

**Oracle® Hospitality Cruise Materials  
Management System**

Security Web Service and Secure Server Tool  
Installer Guide  
Release 7.30.56x  
**F26282-01**

January 2020

---

Copyright © 2020, 2020, Oracle and/or its affiliates. All rights reserved.

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

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

If this software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

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

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

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

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

---

---

# Contents

<b>Figures.....</b>	<b>4</b>
<b>Preface.....</b>	<b>5</b>
Audience .....	5
Customer Support.....	5
Documentation.....	5
Revision History.....	5
<b>1 Prerequisite, Supported Systems and Compatibility .....</b>	<b>6</b>
Prerequisite.....	6
<b>2 Webservices Installation .....</b>	<b>7</b>
Registering XceedCry .....	7
Web Service Installation.....	7
Installing Web Service.....	7
Configure and Verify Web Service.....	9
Secure Server Tool Installation.....	10

---

---

# Figures

Figure 1 - DLL Registration .....	7
Figure 2 – Installation Failure Prompt.....	8
Figure 3 - Installation Selection Menu.....	8
Figure 4 - A Self Signed Certificate .....	8
Figure 5 – Upgrading Web Service .....	9
Figure 6 - Verification of Installation.....	10
Figure 7 - OHCMMSSecureServerTool Configuration Setting .....	11

---

---

# Preface

This document provides instructions on how to install Oracle Hospitality Cruise Material Management (MMS), MMS Security Web Service Installer and MMS Secure Tool Installer.

## Audience

This document is intended for installers, programmers, technical support teams, product specialists, and others who are responsible for setting up MMS.

## Customer Support

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

<https://support.oracle.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 and any associated log files
- Screen shots 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

Date	Description of Change
January 2020	<ul style="list-style-type: none"><li>• Initial publication for MMS Security Web Services and Tool Installer and Installation Guide</li></ul>

---

---

# 1 Prerequisite, Supported Systems and Compatibility

This section describes the minimum requirement for Web Services Installer.

## Prerequisite

- Internet Connection
- IIS Web Server
  - Operating System: Microsoft Windows 2012 R2 / Microsoft Windows 2016 Standard / Microsoft Windows 10
  - RAM: 16GB
  - Hard Disk Size: 512GB
- Local Administrator Access
- Latest MMS Net Setup.zip
- Microsoft Windows 10 with .NET Framework 4.5 enabled
- ODAC or Oracle Client [12.2.0.1.0] compatible with 32-bit system

---

---

## 2 Webservices Installation

The Web Service Installer (WS) is a batch file that automatically install and configure all the required Microsoft Windows features used by the Web Services component.

### Registering XceedCry

1. Download the latest MMS Net Setup.zip from the **Patches & Updates** on My Oracle Support.
2. Unzip the file into `c:\Temp` and navigate to `c:\temp\MMS Net Setup` folder.
3. Register XceedCry Dll Library to System GAC as follows,
  - Open the Command Prompt with Run as Administrator
  - Change the directory to the `C:\Temp\MMS Net Setup\Webserver\References` folder.
  - Run `REGSVR32` command to register the `xceedcry.dll` to the library

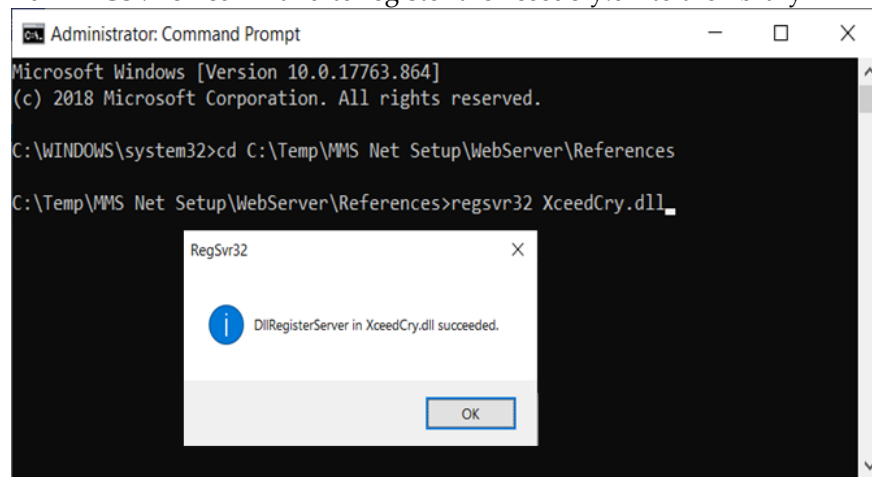


Figure 1 - DLL Registration

### Web Service Installation

This section describes the steps to install the web service components. We recommend to install this component on the machine where MMS database is installed.

#### Installing Web Service

This section describes the steps to install the OHCMMSSecurityWebService and other required Microsoft Windows components.

1. Navigate to `c:\temp\MMS Net Setup` folder.
2. Right-click the **Install.bat** and select **Run as Administrator** to launch the Microsoft Windows command screen.
  - When you try to run the batch file without an Administrator login, the system returns a failure prompt as shown below.

```

C:\Windows\system32\cmd.exe

C:\Temp\PDAService>ECHO OFF
Administrative permissions required. Detecting permissions...
Failure: Current permissions inadequate. Please run as admin.
Press any key to continue . . . _

```

Figure 2 – Installation Failure Prompt

- The system scans for an active Internet connection and prompt a selection menu once the connection is established. Otherwise, the installation will abort.

```

C:\WINDOWS\System32\cmd.exe

C:\WINDOWS\system32>ECHO OFF
Administrative permissions required. Detecting permissions...
Success: Administrative permissions confirmed.

-----
PRESS 1 to start your installation.
-----

1 - Install OHCMMSSecurityWebService and OHCMMSSecureServerTool

Type 1 then press ENTER:

```

Figure 3 - Installation Selection Menu

- Enter the option number and then press **ENTER** to begin the installation.
    - 1 - To install OHCMMSSecurityWebService and OHCMMSSecureServerTool
3. A Self Signed Certificate is required even though the Webserver have a certificate installed. This is to resolve the certification warning from prompting.
- At the Command prompt, enter '1' to list the existing certificates installed on the Web Server.
  - Once the certificate is listed and when prompted with "Please key in the subject name you want to bind", enter the **Subject name**.

```

Administrator: Windows PowerShell

Image Version: 6.3.9600.17031

Enabling feature(s)
[=====100.0%=====]
The operation completed successfully.
Finished NetFx3

Deployment Image Servicing and Management tool
Version: 6.3.9600.17031

Image Version: 6.3.9600.17031

Enabling feature(s)
[=====99.9%===== ]
The operation completed successfully.
Completed
Enabling MSDTC...
Completed
Creating app pool and assigning to website...
Configuring Website: Default Web Site
HTTPS Binding already exists on port ...
Please press 1 to list down existing certificate or press 2 to create new self signed certificate: 2
Please key in your domain name or ip: _

```

Figure 4 - A Self Signed Certificate



- Enter '2' to create a new self-signed certificate, then insert the domain name or IP at the prompt.
- If previous Webservices installation is found, you will be prompted to override the files. Continue by selecting **All**.

```

Completed.
Completed
Overwrite C:\inetpub\wwwroot\OHCMMSSecurityWebService\MMSSecureFunctions.asmx (Yes/No/All)? a
C:\Temp\MMS Net Setup\WebServer\OHCMMSSecurityWebService\MMSSecureFunctions.asmx
C:\Temp\MMS Net Setup\WebServer\OHCMMSSecurityWebService\PrecompiledApp.config
C:\Temp\MMS Net Setup\WebServer\OHCMMSSecurityWebService\Web.config
C:\Temp\MMS Net Setup\WebServer\OHCMMSSecurityWebService\bin\App_Code.compiled
C:\Temp\MMS Net Setup\WebServer\OHCMMSSecurityWebService\bin\App_Code.dll
C:\Temp\MMS Net Setup\WebServer\OHCMMSSecurityWebService\bin\App_global.asax.compiled
C:\Temp\MMS Net Setup\WebServer\OHCMMSSecurityWebService\bin\App_global.asax.dll
C:\Temp\MMS Net Setup\WebServer\OHCMMSSecurityWebService\bin\MMSWebServicesLibrary.dll
C:\Temp\MMS Net Setup\WebServer\OHCMMSSecurityWebService\bin\MMSWebServicesLibrary.XmlSerializers.dll
9 File(s) copied
Assigning Permission to PAR file Folder...
Completed

Restarting IIS now...

Attempting stop...
Internet services successfully stopped
Attempting start...

```

**Figure 5 – Upgrading Web Service**

4. When the web service installation completes, the batch setup will place the OHC MMS Secure Server Tool into specified location "\\Program Files (x86)\Oracle Hospitality Cruise\" with upgradation to existing tool if any.
5. When the installation completes, press any key to close the command window.

## Configure and Verify Web Service

This section describes the steps to add the required settings to the web.config file for OHCMMSSecurityWebService.

### Configure Web.Config File

1. Browse to location C:\inetpub\wwwroot\OHCMMSSecurityWebService folder.
2. Open web.config file with notepad and add path of tnsnames.ora file as value in <appSettings> section and add tnsname of the database to be connected as datasource in <connectionSettings> section of web.config file.

```

<appSettings>
  <add key="TNSNamesPath" value="" />
</appSettings>
<connectionStrings>
  <add name="OracleDBServer" connectionString="Data Source=;User ID={0};Connection Lifetime=10;Connection Timeout=5;Min Pool Size=0;Max Pool Size=1;Pooling=false" providerName="System.Data.OracleClient"/>
</connectionStrings>

```

---

## Verifying an Installation Status

Launch the Internet Explorer and enter below link to verify the installation <https://localhost/OHCMMSecurityWebService/MMSecureFunctions.aspx>

When the installation is successful, the system returns the same browser message, similar to below screen.

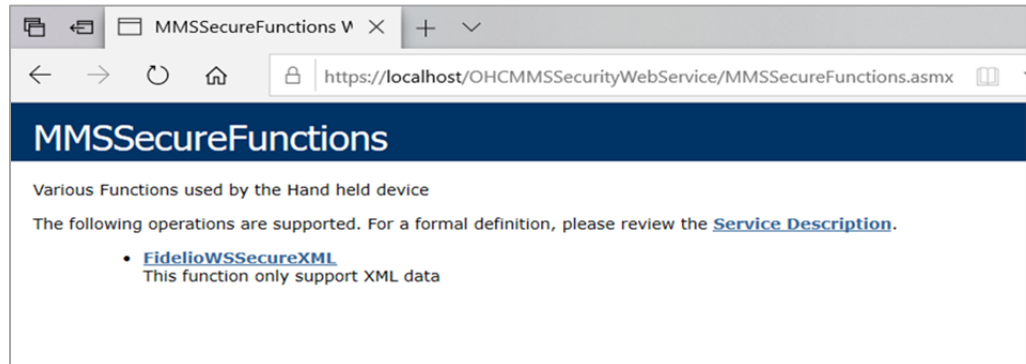


Figure 6 - Verification of Installation.

## Secure Server Tool Installation

This section describes the steps to install the OHCMMSecureServerTool and to the add required settings.

### Adding Settings to Configuration File and Executing Secure Server User Interface.

1. Browse to C:\Program Files (x86)\Oracle Hospitality Cruise\OHCMMSecureServerTool folder
2. Open file OHC MMS Secure Server.exe.config with notepad and add the file of tnsnames.ora and add tnsname of the database to be connected as value in <appSettings> section of the configuration file.

```
OHC MMS Secure Server Tool.exe.config - Notepad
File Edit Format View Help
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
  <configSections>
    <sectionGroup name="applicationSettings" type="System.Configuration.ApplicationSettingsGroup, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" />
    <section name="MMS_Secure_Server_Tester.My.MySettings" type="System.Configuration.ClientSettingsSection" />
  </configSections>
  <startup>
    <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5" />
  </startup>
  <!--
  <appSettings>
    <add key="TNSNamesPath" value="Location or path of file tnsnames.ora" />
    <add key="TNSName" value="Tnsname of datasource" />
  </appSettings>
  <applicationSettings>
    <MMS_Secure_Server_Tester.My.MySettings>
      <setting name="MMS_Secure_Server_Tester_oSecurityService_MMSSecureFunctions"
        serializeAs="String">
        <value>Web address or url of OHCMMSSecurityWebService</value>
      </setting>
    </MMS_Secure_Server_Tester.My.MySettings>
  </applicationSettings>
  -->
  <appSettings>
    <add key="TNSNamesPath" value="" />
    <add key="TNSName" value="" />
  </appSettings>
  <applicationSettings>
    <MMS_Secure_Server_Tester.My.MySettings>
      <setting name="MMS_Secure_Server_Tester_oSecurityService_MMSSecureFunctions"
        serializeAs="String">
        <value>https://localhost/OHCMMSSecurityWebService</value>
      </setting>
    </MMS_Secure_Server_Tester.My.MySettings>
  </applicationSettings>
</configuration>
```

**Figure 7 - OHCMMSSecureServerTool Configuration Setting**

3. Run **OHC MMS Secure Server.exe** as “Run as Administrator” option.
4. At the OHC MMS Secure Server Tool login window, enter the **Database Password, User and User Password** in the fields provided then click the **Set** button.

### Accessing MMS Launch Panel

MMS client will connect to database using those credentials and stores the Encryption Key and password in Encrypted form in Windows Registry.

1. Access MMS Launch Panel
2. Enter the login credentials and click **Login**.
3. Enter a Security Service URL when prompt and click **OK**.
4. Upon next login, the MMS client will first connect using the Windows Registry value, if successful then MMS Launch Panel will open, if failed then again Application will return a Security service to get the password.