|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| [Click to add to Favorites](https://support.oracle.com/epmos/faces/DocumentDisplay?_afrLoop=24130268059820&parent=SrDetailText&sourceId=3-37305896731&id=2188982.1&_afrWindowMode=0&_adf.ctrl-state=b5br22nsj_108) |  | **OBIEE 12c/OAS: How To Configure SSL Including Examples (Doc ID 2188982.1)** | [[To Bottom](https://support.oracle.com/epmos/faces/DocumentDisplay?_afrLoop=24130268059820&parent=SrDetailText&sourceId=3-37305896731&id=2188982.1&_afrWindowMode=0&_adf.ctrl-state=b5br22nsj_108)To Bottom](https://support.oracle.com/epmos/faces/DocumentDisplay?_afrLoop=24130268059820&parent=SrDetailText&sourceId=3-37305896731&id=2188982.1&_afrWindowMode=0&_adf.ctrl-state=b5br22nsj_108) |  |



|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **In this Document**   |  |  | | --- | --- | |  | [Purpose](https://support.oracle.com/epmos/faces/DocumentDisplay?_afrLoop=24130268059820&parent=SrDetailText&sourceId=3-37305896731&id=2188982.1&_afrWindowMode=0&_adf.ctrl-state=b5br22nsj_108#PURPOSE) |  |  |  | | --- | --- | |  | [Scope](https://support.oracle.com/epmos/faces/DocumentDisplay?_afrLoop=24130268059820&parent=SrDetailText&sourceId=3-37305896731&id=2188982.1&_afrWindowMode=0&_adf.ctrl-state=b5br22nsj_108#SCOPE) |  |  |  | | --- | --- | |  | [Details](https://support.oracle.com/epmos/faces/DocumentDisplay?_afrLoop=24130268059820&parent=SrDetailText&sourceId=3-37305896731&id=2188982.1&_afrWindowMode=0&_adf.ctrl-state=b5br22nsj_108#BODYTEXT) |  |  |  | | --- | --- | |  | [**High-Level Steps to enable SSL for OBIEE 12c/OAS**](https://support.oracle.com/epmos/faces/DocumentDisplay?_afrLoop=24130268059820&parent=SrDetailText&sourceId=3-37305896731&id=2188982.1&_afrWindowMode=0&_adf.ctrl-state=b5br22nsj_108#aref_section31) |  |  |  | | --- | --- | |  | [**Step 1: Generate the required certificates and keystores for SSL communication**](https://support.oracle.com/epmos/faces/DocumentDisplay?_afrLoop=24130268059820&parent=SrDetailText&sourceId=3-37305896731&id=2188982.1&_afrWindowMode=0&_adf.ctrl-state=b5br22nsj_108#aref_section32) |  |  |  | | --- | --- | |  | [***Step 2: Configure Weblogic Admin Server, Node Manager and Managed Server for SSL***](https://support.oracle.com/epmos/faces/DocumentDisplay?_afrLoop=24130268059820&parent=SrDetailText&sourceId=3-37305896731&id=2188982.1&_afrWindowMode=0&_adf.ctrl-state=b5br22nsj_108#aref_section33) |  |  |  | | --- | --- | |  | [**Step 3: Configuring Internal WebLogic Server LDAP to Use LDAPs**](https://support.oracle.com/epmos/faces/DocumentDisplay?_afrLoop=24130268059820&parent=SrDetailText&sourceId=3-37305896731&id=2188982.1&_afrWindowMode=0&_adf.ctrl-state=b5br22nsj_108#aref_section34) |  |  |  | | --- | --- | |  | [**Step 4: Configuring Internal WebLogic Server LDAP Trust Store**](https://support.oracle.com/epmos/faces/DocumentDisplay?_afrLoop=24130268059820&parent=SrDetailText&sourceId=3-37305896731&id=2188982.1&_afrWindowMode=0&_adf.ctrl-state=b5br22nsj_108#aref_section35) |  |  |  | | --- | --- | |  | [**Step 5:  Disabling HTTP**](https://support.oracle.com/epmos/faces/DocumentDisplay?_afrLoop=24130268059820&parent=SrDetailText&sourceId=3-37305896731&id=2188982.1&_afrWindowMode=0&_adf.ctrl-state=b5br22nsj_108#aref_section36) |  |  |  | | --- | --- | |  | [**Step 6: Configuring OWSM to Use t3s**](https://support.oracle.com/epmos/faces/DocumentDisplay?_afrLoop=24130268059820&parent=SrDetailText&sourceId=3-37305896731&id=2188982.1&_afrWindowMode=0&_adf.ctrl-state=b5br22nsj_108#aref_section37) |  |  |  | | --- | --- | |  | [**Step 7: Enabling Internal SSL for OBIEE**](https://support.oracle.com/epmos/faces/DocumentDisplay?_afrLoop=24130268059820&parent=SrDetailText&sourceId=3-37305896731&id=2188982.1&_afrWindowMode=0&_adf.ctrl-state=b5br22nsj_108#aref_section38) |  |  |  | | --- | --- | |  | [References](https://support.oracle.com/epmos/faces/DocumentDisplay?_afrLoop=24130268059820&parent=SrDetailText&sourceId=3-37305896731&id=2188982.1&_afrWindowMode=0&_adf.ctrl-state=b5br22nsj_108#REF) |   **Applies to:**  Business Intelligence Suite Enterprise Edition - Version 12.2.1.2.0 and later Business Intelligence Server Enterprise Edition - Version 12.2.1.0.0 and later Oracle Analytics Server - Version 5.5.0 and later Information in this document applies to any platform.  **Purpose**  The document is created to provide step-by-step instruction to enable SSL for OBIEE 12c. It includes and example with one basic use case.  This document is intended to supplement the product documentation.  It is recommended to follow the product documentation.    For detailed information on enabling SSL for OBIEE, please refer to Oracle Fusion Middleware Security Guide for Oracle Business Intelligence Enterprise Edition - [Chapter 5 Configuring SSL in Oracle Business Intelligence](https://docs.oracle.com/middleware/bi12214/biee/BIESC/GUID-B3F876BE-9344-4803-9B99-5A4C64F68D6C.htm#GUID-B3F876BE-9344-4803-9B99-5A4C64F68D6C).    **Scope**  This document is informational and intended for Administrators and advanced users.  Before following this document, the user must have a good understanding of secure socket layer communications (SSL), your environment and your specific implementation details.  **Details**  **High-Level Steps to enable SSL for OBIEE 12c/OAS**   1. Generate the required certificates and keystores for SSL communication 2. Configure Weblogic Admin Server, Node Manager and Managed Server for SSL 3. Configuring Internal WebLogic Server LDAP to Use LDAPs 4. Configuring Internal WebLogic Server LDAP Trust Store 5. Disabling HTTP 6. Configure OWSM to use t3s 7. Enabling Oracle BI EE Internal SSL for BIEE     ***Step 1: Generate the required certificates and keystores for SSL communication***   1. Create a folder to store certificates and keystores.  For example: <ORACLE\_HOME>/SSL 2. To invoke java keytool, set the environment variable PATH to include the JAVA\_HOME/bin directory. It is recommended to use the Java|JDK version used to install OBIEE 12c.  Windows:   set JAVA\_HOME=<path to JAVA install root>  set PATH=%JAVA\_HOME%/bin;%PATH%  Unix:  export JAVA\_HOME=<path to JAVA install root>  export PATH=$JAVA\_HOME/bin:$PATH     1. Create the Java Keystore using Java keytool utility.  keytool -genkey -alias <alias> -keyalg RSA -sigalg SHA256withRSA -keysize 2048 -keypass <password> -keystore mykeystore.jks -storepass <password> -storetype JKS -validity 365  For example:   keytool -genkey -alias obiee -keyalg RSA -sigalg SHA256withRSA -keysize 2048 -keypass Welcome99 -keystore mykeystore.jks -storepass Welcome99 -storetype JKS -validity 365 What is your first and last name? [Unknown]: *<hostname>* What is the name of your organizational unit? [Unknown]: Support What is the name of your organization? [Unknown]: Oracle What is the name of your City or Locality? [Unknown]: Pleasanton What is the name of your State or Province? [Unknown]: California What is the two-letter country code for this unit? [Unknown]: US Is CN=*<hostname>*, OU=Support, O=Oracle, L=Pleasanton, ST=California, C=US correct? [no]: yes  Execute the above command on the command window from the folder <ORACLE\_HOME>/SSL  The above command options are only an example. Keystore can be created with different options and values based on the setup requirement. For more information on keytool options, type keytool and press enter on command prompt.  For CN option in the command, set the value to hostname or FQDN of the machine where OBIEE 12c is setup. Wildcard can also be used as a value for CN. The preferred value is hostname or FQDN.   1. Create a Certificate signing request (CSR) using the following command:  keytool -certreq -v -alias <alias> -keyalg RSA -sigalg SHA256withRSA -file <filename> -keypass <password> -keystore <keystore> -storepass <password>   For example:  keytool -certreq -v -alias obiee -keyalg RSA -sigalg SHA256withRSA -file server.csr -keypass Welcome99 -storepass Welcome99 -keystore mykeystore.jks Certification request stored in file <server.csr> Submit this to your CA     1. Submit the Certification request to your Signing Authority (CA). Certification Authority(CA) is an valid signing authority of your choice (for example: Verisign, Microsoft, etc.) Upon submission of the certificate request, CA returns the certificate for the server (Server Certificate). Copy the CA certificate (intermediate certificates if there are any) and Server Certificate to <ORACLE\_HOME>/SSL folder. 2. Import the CA certificate (Root certificate), Intermediate Certificate (if there is any) and Server Certificate into two locations.   Your Custom Keystore (see examples below)  The JAVA\_HOME keystore (that is the JDK location that you installed, and are running Weblogic with). This location is requires importing the same certificates as the custom keystore for the start.sh| .cmd wrapper scripts which internally call the weblogic scripting tool (wlst.sh | .cmd) to connect to the nodemanager.  Example:    [JDK]/bin/keytool -import -alias <aliasname> -file <path/file.cer> -keystore [JDK]/jre/lib/security/cacerts    The default passwords are 'changeit'. If you have changed the password to something else, then use your configured password.   1. Use the following command to verify whether the keytstore contains the certificates (CA certificate, Intermediate and Server certificate)  keytool -list -keystore <keystore> -storepass <password>  For example:   keytool -list -keystore mykeystore.jks -storepass Welcome99  Note: If the Keystore consists of a chain of certificates it is necessary to use the following command against a keystore for validation:  keytool -list -v -keystore mykeystore.jks  Additionally, you can check if the chaining of the certificate is correct by running the following command:  java utils.ValidateCertChain -jks <alias> mykeystore.jks  Note: If you have .p7b certificates from the Certificate Authority, instead of extracting certificates from it and then importing each to the keystore, another option is to run this command:  keytool -import -trustcacerts -alias obiee -file cert.p7b -keystore mykeystore.jks  Note : You should get a confirmation stating that the "Certificate reply was installed in keystore". This is a confirmation that the chaining was successful.      ***Step 2: Configure Weblogic Admin Server, Node Manager and Managed Server for SSL***    Configure Weblogic Admin Server for SSL.   * Log in to WebLogic console. * Click Lock and Edit. * Select Environment >Servers. Click on Admin Server.  In the 'General' tab:   + Check 'SSL Listen Port Enabled'   + 'SSL Listen Port' : <port> e.g 9501 (make sure the port is available)   + Click 'Save' * Select Keystores tab and click change button to select Custom Identity and Custom Trust for keystores.  (The default option from the install, is Demo Identity and Demo Trust. There are 4 options for keystores. Select them as per your requirement).  Update the information on the keystore page based on the information from keystore creation in Step 1.   + 'Custom Identity Keystore' : <path\_to\_keystore> e.g <ORACLE\_HOME>/ssl/mykeystore.jks   + 'Custom Identity Keystore' : JKS   + 'Custom Identity Keystore Passphrase' : <storepass\_pwd> e.g: Welcome99   + 'Confirm Custom Identity Keystore Passphrase' : <storepass\_pwd> e.g: Welcome99   + 'Custom Trust Keystore' : <path\_to\_keystore> e.g <ORACLE\_HOME>/ssl/mykeystore.jks   + 'Custom Trust Keystore Type' : JKS   + 'Custom Trust Keystore Passphrase' : <storepass\_pwd> e.g: Welcome99   + 'Confirm Custom Trust Keystore Passphrase' : <storepass\_pwd> e.g: Welcome99   + Click 'Save'.   In the above example, the Custom Identity Trust keystore and Custom Trust Keystore are same. If there is a requirement to keep the trust certificates in a separate keystore, then store the trust certificates in Custom Trust Keystore and all other certificates in Custom Identity Trust Keystore.   * Select the 'SSL' tab and enter the relevant information based on Step 1.   + 'Private Key Alias' : <alias\_given\_when\_creating\_key> e.g obiee   + 'Private Key Password' : <keypass\_pwd> e.g Welcome99   + 'Confirm Private Key Password': <keypass\_pwd> e.g Welcome99   + Click 'Save' * Select Environment > Servers. Click Managed Server bi\_server1. * Under General tab and Check the SSL Listen Port.  Click Save. * Activate Changes.         Note: If there is no requirement keep similar configuration for AdminServer and Managed Server        Configure Nodemanager for SSL:   * Update the nodemanager.properties in <DOMAIN\_HOME>/nodemanager folder with Custom Identity Keystore and Custom Trust Keystore information based on Step 1.  KeyStores=CustomIdentityAndCustomTrust CustomIdentityKeyStoreFileName=<Path to the Keystore> CustomIdentityAlias=<Keystore Alias> CustomIdentityPrivateKeyPassPhrase=<Key Passphrase> CustomTrustKeyStoreFileName=<Path to the Keystore  For example:   KeyStores=CustomIdentityAndCustomTrust CustomIdentityKeyStoreFileName=/refresh/home/oracle/middleware/oracle\_home/ssl/mykeystore.jks CustomIdentityAlias=obiee CustomIdentityPrivateKeyPassPhrase=Welcome99 CustomTrustKeyStoreFileName=/refresh/home/oracle/middleware/oracle\_home/ssl/mykeystore.jks     * Import the Public certficates (root and intermediate) to Java Standard Trust Store , <JAVA\_HOME>/jre/lib/security   keytool -import -trustcacerts -alias myCARoot -file /refresh/home/oracle/middleware/oracle\_home/ssl/cacert.pem -keystore cacerts -storepass changeit  keytool -import -trustcacerts -alias myIntermediate -file /refresh/home/oracle/middleware/oracle\_home/ssl/Intercacert.pem -keystore cacerts -storepass changeit     * Stop all the services using stop.cmd or stop.sh in <DOMAIN\_HOME>/bitools/bin folder (Note: stop script may not stop nodemanager completly. In that case, stop nodemanager using <DOMAIN\_HOME>/bin/stopNodeManager.sh or stopNodeManager.cmd script.   ***Step 3: Configuring Internal WebLogic Server LDAP to Use LDAPs***   Reference document Oracle Fusion Middleware Security Guide for Oracle Business Intelligence Enterprise Edition**-**[Configuring Internal WebLogic Server LDAP to Use LDAPs](http://docs.oracle.com/middleware/12212/biee/BIESC/GUID-BAB53CD1-647A-4B4B-A666-B47A88528E39.htm#GUID-89E3664C-02F2-48BF-8328-B928E6985F8A)   This step is not needed if external LDAP authenticator is configured.   * Login to EM. Click weblogic domain>Security >Security Provider configuration * Expand the Identity Store Provider * Click Configure. * Click + or Add to add a new property * Select ldap.url from the list. Enter the value ldaps://<adminserver hostname>:<https port> * Click OK.     ***Step 4: Configuring Internal WebLogic Server LDAP Trust Store***  Refer to the documentation for detailed information  - Oracle Fusion Middleware Security Guide for Oracle Business Intelligence Enterprise Edition - [Configuring Internal WebLogic Server LDAP Trust Store](http://docs.oracle.com/middleware/12211/biee/BIESC/GUID-BAB53CD1-647A-4B4B-A666-B47A88528E39.htm#GUID-8D6B9812-6C7C-4947-9742-01C58764622E) Make sure weblogic Admin and Managed Servers are up and running.   * Login to EM. Click weblogic domain>Security >Security Provider configuration * Expand the Identity Store Provider * Click Configure. * Click + or Add to add a new property * Select virtualize from the list. Enter "true" as the value. Click OK.Click OK. * Restart the services.   Create LDAP Trust Store "adapters.jks" Here is an example:   * Set the following environment variables * export ORACLE\_HOME=/export/home/oracle/middleware/oracle\_home * export WL\_HOME=/export/home/oracle/middleware/oracle\_home/wlserver * export JAVA\_HOME=<path to JAVA install root> * export PATH=$JAVA\_HOME/bin:$PATH * cd $ORACLE\_HOME/oracle\_common/bin  ./libovdconfig.sh -host *<hostname>* -port 9500 -domainPath *<domain\_home>* -userName weblogic -createKeystore        * Import the SSL certificates into adapters.jks created in <DOMAIN\_HOME>/config/fmwconfig/ovd/default/keystores folder.   For Windows environment, use libovdconfig.bat script, here is an example :   libovdconfig.bat -host *<hostname>* -port 9500 -domainPath <domain\_home> -userName weblogic -createKeystore  Note: Please note libovdconfig.sh/bat script need to be executed with non SSL port of AdminServer.  ***Step 5:  Disabling HTTP***    Document referenced Oracle Fusion Middleware Security Guide for Oracle Business Intelligence Enterprise Edition - [Disabling HTTP](http://docs.oracle.com/middleware/12211/biee/BIESC/GUID-BAB53CD1-647A-4B4B-A666-B47A88528E39.htm#GUID-BCB3E229-D67D-48A1-9563-62698CCEC3CB)   * Login to Admin Console * Lock and Edit * Navigate to Environment > Servers > Admin Server * In Admin Server General tab, uncheck Listen Port. * Click Save * Navigate to Environment > Servers > bi\_server1 * In Managed Server bi\_server1 general tab, uncheck Listen Port. Click Save. * Navigate to Environment > Cluster > bi\_cluster * Click Replication tab. Check the Secure Replication. * Click Save. * Activate changes * Restart the services using start.sh or start.cmd in <DOMAIN\_HOME>/bitools/bin folder   ***Step 6: Configuring OWSM to Use t3s***  Note: Perform the step 6 only if the status is "out of sync". If the status is "wired", no need to perform the steps.  Refer to the following documentation for detailed information - Oracle Fusion Middleware Security Guide for Oracle Business Intelligence Enterprise Edition - [Configuring OWSM to Use t3s](http://docs.oracle.com/middleware/12211/biee/BIESC/GUID-BAB53CD1-647A-4B4B-A666-B47A88528E39.htm#GUID-08CBA4DC-C24E-4B33-A4B1-A1B09BE18165)      ***Step 7: Enabling Internal SSL for OBIEE***    Document Referenced: Oracle Fusion Middleware Security Guide for Oracle Business Intelligence Enterprise Edition - [Enabling Oracle BI EE Internal SSL](http://docs.oracle.com/middleware/12211/biee/BIESC/GUID-68147341-943A-4E87-9864-260285B24412.htm#BIESC6423)  execute:  <DOMAIN\_HOME>/bitools/bin/ssl.sh | .cmd script to enable internal SSL for OBIEE  Note: Weblogic server need to be configured with SSL prior to enabling Oracle BIEE internal SSL.  There is an issue with enabling internal Oracle BIEE SSL on Windows prior to OBIEE 12.2.1.3 version. The Presentation Server ( OBIPS ) Fails To Start After Enabling Internal SSL on Windows Platform. This is fixed in 12.2.1.3.x and higher versions    For example:  /ssl.sh internalssl true  Logging to: /refresh/home/oracle/middleware/oracle\_home/user\_projects/domains/bi/bilogs/sslcommand.log  Reading domain Setting protocol to https for server bi\_server1 Rebinding channel certificates for server bi\_server1 Checking certificate exists for endpoint: BI-SECURITY-SOAP.bi\_server1 http://*<hostname>*:9505/bi-security/service - custom channel bi\_internal\_channel1 No new certificates required. Internal BIEE communications have been configured to use SSL with certificates matching the current listening addresses. Rerun if you change the addresses. To achieve end to end security you also need to review the SSL configuration of other components, including the external ports of WebLogic servers.  All certificates have more than 30 days to expiry.  Startup all BIEE servers to consume the new configuration. For example run the start[.sh] command line tool in the same directory as this ssl tool.     * Prior to executing the start.sh script, check whether <DOMAIN\_HOME>/nodemanager/nodemanager.properties  includes the required parameters as documented above. * After enabling Oracle BI EE Internal SSL, start all the services via <DOMAIN\_HOME>/bitools/bin/start.sh | .cmd     After the successful start of the service, validate the configuration by running SSL report and also accessing the https URL's  For example:  ./ssl.sh report Logging to: /refresh/home/oracle/middleware/oracle\_home/user\_projects/domains/bi/bilogs/sslcommand.log  Internal SSL enabled Client verification disabled (One way SSL) Using all available default ciphers Type: OBICCS Scanning endpoint OBICCS.obiccs1 tcp(s)://*<hostname>*:9508(9508)/ - System Component Type: OBIJH Scanning endpoint OBIJH.obijh1 tcp(s)://*<hostname>*:9510(9510)/ - System Component Type: OBIPS Scanning endpoint OBIPS.obips1 tcp(s)://*<hostname>*:9507(9507)/ - System Component Type: OBIS Scanning endpoint OBIS.obis1 tcp(s)://*<hostname>*:9514(9514)/ - System Component Type: OBISCH Scanning endpoint OBISCH.obisch1 tcp(s)://*<hostname>*:9511(9511)/ - System Component Type: BI-SECURITY-SOAP Scanning endpoint BI-SECURITY-SOAP.bi\_server1 https://*<hostname>*:9505/bi-security/service - custom channel bi\_internal\_channel1  Summary: Out of 6 endpoints 6 succeeded, and 0 failed.  Ping successes (6): Target: obiccs1:OBICCS @ *<hostname>*:9508 Java client: SSL ping OK. Protocol: TLSv1.2. Cipher: TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256. One way SSL. Openssl client: SSL ping OK. Target: obijh1:OBIJH @ *<hostname>*:9510 Java client: SSL ping OK. Protocol: TLSv1.2. Cipher: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256. One way SSL. Openssl client: SSL ping OK. Target: obips1:OBIPS @ *<hostname>*:9507 Java client: SSL ping OK. Protocol: TLSv1.2. Cipher: TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256. One way SSL. Openssl client: SSL ping OK. Target: obis1:OBIS @ *<hostname>*:9514 Java client: SSL ping OK. Protocol: TLSv1.2. Cipher: TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256. One way SSL. Openssl client: SSL ping OK. Target: obisch1:OBISCH @ *<hostname>*:9511 Java client: SSL ping OK. Protocol: TLSv1.2. Cipher: TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256. One way SSL. Openssl client: SSL ping OK. Target: bi\_server1:BI-SECURITY-SOAP @ *<hostname>*:9505 Java client: SSL ping OK. Protocol: TLSv1.2. Cipher: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256. One way SSL. Openssl client: SSL ping OK.  Ping failures (0):  The first certificate to expire will expire on: 9/2/36 7:37 AM All certificates have more than 30 days to expiry.    Test the connectivity to Oracle BI EE Clients Administration Tool, Catalog Manager and Job Manager.   * Admin Tool - SSL  Create a DSN with Use SSL checked. One way SSL is configured by default. For Client Certificate verification (Two way SSL), Click Configure SSL to configure the required certificates.    Connect to Repository in Online mode using SSL * Catalog Manager - SSL Perform the below step to connect to catalog manager using https URL.   Import the SSL certificates into Java Standard Truststore, cacerts in <BIClientInstall Root>/oracle\_common/jdk/jre/lib/security folder using keytool utility.   cd <BIClientInstall Root>/oracle\_common/jdk/jre/lib/security  keytool -import -trustcacerts -alias myCARoot -file *<oracle\_home>*/ssl/cacert.pem -keystore cacerts -storepass changeit  keytool -import -trustcacerts -alias myIntermediate -file *<oracle\_home>*/ssl/Intercacert.pem -keystore cacerts -storepass changeit  keytool -import -alias obiee -file *<oracle\_home>*/ssl/server.pem -keystore cacerts -storepass changeit  Connect to Catalog in online mode using SSL   * Job Manager - SSL Check the Use SSL check box. For Client Certificate verification (Two way SSL) update keystore and other configuration in addition to Use SSL.     Connect to Job manager using SSL * Agent -SSL                For Oracle Analytics Server, the following configuration is required to access DV Local Subject Area in SSL configured setup. This configuration also helps any issues with datamodel.sh upload/download commands.             Import the internal trust certificate to Custom keystore used for SSL configuration for weblogic (ex: mykeystore.jks - Refer the weblogic SSL configuration steps in this document)             Internal trust certificate location : <DOMAIN\_HOME>/user\_projects/domains/bi/config/fmwconfig/biconfig/core/ssl/internaltrust/internalca.pem    keytool -import -alias <aliasname for internal trust> -keystore <custom keystore used for weblogic ssl configuration> -storepass <custom keystore password> -file <Internal trust certifiate>  ex: keytool -import -alias internaltrustca -keystore /refresh/home/oracle/middleware/oracle\_home/ssl/mykeystore.jks -storepass Welcome99 -file  /domain\_home/user\_projects/domains/bi/config/fmwconfig/biconfig/core/ssl/internaltrust/internalca.pem               If there is any issue importing pem file, convert it into der format using the following syntax:            ${ORACLE\_HOME}/bi/bifoundation/server/bin/openssl x509 -outform der -in ${DOMAIN\_HOME}/config/fmwconfig/biconfig/core/ssl/internaltrust/internalca.pem -out ./internalca.der |