Oracle[®] Hospitality Hotel Mobile OPERA Web Services Server Installation Guide Release 1.4.3.0 (1.43) **F17753-02**

March 2020



Copyright © 2016, 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 errorfree. 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 on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Contents

1	Preface	4
	Audience	4
	Customer Support	4
	Documentation	4
	Revision History	4
2	Prerequisites	5
3	Configuring Microsoft .NET Frameworks	6
	Verifying Microsoft .NET Frameworks	6
	Installing Microsoft .NET Frameworks	6
4	Configuring Transport Layer Security	7
	Verifying TLS	7
	Enabling TLS	9
5	Configuring Internet Information Services	. 11
	Verifying IIS	11
	Installing IIS	13
6	Generating the SSL Certificate Request	. 16
7	Installing the SSL Certificate	. 20
	Intermediate Certificate	21
8	SSL Bindings	. 24

1 Preface

This document explains how to install and configure OPERA Web Services server components for Oracle Hospitality Hotel Mobile.

Audience

This document is intended for system administrators, support personnel, and users familiar with Oracle Hospitality Hotel Mobile.

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
- 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	
May 2017	Initial publication	
September 2018	• Part number and date revision.	
December 2018	• Part number and date revision.	
March 2020	• Revised for the hotel mobile 1.4.3 release	

2 **Prerequisites**

Verify that the OPERA Web Services host computer has Microsoft Windows Server 2012 or higher. If the server does not have Internet access, use the Microsoft Windows installation CD to install the operating system.

3 Configuring Microsoft .NET Frameworks

Verify that the OPERA Web Services server has Microsoft .NET Frameworks 4.5 and 4.6.1. If the server does not have the frameworks, install them.

Verifying Microsoft .NET Frameworks

Follow these steps to check the server registry for Microsoft .NET Frameworks 4.5 and 4.6.1:

- 1. Log in to the OPERA Web Services server.
- 2. Select **Run** on the **Start menu**.
- 3. In the Open box, enter **regedit.exe**. You need administrative credentials to run regedit.exe.
- 4. In the Registry Editor, open the following subkey:

HKEY_LOCAL_MACHINE -> SOFTWARE -> Microsoft -> NET Framework Setup> NDP -> v4 -> Full

The path to the full subkey includes the subkeys (**Net Framework**) and (**.NET Framework**). The right subkey is **Net Framework Setup**.



5. Check for a DWORD value of **Release**. The **Data** column indicates which version of the .NET Framework is installed. The following URL provides more information on installed versions: https://support.microsoft.com/en-gb/help/318785/how-to-determine-which-versions-and-service-pack-levels-of-the-microsoft-.net-framework-are-installed.

Installing Microsoft .NET Frameworks

If one or both .Net 4.5 and 4.6.1 frameworks are not installed, download the frameworks from: https://www.microsoft.com/download. Run the .exe on each file as an administrator to install and follow the prompts on the screen to compete installation.

4 Configuring Transport Layer Security

The OPERA Web Services server uses Transport Layer Security (TLS) to secure connections between servers and web browsers. By default, TLS is not enabled on Microsoft Windows Server 2008 R2 servers.

Verifying TLS

Follow these steps to verify TLS 1.2 is enabled on the server:

- 1. Start the registry editor by clicking on Start and Run. Type in regedit into the Run field.
- Browse to the following registry key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHA NNEL\Protocols



- 3. Expand the **Protocols** folder, and then expand the **TLS 1.2** folder.
- 4. Within the **Client** and **Server** folders, there are **DisabaledByDefault** and **Enabled** DWORD keys.

🕵 Registry Editor				
File Edit View Favorites Help				
Cleint	Name ab (Defaul Disable Enabled	Type REG_SZ dByDefault REG_DWORD d REG_DWORD	Data (value not set) 0×00000000 (0) 0×00000001 (1)	

5. Right-click and select **Modify** on each **DisabledByDefault** DWORD Key under both **Client** and **Server** folders, and then verify that the **Value** data field is set to **0** and the **Base** is **Hexadecimal**.

Edit DWORD (32-bit) Value	×
Value name:	
DisabledByDefault	
Value data:	Base
	Hexadecimal
	O Decimal
	OK Cancel

6. Right-click and select **Modify** on each **Enabled** DWORD Key under both **Client** and **Server** folders, and then ensure that the **Value** data field is set to **1** and the **Base** is **Hexadecimal**.

Edit DWORD (32-bit) Value		×
Value name: Enabled		_
Value data: 1	Base Hexadecimal Decimal	
	OK Cancel	

Enabling TLS

If TLS 1.2 is not enabled, follow these steps:

- 1. Start the registry editor by clicking on **Start** and **Run**. Type in **regedit** into the **Run** field.
- 2. Select **Computer** at the top of the registry tree. Backup the registry by selecting **File** and then **Export**. Select the location for the backup registry file.



3. Browse to the following registry key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHA NNEL\Protocols

📄 🚽 SecurityProviders	1
SaslProfiles	
Ciphers	
CipherSuites	
KeyExchangeAlgorithms	
🖻 📲 Protocols	
😟 🕀 🔂 😥 😥	

4. Right-click the **Protocols** folder, select **New**, and then select **Key**. This creates a folder. Rename the folder to **TLS 1.2**.



5. Right-click the **TLS 1.2** key, and then add two new keys.



6. Rename the two new keys to **Client** and **Server**.



- 7. Right-click the **Client** key, select **New**, and then select **DWORD** (32-bit) Value from the dropdown list.
- 8. Rename the **DWORD** to **DisabledByDefault**.
- 9. Right-click the name **DisabledByDefault** and select **Modify**.
- 10. Ensure that the **Value** data field is set to **0** and the **Base** is **Hexadecimal**, and then click **OK**.
- 11. Create another **DWORD** for the **Client** key as you did in **Step 7**.
- 12. Rename this second DWORD to Enabled.
- 13. Right-click **Enabled**, and then select **Modify**.
- 14. Ensure that the **Value** data field is set to **1** and the **Base** is **Hexadecimal**, and then click **OK**.
- 15. Repeat steps **7** to **14** for the **Server** key (by creating two DWORDs, **DisabledByDefault** and **Enabled**, and their values underneath the **Server** key).
- 16. Reboot the server.

If you make a mistake or run into issues, revert to your previous registry settings by opening the Registry Editor and importing the backup file you made in step 2.

5 Configuring Internet Information Services

Verifying IIS

Follow these steps to verify that IIS 7 is installed on the server :

1. Open a web browser and go to http://localhost/. If ISS is installed, the following screen appears:



- 2. Make sure that the following IIS features are installed:
 - a. Go to Start -> Administrative Tools -> Server Manager.



b. Expand the Roles folder, and then select Web Server (IIS).



c. Click Role Services.



- d. Verify that the following components are installed:
- ASP.NET •
- .NET Extensibility •
- **ISAPI Extensions** •
- **ISAPI** Filters •

Role Service		Status
<u> </u>	Web Server	Installed
<u></u>	Common HTTP Features	Installed
*	Static Content	Installed
_ه	Default Document	Installed
۵.	Directory Browsing	Installed
_ه	HTTP Errors	Installed
	HTTP Redirection	Not installed
	WebDAV Publishing	Not installed
۵.	Application Development	Installed
۵.	ASP.NET	Installed
_ه	.NET Extensibility	Installed
	ASP	Not installed
	CGI	Not installed
۵.	ISAPI Extensions	Installed
۵.	ISAPI Filters	Installed
	Server Side Includes	Not installed

- Scroll down and verify that the following components are installed: e.
- **IIS Management Console** •
- IIS 6 Metabase Compatibility •
- IIS 6 Management Console •



Installed Not installed Not installed Installed Installed Not installed Not installed Installed Not installed

Installing IIS

To install IIS:

- 1. Click on **Start -> Server Manager -> Roles -> Add Roles**.
- 2. Click Next.



3. Select **Web Server (IIS)**, and then click **Next**.

Adve Directory Certificate Services Role Services Confination Confination Adve Directory Certificate Services Adve Directory Role and Services Certificate Certificate	Percentary.
KAS Server Kas Server Key Services Key Services Key Services Key and Access Services Key and Access Services Key and Access Services Key Services	Web Server (TB) provide a management, and scalebul application infrastructure.

4. Click **Next** in Introduction to Web Server (IIS).

lefore You Begin	Introduction to Web Server (IIS)
erver Roles Web Server (005)	We proves are computers that have specific software that allows them to accept requests from client computers and interton response to those nerval pairs. We bis averus this you share information over the biscenset, a through instantes and entranets. The Web Server role includes Literate I/Fernanzian Services (13) 7.0, a utilite Web pairs that the pairs IS 7.0, A 24 Hist, and Workson Communication Foundation. Its 7.0 also features the service of the service and the service of t
Role Services	enhanced security, simplified diagnostics, and delegated administration.
onfirmation	Things to Note
togresi Ieouks	 Using Windows System Resource Manager (WSRM) can help ensure equitable servicing of Web server traffic, especially when there are multiple roles on this computer.
	 The default installation for the Web Server (DS) role includes the installation of role services that enable you to serve static content, noise insure contomications (such as default documents and HTP enors), monitor and log server activity, and configure static content compression.
	Additional Information
	Overview of Web Server (IIIS)
	Overview of Available Role Services in US 7.0
	IIS.Checklets
	Common Administrative Laste in US Overview of WSBM

- 5. Select the following components to install them:
 - .NET Extensibility
 - ISAPI Extensions
 - ISAPI Filters
 - ASP.NET

Server Roles	Role services:	Description:
Web Server (IDS) Rale Servesi Conferention Progress Results -	Web Server Web Server Server Sets Content Default Counter(Default C	Discrete program a first method of the second se
	More about role services	

- 6. Scroll down, select the following components, and then click Next.
 - IIS Management Console
 - IIS 6 Metabase Compatibility
 - IIS 6 Management Console



7. Click Install.

d how it can help optimize

8. Click Close.

Installation Re Before You Begin Server Roles Web Server (IIS) Bale Services	The following roles, role services, or fea 1 warning message below	tures were installed successfully: 2 evolution To sense that was evolvised alloct rule or features is a
Confirmation	automatically updated, turn on W	Indows Update in Control Panel.
Results	Her (downry ole services were not) Web Server Static Context Static Context Default Context Default Context Default Context Method North Default HTIP Foras Application HTIP Foras All To branchity Static Lonnoide ISAFI Channelon ISAFI Channelon ISAFI Rens Hellh and Desponits HTIP Logging Reguet Markin	steć:
	Print, e-mail, or save the installation rep	<u>ert</u>
		< Previous Next > Close Cancel

 Register .NET with IIS by running the following commands as an administrator: C:\Windows\Microsoft.NET\Framework64\v2.0.50727\aspnet_regiis.exe -i C:\Windows\Microsoft.NET\Framework64\v4.0.38319\aspnet_regiis.exe -i



10. To verify that IIS 7 is installed on the server, open your web browser and go to http://localhost/. If ISS 7 is installed, the following page appears:



6 Generating the SSL Certificate Request

Oracle Hospitality Hotel Mobile uses an SHA-2 SSL certificate signed by a known public certificate authority. The SSL should handle TLS 1.2. This section explains how to generate the certificate request for hotels to generate and use the certificate.

Do not use commas in any of the fields when creating your Certificate Signing Request (CSR). Commas are interpreted as the end of the field and cause an invalid CSR to be generated. Do not use any of the following characters in the web server distinguished name: ! @ # % ^* () ~ ? >< & /\

- Go to Start -> Control Panel -> Administrative Tools -> Internet Information Services (IIS) Manager to launch the Internet Information Services (IIS) Manager.
- 2. In the Connections panel on the left, select the correct server name and open the **Server Certificates** features by double-clicking the Server Certificates.

annections Start Dane Group by: Authentication Authentication Compression Default Directory Browsing Error Pages Hander MDME Types Modules Output Cathing Cathing Server Viologing MDME Types Worker Processes	Ele Yew Help	-	1
	onnections	WIN2K8-GPS Home	Actions Hanage Server Restart Stop View Application Pools View Sites Restart Help Online Help

3. In the Actions panel, click **Create Certificate Request** to open the **Request Certificate** wizard.

If you already have a certificate that is near expiration date and you need to renew it, select **Create Certificate Request**. Do not use the Renew option on the certificate from the Server Certificates action menu. The renewal function can sometimes create an incompatible CSR.

	5) manager		
Connections			Actions
3- E 2 8	Server Cer	tificates	Import
Start Page	Use this feature to reques	t and manage certificates that the Web	Create Certificate Request
WINZK8-GPS (WINZK8-GPS (Adm	server can use with Web s	ites configured for SSL.	Complete Certificate Request.
	Name +	Issued To	Create Domain Certificate
			Create Self-Signed Certificate.
			😧 Help Online Help
	Features View	▶ ▶	1

4. Enter the Distinguished Name information in the **Distinguished Name Properties** window in the wizard:

Request Certificate		? ×
Distinguishe	d Name Properties	
Specify the required informa as official names and they c	tion for the certificate. State/province and City/locality must be specified annot contain abbreviations.	
Common name:		
Organization:		
Organizational unit:		
City/locality		
State/province:		
Country/region:	IN	2
	·	
	Previous Next Finish Ca	ancel

Attribute	Description	
Common name	Domain to be secured by certificate	
Organization	Organization's legal business name	
Organizational Unit	Department in the organization	
City/Locality	Business location - city	
State/Province	Business location – state/province	
Country/Region	Business location - country	

- 5. Click Next.
- 6. Select Microsoft RSA Channel Cryptographic Provider as the **Cryptographic service provider**. For **Bit Length**, select 2048, and then click **Next**.

equest Certificate				?
Cryptographic Service Pro	vider Prop	erties		
Select a cryptographic service provider and a bi determines the certificate's encryption strength However, a greater bit length may decrease pe Cryptographic service provider:	t length. The l . The greater rformance.	bit length of the e the bit length, the	ncryption key e stronger the sec	curity.
Microsoft RSA SChannel Cryptographic Provider	é.	•		
Bit length:				
2048				
			_	
	Previous	Next	Finish	Cancel

7. Specify the location and file name for your CSR as shown in the following figure:

File Name	
Specify the file name for the certificate request. This information can be sent to a certification authority for signing. Specify a file name for the certificate request:	
C: Users (Prinsappov Lueskop (Innivumb C-Prinsing) L.Cxt	
Previous Next Finish	Cancel

8. Take note of where the CSR is being stored, as the hotel needs to access this file when requesting a certificate. The file should contain a CSR similar to what appears in the following example:

- 9. To request a certificate from the Certificate Authority, the hotel needs to open the generated file containing the newly created Certificate Signing Request (CSR) and copy its content into the specified field.
- 10. Copy the full CSR including the -----BEGIN NEW CERTIFICATE REQUEST-----

and

-----END NEW CERTIFICATE REQUEST-----

lines. Make sure that here are no trailing spaces or carriage returns in the CSR.

7 Installing the SSL Certificate

To install the SSL acquired by the property, copy the certificate files to the OPERA Web Services server and follow these steps:

- 1. Go to Start -> Control Panel -> Administrative Tools -> Internet Information Services (IIS) Manager.
- 2. In the Connections panel on the left, select the correct server name and open the **Server Certificates** features by double-clicking the Server Certificates.



3. In the Actions panel on the right, click **Complete Certificate Request**.



4. Click the button to select the server certificate you received from the certificate authority. If the certificate does not have a **.cer** file extension, select to view all types. Enter any name so you can keep track of the certificate on this server. Click **OK**.

Complete Certificate Request	? ×
Specify Certificate Authority Response	
Complete a previously created certificate request by retrieving the file that contains the certificate authority's response.	
File name containing the certification authority's response:	
C:\Users\Administrator\Downloads\certnew.cer	
Friendly name:	
Meo55OPERA	
OK Car	ncel

5. If successful, the newly installed certificate will be shown in the list. If an error stating that the request or private key cannot be found, make sure that the correct certificate is used and that it is installed in the same server that the CSR was generated from. If you are not sure about those two things, ask the property for verification so they can contact the certificate authority if the problem persist.

Services (II	5) Manager		
G S MEOSSOPERA →			🐱 🐼 I 🛛 🕶
Çe View Help			
Connections	Conver Contificate		Actions
🔍 - 🕞 🖄 🔝		:5	Import
Start Page MEOSSOPERA (MEOSSOPERA)A	Use this feature to request and man Web server can use with Web sites o	age certificates that the onfigured for SSL.	Create Certificate Request Complete Certificate Request
⊕ 🗃 Sites	Name 🔺	Issued To	Create Domain Certificate
	MeO55OPERA	MEO55OPERA	Create Self-Signed Certificate
			View
			Export
			Renew
			× Remove
			🕢 Help
			Online Help
	📰 Features View 💦 Content View		
Ready			• <u>1</u> .:

Intermediate Certificate

Most SSL providers issue server certificates of an Intermediate certificate so you install this Intermediate certificate to the server as well or will receive a Certificate Not Trusted Error. Follow these steps to install each Intermediate certificate:

- 1. Locate the intermediate certificate where Certificate files where stored on the OPERA Web Services server.
- 2. Double-click each intermediate certificate to open the certificate details.
- 3. At the bottom of the General tab, click **Install Certificate** to start the certificate import wizard.

4. Click Next.



5. Select **Place all certificates in the following store**, and then click **Browse**.

0	ertificate Store			
	Certificate stores are system are	as where certificates are k	ept.	
	Windows can automatically select	t a certificate store, or you	can specify a locati	on for
	C Automatically select the o	ertificate store based on th	e type of certificate	
	@ Blace all certificates in the	following store		
	Cercricate store:			
			Brows	D

6. Select **Show physical stores** as shown in the following figure:

Select Certificate Store	×
Select the certificate store you want to use.	
Preview Build Roots Remote Desktop Smart Card Trusted Roots Trusted Devices	^
Windows Live ID Token Issuer	~
Show physical stores	
OK Cancel	

7. Expand the **Intermediate Certification Authorities** folder, and then select **Local Computer** beneath it.



8. Click **OK**, **Next**, and then **Finish**.

8 SSL Bindings

- Go to Start -> Control Panel -> Administrative Tools -> Internet Information Services (IIS) Manager to bind the certificate to the website.
- 2. In the connections column, expand the **Sites** folder, and then click the website to bind to the certificate. Click **Bindings** in the Edit Site section.

Internet Information Services (IIS) Manager		
🔾 🚫 😜 🕨 MEOSSOPERA 🔸	Sites 🔸 Default Web Site 🔸		🗾 🔤 🖂 🗎
File View Help			
onnections		Cite Lleves	Actions
Application Pools Sites Sites Sites	Filter:	Site Horne	Explore Edit Permissions Edit Site Bindings Basic Settings Wing only actions
	.NET .NET Authorizati Compilation	ANET Error Pages	View Applications View Virtual Directories Manage Web Site 🔗
	Globalization	.NET Trust Levels	Start Stop Browse Web Site
	Application Connection Settings Strings	Machine Key	Browse *:80 (http) Browse *:443 (https) Advanced Settings
	Features View Content	t View	C

3. Click Add.

ype	Host Name	Port	IP Address	Bind	Add
http		80			Edit
•					Remove
Ś.					Browse

4. Change the Type to https, and then select the SSL certificate you just installed. Click OK.

Edit Site Binding			? ×
Type: https	IP address:		Port:
Host name:			
SSL certificate:			
MeO55OPERA			View
		ОК	Cancel

The binding for port 443 appears.

5. Click Close.

ite Bindir	ngs				? >
Туре	Host Name	Port	IP Address 8	Binding	Add
http		80	*		
https		443	*		Edit,
					Remove
					Browse
•				▶	
					Close