

ORACLE FUSION MIDDLEWARE Oracle B2B 11g Technical Note

Technical Note: 11g_006 Security

This technical note lists the security options available in Oracle B2B

Table of Contents

<i>Users</i>	2
<i>Roles</i>	2
Step 1: Create the user in the WebLogic Server	3
Step 2: Add the User in Oracle B2B	3
<i>Document Obfuscation</i>	5
<i>Document Provisioning</i>	5
<i>Secure Socket Layer (SSL) - HTTPS</i>	6
Step 1: WebLogic Server	6
Step 2: Oracle B2B	7
<i>Signing and Encryption</i>	8
Step 1: Setting the JKS file	8
Step 2: Selecting Signing / Encryption	8
Signing (protocol specific)	8
Encryption (protocol specific)	8

Users

Creating users to access Oracle B2B

- Users are created in the WebLogic Server
- Users are register and assigned roles in Oracle B2B

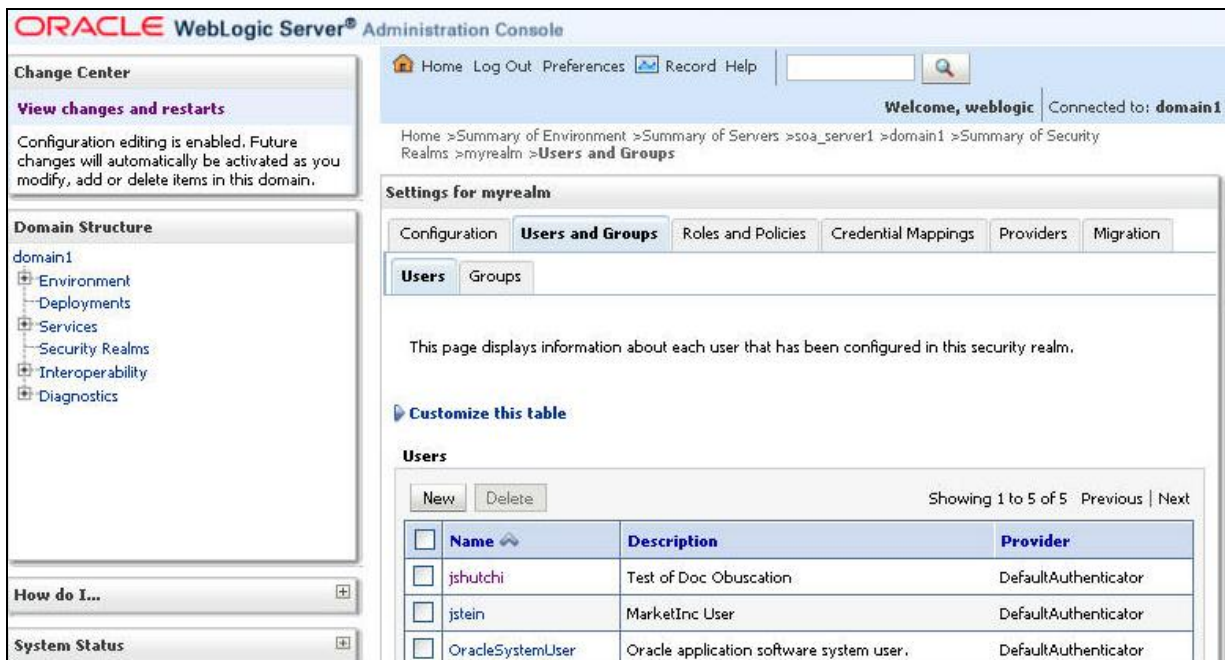
Roles

There are two role “Administrator” and “Monitor”.

- **Default Administrator:** →Created during installation
 - Has access to all functionality
- **Host Administrator** →Created under the host profile
 - Has access to all functionality
- **Host Monitor** →Created under the host profile
 - Can access the partner reports
 - Can access the partner Metrics
- **Remote Administrator (Partner)** →Created under the partner profile
 - Can view the partner Agreements
 - Can manage the partner Profile
 - Can manage the partner Document Information
 - Can view the Partner Reports
 - Cannot:
 - Import/ Export, Deploy, Manage Deployment, Types, Schedule Batch, Manage Batch, Callouts, Purge , Listening Channels , Configuration
- **Remote Monitor** →Created under the partner profile
 - Can view the partner reports
 - Cannot access Metrics

Step 1: Create the user in the WebLogic Server

In WebLogic Server go to “Security Realms”, select “Users and Groups” and add the user.



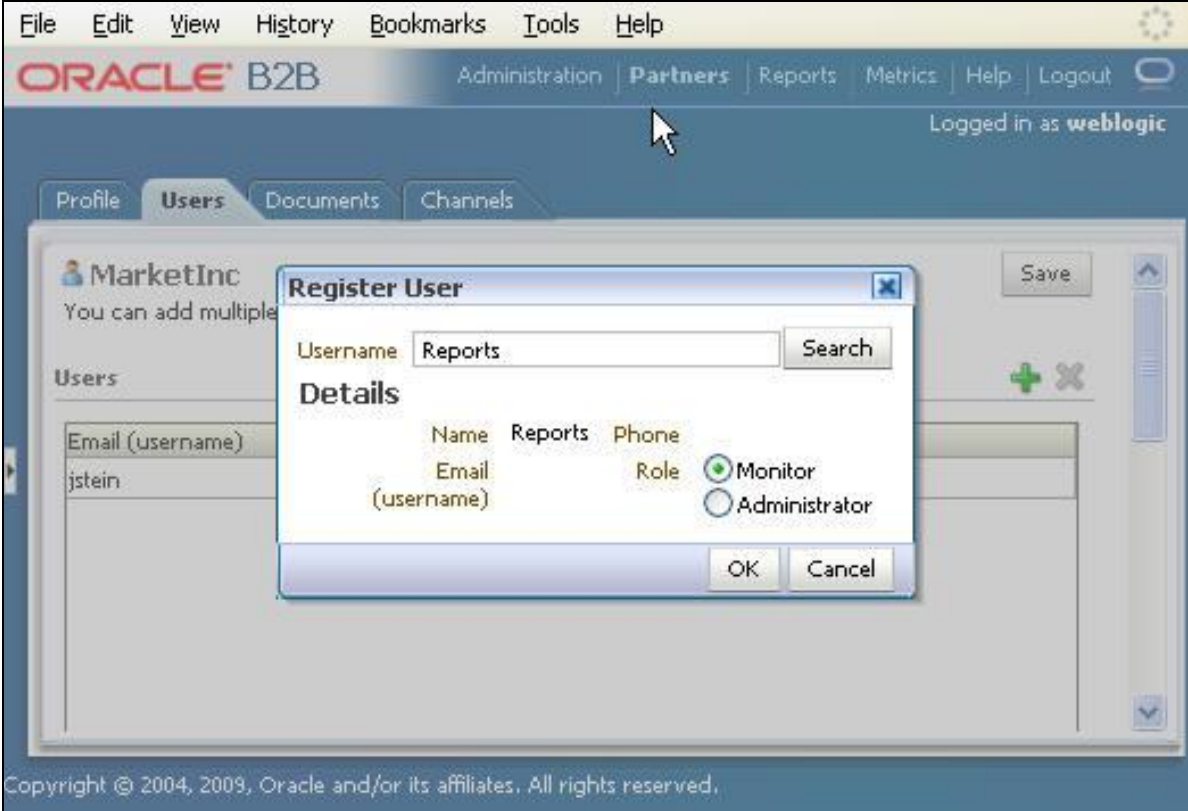
The screenshot shows the Oracle WebLogic Server Administration Console. The left sidebar contains a 'Domain Structure' tree with 'Security Realms' selected. The main content area is titled 'Settings for myrealm' and has tabs for 'Configuration', 'Users and Groups', 'Roles and Policies', 'Credential Mappings', 'Providers', and 'Migration'. The 'Users and Groups' tab is active, and the 'Users' sub-tab is selected. Below the sub-tabs, there is a message: 'This page displays information about each user that has been configured in this security realm.' A 'Customize this table' link is visible. Below that, there is a 'Users' section with 'New' and 'Delete' buttons. A table shows the following data:

<input type="checkbox"/>	Name	Description	Provider
<input type="checkbox"/>	jshutchi	Test of Doc Obuscation	DefaultAuthenticator
<input type="checkbox"/>	jstein	MarketInc User	DefaultAuthenticator
<input type="checkbox"/>	OracleSystemUser	Oracle application software system user.	DefaultAuthenticator

Step 2: Add the User in Oracle B2B

In Oracle B2B under “Users”

- Register the user
- Select a role



Document Obfuscation

Oracle B2B supports payload obfuscation. e.g. Data at rest is encrypted. The security infrastructure of Oracle Fusion Middleware is used to obfuscate, store, and retrieve the payloads. The payload is encrypted in the database and dynamically decrypted for display in Oracle B2B

In Enterprise Manager set parameter: `b2b.payloadObfuscation = true`

Document Provisioning

For a selected user defines the Supported Document Types

- If no documents are selected then the user can access ALL document details / payloads
- If any document(s) are selected, then the user can only access that set of documents

The screenshot shows the Oracle B2B configuration interface for a user named 'MarketInc'. The 'Users' tab is selected, and a table lists the user 'jstein' with the role 'Administrator'. Below this, the 'Supported Document Types' section is visible, containing a list of document type names.

Email (username)	Role	Display
jstein	Administrator	

Document Type Names
1Sync-6.4-catalogueRequest
1Sync-6.4-catalogueResponse
RosettaNet-V01.00-Pip7B1WorkInProgressNotification
RosettaNet-V02.00-Pip3A4PurchaseOrderConfirmation
RosettaNet-V02.00-Pip3A4PurchaseOrderRequest

Secure Socket Layer (SSL) - HTTPs

SSL (Secure Sockets Layer) is a protocol for managing the security for transmitting a document over the Internet. SSL uses a cryptographic system for encryption and decryption

- Public key:
 - Is used to encrypt information
 - Use by everyone
- Private key
 - Used to decrypt information
 - Used by the recipient

Step 1: WebLogic Server

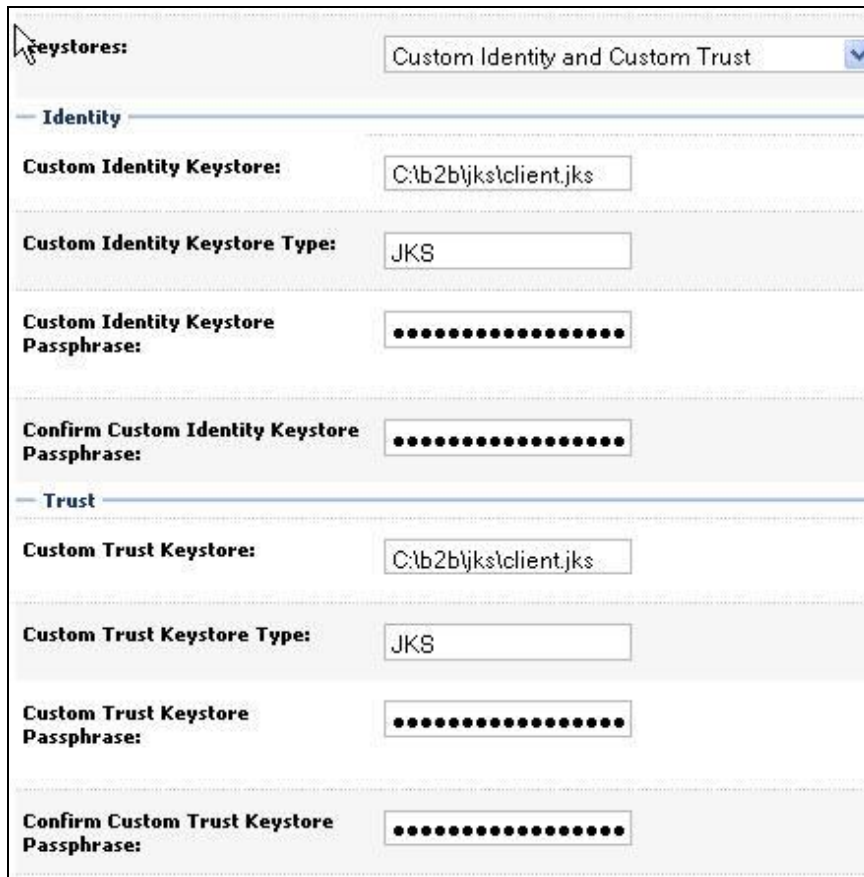
Environment → Server → soa_server

- General tab: Enable SSL (Note port)



A screenshot of a configuration window showing the 'General' tab. At the top, there is a checked checkbox labeled 'SSL Listen Port Enabled'. Below this, there is a field labeled 'SSL Listen Port:' with the value '8002' entered in the adjacent text box.

- Keystore tab: Enter Identity & Trust information



A screenshot of a configuration window showing the 'Keystore' tab. The 'Keystores:' dropdown menu is set to 'Custom Identity and Custom Trust'. The 'Identity' section includes fields for 'Custom Identity Keystore:' (C:\b2b\jks\client.jks), 'Custom Identity Keystore Type:' (JKS), 'Custom Identity Keystore Passphrase:' (masked with dots), and 'Confirm Custom Identity Keystore Passphrase:' (masked with dots). The 'Trust' section includes fields for 'Custom Trust Keystore:' (C:\b2b\jks\client.jks), 'Custom Trust Keystore Type:' (JKS), 'Custom Trust Keystore Passphrase:' (masked with dots), and 'Confirm Custom Trust Keystore Passphrase:' (masked with dots).

- SSL tab Add identity information

Identity and Trust Locations: Keystores

Identity

Private Key Location: from Custom Identity Keystore

Private Key Alias: cn=client

Private Key Passphrase: [Masked]

Confirm Private Key Passphrase: [Masked]

Step 2: Oracle B2B

In the delivery channel of the remote partner change in the URL:

- Change http to: https
- Change the port ex: 8002
 - Example :https://jshutchi-us.us.oracle.com:8002/b2b/httpReceiver
- Test the connection:

Signing and Encryption

- **Message Signed:** Digitally signing of the document ensuring that the signer cannot claim they did not sign it.
- **Acknowledgment Signed:** Digitally Signing an acknowledgment ensuring that the signer cannot claim they did not sign it
- **Encryption:** Transforming plain text using a cipher to make it unreadable. A key is required to decrypt

Step 1: Setting the JKS file

In Oracle B2B under the host profile add the keystore location and password

Step 2: Selecting Signing / Encryption

Under the remote Partner the security options are:

- Ack Signed
- Message Signed
- Message Encrypted

Signing (protocol specific)

- ebMS 2.0
 - XMLDISIG with SHA1 – RSA*
 - XMLDISIG with SHA1 - DSA*
- RosettaNet - V02.00
 - SMIME 3.0 with SHA-RSA*
 - SMIME 3.0 with MD5-RSA*
 - SMIME 2.0 with SHA-RSA*
 - SMIME 2.0 with MD5-RSA*
- AS1 | AS2 - 1.1
 - SMIME 3.0 with SHA-RSA*
 - SMIME 3.0 with MD5-RSA*

Encryption (protocol specific)

- ebMS 2.0
 - XMLEMC with 3DES - RSA v1.5*
 - XMLEMC with AES-128 – RSA-OAEP*
 - XMLEMC with AES-192 – RSA-OAEP*
 - XMLEMC with AES-256 – RSA-OAEP*
- RosettaNet - V02.00
 - SMIME 3.0 with DES*
 - SMIME 3.0 with 3DES*
 - SMIME 3.0 with RC2-40*
 - SMIME 3.0 with RC2-64*
 - SMIME 3.0 with RC2-128*
 - SMIME 2.0 with DES*
 - SMIME 2.0 with 3DES*
 - SMIME 2.0 with RC2-40*
 - SMIME 2.0 with RC2-64*
 - SMIME 2.0 with RC2-128*
- AS1 | AS2 - 1.1
 - SMIME 3.0 with DES*
 - SMIME 3.0 with 3DES*
 - SMIME 3.0 with RC2-40*
 - SMIME 3.0 with RC2-64*
 - SMIME 3.0 with RC2-128*