in the same current 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, make sure the certificate chain is in appropriate format 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 server -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.
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.

Step 2: Create the Key Pair for Cruise SPMS Border Control API Authentication

Background

OAuth 2.0 is the user authorization mechanism used by Cruise SPMS 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 checksums 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..."
        }
    ]
```

Step 3: Install Cruise 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, manually remove or disable the features that you do not need after the installation.

The installation requires the user performing the installation to have Administrator privileges.

Installing Cruise Border Control 23.0

1. Log in as a Microsoft Windows Administrative user.

2. Start the installation program by right-clicking the **Cruise Border Control 23.0.0.0.exe** and select **Run as Administrator**.

Figure 2-1   Cruise Border Control Installation Wizard Long Path Enablement
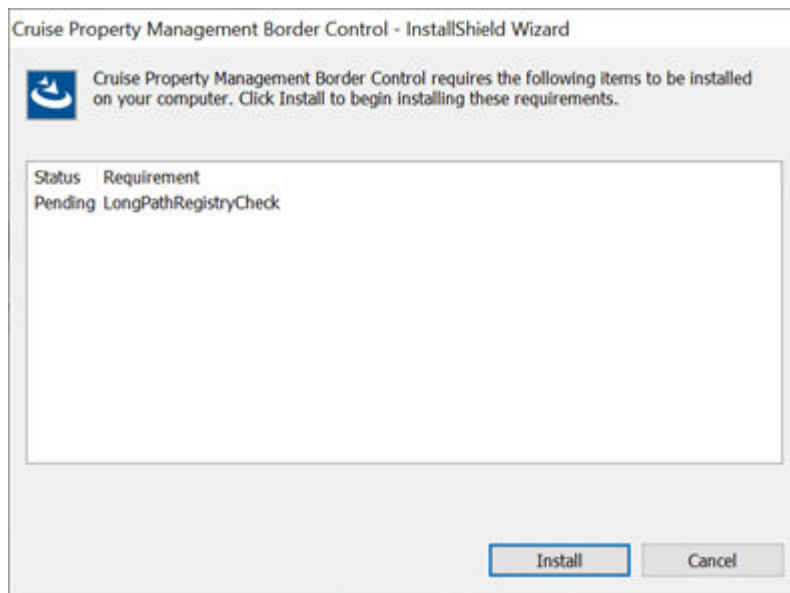
3. Click **Install** to apply the LongPathRegistryCheck to enable Long Paths setting in the registry. At the prompt continue by clicking '**Yes**' and a message is shown if the change is applied to the registry is successfully or not. This setting is required for a successful 23.0 install. By default, Windows only support file path length of 260 characters and this setting allow windows to support beyond 260 characters.

Figure 2-2   SPMS Platform Property Management Installation Wizard — Welcome Page
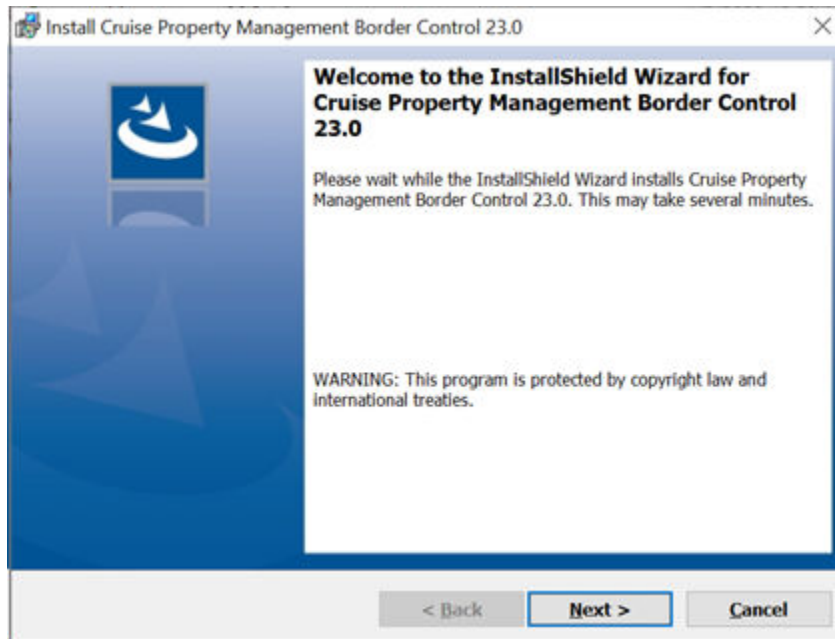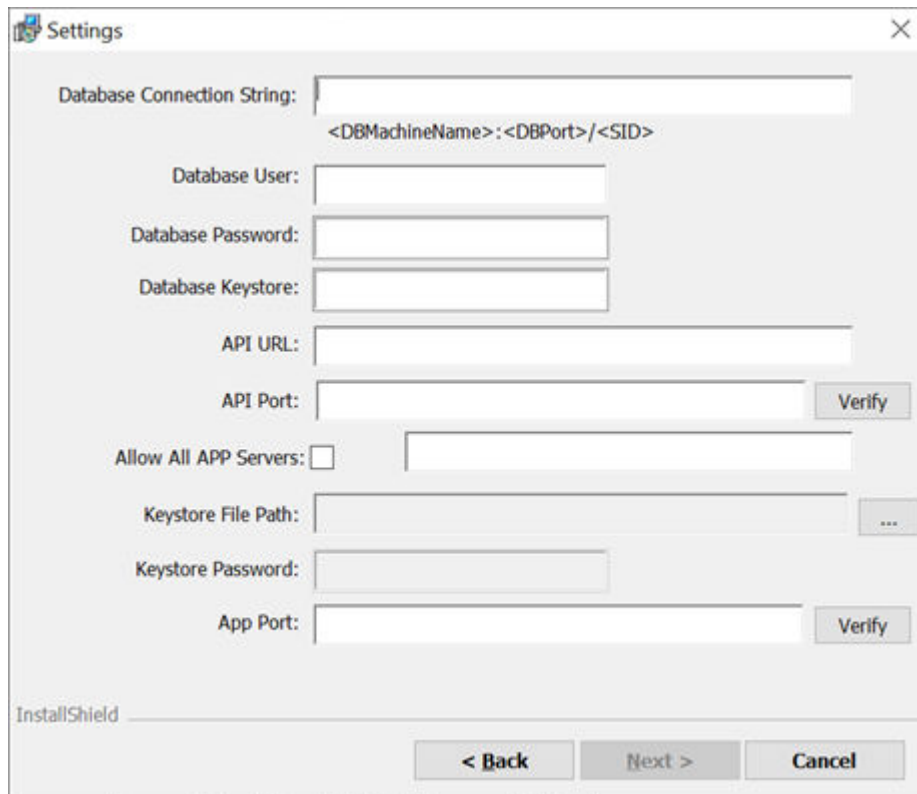
4. Click **Next** and navigate to the "Custom Setup" window. If you want to perform a custom installation, select the option to set the feature as "This feature will not be available". The default folder to install has changed from "`C:\Oracle Hospitality Cruise\`"

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

5. To grant the folder permission,

   - Access the Properties dialog box.

   - Select the **Security** tab.

   - Click **Edit**.

   - In the Group or user name section, select the user(s) you wish to set **permissions** for.

   - In the Permissions section, use the check boxes to select the appropriate **permission level**.

   - Click **Apply**.

   - Click **OK**.

Figure 2-3   Cruise Border Control Installation Wizard- Custom Setup
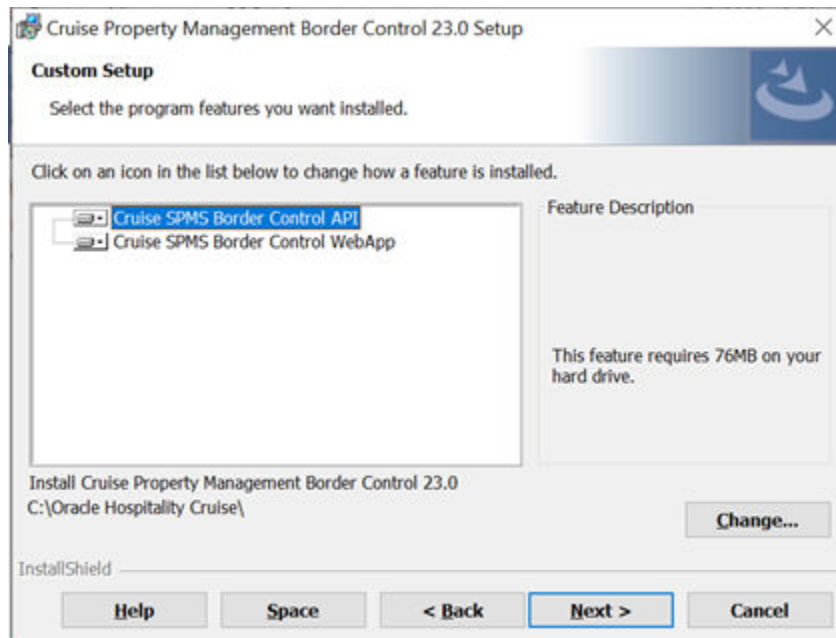
6. Click **Next** to update the settings window for the fields below:

   - **Database connection String**: `<DBMachineName>:<DBPort>/<SID>`

   - **Database User:** DB Password.

   - **Database Keystore:** DB Keystore's password for database encryption. Minimum password length is 8 characters.

   - **API URL:** API Server's URL.

   - **API Port:** API Server's port. If you need to install multiple instances of the Border Control API, enter the ports in comma separated format. By default, the Install shield populates ports 7543, 8543. If these ports are unavailable or used, you need to choose an unused port for the installation. The verify button to the right checks and displays a message if any of the entered ports are used for other applications or processes.

   - **Allow All APP Servers:** Server machines with APP installed that are allowed to access the API, ***** meaning all the servers are allowed.

   - **Keystore File Path:** Keystore file path which contain .JKS file extension. See below note.

   - **Keystore password:** Keystore password.

   - **App Port:** Web App port. If you need to install multiple instances of Border Control Web App, enter the ports in comma separated format. By default, Install shield populates port 7190, 8190. If these ports are unavailable or used, you need to choose an unused port for the installation. The verify button to the right checks and displays a message if any of the entered ports are used for other applications or processes. Use the command "**netstat -ano -p tcp**" at the command line to view the tcp ports in use by different applications

Figure 2-4   Cruise Border Control Installation Settings

7. When the option **Allow All APP Servers** is checked, the message box above shall prompt, alerting the user of the chosen option.

Figure 2-5   Allow All APP Servers Notification
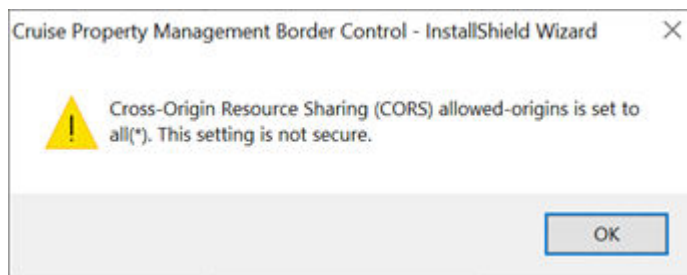
8. Click **Next** to update the OAuth Configuration settings for the fields below:

    • **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 **Install** to begin installation.

> **✏ Note:**
>
> For a better end user experience, at the end of the installation a config.txt file containing all the configurations, excluding the passwords is created and added to folder `UserProfile/AppData/Local/Oracle Hospitality Cruise`. This file is reloaded on upgrade/re-install, so that end user does not have to re-enter the configuration

10. During the install, a couple of PowerShell windows will launch and closed automatically.

11. API's configuration is stored in the `application.properties` file.

12. At the end of the installation, the system creates two (2) new Windows Services and they are **Oracle Hospitality Cruise SPMS Border Control WebApp** and **Oracle Hospitality Cruise SPMS Border Control API**.

Figure 2-6   Cruise SPMS Border Control Window Services

Oracle Hospitality Cruise SPMS Border Control API : 7543	Cruise SPMS Border Control API service	Running
Oracle Hospitality Cruise SPMS Border Control WebApp : 7190	Cruise SPMS Border Control Web Application	Running

13. The system will also create three (3) sub-folders under `Oracle Hospitality Cruise\Cruise SPMS Border Control\v23.0` – 'API', 'WebApp' and 'Scripts'.

Uninstalling Cruise SPMS Border Control 23.0

1. Start the installation program by right-clicking the Cruise Property Management Border Control 23.0.0.0.exe and select **Run as Administrator**. If 23.0 is already installed, the Setup starts in Maintenance mode, allowing you to reinstall.

2. Select the available option and wait until uninstall is complete. In the case of Reinstall, follow the prompts presented to uninstall and install.

3. The system removes the following:

   a. From the `Oracle Hospitality Cruise\Cruise SPMS Border Control\v23.0` folder: API', 'WebApp' and 'Scripts' folders.

   b. **Windows Services:** Oracle Hospitality Cruise SPMS Border Control API and Oracle Hospitality Cruise SPMS Border Control WebApp.

SPMS Platform for High Availability (HA)

To set up a High Availably environment for Cruise Border Control API and the associated web applications, Oracle recommends:

- Running multiple instances of API Services on the same server (to protect against failure of a single instance on that server).

- Running multiple instances of the Web Application on the same server (to protect against failure of a single instance on that server).

- Setup of multiple servers with the same configurations as 1 and 2 (to protect against a single server failing).

- Use a High Availability (HA) Oracle database environment (such as Oracle RAC).

- Provide multiple instances of the load balancer and connect them together through technology like the Virtual Router Redundancy Protocol (VRRP).
- Route all requests between the browser and the API through the load balancers.
- Route all requests between the browser and the administration/mobile app through the load balancers.
- Set up rate limiting on the load balancer to prevent Distributed Denial of Service (DDOS) attacks.

> **Important:**
>
> Before you change any of the Database Encryption Key/Password and if you have Cruise Border Control REST API Server installed, you *must* uninstall and then reinstall the application after the password change.

3
Getting Started

As a prerequisite, the European Travel Information and Authorisation System (ETIAS) will undergo a detailed checked of each applicant to determine whether they can be allowed to enter any Schengen Zone country. Therefore, ships must submit their passengers/guests list for verification before they are allowed to depart from the harbor, and the Entry/Exit System (EES) is used for the purpose to generate the EES data file for submission, either manually or uploaded to an application provided by EES. Once EES processed the application file and generate a response file, you are required to upload the response file data and update the passengers/guest's ETIAS status into SPMS using EES module

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 URL for the application.

3. At the login page, sign in with your user name and password.

Log in to the application

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

> ✎ **Note:**
>
> The user name and password 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 number of minutes is based the value defined in the parameter **Lockout Minutes**.

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

3. Upon successful login, your user name and profile picture is displayed 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. If the user account does not have permission to the application, you will get a page error **Permission is required to view this application**

4

Setting Up EES

The Entry/Exit (EES) application setup page allows you to configure nationality group and travel document types to exclude that are needed by EES system.

Figure 4-1   EES Setup
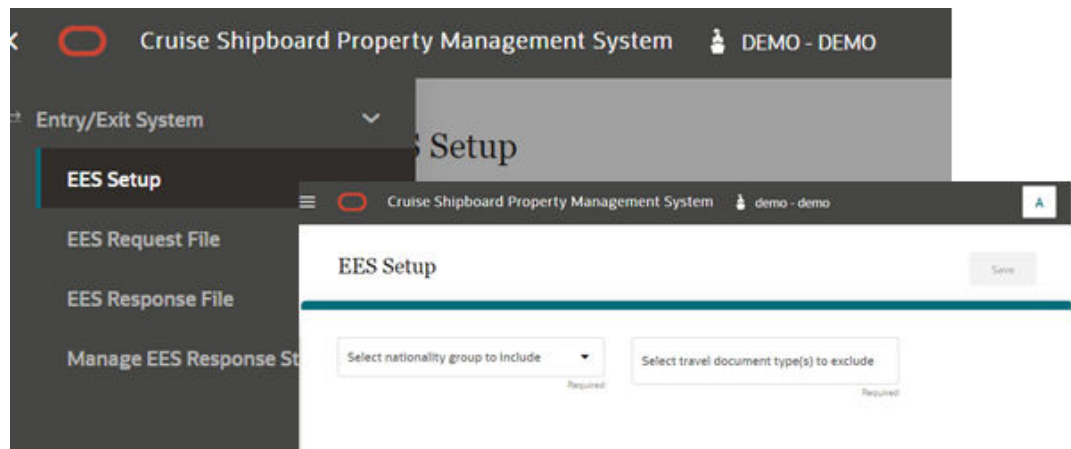
Configure EES Setup Details

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. Select 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. Select **Save** button to update the change. A confirmation message 'Setup Completed' will appear.

5

Generating Request File

The EES Request File page allows you to view previously generated request files, and an option to create a new request file for submission to the EES system for guest manifest verification.

Figure 5-1   EES Request File Page
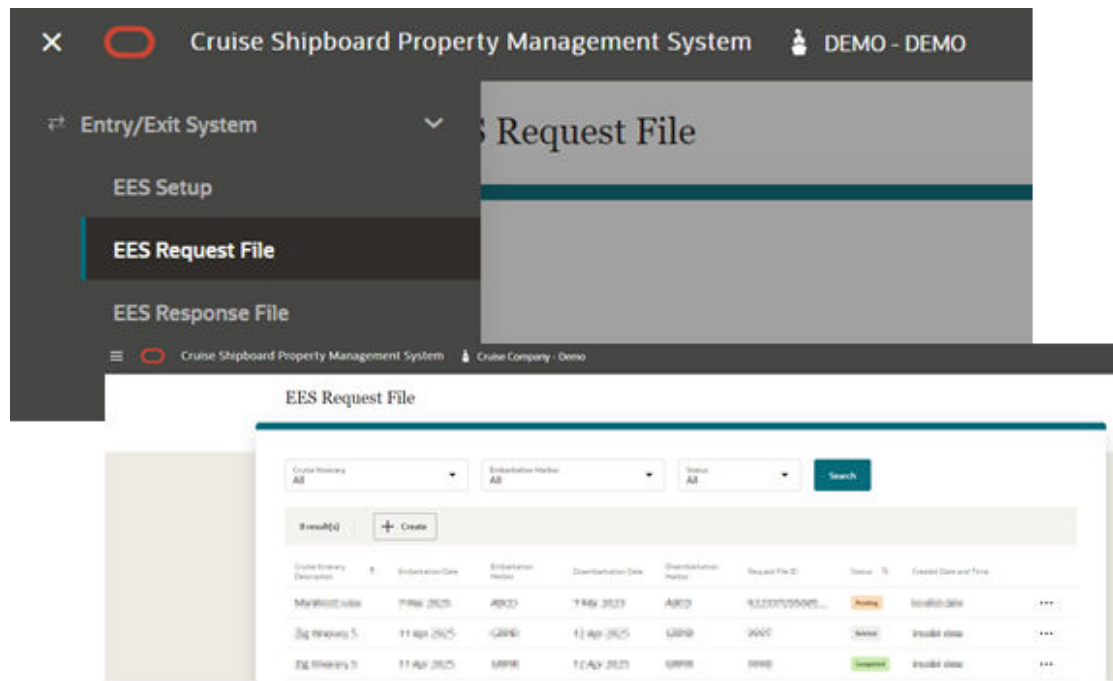
In the EES Request File page, all the records of previously generated EES request files are shown. You can search a record using one of the search filters - cruise itinerary, embarkation harbor and request file status.

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
- **Delete:** Only applicable for status that is Pending

Creating Request File

1. From the Navigation Menu, select **Entry/Exit System** then the **EES Request File**.
2. Select **Create** button to open the Create Request File page.

3. At the Create Request File screen, the guest manifest listing will populate based on below selection criteria:

    • **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 Date, Disembarkation Date, Disembarkation Harbor and Disembarkation Time. Modification on these fields is not allowed as it is based on the selected Embarkation Harbor.

5. Select the **Process** button and the system will retrieve listing of the guest manifest records that meet the selected criteria. The record shown would only consist of checked in reservation status and the actual embarkation date that matches the embarkation harbor date.

6. You can also search the guest record by entering these keywords: a surname, given name, stateroom number or folio number.

7. A guest data is deemed as an error and highlighted in red if the guest 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 manifest guest data list has an error. You need to correct all the erroneous guest data in SPMS Legacy, and then refresh the guest manifest by selecting the **Process** button. If there's no error in the reloaded guest data, the **Generate** button become enabled. You can also enable the button by deleting the erroneous data from the manifest, and then selecting the **Ellipsis** button followed by the **Delete** button.

9. Select the **Generate** button to generate the csv file. The filename format is 'EESReqYYMMDDHHMM00', in which the YYMMDDHHMM00 is appended after the generated Request File ID "EESReq".

10. The generated EES request file is saved into the user defined browser download location.

Deleting Request File

1. On the EES Request File Listing page, select the request file record to delete and then the **Ellipsis** button.

2. Select **Delete** button. At the confirmation message 'Delete EES request?', selecting **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 guest manifest in this Request File is auto flagged as deleted too. To regenerate, see topic *Create EES 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. Select **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-create the same EES Request File with the exact data from the selected File ID. This option is only available when the EES request file status is pending, and disabled if the status is completed or deleted.

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. Select **Re-generate** to open the View Request File page and then the **Re-generate File** button to proceed.

6

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. Select **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. Select the **X** icon to remove unwanted response files.

5. The **Process** button is enabled once the response file is uploaded. Select the **Process** button to proceed and a dialog box with message 'Processing of file(s) may take some time" appears. Selecting **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.

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. Selecting the **Search** button will bring up all the EES response file records that match 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. Select **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 guest details records with EES status.

7

Managing EES Response Status

This module allows you to perform a search on processed guest records in EES response file. The **Delete** option is enabled for guest records that has "Not OK EES" or "Not OK ETIAS" status, and is disabled for guest records that has with "OK" and "NA" status.

Searching for Guest Records

1. From the Navigation Menu, select **EES Entry/Exit System**, and then **Manage EES Response Status**.

2. Perform search for guest record using search filters Cruise itinerary, Embarkation Harbor, EES Response Status, First Name, Last Name, Stateroom or Folio Number.

3. Select **Search** button. The guest records that matching the search criteria appear on Manage EES Response Status listing.

Deleting Guest Record

1. On the Manage EES Response Status Listing page, select guest record with response status "Not OK EES" or "Not OK ETIAS" that you want to delete and click the **Ellipsis** button.

2. Select **Delete** button. A confirmation message 'Delete [Last Name][First Name] from the EES verification? Deleting this guest record, the guest EES Status will be removed.' will appear.

3. Selecting the **Cancel** button will close the dialog box and the **Delete** button will proceed to remove this guest record from the listing.

4. Select **Delete** button. A confirmation message **Record Deleted** appear and removes the selected guest records from the listing.

8
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 the mouse 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 Arrival Port with Arrival Country

1. Each of the arrival ports defined in the cruise itinerary would need to define the arrival country, as this is part of the required fields needed by the EES request file and the new user definable security alert setup "**EES Status checking for the guest going ashore**".
2. From the Administration Menu, select **System Setup** then the **System Cruise Setup**.
3. Select the setup Cruise and expand the record for itinerary listing. Click on each itinerary record and define the country in the **Arrival Country** field.
4. Click **Apply** to save the change.

# 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**, enabling you to configure an alert for use in the Gangway Security module.

Once setup, the security alert will check on 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 8-1   User Definable Security Alert Setup

9
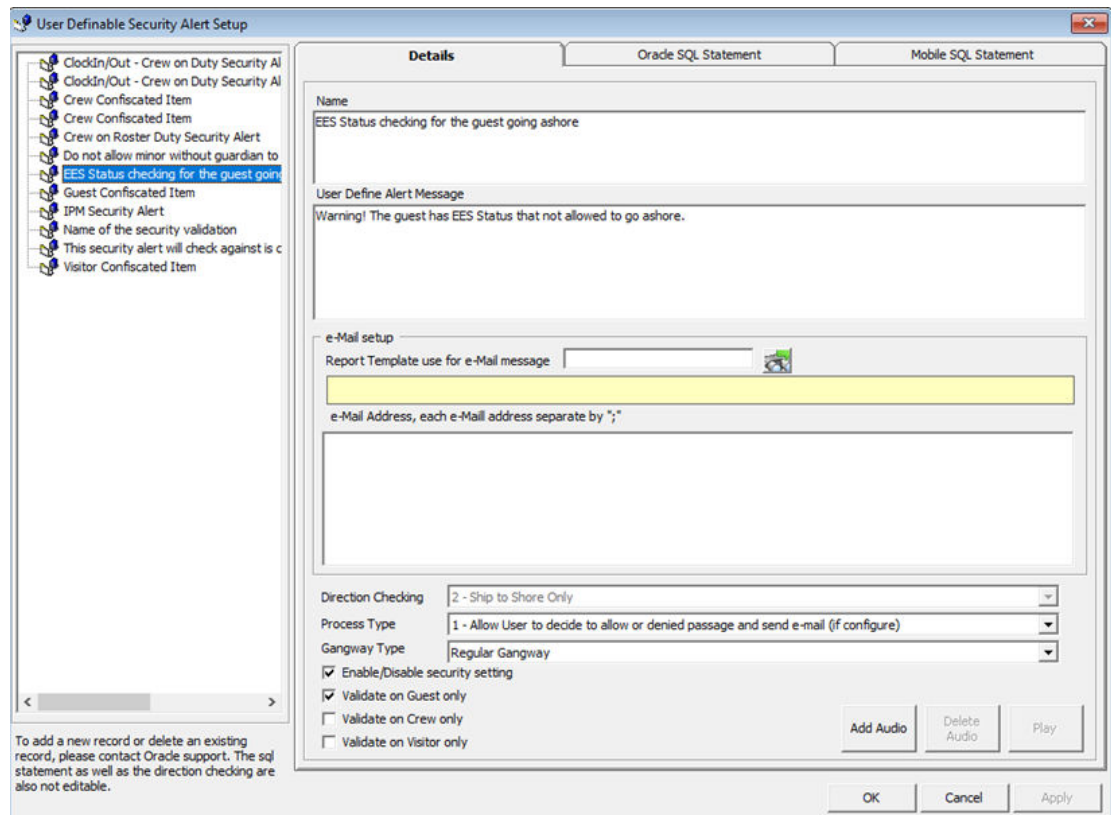
Advance Quick Check In Module

A new field EES Status is added in Advance Quick Check In and you will 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

10
Management Module

Like Advance Quick Check In, a new field is also added in Management module, Cashier, Guest Handling. This field is defaulted 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.

11

WPF Security Module

You will need to configure the same alert in WPF Security module for 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.