

**Oracle® AutoVue VueLink for Oracle WebCenter
Content**

Security Guide

Release 21.0.1

F17212-02

November 2019

F17212-02

Copyright © 1998, 2019, Oracle and/or its affiliates. All rights reserved.

The Programs (which include both the software and documentation) contain proprietary information; they are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright, patent, and other intellectual and industrial property laws. Reverse engineering, disassembly, or decompilation of the Programs, except to the extent required to obtain interoperability with other independently created software or as specified by law, is prohibited.

The information contained in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. This document is not warranted to be error-free. Except as may be expressly permitted in your license agreement for these Programs, no part of these Programs may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose.

If the Programs are delivered to the United States Government or anyone licensing or using the Programs on behalf of the United States Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

The Programs are not intended for use in any nuclear, aviation, mass transit, medical, or other inherently dangerous applications. It shall be the licensee's responsibility to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use of such applications if the Programs are used for such purposes, and we disclaim liability for any damages caused by such use of the Programs. s.

The Programs may provide links to Web sites and access to content, products, and services from third parties. Oracle is not responsible for the availability of, or any content provided on, third-party Web sites. You bear all risks associated with the use of such content. If you choose to purchase any products or services from a third party, the relationship is directly between you and the third party. Oracle is not responsible for: (a) the quality of third-party products or services; or (b) fulfilling any of the terms of the agreement with the third party, including delivery of products or services and warranty obligations related to purchased products or services. Oracle is not responsible for any loss or damage of any sort that you may incur from dealing with any third party.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Contents

Preface	v
Audience	v
Related Documents	v
Conventions	v
 1 Overview	
Product Overview	1-1
General Security Principles	1-1
Keep up to date on Software	1-1
Keep up to date on Latest Security Information	1-1
Restrict Network Access to VueLink for WCC and Application Server	1-1
Authentication	1-1
 2 Secure Installation and Configuration	
Installation Overview	2-1
Post-Installation Configuration	2-1
Configure HTTPS/SSL Deployment	2-1
Configuring One-Way SSL Communication	2-3
Oracle AutoVue VueLink for Oracle WCC	2-3
Oracle WebLogic Server	2-3
AutoVue Server	2-3
Enterprise Security API Resource Files	2-3
 3 Security Features	
The Security Model	3-1
Configuring and Using Restrict IP Access	3-1
Configuring and Using Authorization	3-2
Configuring and Using Java Security Manager for Oracle WebLogic	3-2
Java Security Manager for VueLink for WCC	3-2
Session Management	3-4
Monitoring Login Attempts	3-4
 4 High-Availability Environment Recommendations	
Seamless Failover	4-1

Active-Passive Cluster Deployment	4-1
Load Balancing	4-2
Passing Cookies to AutoVue Server and VueLink for WCC.....	4-2

A Feedback

General AutoVue Information.....	A-1
Oracle Customer Support	A-1
My Oracle Support AutoVue Community	A-1
Sales Inquiries	A-1

Preface

This documentation provides guidelines on how to secure Oracle AutoVue VueLink for Oracle WCC.

Audience

This document is intended for Oracle partners and customers whose role is to deploy and manage Oracle AutoVue VueLink for Oracle WCC.

Related Documents

For more information, see the following documents:

- *Oracle AutoVue VueLink for Oracle WCC System Administrator Manual*
- *Oracle AutoVue VueLink for Oracle WCC User's Manual*

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
<code>monospace</code>	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Overview

This section provides guidelines on how to securely install and configure Oracle AutoVue VueLink for Oracle WCC.

Product Overview

VueLink provides an interface between the Oracle WebCenter Content server and Oracle AutoVue, Client/Server Deployment. This interface enables you to add powerful viewing and markup capabilities to your WebCenter Content via a Web browser in an intranet or the Internet.

General Security Principles

This section outlines the general security principles of VueLink for WCC.

Keep up to date on Software

One of the principles of good security practice is to keep all software versions and patches up-to-date. Throughout this document a VueLink for WCC maintenance level of 21.0.1 or later is assumed.

Keep up to date on Latest Security Information

Oracle continually improves its software and documentation. Make sure you install the latest version of VueLink for WCC.

Restrict Network Access to VueLink for WCC and Application Server

Keep the VueLink for WCC and application server behind a firewall. In addition, restrict access to components on Oracle Weblogic Server by leveraging a filtering mechanism provided by Weblogic application server.

Authentication

Allow a system to verify the identity of users that request access to VueLink for WCC.

Secure Installation and Configuration

This section describes how to securely install and configure Oracle AutoVue VueLink for Oracle WCC.

Installation Overview

VueLink for WCC is distributed as a ZIP file, VLForUCM.zip. To install, unzip the file to a secure location.

Note: Make sure that the client has an up-to-date version of the JRE. Refer to the *Oracle AutoVue, Client/Server Deployment Release Notes* for more information.

Post-Installation Configuration

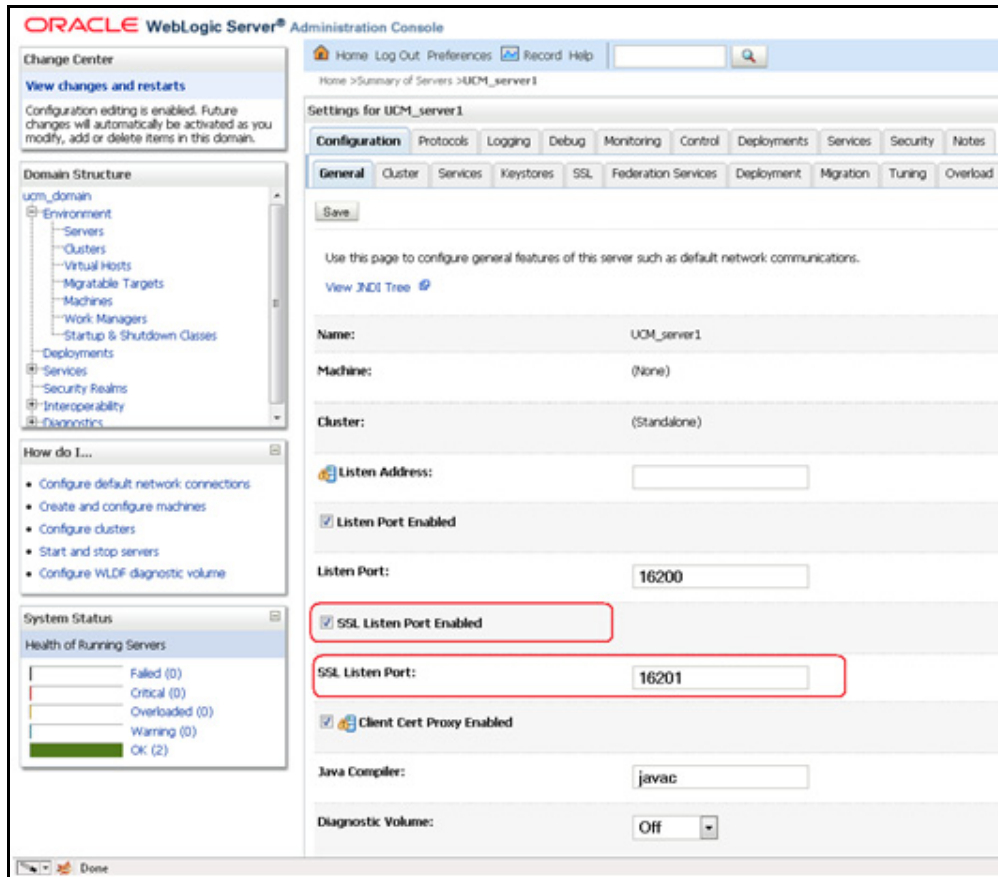
This section discusses security-related configurations that can be made after installing VueLink for WCC.

Configure HTTPS/SSL Deployment

When establishing secure communication between the VueLink for WCC and AutoVue, it is necessary to set up an HTTPS configuration. Since VueLink is only certified with Oracle Weblogic, the following steps describe the setup based on Weblogic Application server.

Note: By default, communication between the VueServlet and AutoVue server are configured using Secure Socket Layer (SSL) protocol.

1. You must first enable HTTPS on the application server.
 - In the Weblogic administration console, select the server that the VueLink is deployed on.
 - From the General Configuration tab, select **SSL Listen Port Enabled**.
 - Set the port number.
By default in Weblogic, but not mandatory, the HTTPS port is one number higher than the HTTP port.



2. A demo certificate is included with Weblogic. It is recommended that you replace this demo certificate with one signed by an internal certificate authority or signed by an external, commercial CA such as Verisign. Refer to the latest version of the Fusion Middleware Administering Security for Oracle WebLogic Server for information on how to replace the demo certificate.
3. Verify the certificate and that the HTTPS connection is working by accessing the VueLink URL through HTTPS protocol and port. For example:

`https://<VueLink host server name>:<HTTPS port>/autovue/servlet/DMS`

If you accept the certificate, you are given the option of storing the certificate in the browser's certificate repository. If you do not accept it, the page just gets blocked.

4. You do not have to import a certificate if you are using the production certificate (ie recognized Certificate Authority signed).

If you do not have a production certificate, then you have to import the certificate into the AutoVue Java Virtual Machine (JVM).

To do so:

- Obtain a copy of the application server's certificate by exporting it from the browser that you used to verify the VueLink HTTPS URL.
- Save the copy of the certificate as a .DER format certificate file.
- Use the JAVA keytool to import the certificate from the file into the JVM that is used by the AutoVue server. For example:

```
keytool -import -file <path to the .DER file> -keystore <path to the java
cacerts file>
```

Make sure to restart the AutoVue server after importing the certificate.

Note: The certificate is being imported into the trust store of the Java virtual machine that is being used to run the AutoVue server.

5. Make sure to login to the WebCenter Content via HTTPS. If WebCenter Content is not leveraging the same application server as VueLink, then follow step 1 to enable SSL on the application server that WebCenter Content is using.

Configuring One-Way SSL Communication

An SSL-enabled development environment for VueLink for WCC includes the following components: VueLink for WCC, AutoVue server, and Oracle WebLogic Server. In one-way SSL, it is required that the server provides a certificate in order to establish a link between a browser and server.

Oracle AutoVue VueLink for Oracle WCC

Use the default SSL configuration. Ensure that the web.xml descriptor file for VueLink for WCC uses the following VueServlet init-param:

```
<init-param>
<param-name>EnableSSL</param-name>
<param-value>true</param-value>
</init-param>
```

Oracle WebLogic Server

For information on how to set SSL refer to the "Setting Up SSL: Main Steps" section of the *Oracle Fusion Middleware Securing Oracle WebLogic Server* document.

AutoVue Server

For information on how to set SSL for Oracle AutoVue if you have a valid CA-issued certificate, refer to the *Oracle AutoVue Client/Server Deployment Security Guide*.

Note: During development you may create a self-signed certificate to test. Alternately, you may use the two default demo keystores provided by the WebLogic Server to setup SSL communication between WebLogic Server and the AutoVue server. For more information, refer to the *Oracle AutoVue Client/Server Deployment Security Guide*.

Enterprise Security API Resource Files

VueLink for WCC is based on the AutoVue Integration Software Development Kit (ISDK) version 21. In this version, a subset of the OWASP ESAPI has been embedded in the ISDK and configured to use separate resource files than the standard implementation. This allows integrators to use the stock OWASP ESAPI package for their own uses without interference.

VueLink for WCC uses the following two resource files (*ESAPI.properties* and *Validation.properties*) provided by the ESAPI and customizes the ESAPI.properties file.

After unzipping VueLink for WCC media pack, the two resource files can be accessed from the unzipped folder. For example, <VueLink for WCC>/ESAPI_resources directory.

Since ESAPI requires that a file path must match the canonical path exactly, all file paths defined in the web.xml descriptor file are case-sensitive. All files defined in web.xml must meet the following requirements of the rules defined in the ESAPI.properties file:

- The filename must match the regular expression defined by Validator.FileName.
- The directory must match the regular expression defined by Validator.DirectoryName.
- The file extension must be included in the allowed list as defined by HttpUtilities.ApprovedUploadExtensions.

ESAPI has a default search order to find and load its resource files. That is, the application server searches specific folder locations for the resource files and then loads these resources before loading applications. It is possible to change the location of the resource files by using -Dorg.owasp.esapi.resources JAVA_OPTIONS in the WebLogic application servers' startup or in the setDomainEnv script.

Example 2-1 Changing the location of the resource files

Step 1: Copy the contents from inside the ESAPI_resources folder to a secure directory.

For example: C:\mysafe_esapi_resources_locations

Step 2: Edit startWebLog.cmd and add a new JAVA_OPTIONS.

For example: Set JAVA_OPTIONS=...-Dorg.owasp.esapi.resources=C:\mysafe_esapi_resources_location

Step 3: Start WebLogic Server. The WebLogic Server console should state that the C:\mysafe_easpi_resources_location\EASPI.properties is found in 'org.owasp.esapi.resources' directory.

Note: You must safe-guard your ESAPI resources directory to avoid unauthorized access.

Security Features

This section outlines specific security mechanisms offered by VueLink for WCC.

The Security Model

Oracle WebCenter Content is a foundational technology for environments having document management requirements. Essentially, in all deployments, WebCenter is extensively customized to meet end-user needs. Most file access control will be driven by and implemented at higher levels, and must be accommodated by the VueLink. The main VueLink security requirements arise from the need to protect data from deliberate unauthorized attempts to access repository contents.

The critical security features that provide these protections are:

- Restrict IP Access - Restrict access to the WebCenter Content and VueLink.
- Authorization - This is only for documents stored inside WebCenter Content.

Configuring and Using Restrict IP Access

Oracle WebCenter Content includes its own restricted IP access control. If VueLink for WCC is deployed on a different machine than that of the WebCenter Content server, then you must make sure that the VueLink IP address is added to SockeHostAddressSecurityFilter in <WebCenter Content home domain>/ucm/cs/config/config.cfg. Restart the WebCenter Content server after modification.

It is also recommended to tighten the deployment and limit access to the VueLink through a filtering mechanism provided by the WebLogic application server.

The following steps describe how to configure the filtering mechanism.

1. Log onto WebLogic Admin console.
2. From the left panel, select the domain that you want to configure (the domain that the VueLink is deployed on).
3. Select **Security** and then **Filter**.
4. Select the **Connection Logger Enabled** checkbox to enable the logging of accepted messages. The Connection Logger logs successful connections and connection data in the server. This information can be used to debug problems relating to server connections.
5. In the **Connection Filter** field, specify the connection filter class to be used in the domain.

To configure the default connection, specify

```
weblogic.security.net.ConnectionFilterImpl
```

6. In the **Connection Filter Rules** field, enter the syntax for the connection filter rules. The syntax is as follows:

```
Target localAddress localPort action protocols
```

The following is the recommended rule set:

```
# Allow access from the Weblogic application server machine
<Weblogic IP or hostname> * * allow
# Allow access from the AutoVue machine
<autovue IP or hostname> * * allow
# Refuse the other access for all other machines
0.0.0.0/0 * * deny
```

Replace the *<Weblogic IP or hostname>* and *<autovue IP or hostname>* with the actual hostname or IP address of the machines.

For information on connection filter rules and syntax, refer to the "Using Network Connection Filters" section in the *Oracle Fusion Middleware Oracle WebLogic Server Administration Console Help*.

7. Click **Save**.
8. Restart the WebLogic Server so that your changes can take effect.

Note: If you accidentally enter rules that completely block access to the WebLogic server, and are no longer able to access the admin console, you must locate the config.xml file inside the WebLogic server machine (under the domain directory) and remove the `<connection-filter-rule>` parameters that deny access to the server from legitimate machines.

Configuring and Using Authorization

VueLink relies on the security feature provided by Oracle WebCenter Content. WebCenter Content secures the document based on the user access level to the document. For detailed information, refer to the "Administering Security" section in the *Oracle Fusion Middleware Administering Oracle WebCenter Content 12c Manual*.

Configuring and Using Java Security Manager for Oracle WebLogic

The Java Security Manager is used with WebLogic Server in order to provide additional protection for resources running on a Java Virtual Machine (JVM).

For detailed information on setting up the Java Security Manager, refer to the *Oracle Fusion Middleware Programming Security for Oracle WebLogic Server*.

Java Security Manager for VueLink for WCC

Deploy VueLink for WCC on a WebLogic Server on a separate managed server than the one Oracle WebCenter Content is deployed on. The following provides an example of how to do so.

Example 3-1 Configuring Java Security Manager for VueLink for WCC on Windows OSes

1. Browse to the <<Weblogic_Home_Directory>>\wlserver_10.3\server\lib folder.
2. Make a copy of weblogic.policy and rename it to vuelink.policy.
3. Add the following permission granting to vuelink.policy:

```
//The path C:/Users/Administrator/AppData/Local/Temp is the
//location of the current user's (in this case, the administrator) Temp folder.
grant codeBase "file:C:/Users/Administrator/AppData/Local/Temp/-" {
    permission java.util.PropertyPermission "*", "read,write";
    permission java.io.FilePermission "C:/Oracle/Middleware/user_
projects/domains/ucm_domain/servers/VueLinkServer/stage/vuelink/-",
"read,write";
    permission java.io.FilePermission "C:/Oracle/Middleware/user_
projects/domains/ucm_domain/servers/VueLinkServer/tmp/_WL_user/vuelink/-",
"read,write";
    permission java.io.FilePermission
"C:/Users/Administrator/AppData/Local/Temp/-", "read,write,delete";
    permission java.io.FilePermission "C:/Temp/-", "read,write,delete";
    //The VueLink log folder defined in log4j.properties
    permission java.lang.RuntimePermission "weblogic.kernelPermission";
    permission java.lang.RuntimePermission "accessDeclaredMembers";
    permission java.lang.RuntimePermission "getClassLoader";
    permission java.net.SocketPermission "*", "connect";
};
```

4. The following permission granting can be added either to vuelink.policy or to the weblogic.xml file of VueLink for WCC. It is only required to add it to one location.

- In vuelink.policy, add the following:

```
grant codeBase "file:C:/Oracle/Middleware/user_projects/domains/ucm_
domain/servers/VueLinkServer/tmp/_WL_user/vuelink/-" {
    permission java.security.AllPermission;
};
```

If more restrictive permissions are required, then they can be added to vuelink.policy. For example:

```
grant codeBase "file:C:/Oracle/Middleware/user_projects/domains/ucm_
domain/servers/VueLinkServer/tmp/_WL_user/vuelink/-" {
    permission java.io.FilePermission "<<ALL FILES>>",
"read,write,execute,delete";
    permission java.util.PropertyPermission "*", "read,write";
    permission java.util.logging.LoggingPermission "control";
    permission java.lang.RuntimePermission "*";
    permission java.security.SecurityPermission "insertProvider.SunJSSE";
};
```

- In weblogic.xml of VueLink for WCC, add the following:

```
<wls:security-permission>
<wls:description>
Allow vuelink all permission
</wls:description>
<wls:security-permission-spec>
    grant {
        permission java.security.AllPermission;
    };
    </wls:security-permission-spec>
</wls:security-permission>
```

5. Start the VueLink server which has deployed VueLink for WCC using the following JAVA_OPTIONS:

```
JAVA_OPTIONS="${JAVA_OPTIONS} -Djava.security.manager  
-Djava.security.policy==C:/Oracle/Middleware/wlserver_  
10.3/server/lib/vuelink.policy"
```

Session Management

The user session established in the VueLink is synchronized with the session in WebCenter Content. When the user logs out of WebCenter Content, or when the session with WebCenter Content expires, AutoVue pops up an authentication dialog prompting for user credentials in order to allow the user to finish any incomplete activities.

Monitoring Login Attempts

If a user login attempt fails, an AutoVue authentication dialog appears. All login attempts are saved in the VueLink and AutoVue server logs (log4j). These logs can then be examined/audited by the system administrator to troubleshoot any issues experienced on the AutoVue server or VueLink. If you are unable to resolve the issue yourself, provide the logging information to an Oracle Global Customer Support representative. Refer to the *Oracle AutoVue, Client/Server Deployment Installation and Configuration Guide* and *Oracle AutoVue VueLink for Oracle WCC System Administrator Manual* for AutoVue and VueLink log file information, respectively.

High-Availability Environment Recommendations

This section provides general cluster deployment recommendations. In environments where information availability is critical, Oracle WebCenter components provide high availability capabilities. By configuring several servers, users can access the system without loss of service even in the event of a server failure. This section provides general cluster deployment recommendations related to the VueLink for WCC deployment.

Seamless Failover

VueLink for WCC is not verified in seamless failover mode. That is, in the event the active instance fails, all unfinished tasks are lost. The passive instance becomes active and starts processing new requests.

Active-Passive Cluster Deployment

The active-passive topology is the recommended cluster deployment for VueLink for WCC.

Note: If the VueLink is deployed on the same application server as WebCenter, you do not have to configure the following parameters:

- 'VueLinkHostName'
 - 'VueLinkPort4HTTP'
 - 'VueLinkPort4HTTPS'
 - 'VueLinkContext'
-

Active-active solutions deploy two or more active system instances and can be used to improve scalability as well as provide high availability. In active-active deployments, all instances handle requests concurrently.

Active-passive solutions deploy an active instance that handles requests and a passive instance that is on standby. In addition, a heartbeat mechanism is set up between these two instances. This mechanism is provided and managed through operating system vendor-specific clusterware. Generally, vendor-specific cluster agents are also available to automatically monitor the failover between cluster nodes, so that when the active instance fails, an agent shuts down the active instance completely, brings up the passive instance, and application services can successfully resume processing. As a

result, the active-passive roles are now switched. The same procedure can be done manually for planned or unplanned downtime. Active-passive solutions are also generally referred to as cold failover clusters.

Note: VueLink for WCC does not require any special configuration for active-passive cluster and works based on the recommendations from the Configuring the OHS Server.

The Oracle HTTP Server uses a session-based round-robin load balancing mechanism. While the load balancer attempts to rotate between all node, it maintains an established session to a single node (all requests with that session ID are directed to the same node).

Load Balancing

Load balancing can be achieved using a hardware load balancer when using an active-passive topology.

Passing Cookies to AutoVue Server and VueLink for WCC

Parameter DMS_PRESERVE_COOKIES can be set to specify the cookies that should be passed from the AutoVue client to the AutoVue Server and VueLink. This parameter is defined in the viewer launch page (view_in_autovue_page.htm). Currently the parameter is set to 'true' in the distribution, which passes all WCC related cookies to be passed to the AutoVue Server and VueLink. In more restricted environments, the list could be made more explicit to restrict the values that are passed. Vuelink requires the following key values:

- JSESSIONID: WebCenter Content session identifier. This value is used so that the load balancer can maintain sticky sessions.
- PK: Public key. This value is needed by the VueLink when communicating with WebCenter Content.
- username: username. This value is needed by the VueLink when communicating with WebCenter Content

DMS_PRESERVE_COOKIES ensures that JSESSIONID, PK, and username cookies are passed from the AutoVue Client to the AutoVue server and then onto the VueLink.

For more information on DMS_PRESERVE_COOKIES, refer to the *Oracle AutoVue, Client/Server Deployment Installation and Configuration Guide*.

Feedback

If you have any questions or require support for AutoVue please contact your system administrator.

If at any time you have questions or concerns regarding AutoVue, please contact us.

General AutoVue Information

Web Site <http://www.oracle.com/us/products/applications/autovue/index.html>

Blog <http://blogs.oracle.com/enterprisevisualization/>

Oracle Customer Support

Web Site <http://www.oracle.com/support/index.html>

My Oracle Support AutoVue Community

Web Site <https://communities.oracle.com/portal/server.pt>

Sales Inquiries

Web Site <https://www.oracle.com/corporate/contact/global.html>
