Oracle® Hospitality OPERA Property Management

Hardware Sizing Guide for Microsoft OS
Release 5.0.04.03 and higher
E78130-01

January 2018

Contents

Preface

This document serves as a guide when determining hardware requirements (such as servers, printers, workstations) for hotel installations running Oracle Hospitality OPERA Property Management Versions 5.0.04.03+ and 5.5.x (previously known as 5.0.05). The installation requires Oracle WebLogic application server media.

Audience

The Hardware Sizing Guide is intended for customers of Oracle Hospitality OPERA Property Management Versions 5.0.04.03+ and 5.5.x. Using this guide, customers can determine their hardware needs and discuss them with the appropriate personnel for installation and implementation.

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/
Additional Resources:
- *Network and Communications Guidelines*
- *OPERA Property Management Workstation Setup Guide Release 5.5*
- *OPERA 5 and OPERA Cloud Client and Server Compatibility Matrix*

Revision History

Date	Description of Change
December 2014	Initial 5.0.04.03 sizing guide.
September 2016	Conform to Oracle Corporation documentation standards. Updated data in certain tables to reflect current technology.
April 2017	Added Additional Resources and general edits.

| July 2017 | Added 5.5.x info, Resiliency and Redundancy, Determining existing server information, Frequently Asked Questions, Oracle Hospitality Network Requirements, Introduction to Network Design, OPERA Server and Application Components, Virtualization, Hotel Mobile, and OPERA Hardware Sizing Template. |

1   Sizing Methodology Overview

Servers

Servers have three main components:
1.   CPU
2.   Memory
3.   Drives

Each component has factors that determine the proper size:
- At a high level, CPU and memory are driven by the number of users and the type of processing.
- Disk configuration is driven by data size and the necessity for speed of access (reduced IO contention).

The sizes published in this document are based on analysis of empirical data from Beta sites and load testing results. The hardware specifications are based on available hardware at the time of writing.

The number of connections is the sum of the number of PCs with the ability to connect to Oracle Hospitality OPERA Property Management at one time, plus the number of external connection sources, such as third party software and interface PCs.

Examples and generic calculations are included for determining the user equivalent load of CRS interfaces, GDS, and OWS.

Server sizes are designed to support all Oracle Hospitality OPERA Property Management modules in any configuration, as long as the number of connections is not exceeded. Compatibility and performance of Oracle Hospitality OPERA Property Management hotel servers with other products such as Yield Management, Materials Management, or Back Office products has not been evaluated and should be considered separately when specifying servers.

Large Installations (Over 150 Concurrent Connections)

Larger installs classified as greater than 150 users require a detailed analysis for proper sizing. Contact your Oracle account representative for help with large configurations, as there are many possibilities based on customer preferences.

Supported Platforms

For supported platforms, refer to the document *OPERA 5 and OPERA Cloud Client and Server Compatibility Matrix* on the Oracle Help Center.

2 Resiliency and Redundancy

Mitigating Business Risk - Risk vs. Cost

The amount of investment a hotel makes in Resiliency and Redundancy should be judged to equal the business risk (i.e., the larger the hotel, the greater the number of users and services should mean a greater investment in Resiliency and Redundancy). This may mean an investment in:

- High quality, long standby time UPS with integrated power filters
- Best practices for backups and regular restore testing

Today's servers are very powerful and give us the ability to handle very large numbers of connections. However, it may be sensible from a business risk perspective to use one of the resilient configurations available rather than putting both DB and Application services on a single server. If a hotel IT manager is unsure, they should get a recommendation for Resiliency and Redundancy best practices from Oracle Hospitality.

OPERA Versions

This is a hardware sizing document for current versions of OPERA. All references to supported environments and platforms are in reference to OPERA Version 5.0.04.x and 5.5.x. Please contact Oracle Hospitality for recommendations on Hardware Sizing for other versions of OPERA.

Supported Platforms

As of this writing OPERA versions lower than 5.0.04.03 are only certified on Microsoft Windows 2008r2.

Microsoft Windows Server 2012r2 is only certified for OPERA Versions 5.0.04.03 and above including Database, Application, and Single Servers.

OXI, Property Interfaces, and HTNG Interfaces are certified on Microsoft Windows 7 as well as Microsoft Windows 2008r2.

All references to Microsoft Windows 2008 in this document are to be understood as references to Microsoft Windows 2008r2. Microsoft Windows 2008r1 is not considered to be a valid platform for OPERA installations.

All references to Microsoft Windows 2008r2 in this document include Microsoft Windows 2008r2 Standard or Enterprise Server unless otherwise noted.

All references to Microsoft Windows 7, 8, or 8.1 in this document include Microsoft Windows 7, 8, or 8.1 Professional, Enterprise or Ultimate unless otherwise noted. Both

x32 and x64 are supported unless otherwise noted. NO Starter or Home versions are supported.

All references to Microsoft Windows 2012 in this document mean Microsoft Windows 2012r2 Standard Server unless otherwise noted.

3   Determining Existing Server Information

If you are looking to upgrade your OPERA environment and need to determine if your current system is able to handle the load, there are a few key pieces of information that Oracle Hospitality will need to effectively determine sizing.

First we need your property information, including:
- Total Concurrent Users (peak/maximum concurrent application users accessing the system)
- Total Number of Properties
- Total number of Property Interfaces
- Total number of OXI Interfaces
- Total number of HTNG and other Interfaces

To estimate concurrent users, a general guideline is 10% of the hotel room count.

Second, we need your current OPERA Server details, including:
- Operating System
- Number and speed of CPU
- Amount of RAM
- Speed and size of disks
- Array configuration and Drive Layout

OPERA Upgrades

While the upgrade process is very straight forward, the hotel should ensure that there is a successful and valid backup of the OPERA Application folder (D:\MICROS) and the Oracle database through the Oracle agent. Failure to do so may result in total data loss should unexpected issues arise.

4   OPERA Xpress Limited Services Server Sizing (6 Users)

OPERA Xpress Limited Services sizing applies to the release of Oracle Hospitality OPERA Property Management Version 5.0.04.03 or higher. For other configurations, refer to either the Single server sizing or use the Standard dual server sizing in this document. The following criteria must be met in order to use these specifications:

1. The server machine is dedicated only to OPERA Xpress and serves no other purpose.
2. Maximum of:
     - 6 concurrent PMS users
     - 4 property interfaces
     - 1 central systems interface connection (OXI) allowed
3. PMS module is the only product in use. Other Oracle Hospitality OPERA Property Management modules are not designed to be used in this server configuration. Refer to 2 and 4 CPU single server sizing for deployment options with other modules active.
4. Use of the OPERA Xpress server as a workstation is not supported.
5. Separate workstations are required for each user.
6. Printers should be connected to workstations, not to the server.

OPERA Xpress Server – 6 Users Specifications

Operating System	Supported 64 bit Microsoft Windows Server OS	
Number of Users	Up to 6 Users	
	Minimum	Recommended
CPU	2 CPU core, fastest available	4 CPU core, fastest available
Memory	8 GB	12 GB
Disk Minimum	1 x 500 GB IDE 7200k RPM drive. No specific drive letter requirements. Optional recommended upgrades: ▪ Additional IDE disk for RAID 1 configuration ▪ Upgrade to ATA or SCSI and RAID Controller Hardware RAID controller is required in order to use RAID Disk configuration.	
Interface Ports	4 port RS232 expansion card. Built-in surge protection highly recommended.	
Backup Device	IDE tape drive. Microsoft Windows Backup can be used to perform cold backups to tape. Hot Backups require regionally approved backup software and additional disk space for Archive logs.	
Printer	Laser printer.	

5   OPERA Single Server Sizing

OPERA Single Server combines the Oracle Database and the OPERA Application onto
one server.
All OPERA servers must be dedicated only to OPERA and can serve no other purpose.

2 CPU Cores – 20 Users

This Single Server Sizing (2 CPU cores) applies to Oracle Hospitality OPERA Property
Management PMS and S&C modules of release 5.0.04.03 or higher.

The following criteria must be met to use these specifications:
1. The server machine is dedicated only to Oracle Hospitality OPERA Property
   Management and can serve no other purpose.
2. Maximum of:
   - 20 concurrent users
   - 8 property interface
   - 1 central systems interface connection (OXI) allowed
3. Postscript print drivers are the only print drivers allowed on the server.

OPERA Single Server Specifications		
Up to 20 Users (No more than 8 interfaces and 1 OXI interface on this hardware)		
Operating System	Microsoft Windows 2008r2 Standard or Enterprise, Microsoft Windows 2012r2 Standard only for 5.0.04.03+	Microsoft Windows 2008r2 Standard or Enterprise, Microsoft Windows 2012r2 Standard only for 5.0.04.03+
	Minimum	**Recommended**
CPU	2 Cores, 1.8 GHz or faster	2 Cores, 2.6 GHz or faster
Memory Minimum	16 GB	16 GB
Disk Minimum	2 Disks – 10k SAS drives, both drives in a RAID1 array. Disks should be a minimum of 600 GB each. Recommend 100 GB C: drive and remainder of available space assigned to D: drive (at least 100 GB). OPERA software will be installed by default on D: drive.	4 Disks – 15k SAS drives, all disks in a single RAID1+0 array. Disks should be a minimum of 300 GB each. Recommend 100 GB C: drive and remainder of available space assigned to D: drive (at least 200 GB). OPERA software will be installed by default on D: drive.
	Hardware RAID controller is required in order to use RAID. Software RAID controller is not supported.	Hardware RAID controller is required in order to use RAID. Software RAID controller is not supported.

Interface Ports	Enterprise level 4-8 port RS232 Serial expansion card or Serial to IP device (built in surge protection highly recommended).	Enterprise level 4-8 port RS232 Serial expansion card or Serial to IP device (built in surge protection highly recommended).
Backups	Although Oracle Hospitality does not configure or support customer backups, a backup location will be needed. A disk, tape or offsite (cloud) backup location will need to be configured by the customer IT staff to be able to fully backup the OPERA Database and Application files.	Although Oracle Hospitality does not configure or support customer backups, a backup location will be needed. A disk, tape or offsite (cloud) backup location will need to be configured by the customer IT staff to be able to fully backup the OPERA Database and Application files.
Printer	Networkable laser printers with PostScript drivers are recommended.	

Implementation time is considerably high with a 1.8 GHz CPU clock. We suggest using a CPU with more than 2.6 GHz for OPERA purposes (all sizings).Consideration should be given to using a separate PC for support connectivity for sites with more than 10 users. Connecting to the server via any remote desktop tools, terminal services, or VNC takes resources and can impact performance if the site has the maximum allowed users connected. A support PC also allows Support to have a dedicated client machine to investigate any issues that the site may report.

4 CPU Cores – 40 Users

This Single Server Sizing (4 CPU cores) applies to Oracle Hospitality OPERA Property Management PMS and S&C modules of release 5.0.04.03 or higher.

The following criteria must be met to use these specifications:
1. The server machine is dedicated only to Oracle Hospitality OPERA Property Management and can serve no other purpose.
2. Print spooling, third-party software, and other network services are not supported on the Oracle Hospitality OPERA Property Management Server.
3. Maximum of:
   - 40 concurrent users
   - 4 properties if configured for multi property
   - 1 central systems interface connection (OXI) allowed
4. Property interfaces should be installed on a separate server. More details can be found in the section *Supporting Hardware Sizing*.
5. Postscript print drivers are the only print drivers allowed on the server.

OPERA Single Server Specifications		
Up to 40 Users (No more than 8 interfaces and 1 OXI interface on this hardware)		
Operating System	Microsoft Windows 2008r2 Standard or Enterprise, Microsoft Windows 2012r2 Standard only for 5.0.04.03+	Microsoft Windows 2008r2 Standard or Enterprise, Microsoft Windows 2012r2 Standard only for 5.0.04.03+
	Minimum	**Recommended**
CPU	4 Cores, 1.8 GHz or faster	4 Cores, 1.8 GHz or faster
Memory Minimum	16 GB	24 GB
Disk Minimum	8 Disks – 10k SAS drives, all disks in a single RAID1+0 array. Disks should be a minimum of 146 GB each. Recommend 100 GB C: drive and remainder of available space assigned to D: drive (at least 200 GB). OPERA software will be installed by default on D: drive.	8 Disks – 15k SAS drives, all disks in a single RAID1+0 array. Disks should be a minimum of 300 GB each. Recommend 100 GB C: drive and remainder of available space assigned to D: drive (at least 200 GB). OPERA software will be installed by default on D: drive.
	Hardware RAID controller is required in order to use RAID. Software RAID controller is not supported.	Hardware RAID controller is required in order to use RAID. Software RAID controller is not supported.
Interface Ports	Enterprise level 4-8 port RS232 Serial expansion card or Serial to IP device (built in surge protection highly recommended).	Enterprise level 4-8 port RS232 Serial expansion card or Serial to IP device (built in surge protection highly recommended).
Backups	Although Oracle Hospitality does not configure or support customer backups, a backup location will be needed. A disk, tape or offsite (cloud) backup location will need to be configured by the customer IT staff to be able to fully backup the OPERA Database and Application files.	Although Oracle Hospitality does not configure or support customer backups, a backup location will be needed. A disk, tape or offsite (cloud) backup location will need to be configured by the customer IT staff to be able to fully backup the OPERA Database and Application files.
Printer	Networkable laser printers with PostScript drivers are recommended.	

Consideration should be given to using a separate PC for support connectivity. A support PC allows Support to have a dedicated client machine to investigate any issues that the site may report.

8 CPU Cores – 80 Users

This sizing for 8 CPU cores (80 users) applies to Oracle Hospitality OPERA Property Management PMS and S&C modules of release 5.0.04.03 or higher.

The following criteria must be met to use these specifications:
1. The server machine is dedicated only to Oracle Hospitality OPERA Property Management and can serve no other purpose.
2. Print spooling, third party software, and other network services are not supported on the OPERA Server.
3. Maximum of:
   - Up to 80 concurrent users
   - 1 central systems interface connection (OXI) allowed
   - 4 properties if configured for multi property
4. Property interfaces should be installed on a separate server.
5. More details can be found in the section *Supporting Hardware Sizing*.
6. Postscript print drivers are the only print drivers allowed on the server.

OPERA Single Server Specifications		
Up to 80 Users (No more than 8 interfaces and 1 OXI interface on this hardware)		
Operating System	Microsoft Windows 2008r2 Standard or Enterprise, Microsoft Windows 2012r2 Standard only for 5.0.04.03+	Microsoft Windows 2008r2 Standard or Enterprise, Microsoft Windows 2012r2 Standard only for 5.0.04.03+
	Minimum	**Recommended**
CPU	2 x 4 Cores, 1.8 GHz or faster	2 x 4 Cores, 1.8 GHz or faster
Memory Minimum	24 GB	24 GB
Disk Minimum	8 Disks – 10k SAS drives, all disks in a single RAID1+0 array. Disks should be a minimum of 300 GB each. Recommend 100 GB C: drive and remainder of available space assigned to D: drive (at least 200 GB). OPERA software will be installed by default on D: drive.	8 Disks – 15k SAS drives, all disks in a single RAID1+0 array. Disks should be a minimum of 300 GB each. Recommend 100 GB C: drive and remainder of available space assigned to D: drive (at least 300 GB). OPERA software will be installed by default on D: drive.
	Hardware RAID controller is required in order to use RAID. Software RAID controller is not supported.	Hardware RAID controller is required in order to use RAID. Software RAID controller is not supported.

Interface Ports	Enterprise level 4-8 port RS232 Serial expansion card or Serial to IP device (built in surge protection highly recommended).	Enterprise level 4-8 port RS232 Serial expansion card or Serial to IP device (built in surge protection highly recommended).
Backups	Although Oracle Hospitality does not configure or support customer backups, a backup location will be needed. A disk, tape or offsite (cloud) backup location will need to be configured by the customer IT staff to be able to fully backup the OPERA Database and Application files.	Although Oracle Hospitality does not configure or support customer backups, a backup location will be needed. A disk, tape or offsite (cloud) backup location will need to be configured by the customer IT staff to be able to fully backup the OPERA Database and Application files.
Printer	Networkable laser printers with PostScript drivers are recommended.	

Consideration should be given to using a separate PC for support connectivity. A support PC allows Support to have a dedicated client machine to investigate any issues that the site may report.

8 CPU Cores – 140 Users

The 8 CPU cores – 140 users sizing applies to Oracle Hospitality OPERA Property Management PMS and S&C modules of release 5.0.04.03 or higher.
The following criteria must be met to use these specifications:
1. The server machine is dedicated only to Oracle Hospitality OPERA Property Management and can serve no other purpose.
2. Print spooling, third party software, and other network services are not supported on the OPERA Server.
3. Postscript print drivers are the only print drivers allowed on the server.
4. Maximum of:
   - Up to 140 concurrent users
   - 1 central systems interface connection (OXI) allowed
   - 4 properties if configured for multi property
5. Property interfaces should be installed on a separate server. More details can be found in the section *Supporting Hardware Sizing*.

OPERA Single Server Specifications	
Up to 140 Users (No more than 8 interfaces and 1 OXI interface on this hardware)	
Operating System	Microsoft Windows 2008r2 Standard or Enterprise, Microsoft Windows 2012r2 Standard only for 5.0.04.03+
	Recommended

CPU	2 x 4 Cores, 1.8 GHz or faster
Memory	32 GB
Disk Minimum	16 Disks – 15k SAS drives, all disks in a single RAID1+0 array. Disks should be a minimum of 300 GB each. Recommend 100 GB C: drive and remainder of available space assigned to D: drive (at least 400 GB). OPERA software will be installed by default on D: drive.
	Hardware RAID controller is required in order to use RAID. Software RAID controller is not supported.
Interface Ports	Separate Interface workstation or server recommended.
Backups	Although Oracle Hospitality does not configure or support customer backups, a backup location will be needed. A disk, tape or offsite (cloud) backup location will need to be configured by the customer IT staff to be able to fully backup the OPERA Database and Application files.
Printer	Networkable laser printers with PostScript drivers are recommended.

Consideration should be given to using a separate PC for support connectivity. A support PC allows support to have a dedicated client machine to investigate any issues that the site may report.

6 Separate OPERA Application / Database Server Sizing

All OPERA servers must be dedicated only to OPERA and can serve no other purpose.

Separate OPERA Application / Database Server Specifications		
Up to 40 Users (No more than 8 interfaces and 1 OXI interface on this Application		
Operating System	Microsoft Windows 2008r2 Standard or Enterprise, Microsoft Windows 2012r2 Standard only for 5.0.04.03+	Microsoft Windows 2008r2 Standard or Enterprise, Microsoft Windows 2012r2 Standard only for 5.0.04.03+
	Application Server	**Database Server**
CPU	4 Cores, 1.8 GHz or faster	4 Cores, 1.8 GHz or faster
Memory Minimum	8 GB	16 GB
Disk Minimum	2 Disks – 10k SAS drives, both drives in a RAID1 array. Disks should be a minimum of 146 GB each. Recommend 100 GB C: drive and remainder of available space assigned to D: drive (at least 100 GB). OPERA software will be installed by default on D: drive.	6 Disks – 15k SAS drives, all disks in a single RAID1+0 array. Disks should be a minimum of 146 GB each. Recommend 100 GB C: drive and remainder of available space assigned to D: drive (at least 100 GB). OPERA software will be installed by default on D: drive.
	Hardware RAID controller is required in order to use RAID. Software RAID controller is not supported.	Hardware RAID controller is required in order to use RAID. Software RAID controller is not supported.
Interface Ports	Enterprise level 4-8 port RS232 Serial expansion card or Serial to IP device (built in surge protection highly recommended).	N/A
Backups	Although Oracle Hospitality does not configure or support customer backups, a backup location will be needed. A disk, tape or offsite (cloud) backup location will need to be configured by the customer IT staff to be able to fully backup the OPERA Database and Application files.	Although Oracle Hospitality does not configure or support customer backups, a backup location will be needed. A disk, tape or offsite (cloud) backup location will need to be configured by the customer IT staff to be able to fully backup the OPERA Database and Application files.

Printer	Networkable laser printers with PostScript drivers are recommended.

Separate OPERA Application / Database Server Specifications		
Up to 80 Users (No more than 8 interfaces and 1 OXI interface on this Application		
Operating System	Microsoft Windows 2008r2 Standard or Enterprise, Microsoft Windows 2012r2 Standard only for 5.0.04.03+	Microsoft Windows 2008r2 Standard or Enterprise, Microsoft Windows 2012r2 Standard only for 5.0.04.03+
	Application Server	**Database Server**
CPU	4 Cores, 1.8 GHz or faster	4 Cores, 1.8 GHz or faster
Memory Minimum	16 GB	16 GB
Disk Minimum	2 Disks – 10k SAS drives, both drives in a RAID1 array. Disks should be a minimum of 300 GB each. Recommend 100 GB C: drive and remainder of available space assigned to D: drive (at least 100 GB). OPERA software will be installed by default on D: drive.	6 Disks – 15k SAS drives, all disks in a single RAID1+0 array. Disks should be a minimum of 300 GB each. Recommend 100 GB C: drive and remainder of available space assigned to D: drive (at least 200 GB). OPERA software will be installed by default on D: drive.
	Hardware RAID controller is required in order to use RAID. Software RAID controller is not supported.	Hardware RAID controller is required in order to use RAID. Software RAID controller is not supported.
Interface Ports	Enterprise level 4-8 port RS232 Serial expansion card or Serial to IP device (built in surge protection highly recommended).	N/A
Backups	Although Oracle Hospitality does not configure or support customer backups, a backup location will be needed. A disk, tape or offsite (cloud) backup location will need to be configured by the customer IT staff to be able to fully backup the OPERA Database and Application files.	Although Oracle Hospitality does not configure or support customer backups, a backup location will be needed. A disk, tape or offsite (cloud) backup location will need to be configured by the customer IT staff to be able to fully backup the OPERA Database and Application files.
Printer	Networkable laser printers with PostScript drivers are recommended.	

Separate OPERA Application / Database Server Specifications		
Up to 140 Users (No more than 8 interfaces and 1 OXI interface on this Application		
Operating System	Microsoft Windows 2008r2 Standard or Enterprise, Microsoft Windows 2012r2 Standard only for 5.0.04.03+	Microsoft Windows 2008r2 Standard or Enterprise, Microsoft Windows 2012r2 Standard only for 5.0.04.03+
	Application Server	**Database Server**
CPU	6 Cores, 1.8 GHz or faster	2 x4 Cores, 1.8 GHz or faster
Memory Minimum	24 GB	16 GB
Disk Minimum	4 Disks – 10k SAS drives, all disks in a single RAID1+0 array. Disks should be a minimum of 300 GB each. Recommend 100 GB C: drive and remainder of available space assigned to D: drive (at least 200 GB). OPERA software will be installed by default on D: drive.	8 Disks – 15k SAS drives, all disks in a single RAID1+0 array. Disks should be a minimum of 300 GB each. Recommend 100 GB C: drive and remainder of available space assigned to D: drive (at least 300 GB). OPERA software will be installed by default on D: drive.
	Hardware RAID controller is required in order to use RAID. Software RAID controller is not supported.	Hardware RAID controller is required in order to use RAID. Software RAID controller is not supported.
Interface Ports	Separate Interface workstation or server recommended.	N/A
Backups	Although Oracle Hospitality does not configure or support customer backups, a backup location will be needed. A disk, tape or offsite (cloud) backup location will need to be configured by the customer IT staff to be able to fully backup the OPERA Database and Application files.	Although Oracle Hospitality does not configure or support customer backups, a backup location will be needed. A disk, tape or offsite (cloud) backup location will need to be configured by the customer IT staff to be able to fully backup the OPERA Database and Application files.
Printer	Networkable laser printers with PostScript drivers are recommended.	

7   Server Sizing

Microsoft Windows Server OXI and OXI HUB Server Sizing

In most cases the OXI component of the application can reside on the application server however Oracle Hospitality recommends that interfaces that require the ability to post into the OPERA network from the Internet be separated from the OPERA network using a DMZ. Contact a qualified IT consultant for assistance with this configuration.

Operating System	Microsoft Windows 7 Pro x64, Microsoft Windows 8 Pro x64 Microsoft Windows 2008r2 Standard Microsoft Windows 2012r2 Standard only for 5.0.04.03+
	OXI Server / Workstation
CPU	4 Cores, 1.8 GHz or faster
Memory Minimum	8 GB
Disk Minimum	1 Disk – at least 80 GB free space available after operating system is installed

OXI HUB messages per day < 75,000 75,000 – 200,000

OXI HUB messages per day		Up to 200,000
Monitor Server	CPU	1 x Quad Core
	Memory	8 GB
	Drive Count x size	1 x 80 GB

Microsoft Windows Server OEDS Server Sizing

Services (Note 2)		Sizing
Per Major Distribution Channel, GDS Pegasus, GDS XML, OWS XML etc. (1 server will support 50,000 messages per hour).	CPU Memory Drive Count x size	1 x Quad Core 8 GB 1 x 80 GB
Up to 2 low volume XML interfaces, (< 1000 messages per hour).	CPU Memory Drive Count x size	1 x Quad Core 8 GB 1 x 80 GB
OEDS Server running Hotel Mobile and component REST services, (150 rooms / 2 active mobile users). **(Note 3)**	CPU Memory Drive Count x size	1 x Quad Core 12 GB 1 x 80 GB

Note 1: Estimating OXI messages per day. (Total number of Rooms / Avg stay length) * 2) * %Occupancy. Use of statistics from existing central interfaces will provide a more accurate determination of the number of messages per day.

Note 2: Estimating OWS messages. ((Annual bookings) * % annual bookings acquired from internet) * 1000 Availability requests per actual booking) = OWS messages per year. OWS messages per year / 365 = OWS messages per day.

Typical internet traffic occurs in peaks. Assume that all the messages per day are actually processed within a 12 hour period.

OWS messages per day / 12 hours = Average OWS hourly message load.
Average OWS XML message size = 1.5 Kbytes

Note 3: Estimating Hotel Mobile requirements beyond standard OEDS Server requirements. It is estimated that active mobile users will generate ~3000 OEDS requests/hour in a 150 room hotel environment. Hotel Mobile REST layer requires additional 2 GB memory. Minimum CPU requirements will be sufficient for associated load.

OPERA Interface PC/Server and Workstation Hardware Sizing

Interface Workstation or Server (Note 1)	**OS**	**Microsoft Windows 7 Pro Microsoft Windows 8 Pro Microsoft Windows 8.1 Pro Microsoft Windows 2008r2**	This formula can be used in determining the memory for an interface workstation or server. 80MB for each installed property interface, defined as voicemail, call accounting, movies, etc. Add 40MB per additional PMS in case of multi-property setup. Add 150MB for the IFC controller.
	CPU	2 Cores	
	Memory **(Note 3)**	4 GB	
	Min. Free	20 GB	

User Workstation (Note 1)		Minimum	Recommended	
	OS (Note 4)	Microsoft Windows 7 Pro Microsoft Windows 8 Pro Microsoft Windows 8.1 Pro Microsoft Windows 10 Pro	Microsoft Windows 7 Pro Microsoft Windows 8 Pro Microsoft Windows 8.1 Pro Microsoft Windows 10 Pro	See note 2 for bandwidth requirements. See note 5 for minimum OPERA versions supported on each OS. Microsoft Windows 10 Pro or Enterprise must be X64. Microsoft Internet Explorer 7, 8, 9, 10, and 11 are supported. For Microsoft Internet Explorer 10 and 11, opera must be a minimum Version .0.04.00/3
	CPU	2 Cores	2 Cores	
	Memory (Note 3)	3 GB	4 GB	
	Min. free disk	100 MB	200 MB	The Microsoft Edge browser is not supported.

Note 1: Minimum workstation configuration supports one OPERA Session and a small application (< 5 MB memory usage). Users who require multiple OPERA sessions or use other large applications may require more RAM and other resources.

Note 2: Bandwidth of 16kb (kilobits) per user minimum available to OPERA for WAN connections. If the WAN circuit is used to transport other software like email, web browsing, etc., then it is highly recommended that QOS (Quality of Service) software or a dedicated circuit be used to ensure that mission critical applications have priority use of the bandwidth. For latency information, refer to *Network and Communications Guidelines* on the Oracle Help Center.

Note 3: Workstations installed with personal firewall software and/or anti-virus clients could require additional memory.

Note 4: Both 32bit and 64bit workstations are supported unless otherwise noted. On 64bit workstations, the 32bit browser must be used.

Note 5: OS Minimum Supported OPERA version:

Microsoft Windows 7 Pro	5.0.04.00
Microsoft Windows 8 Pro	5.0.04.00/3
Microsoft Windows 8.1 Pro	5.0.04.01/21, 5.0.04.02/12, 5.0.04.03/7
Microsoft Windows 10 Pro x64	5.0.04.03/7

Guidelines for OPERA BI Sizing

OPERA Business Intelligence sizing varies significantly on how the customer uses the product. Different combinations and configuration of cubes, length of online historical data, length of future data modeling, and the configuration of OPERA components can all impact the sizing for the BI data. Disk space requirements can vary greatly, so always err on the side of extra storage space.

BI Single Property Sizes

Number of Rooms (Note 1)	GB of Disk Space Required for OBI Cubes (Note 2)	GB of Disk Space Required for Block/Reservation Detail Data (optional) (Note 2)	Amount of extra CPU Cores and Physical Memory Required (Notes 3, 4, 6)
1 - 100	15	10	+1 CPU core
101 – 300	45	30	+1 CPU core
301 – 500	75	50	+1 CPU core
501 – 1000	150	100	+2 CPU cores +1 GB RAM
1001 – 2000	250	150	+4 CPU cores +2 GB RAM
2001 – 3000	350	200	+8 CPU cores +4 GB RAM
3001+	Custom (Note 5)	Custom (Note 5)	+16 CPU cores +8 GB RAM

Note 1: If there are multiple properties, then add 20% extra space for each property. (Example: A 4 multi property OPERA installation with 1,200 rooms would need 250 + (250*(4*0.2)) = 450 GB of space). If Codes and Categories are standardized and strictly enforced, this value can be reduced to 10%.

Note 2: The disk space requirements in the table include an additional 20% disk space allocation for larger than standard database temp segment needs.

Note 3: For installs larger than 1000 rooms, it is required to have a separate application server for running OPERA BI.

Note 4: For installs with 1000-3000 rooms, it is recommended to have a separate database server for running OPERA BI. For installs with 3000+ rooms, it is required to have a separate database server for running OPERA.

Note 5: For custom sizing, the most accurate method for calculating needed disk space is to build sample test cubes with customer production data. It is preferred for this to be done before disk size requirements are finalized.

Note 6: For installs larger than 500 rooms, the extra physical memory is needed for increasing the DB parameter OLAP_PAGE_POOL_SIZE (manual memory settings) or PGA_AGGREGATE_TARGET (auto tuned memory settings).

8   OPERA Microsoft Windows Server Sizing

Microsoft Windows OPERA Property Management Server Sizing

Number of Connections (Note 1)		<20	21-40	41-80	81-120	121-150	
DB Server (Note 2)	CPU	See *Single Server Specs*	2 CPU core, fastest available	2 CPU core, fastest available	4 CPU core, fastest available	4 CPU core, fastest available	
	Memory		4 GB	6 GB	8 GB	8 GB	
	SCSI Drive Count and size (RAID 1) **(Note 3)**		(4 x 72 GB)	(6 x 72 GB)	(8 x 72 GB)	(8 x 72 GB)	
App Server (Notes 2, 4)	CPU		2 CPU core, fastest available	2 CPU core, fastest available	4 CPU core, fastest available	2 Servers in Parallel **(Note 6)** 2 CPU core, fastest available	4 CPU core, fastest available
	Memory		8 GB	12 GB	16 GB 64 bit OS	16 GB	24 GB 64 bit OS
	Drive size (RAID 1 or 5) **(Note 5)**		36 GB usable drive space	36 GB usable drive space	72 GB usable drive space	36 GB usable drive space	72 GB usable drive space

Note 1: Number of Connections is the sum of the number of PCs with the ability to connect to OPERA at one time plus the number of external connection sources, such as third party software, interfaces, Web Booking, and other. For more information on determining the number of users and the interface traffic load, refer to the section *Guidelines for Determining User Counts*.

Note 2: Servers are sized to support hot backups using 3rd party backup solutions that use an Oracle Agent.

Note 3: RAID level 5 not supported for drives containing data files due to disk write performance impact. Using bigger drives and reducing the number can negatively impact I/O performance. Number of drives is more important than size for IO distribution. It is not intended that external disk storage be required for standard installations. 72 GB configurations for DB server are based on SCSI Ultra320 or SAS controllers and drives with < 5ms seek times. Recommended drive configurations are RAID 1, 0+1, or 1+0.

Note 4: Application Server sizing based on 1 current generation CPU core per 40 concurrent users. Memory sizing based on median of memory consumption of a mix of "medium-lightly" active users 32MB user and "heavily" active users 64 MB/user.

Note 5: RAID level 1 or RAID level 5 supported for Application Server. Application Server is not I/O intensive but requires disk space for storage of NA reports and export files as well as temporary space used in generating other reports. When using multiple applications servers a shared disk location for NA reports and exports needs to be available. UNC locations on network file servers, DFS and mapped drives can all be used for this purpose.

Note 6: For multiple applications servers, Oracle recommends the implementation of Network Load balancers. These can either be hardware based such as F5, Cisco Load Director or software based, such as Microsoft Windows network load balancing and DNS round robin. Contact your Oracle account representative for details on options and solutions that may be available as a service.

Microsoft Windows OXI HUB Queue Manager Sizing

OXI HUB messages per day (Note 1)		< 75,000	75,000 – 200,000
Monitor Server	CPU	2x2.0 GHz or 1x Dual Core	2 Servers as per specifications for <75,000
	Memory	1 GB (recommend 2 GB)	
	Drive Count x size	1 x 18 GB	

Note 1: Estimating OXI messages per day.
((Total number of Rooms / Avg stay length) * 2) * % Occupancy. Use of statistics from existing central interfaces provides a more accurate determination of the number of messages per day.

Microsoft Windows OWS, GDS, OAP Server Sizing

Services (Note 2)		Sizing
Per Major Distribution Channel, GDS Pegasus, GDS XML, OWS XML etc. (1 server supports 50,000 messages per hour)	CPU	2x2.0 GHz or 1x Dual Core
	Memory	1 GB (recommend 2 GB)
	Drive Count x size	1 x 72 GB
Up to 2 low volume XML interfaces, (< 1000 messages per hour)	CPU	1x2.0 GHz
	Memory	512 MB (recommend 2 GB)
	Drive Count x size	1 x 72 GB

Note 2: Estimating OWS messages.

((Annual bookings) * % annual bookings acquired from internet) * 1000 Availability requests per actual booking) = OWS messages per year. OWS messages per year / 365 = OWS messages per day.

Typical internet traffic occurs in peaks. Assume that all the messages per day are actually processed within a 12 hour period.

OWS messages per day / 12 hours = Average OWS hourly message load.

Average OWS XML message size = 1.5 Kbytes

9 Supporting Hardware Sizing

This section details the minimum and recommended configurations to ensure that OPERA will perform optimally. Between each of these configurations there are some standard requirements that need to be discussed. This will ensure that there are no unexpected issues during and after installation or upgrade.

1. A dedicated server is required for most Oracle Hospitality products. Please contact your Sales Executive or Account manager for further assistance or clarification.
2. The server cannot be used as a workstation.
3. The OPERA server should be housed in a secure area with limited access.
4. Printers should normally be connected to a print server or workstations and not the OPERA server. If they are installed to the OPERA server performance may suffer.
5. Consideration should be given to using a separate workstation for support connectivity.

Additional Considerations

Concurrent Connections is the sum of the number of workstations with the ability to connect to OPERA at one time plus the number of external connection sources, i.e. third party software, interfaces, Web Booking, etc.

Servers are sized to support hot backups using 3rd party backup solutions that use an Oracle Agent.

Raid level 5 is not supported for drives containing database data files due to disk write performance impact. Using a lesser number of drives than recommended can negatively impact I/O performance, regardless of the size of the disks or the amount of space needed. Number of drives is more important than size for I/O distribution. It is not intended that external disk storage be required for standard installations. Configurations for Database or Single Server are based on SAS controllers and drives with < 5ms seek times. Recommended drive configurations are Raid 10 (Also referred to as RAID 1+0).

Application server sizing is based on 1 CPU core per 40 concurrent users and 64MB RAM per concurrent user.

Raid levels 1, 5 or 10 are supported for Application servers. The OPERA Application Server is not I/O intensive but requires disk space for storage of Night Audit reports and export files as well as temporary space used in generating other reports. Disk space requirements may change in a multi-property environment or if multiple Applications servers are present in the same environment.

When using multiple applications servers a shared disk location for Night Audit reports and exports will need to be available via UNC path. It is recommended that UNC locations are not on an OPERA Application server.

For multiple Applications servers Oracle Hospitality recommends the implementation of Hardware Network Load balancers. Please be advised that Oracle Hospitality does not configure hardware load balancers. It is possible but not recommended to use a software based load balancer (e.g., Microsoft Windows Network Load Balancing or DNS round robin). It is recommended to properly size a single Application server rather than multiple Application servers if the customer IT staff is not able to install, configure and manage a hardware load balancer.

Interface PC

OS	Microsoft Windows 7 Professional	Determining interface PC memory:
CPU	1 x Dual Core	• 80 MB for each installed property interface, such as Voicemail, Call Accounting, and Movies.
Memory	3 GB	
Min. Free Disk Space	4 GB	• Add 40 MB per additional PMS in case of Multi Property setup.
		• Add 150 MB for the IFC Controller.

Microsoft Windows 7 Workstation

	Minimum (Note 1)	**Recommended**	
OS	Microsoft Windows 7 Business **(Note 2)**	Microsoft Windows 7 Enterprise **(Note 2)**	Bandwidth of 16 KB per user is the minimum available for WAN connections. For latency information, refer to *Network and Communications Guidelines* on the Oracle Help Center.
CPU	1 x Dual Core	1 x Dual Core	
Memory	Above 2 GB	Above 2 GB	
Min. Free Disk Space	80 MB	80 MB	

Note 1: Minimum PC configuration supports one OPERA session and a small application (< 5 MB memory usage). Users who require multiple sessions or use other large applications need a Power User sized PC. Power User sizing should support two sessions with one other application. Power users with larger needs should add more memory.

Note 2: PCs installed with Microsoft Windows 7 require additional configuration. On 64-bit workstations, use the 32-bit browser. For more information, refer to the document *OPERA Property Management Workstation Setup Guide Release 5.5* on the Oracle Help Center.

PCs installed with personal firewall software and/or current anti-virus clients could require additional memory than specified above.

10 Guidelines for Determining User Counts

The best method to determine the correct site sizing is to obtain actual numbers from existing systems and business input for changes that occur after the Oracle Hospitality OPERA Property Management system is deployed. Sometimes it is not possible to gather all required information for a variety of reasons such as a new site, expansion, or no previous comparable system.

Here are some guidelines to follow to estimate the hardware sizing. The numbers obtained with these methods should be reviewed by Oracle and the customer to ensure everyone understands the assumptions that were made and make adjustments as necessary.

1. Application users:
   a. Each time a user launches a browser and logs into OPERA, it counts as a User.
   b. OPERA launches Child sessions during normal use of the application. These sessions are already included in the sizing.
   c. As a rule of thumb, OPERA PMS user count averages at about 10% of the number of rooms. Slightly higher for high-end properties, and slightly lower for Express type hotels. PMS user counts <5% or >20% of the number rooms may be fine, however they warrant a double check with the customer to ensure these numbers are accurate.
   d. S&C and ORS user counts are very site dependent and need to be gathered from the customer.
2. Property interfaces:
   a. Count one equivalent OPERA user for 4 property interfaces in database sizing.
   b. On IFC8 installations, count one equivalent OPERA user for 4 property interfaces in application server sizing.
3. 2 way CRS interface:
   a. 6 equivalent OPERA users are considered per 1000 rooms in database sizing. This general rule uses two formulas: 1) 1200 reservation messages per day per user and 2) the 100 bookings per day per user. These figures are empirically derived from production sites and load testing information. As block messages can hold a large number of details, block messages need to be converted to equivalent reservation messages. A 10 day block with 20 rooms would equate to 100 reservation messages.
      i. $\dfrac{\text{\# Rooms * 7 Msgs per room per day}}{\text{1200 msg per day per user}}$ = equivalent users.
      ii. $\dfrac{\text{\# Rooms * avg Stay Length * \% occupancy}}{\text{100 bookings per day per user}}$ = equivalent users.
   b. Retention of up to 4 days of interface messages is included in the server disk sizing. If the retention period for OXI messages is increased, additional disk space is needed.
      100 Rooms would require ~ 50MB per additional day of retention.
4. OPERA Electronic Distribution Systems (OEDS), such as GDS, OWS, ADS:

a. These interfaces can have a large effect on sizing since the actual load is generated by basically uncontrolled end users. It is very important that the customer understand how peaks in load from these interfaces can affect sizing / performance.
b. In the past, the calculation of 250 messages = 1 OPERA user was used. Different versions of OPERA and different rate configurations affect the cost of an OWS message so this number is subject to changes in each customer location. Generally, take the cost (measured in logical reads) of 1 general availability lookup message (X) and use the following formula to determine the number of messages/hour that equal 1 OPERA user:
    i. 1,200,000 / X = Messages per hour
c. If other means are not available to measure / estimate the message rate from these interfaces, use the following formula. Typical electronic traffic occurs in peaks. Empirical analysis indicates that 80% of all traffic occurs in 6 hours. For calculation purposes, assume all traffic occurs in 6 hours.
    i. (Bookings per day from interface * Look to book ratio for the interface) / 6 = avg peak msgs per hour.
    Est. Look to book ratios. OWS 1000, GDS 200.

11 Frequently Asked Questions

Below is a series of commonly asked questions that may help you. If you find a question that is not answered here, please contact your Sales executive or Account Manager for assistance.

Q. What does the hardware team need to determine if a server is sufficient for OPERA?
A. Please reference the Hardware Sizing Spreadsheet. Any additional information that could be a contributing factor should also be presented for review.

Q. What operating systems are supported for OPERA Servers?
A. Microsoft Windows 2008r2 Standard or Enterprise for OPERA Version 5.0.04.x and above.
Microsoft Windows Server 2012r2 is only certified for OPERA Versions 5.0.04.03 and above.

Q. What operating systems are supported for Property Interfaces?
A:
Microsoft Windows 7 Pro, Business, or Enterprise (32 or 64-bit)
Microsoft Windows 8 Pro, Business, or Enterprise (32 or 64-bit)
Microsoft Windows 8.1 Pro, Business, or Enterprise (32 or 64-bit)
Microsoft Windows 10 (64-bit)
Microsoft Windows 2008r2 Standard or Enterprise
Microsoft Windows 2012r2 Server

The Oracle Hotel Property Interface supports using a computer running a VMware ESXi release 5.1.0 and higher.

Q. How big should the operating system (C:) partition be?
A. Our recommendation is at least 100 GB but this value is dynamic as hardware and software requirements change.

Q. What naming convention can I use for the server?
A. OPERA server names should be between 3 and 15 characters, without an underscore, space or any other special characters. A dash (-) is acceptable but not recommended. The server name should begin with a letter and not a number or any other special character. Our recommendation is to use a standard format that includes in order the first 4 characters of the hotel name, operating system, function, and number. For example: Hotel MICROS would be MICRPMSW2K8SS. You can amend this guideline to suit your needs as this is only offered as a suggestion.

Q. Will Oracle Hospitality install the Operating System?
A. Yes, but only with the purchase of OPERA Server Hardware from Oracle, the server would arrive on site pre-configured with the operating system and OPERA installed. [WHERE AVAILABLE]

Q. What can I not use in naming the server?
A. In order to avoid technical difficulties, do NOT use the following expressions as Computer name: OPERA, ORACLE, Server, LocalHost, Expressions containing an underscore (_), spaces, or other special characters.

Virtualization, Terminal Services, Citrix Support

Q. Do you support Terminal Services or Citrix Implementations?
A. Oracle has no technical expertise on the implementation or configuration of Terminal Services or Citrix. Customers wishing to use these products do so at their own risk.

Q. How can we get assistance if we have a technical issue with OPERA in these environments?
A. Our Support teams will make every effort to troubleshoot any issue as long as the issue is clearly related to the OPERA Property Management System. Oracle Support will request that you seek assistance from your third party provider if the issue is not directly reproducible or known in a non VM, TS or Citrix environment.

Hard Drive Configurations and Specifications

Q. If the recommendation for disk drives is 8 drives, can I use 4 larger drives instead?
A. No, OPERA is an I/O intensive application that requires writing to multiple disk spindles to spread the workload and maintain performance.

Q. What drive configurations are supported?
A. Any server or workstation that houses mission critical data should be configured using hardware Redundant Array of Independent Disks (RAID) Level 1 or 1+0. This is a requirement for Database and Single Servers. In addition RAID1, RAID1+0 and RAID 5 can be used for Application Servers, OXI, and OEDS servers.

Storage Area Network Devices

Q. Can I have the Oracle data files on a SAN?
A. Yes, however the data files must reside on SAS drives configured in a RAID 1+0 array.

Q. What Storage Area Network (SAN) devices are supported?
A. Depending on sizing requirements, Only Direct Attached and Fiber SANs are currently supported with 15K SAS drives. iSCSI is not supported.

Q. Are Network Area Storage (NAS) devices supported?
A. No. NAS Devices are not supported for OPERA Databases.

Backup and Antivirus Information

Q. What backup solutions are supported?
A. Oracle does not provide support for any customer backups. Third party products such as Symantec Backup Exec can be used to perform hot backups, with the use of an Oracle agent, but are not supported by Oracle.

Q. What exceptions need to be added to any Antivirus software for OPERA Servers?
A. Please exclude the following folders:
C:\Oracle\Oradata
D:\Oracle\Oradata
D:\Oracle\Admin
File types: .ARC, .CTL, .DBF, .ORA and .RDO

Q. What folders need to be backed up to restore Property Interfaces?
A. The XML information used by the interface program are stored in C:\ or D:\Fidelio.If you have SDC then additional folders may be present such as C:\ or D:\Elevon or SDC which needs to be backed up to restore credit cards.

Q. Does Oracle recommend that the OPERA server be placed on a domain?
A. Absolutely. The OPERA application does not require a domain for Versions 5.0.04.02 and prior however printing and workstation / user authentication issues will be greatly reduced in a domain environment. Additionally, OPERA is LDAP aware and can be tied into the domain environment as well.
For OPERA Versions 5.0.04.03 and Higher a domain is necessary due to SSL requirements.

Q. I don't have a domain controller in place right now. What if I add one later?
A. **For OPERA Versions 5.0.04.02 and prior** - No problem. OPERA only points to the NETBIOS name of the server. If a server has been joined to the domain, the workstations will still only point to the server's name. As an example, if your server name is PMSSERVER.MICROS.US.INT, users would only point to PMSSERVER.
For OPERA Versions 5.0.04.03 and Higher - Once the mandatory SSL certificate request is generated there is no way to change it and any change in the server name or domain would require the entire OPERA Installation to be removed and re-installed.

Q. Can the OPERA Server function as a domain controller?
A. No, due to PCI compliance, this is not a recommended or supported configuration.

Q. What ports does OPERA use?
A. Please refer to the section entitled *Overview of Required Network Communication Ports* later in this document.

Q. Does OPERA support SSL on port 443?

A. Yes, In order to comply with both requirement 8.4 of the PCI-DSS and requirement 3.3 of the PADSS, user access credentials are required to be obfuscated (encrypted) when stored or in transit within the internal network. For its OPERA Enterprise Solution products, (OPERA), the PA-DSS Implementation Guides state that in order to comply with PCI-DSS requirement 8.4 and PA-DSS requirement 3.3, OPERA must be deployed with Secure Socket Layer (SSLv3) certificates installed on certain OPERA servers.

Q. What print drivers do I need?

A. If the printers are to be installed on the OPERA servers then only PostScript drivers are approved. All other devices can use PCL or PostScript.

12 Oracle Hospitality Network Requirements

Refer to *Network and Communications Guidelines* on the Oracle Help Center.

13 Introduction to Network Design

One way to categorize the different types of computer network designs is by their scope or scale. For historical reasons, the networking industry refers to nearly every type of design as some kind of area network. Common examples of area network types are:

- LAN - Local Area Network
- WLAN - Wireless Local Area Network
- WAN - Wide Area Network
- MAN - Metropolitan Area Network
- SAN - Storage Area Network, System Area Network, Server Area Network, or sometimes Small Area Network
- CAN - Campus Area Network, Controller Area Network, or sometimes Cluster Area Network

LAN and WAN were the original categories of area networks, while the others have gradually emerged over many years of technology evolution. We will only be covering those networks that are pertinent to OPERA.

Local Area Network (Internal Network)

A local area network (LAN) supplies networking capability to a group of computers in close proximity to each other such as in an office building, a school, or a home. A LAN is useful for sharing resources like files, printers, games or other applications. A LAN in turn often connects to other LANs, and to the Internet or other WAN.

Most local area networks are built with relatively inexpensive hardware such as Ethernet cables, network adapters, and hubs. Wireless LAN and other more advanced LAN hardware options also exist.

Demilitarized Zone (DMZ)

In a DMZ configuration, most computers on the LAN run behind a firewall connected to a public network like the Internet. One or more computers also run outside the firewall, in the DMZ. Those computers on the outside intercept traffic and broker requests for the rest of the LAN, adding an extra layer of protection for computers behind the firewall.

Traditional DMZs allow computers behind the firewall to initiate requests outbound to the DMZ. Computers in the DMZ in turn respond, forward or re-issue requests out to the Internet or other public network, as proxy servers do. (Many DMZ implementations, in fact, simply utilize a proxy server or servers as the computers within the DMZ.) The LAN firewall, though, prevents computers in the DMZ from initiating inbound requests.

DMZ is a commonly-touted feature of home broadband routers. However, in most instances these features are not true DMZs. Broadband routers often implement a DMZ simply through additional firewall rules, meaning that incoming requests reach the firewall directly. In a true DMZ, incoming requests must first pass through a DMZ computer before reaching the firewall.

External Network

A WAN spans a large geographic area, such as a state, province or country. WANs often connect multiple smaller networks, such as local area networks (LANs) or metro area networks (MANs).

The world's most popular WAN is the Internet. Some segments of the Internet, like VPN-based extranets, are also WANs in themselves. Finally, many WANs are corporate or research networks that utilize leased lines.

High-Level Network Diagram

General Networking Environment with OEDS \ OXI
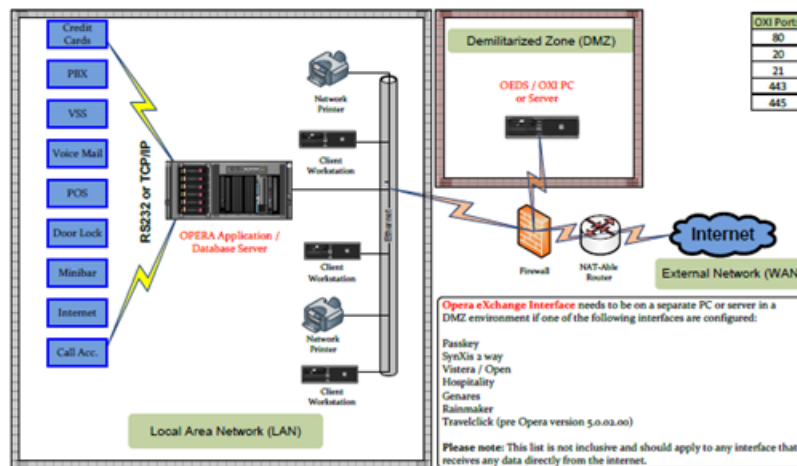
Overview of Required Network Communication Ports

Port Number	Configurable	Always Required	Protocol	Used for / Comments	Servers
20 / 21	N	N	TCP	Standard FTP Ports	All
22	N	N	TCP /UDP	Standard Secure Shell (SSH) Port	All
23	N	N	TCP	Standard Telnet Port	All

Port Number	Configurable	Always Required	Protocol	Used for / Comments	Servers
25	N	Y (DB Servers)	TCP	Default SMTP Port / Is required on DB server	DB
		N (Other Servers)		To mail server configured in OPERA	
80	Y	Y	TCP	Default HTTP Port / Can be changed (OappCfgEd)	APP
				Workstations to Application Server	DB
				Interface Servers (IFC 8) to Application Servers	IFC
				Database Servers to Application Servers	OXI
				Database Servers to internet IP addresses when using certain options (e.g., Address)	
				Certain OXI interfaces also need this port	
443	Y	N	TCP	Default HTTPS Port / Can be changed (OappCfgEd)	APP
				Workstations to Application Server	DB
				Interface Servers (IFC 8) to Application Servers	IFC
				Database Servers to Application Servers	OXI
				Database Servers to internet IP addresses when using certain options (e.g., Address)	
				Certain OXI interfaces also need this port	
445	N	Y (App Server) **(Note 1)**	TCP / UDP	Microsoft File Sharing / Active Directory / Share Port	APP
		N		Between Application and File Server	FILE

Port Number	Configurable	Always Required	Protocol	Used for / Comments	Servers
1521	Y	Y (DB Servers)	TCP	Default Oracle Listener Port **(Note 2)**	DB
		N (Other Servers)		Application Servers to DB Servers	APP
				Old Interface Servers (IFC7) to DB Servers	IFC
				Certain OXI Servers to DB Servers	OXI
				Other Servers that require an Oracle Client / SQLNet connection to the DB	OTH
1526	Y	N	TCP	Commonly used alternative Oracle Listener Port **(Note 2)**	DB
				Other commonly used ports are 1522, 1571, 1581	
1630	Y	N	TCP	Oracle Connection Manager Default Port	DB
				In some rather rare scenarios it is needed to configure OCM on the DB Servers	
3389				From DB Servers to Application Servers (QAS Servers)	APP
	N	N	TCP	Microsoft Remote Desktop Port	All
4400	Y	Y	TCP	This Port is commonly used as an alternative HTTP Port (see 80)	APP
					DB
					IFC
					OXI
5001	Y	Y (IFC8 Servers)	TCP	The Default Port used for connections from IFC8 to the IFC8 Controller	IFC
		N (Other Servers)			
5002 to 5020	Y	Y (IFC8 Servers)	TCP	Communication Ports between IFC8 and Third Party Systems **(Note 3)**	IFC
		N (Other Servers)			

Note 1: Only needed when a UNC configuration is used (e.g., the export folder) between Application Server and File Server.

Note 2: Only the initial communication takes place on this port. The connection will be handed over using a different port above 1024. In case your Firewall does not support SQLNet, ports above 1024 will need to be opened.

Note 3: In most cases the IFC8 Server is TCP/IP server and the third party vendor is TCP/IP client - OPERA decides the ports used. In rare cases the third party vendor is TCP/IP server and OPERA is TCP/IP client - the vendor decides the ports used.

Network Data Graphical View
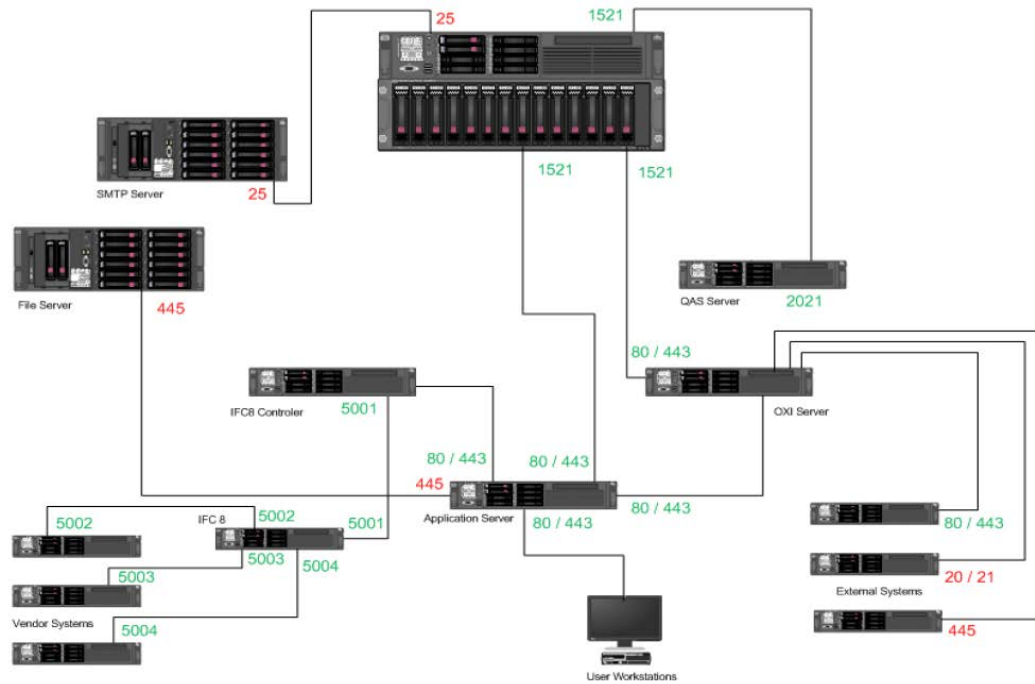
14 OPERA Server and Application Components

The OPERA Enterprise Suite has a number of different components that interact in a variety of possible configurations.

Property Management System (PMS) Servers

Due to the scalability of the OPERA Property Management System, the database and application server components can be configured in a number of different ways. Generally these will be based upon the volume of transactions that will be processed on a daily basis. Our most common installation combines the Oracle Database and Application Server components onto one server class machine (Single Server). In cases where the server resource load is expected to be high, the OPERA PMS solution can span from a single server solution to an Oracle Real Application Cluster, known as RAC. For more details about these configurations, please contact your sales or account executive.

OPERA Electronic Distribution Suite (OEDS) Servers

Depending on your implementation needs, Oracle Hospitality offers a variety of products under the name OPERA Electronic Distribution Suite (OEDS). OEDS components include many individual services and processes that may or may not be installed or required depending on configuration and property requirements. These commonly could include OWS, HTNG, ADS, GDS, Kiosk, or Gaming interfaces. The general behavior for all components in the suite is similar.

At a basic level OEDS may be installed in one of two possible configurations. The first requires that the OEDS Server be placed in a DMZ. This is necessary if the server must receive data directly from the internet. Alternately, if there are no requirements to receive as previously mentioned then the servers should be located within the bounds of the corporate firewall.

OXI / OEDS in a DMZ Environment
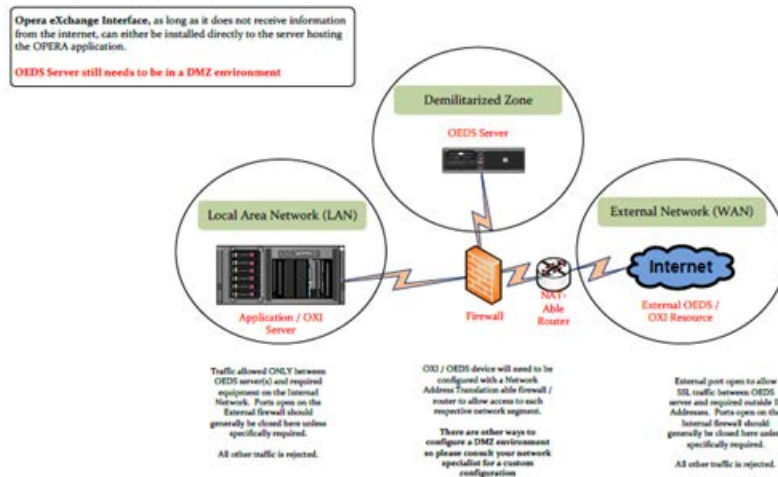
OEDS Servers with a Direct Connection to the Internet

The above diagram shows the recommended location of the OEDS server(s) for all interfaces that require the ability to post into the OPERA network from the Internet. Oracle Hospitality recommends the server be located in a DMZ. There are a few different ways to configure a DMZ so please talk with your qualified network technician on the configuration that works for your environment.

Additionally, the internal firewall should be SQL*Net enabled to handle the Oracle database links and should allow ONLY SQL*Net traffic between the OEDS server(s) and the OPERA database(s). If the firewall is not SQL*Net aware, then the firewall will need to close all ports below 1024 and should allow all other ports for communication between the OEDS server(s) and the OPERA database(s). All other traffic should be rejected. Oracle Hospitality will assume that the customer has put such a network in place to protect against unwanted access from the Internet to the internal corporate network. Oracle Hospitality will NOT take any responsibility for security issues that may rise after installation of any OPERA component. It is the responsibility of the customer to ensure that there is a secure network in place. The above diagram is only for reference purposes.

OEDS Servers without a Direct Connection to the Internet

OEDS server(s) for all interfaces that do not require the ability to post from the internet into the properties LAN do not need to be housed in a DMZ. In this case, Oracle Hospitality recommends OEDS be installed on a standalone machine (due to resource requirements) except in select circumstances. The properties firewall should be configured to block ALL incoming traffic from the public internet. Oracle Hospitality will NOT take any responsibility for security issues that may arise after installation of any OPERA component. It is the client's responsibility to have a secure network in place. The above diagram is only for reference purposes.

OPERA eXchange Interface (OXI) Components and Servers

OXI interfaces are designed to be flexible and as such may be configured in a number of different fashions. The components used for message exchange and processing are:

- OPERA Application HTTP Server.
- Accepts incoming traffic from the external system.
- OXI Processor (Microsoft Windows NT Service).
- Processes messages as the point of communication between OPERA's HTTP server and the OPERA API.
- Posts outgoing messages to the external system.

It is not required that the OXI Processor and OPERA Application HTTP Server be installed on the same machine though so such a configuration is often the case. However, incoming messages MUST be able to reach the HTTP Server and outgoing messages MUST be able to reach the external system. The communication flow between OPERA and the external system will be one of the following:

- **Push/Push** – Both systems push messages to other system when messages are available. External system sends messages for OXI to OPERA's HTTP server and OXI sends messages to external system's HTTP server.
- **Push/Pull** – External system pushes messages to OPERA when messages are available and polls OPERA's HTTP server for availability of messages (OR) OPERA pushes messages to external system when messages are available and polls external system's HTTP server for availability of messages.
- **Pull/Pull** – Both systems poll the other system for messages and pull them when available (No implementations currently exist).

In each of these cases, it is important to evaluate which system initiates connectivity under different circumstances and where each system resides. For example, in the case of a Push/Pull interface where OPERA will initiate all messages and connect to an external system located in an offsite datacenter, it is important to keep in mind that communications will pass over the public internet and should be encrypted with an SSL certificate installed on the external system side. No incoming ports are required through the firewall for this interface.

OXI may be installed in one of two possible configurations (including accompanying firewall configurations). Depending on the requirements of the OXI interface itself, it may or may not be required that the external system have the ability to post into the DMZ. In many cases, the external system does not in fact post INTO the property. Communication is instead initiated from the property and all messages are pulled FROM the vendor.

OXI External System Posting INTO OPERA Network

OXI / OEDS in a DMZ Environment
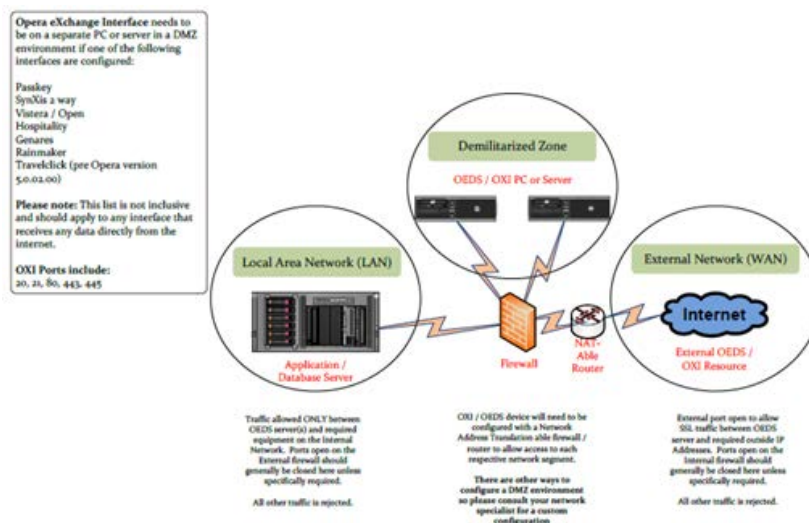
The above diagram shows the recommended location of the OXI server(s) for all OXI interfaces that require the ability to post into the OPERA network from the Internet.

Oracle Hospitality recommends the server be located between an external and internal firewall (a DMZ). The external firewall (shown on the right) controls access from the Internet through a dedicated port by using the external IP address. The internal firewall (shown on the left) controls access from the OXI PC to the OPERA database(s) by using the internal IP address. The internal firewall should be SQL*Net enabled to handle the Oracle database links and should allow ONLY SQL*Net traffic between the OXI Server and the OPERA database(s). If the firewall is not SQL*Net aware, then the firewall will need to close all ports below 1024 and should allow all other ports for communication between the OXI server and the OPERA database(s). All other traffic should be rejected.

Servers located within the DMZ should have 2 NICs (network interface cards), one with a public (external) IP address and one with the local LAN IP address. The server may also have just 1 NIC provided the proper network routing to handle this is in place.

Oracle Hospitality will assume that the customer has put such a network in place to protect against unwanted access from the Internet to the hotel's LAN.

Oracle Hospitality will NOT take any responsibility for security issues that may arise after installation of any OPERA component. It is the client's responsibility to have a secure network in place. The above diagram is only for reference purposes.

OXI External System NOT Posting Into OPERA Network

Like OEDS, there are two possible configurations exist for those OXI interfaces where the external system is NOT posting into the network containing the OPERA system. First, the communication between the external system and OPERA may exist entirely on the internal network.

The second possible configuration for those OXI interfaces where the external system is NOT posting into the OPERA network is one where the external system exists on the external network (across the public internet). In this case, OXI will initiate communication and pull messages from the external system. A DMZ is not required in this case as incoming traffic is not present and ALL incoming ports should be blocked from the internet. The outgoing port to the external system from the OPERA server must be open.

The above two diagrams show the recommended location of the OXI server(s) for all OXI interfaces that DO NOT require the ability to post into the OPERA network from the Internet. In these cases, if traffic volume requires it, OXI may be installed on a standalone machine or may be installed on an OPERA Application or Single Server.

In this case, Oracle Hospitality recommends OXI be installed on the OPERA Application Server whenever possible. If the network traffic or concurrent user count requires it, a separate server may be installed. The external firewall should be configured to block ALL incoming traffic from the public internet.

Oracle Hospitality will assume that the customer has put such a network in place to protect against unwanted access from the Internet to the hotel's LAN.

Oracle Hospitality does NOT take any responsibility for security issues that may arise after installation of any OPERA component. It is the client's responsibility to have a secure network in place. The above diagram is only for reference purposes.

OXI Variations Summary

The variation in OXI configurations is summarized in the table below. This should not be considered a complete or definitive listing as custom configurations are always possible. Oracle Hospitality recommends reviewing your configuration with a qualified networking resource to ensure your configuration is as secure as possible.

OXI Communication Flow	External Server On-Site or on Internal Network		External Server Off-Site (External Network)	
Push/Push	SSL/DMZ for OPERA	SSL/DMZ for External	SSL/DMZ for OPERA	SSL/DMZ for External
	No	No	Yes	Yes

OXI Communication Flow	External Server On-Site or on Internal Network		External Server Off-Site (External Network)	
Push/Pull OPERA Initiating Calls	SSL/DMZ for OPERA	SSL/DMZ for External	SSL/DMZ for OPERA	SSL/DMZ for External
	No	No	No	Yes
Push/Pull External System Initiating Calls	SSL/DMZ for OPERA	SSL/DMZ for OPERA	SSL/DMZ for OPERA	SSL/DMZ for External
	No	No	Yes	No
Pull/Pull	SSL/DMZ for OPERA	SSL/DMZ for External	SSL/DMZ for OPERA	SSL/DMZ for External
	No	No	No	No

For those scenarios in the table above where SSL/DMZ is required for OPERA, Oracle Hospitality strongly recommends a network implementation similar to that in the above diagram labeled OXI External System Posting INTO Property. For those scenarios where SSL/DMZ is not required for OPERA, a DMZ may still be required for another system such as OEDS, but not for OXI. In such a case, a network implementation similar to that in the above diagrams labeled OXI External System NOT Posting INTO Property is acceptable.

Property Level Interfaces

OPERA supports thousands of property level interfaces. In many cases these require a physical connection (via COM port) to a machine running the OPERA Interface Controller software (an Interface PC) that handles translation between the physical connection and the OPERA Application Server. To allow for multiple COM port connections to a single machine, a multiport serial card is often used to expand the COM port capacity of the Interface PC. In other cases, the physical connection may be via TCP/IP to the same Controller. An Interface PC is generally limited to eight Interfaces as this is where the expanded COM port capacity is usually exhausted.

In some cases, it is possible to connect COM ports from a different machine to an interface PC running the Interface Controller. In such a configuration, port 5001 is generally configured from TCP/IP transmission from the machine hosting the COM port to the machine hosing the Interface Controller. For TCP/IP interfaces using the IFC PC as the TCP/IP server, ports 5002 through 5020 are usually configured. If the equipment on the interface side will be the TCP/IP server, then please check with your vendor.

All equipment relating to Property Level Interfaces should be a member of the Internal Network, should NOT be located in the DMZ, and should not be accessible from the internet.

Internal Network

OPERA Application Server

Property Level Interface PC

TCP/IP or Serial

TCP/IP or Serial

Credit Cards	PBX	VSS	Voice Mail
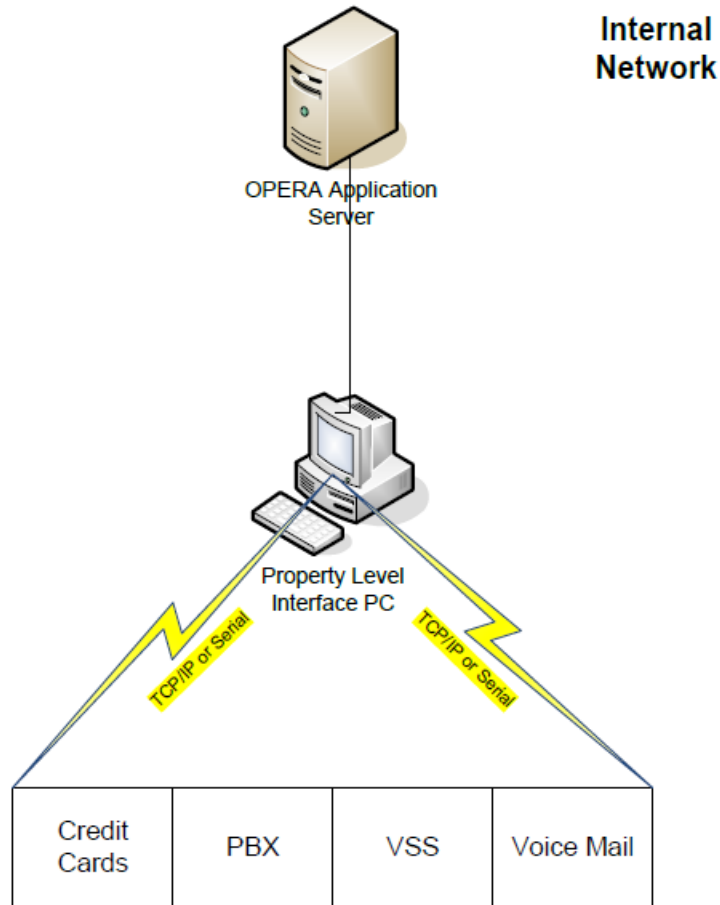
OPERA Client/Server Communications

Traffic between an OPERA client machine and the OPERA Application server is broken into two types:

- Type-1 traffic is a forms applet that communicates with the forms servlet using a pure Oracle proprietary message format and hard-coded DES3 encryption. This includes everything that is communicated via the OPERA UI (most of the traffic to/from the server).
- Type-2 traffic is everything else and is exactly what would generally be expected from an HTTP call to any website. Implementing an SSL certificate ensures this stream of information is encrypted prior to transmission.

Once an SSL certificate has been installed on an App Server, Type-2 traffic will be directed over the SSL port (typically 443). Type-1 traffic will continue to be directed over the non-SSL port. Type-1 traffic continues to be directed over the non-SSL enabled port for two reasons:

- Type-1 messages are already encrypted. Adding an HTTPS layer would be unnecessary overhead

- Type-1 messages are small but very frequent. This means there are numerous roundtrips. Adding HTTPS doubles the number of roundtrips on the network and significantly increases application response times. In scenarios with higher latency or high traffic volume, this results in significant performance degradation. For latency information, refer to *Network and Communications Guidelines* on the Oracle Help Center.

Due to this architecture, OPERA still requires two ports to operate (defaults are 80 and 443). If a firewall will be in place to filter activity, its configuration must allow for communication of both ports between client and application server.

Secure Socket Layer (SSL) and OPERA

Beginning with Version 4.0.xx.xx, the OPERA application server supports the implementation of an SSL certificate.

For OPERA Versions 4.0 – 5.0.04.02

Oracle Hospitality strongly recommends OPERA be implemented with an SSL certificate in place. A proper SSL Implementation will force all un-encrypted user traffic to proceed over the SSL encrypted port so that a user is not able to bypass the secure certificate for sign-on. Users that direct their browser to an un-encrypted (HTTP) URL will be redirected to an encrypted (HTTPS) URL. This will protect all traffic that is not already encrypted by the Oracle forms applet. As mentioned in the previous section, Client/Server communications will use two ports for transmission, one that will be encrypted using the SSL certificate and one that will not (because this traffic is already encrypted).

Delivering non-encrypted traffic over the same port that delivers SSL encrypted traffic in a non-encrypted fashion is not an option – this is not possible in Apache (the Web Server component of Oracle Application Server). So delivery of traffic that is both encrypted and unencrypted from the Web server point of view requires two ports minimum.

It is technically possible to redirect the non-encrypted traffic through the SSL tunnel in the Apache or Oracle configuration. However, this would double-encrypt those components that are already encrypted, increase server roundtrips, and increase application response times. Oracle neither recommends nor supports this configuration.

For OPERA Versions 5.0.04.03 and Higher

SSL is now a requirement and self-signed certificates are no longer supported. The below items list the requirements for SSL:
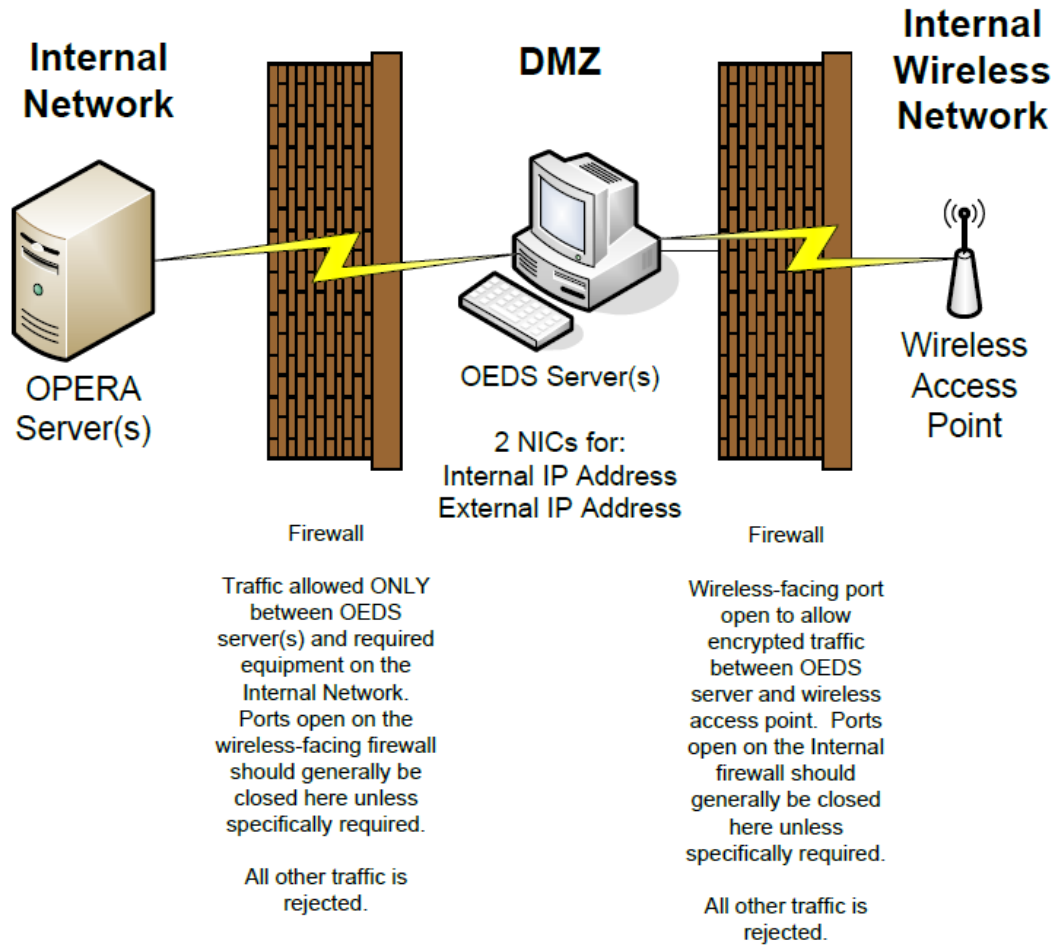
- Certificate must be based on a Fully Qualified Domain Name. Certificates based on only the machine name are not supported.

- Certificate must be signed by a Certificate Authority, self-signed certificates are not supported. If the client has their own internal certificate authority this is supported however they must be able to provide ALL corresponding CA Certs that were used to sign the certificate. A chain certificate will not work in this case for the CA Certs, and individual certificate is needed for each certificate in the chain.

- All Certificates must be provided in the X.509 format, other formats are not supported. The customer is responsible for converting the certificate to X.509 format if the Certificate Authority cannot issue in the X.509 Format.

- .LOCAL and .INTERNAL domains are not supported for the Fully Qualified Domain Name. This is due to Certificate Authorities no longer signing certificates with these domain names. If the customer has their own internal Certificate Authority and they are able to sign certificates with .LOCAL or .INTERNAL domain names then an exception can be granted. However once the certificate request is generated there is no way to change it and the OPERA Installation must be removed and re-installed. This will be billable time if the customer wants to proceed with a .LOCAL or .INTERNAL domain and finds they are unable to sign the certificate.

- Certificate authorities will verify ownership of the domain in the certificate request. Properties should not attempt to make up a domain as this will cause delays in obtaining a certificate.

- Property IT is responsible for all internal DNS routing to ensure workstations can connect to the server via the Fully Qualified Domain name.

Wireless Access Points and OPERA

Oracle Hospitality recommends that OPERA not be run wirelessly unless specific operational processes and application components require it. Examples where this may be desirable include a self-service kiosk or a handheld check-in device. In such a circumstance, Oracle Hospitality strongly recommends that the accompanying OEDS server be located in its own DMZ separate from any other external access servers (OEDS or OXI) that may also exist in a DMZ facing the internet.

Wireless devices should be configured to require strong encryption mechanisms such as AES and all firmware should be updated to support strong encryption for both authentication and transmission. WEP should not be used. The wireless network itself should be an internal network insofar as that is possible. Guest wireless access should not occur on this network.

Internal Network

OPERA Server(s)

DMZ

OEDS Server(s)

2 NICs for:
Internal IP Address
External IP Address

Internal Wireless Network

Wireless Access Point

Firewall

Traffic allowed ONLY between OEDS server(s) and required equipment on the Internal Network. Ports open on the wireless-facing firewall should generally be closed here unless specifically required.

All other traffic is rejected.

Firewall

Wireless-facing port open to allow encrypted traffic between OEDS server and wireless access point. Ports open on the Internal firewall should generally be closed here unless specifically required.

All other traffic is rejected.

User Accounts

User accounts for the OPERA application are handled in a secure manner and will be reviewed during the OPERA configuration that occurs as part of the implementation and training process. User accounts in the Microsoft Windows and network environment must be managed by an external process. Oracle Hospitality recommends against the use of generic user accounts for any level of system access and instead recommends that unique Operating System or network credentials be established for each individual and that these credentials include the use of strong passwords. Strong passwords should include the following rules:

- Passwords must expire at most every 90 days
- Passwords must be at least 7 characters in length
- Passwords must include at least one each of alphabetic and numeric characters

At all times when user credentials will be transmitted against any internal or external network, they must be encrypted. To facilitate this, Oracle Hospitality strongly recommends implementing OPERA with an SSL certificate in place on the Application Server.

Microsoft Windows User Accounts

The Microsoft Windows operating system provides the capability to create and manage unique credentials for each user that requires access. Managing credentials at the operating system level can be somewhat cumbersome as credentials from one machine do not transfer to another machine. If a user will access two computers, then that user would require an account on each machine.

Microsoft Active Directory

An Active Directory installation can facilitate management of user access credentials. Active Directory allows the creation of a domain environment to which each computer on the network can be assigned. Domain level user accounts then have the ability to log into any machine connected to the domain provided the machine allows these logins.

Microsoft Active Directory Integration to OPERA

OPERA provides the ability to integrate with an Active Directory installation via the Lightweight Directory Access Protocol (LDAP) to allow users to use the same login credentials at the operating system and network level and at the OPERA Application level. This simplifies the management of user credentials by allowing credentials for the operating system, network resources, and the OPERA Application to be managed in a single location.

Credit Card Data Flow

The flow of credit card data through the OPERA system is relatively straightforward. From the point of entry (client workstation), information is transmitted to the database server which then makes the posting to the credit card gateway.

At the workstation, UI is received via an Oracle Forms stream. Credit card is swiped or manually entered.

PMS Client

OPERA PMS Workstation

PAN
Expiration
Track Data (if swiped)
Transmission is an Oracle Forms stream.

The OPERA Application Server serves user interface to the web browser on the PMS workstation via two layers. UI activity is via an encrypted Oracle Forms stream. External activity (e.g., reports) is via HTTP or HTTPS call (HTTPS is recommended).

PMS Server

OPERA Application Server

PAN
Expiration
Track Data (if swiped)
Transmission is an SQL*Net connection

The OPERA database and the OPERA Credit Card driver reside within the database architecture. Internally, an XML message is created and transmitted directly from the database to the URL specified in configuration.

For long-term storage, PAN and expiration date may be stored in an encrypted table. Track data is NEVER stored.

The OPERA database server runs on a Windows OS with an Oracle Database.

OPERA Database Server

OPERA Databae and Credit Card Driver

PAN
Expiration
Track Data (if swiped)
Transmission is via
HTTPS (SSL v3) to an Offsite gateway or could be either
HTTP or HTTPS to an Onsite gateway.

Onsite or Offsite

Credit Card Gateway

Known Issues and Security Enhancements

A current listing of all identified security-related issues with the OPERA product suite can be obtained at: https://www.oracle.com/technetwork/topics/security/alerts-086861.html

15 Virtualization

Support for Virtual Environments

Oracle has not certified any of its products on any VMware or other virtualization environment. Oracle Support will assist customers running Oracle products in virtual environments in the following manner: Oracle will only provide support for issues that either are known to occur on the native OS, or can be demonstrated not to be as a result of running in a VM (virtual machine).

If a problem is a known Oracle issue, Oracle support will recommend the appropriate solution on the native OS. If that solution does not work in the VM environment, the customer will be referred to the VM vendor for support. When the customer can demonstrate that the Oracle solution does not work when running on the native OS, Oracle will resume support, including logging a bug with Oracle Development for investigation if required.

If the problem is determined not to be a known Oracle issue, we will refer the customer to the VM vendor for support. When the customer can demonstrate that the issue occurs when running on the native OS, Oracle will resume support, including logging a bug with Oracle Development for investigation if required.

Oracle has not certified any of its products on VMware or any virtual environment.

Oracle RAC (Real Application Cluster) can NOT be installed in any virtualized environment.

More information about virtualization is at the following URL: http://www.oracle.com/technetwork/middleware/ias/oracleas-supported-virtualization-089265.html#vmwaresupportpolicy

16 OPERA Hardware Sizing Template

GENERAL INFORMATION

Current OPERA Version		List Serial Interfaces	
Target OPERA Version		List IP Interfaces	
Current Oracle Version		List HTNG Interfaces	
Target Oracle Version		List OXI Interfaces	
Current Interface Version			
Total # of Properties			
Total # of Interfaces			
Hotel Room Count			
Concurrent User Count			

*All fields above are MANDATORY - enter best estimate

Determining Hardware Sizing Template

Single or Database Server		How Many Server?		IP Address:		Logical Drives	Disk Size	Free Space
Server Model		CPU Model		# Physical Disks		C:		
Server Name		CPU Speed		Capacity per Disk		D:		
Operating System		Total CPU Cores		Physical Disk Speed				
32 or 64 Bit		RAM (GB)		Disk RAID level				

Application Server		How Many Server?		IP Address:		Logical Drives	Disk Size	Free Space
Server Model		CPU Model		# Physical Disks		C:		
Server Name		CPU Speed		Capacity per Disk		D:		
Operating System		Total CPU Cores		Physical Disk Speed				
32 or 64 Bit		RAM (GB)		Disk RAID level				

Interface Server / PC		How Many Server?		IP Address:		Logical Drives	Disk Size	Free Space
Server Model		CPU Model		# Physical Disks		C:		
Server Name		CPU Speed		Capacity per Disk		D:		
Operating System		Total CPU Cores		Physical Disk Speed				
32 or 64 Bit		RAM (GB)		Disk RAID level				

OXI Server		How Many Server?		IP Address:		Logical Drives	Disk Size	Free Space
Server Model		CPU Model		# Physical Disks		C:		
Server Name		CPU Speed		Capacity per Disk		D:		
Operating System		Total CPU Cores		Physical Disk Speed				
32 or 64 Bit		RAM (GB)		Disk RAID level				

An editable version is available by request.