Oracle® AutoVue VueLink for Oracle UCM

Security Guide

Release 20.1.0

December 2011

Oracle AutoVue VueLink for Oracle UCM/Security Guide, Release 20.1.0

Contents

4 Feedback

Preface

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

Audience

This document is intended for Oracle partners and third-party developers (such as integrators) whose role is to deploy and manage Oracle AutoVue VueLink for Oracle UCM.

Related Documents

For more information, see the following documents:

- *Oracle AutoVue VueLink for Oracle UCM System Administrator Manual*
- *Oracle AutoVue VueLink for Oracle UCM Clustering Guide*
- *Oracle AutoVue VueLink for Oracle UCM 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.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1

Overview

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

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 UCM.

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 UCM maintenance level of 20.1.0 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 UCM.

Restrict Network Access to VueLink for UCM and Application Server

Keep the VueLink for UCM 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 UCM.

// 2

Secure Installation and Configuration

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

Installation Overview

VueLink for UCM 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

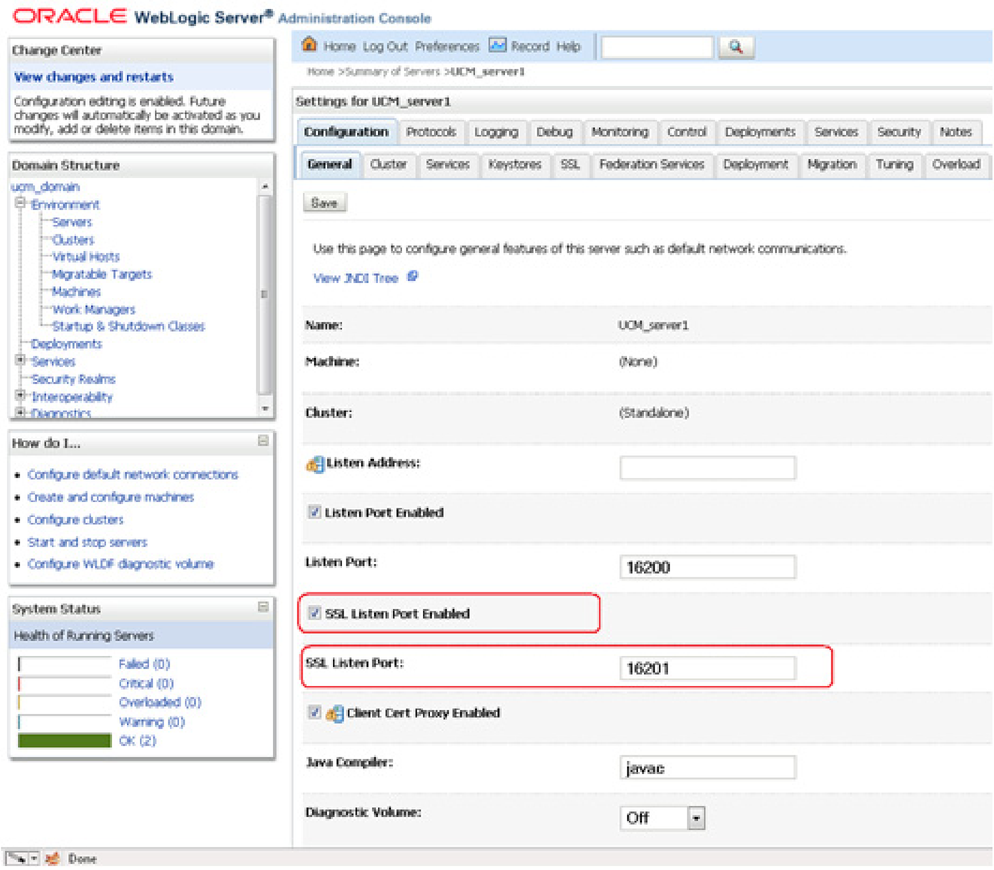
This section discusses security-related configurations that can be made after installing VueLink for UCM.

Configure HTTPS/SSL Deployment

When establishing secure communication between the VueLink for UCM 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.


ORACLE WebLogic Server® Administration Console
Change Center
View changes and restarts
Domain Structure
ucm_domain
Environment
Servers
Clusters
Virtual Hosts
Migratable Targets
Machines
Work Managers
Startup & Shutdown Classes
Deployments
Services
Security Realms
Interoperability
Diagnostics
How do I...
Configure default network connections
Create and configure machines
Configure clusters
Start and stop servers
Configure WLDF diagnostic volume
System Status
Health of Running Servers
Failed (0)
Critical (0)
Overloaded (0)
Warning (0)
OK (2)
Home Log Out Preferences Record Help
Home >Summary of Servers >UCM_server1
Settings for UCM_server1
Configuration Protocols Logging Debug Monitoring Control Deployments Services Security Notes
General Cluster Services Keystores SSL Federation Services Deployment Migration Tuning Overload
Save
View JNDI Tree
Done

Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

Use this page to configure general features of this server such as default network communications.

Name: UCM_server1

Machine: (None)

Cluster: (Standalone)

Listen Address:

☑ Listen Port Enabled

Listen Port: 16200

☑ SSL Listen Port Enabled

SSL Listen Port: 16201

☑ Client Cert Proxy Enabled

Java Compiler: javac

Diagnostic Volume: Off

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 *Weblogic Administration Guide* 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>/vuelink/DMS
   ```

   If the certificate is not trusted, the browser prompts you to accept it. If you do not accept it, then the certificate is stored automatically in the browser certificate repository.

4. Import the certificate into the AutoVue Java Virtual Machine (JVM).

   The application server certificate must be imported into the JVM that AutoVue is using. 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

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 UCM includes the following components: VueLink for UCM, 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 UCM

Use the default SSL configuration. Ensure that the web.xml descriptor file for VueLink for UCM 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*.

Configuring Two-Way SSL Communication

This section describes how to configure a two-way SSL communication with the WebLogic Server. Two-way SSL requires that the client, in addition to the server, submits a certificate. Note that it is necessary to have one-way SSL working before moving on to two-way. Refer to section "Configuring One-Way SSL Communication" for more information.

Step 1: Configure one-way SSL

Refer to section "Configuring One-Way SSL Communication" for more information.

Step 2: Create a client certificate

1. Run setDomainEnv.cmd script in your domain’s bin directory.
2. Change to a working directory of your choice.
3. User CertGen to create a client certificate as in the following example:

```
java utils.CertGen -certfile certfile.cer -keyfile keyfile.key -keyfilepass
```

```
mypassword -cn myclient
```

4. The files are created in DER and PEM formats. Note that most browsers do not recognize PEM/DER files. As a result, the key and certificate must be converted into a PKCS #12 file. To do so, enter the following:

```
java utils.ImportPrivateKey -keystore myclient.p12 -storepass mypassword
-storetype pkcs12 -keypass mypassword -alias personal -certfile
certfile.cer.pem -keyfile keyfile.key.pem -keyfilepass mypassword
```

Step 3: Load the client certificate into your browser

- For Internet Explorer (IE)
  1. From the IE menu, select **Tools**, **Internet Options**, **Content**, and then **Certificates**.
  2. Click on the **Personal** tab.
  3. Import myclient.p12 (the password is *mypassword*)
- For FireFox
  1. From the FireFox menu, select **Tools**, **Options**, **Advanced**, and then **Encryption**.
  2. To see the client certificate request, select **Ask me every time**.
  3. Click **View Certificates**.
  4. Click on the **Your Certificates** tab.
  5. Import myclient.p12 (the password is *mypassword*).

Step 4: Import client certificate into JRE (FireFox only)

1. Open the Java Control Panel.
2. Select **Security** and then **Certificate**.
3. Import myclient.p12 as a Certificate Type into Client Authentication.

Step 5: Set two-way SSL

1. Select the server from the WebLogic admin console.
2. Click the **SSL** tab, select **Advanced**, **Two Way Client Cert Behavior**, and then select **Client Cert Requested and Enforced**.
3. Select **Use Server Certs**.

Note: This step is needed for the VueLink to use server credentials.

4. Save the settings.
5. Restart the server for the changes to take effect.

Step 6: Import client certificate to WebLogic truststore

1. Import the CertGenCA.der certificate located in weblogic/server/lib directory to the WebLogic truststore with the following command:

```
keytool -import -file CertGenCA.der -keystore serverTrustStore.jks -alias
certgenca
```

Step 7: Select a digital certificate when connecting to the browser

When connecting to the UCM or WebLogic console after you set-up two-way SSL, a Choose a Digital Certificate dialog appears. From the dialog, select the myclient certificate listed and then click **OK**.

Enterprise Security API Resource Files

This release of the VueLink for UCM introduces Open Web Application Security Project (OWASP) Enterprise Security API (ESAPI) Java Edition and related ESAPI to provided enhanced security.

VueLink for UCM 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 UCM media pack, the two resource files can be accessed from the unzipped folder. For example, <VueLink for UCM>/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.espai.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.

3

Security Features

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

The Security Model

The VueLink security requirements arise from the need to protect data from deliberate unauthorized attempts to access the file.

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 UCM 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 "Managing Security and User Access" section in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Content Server 11g Release 1*.

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 UCM

Deploy VueLink for UCM 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 UCM 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 UCM. 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 UCM, 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 UCM 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 UCM System Administrator Manual* for AutoVue and VueLink log file information, respectively.

4

Feedback

If you have any questions or require support for VueLink please contact your system administrator. Some customization and maintenance must be done on the server and cannot be implemented on the client machine. If the administrator is unable to resolve the issue, please contact Oracle Corp.

General Inquiries

Telephone	+1.514.905.8400 or +1.800.363.5805
E-mail	autovuesales_ww@oracle.com
Web Site	http://www.oracle.com/us/products/applications/autovue/index.html

Sales Inquiries

Telephone	+1.514.905.8400 or +1.800.363.5805
E-mail	autovuesales_ww@oracle.com

Customer Support

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