

Installation and Configuration Worksheet for AquaLogic Ensemble 1.0 MP2

This document contains worksheets for installing and configuring AquaLogic Ensemble 1.0. Print this document and use it to gather the host computer, portal, database, and additional information that you need to install and configure the Ensemble application and Security and Directory Service.

Use the Installation Worksheet to gather values for settings that you configure when running the Ensemble installer.

Use the Configuration Worksheet to gather values for settings that you configure when running AquaLogic Configuration Manager.

Installation Worksheet

Use this worksheet to gather values for settings that you configure when running the Ensemble installation wizard.

Table 1 Installation Worksheet

Installation Setting	Description and Notes	Default Value	Your Value
Installation Directory	In the <i>Installation Guide for BEA AquaLogic Ensemble</i> , the Ensemble install folder is referred to as <i>install_dir</i> .	<ul style="list-style-type: none"> C:\bea\alui (Windows) /opt/bea/alui (UNIX) 	
Configuration Manager - Port	<p>The port number on which you want Configuration Manager to service Ensemble requests.</p> <p>After running the installer, you will be able to access Configuration Manager by using the following URL:</p> <p><code>https://localhost:port_number/cm/login.jsf</code></p>	12345	
Configuration Manager - Password	The Administrator password that you will use to log in to Configuration Manager.		
Installation Location for Image Service Files	Install Image Service files on the computer on which the Image Service is installed. The path points to the directory where the Image Service is installed.	<ul style="list-style-type: none"> C:\bea\alui\ptimages (Windows) /opt/bea/alui/ptimages (UNIX/Linux) 	

Configuration Worksheet

Use this worksheet to gather values for settings that you configure when running AquaLogic Configuration Manager. The settings in this worksheet are listed in the same order as they appear in Configuration Manager.

Settings that must be configured on install are indicated by an **X** in the **Must Config** column.

Note: You may have already configured the Security and Directory Service when configuring AquaLogic Interaction. When this is the case, you still need to enter information for these services into Configuration Manager to correctly configure Ensemble.

Table 2 Configuration Worksheet

Must Config	Setting	Description and Notes	Default Value	Your Value
ENSEMBLE ADMINISTRATIVE UI				
	• Logging	Settings for enabling communication with ALI Logging Utilities		
	– Server	<p>The application name that will uniquely identify log messages sent from this application. ALI Logging Utilities use this string to determine the location from which log messages originate. The application name must be a string that meets the following restrictions:</p> <ul style="list-style-type: none"> • It must not be empty • It must not exceed 128 in length. • It may only contain non-white-space visible ASCII characters and the space character. <p>Most ALI products follow the naming convention [product-name].[machine-name]. [user-name].</p>	Autopopulated by default with a string of the form ensembleadm inui.machine_name	
	– Local Only	Select to limit broadcast of this application's logging messages to the computer on which this application is installed. Changing this could impact performance.	yes	

Table 2 Configuration Worksheet

Must Config	Setting	Description and Notes	Default Value	Your Value
	<ul style="list-style-type: none"> Application Settings 			
	– HTTP Enabled	Select if HTTP should be used for the application's web protocol. This controls the physical port on which the Ensemble Admin UI will run.	yes	
	– HTTP Port	Specify the port on which the application listens for HTTP requests.	20070	
For HTTPS	– HTTPS Enabled	Select if HTTPS should be used for the application's web protocol.	no	
	– HTTPS Port	Specify the port on which the application listens for HTTPS requests. This controls the physical port on which the Ensemble Admin UI will run.	20071	
	– AJP/1.3 Enabled	Select if AJP/1.3 should be used for the application's web protocol	no	
	– AJP/1.3 Port	Specify the port number on which the application listens for AJP/1.3 requests.	3002	
ENSEMBLE				
	<ul style="list-style-type: none"> Analytics 	Settings for configuring AL Analytics with Ensemble.		
	– Enabled	Select to enable Analytics with this application.	no	
	<ul style="list-style-type: none"> Analytics Communication 	Settings for configuring AL Analytics with Ensemble		

Table 2 Configuration Worksheet

Must Config	Setting	Description and Notes	Default Value	Your Value
	– Enable Unicast	Enable or disable unicast. Not using unicast can have performance impact.	yes	
For Ana-lytics	– Server	The fully-qualified domain name of the computer on which the BEA AL Analytics and BEA AL Analytics Collector services are installed.		
	– Port	The port used by the BEA AL Analytics Collector service.	31314	
	• Image Server	Settings for describing the locations of the ALI Image Service. The Base URL, Secure URL, and Connect URL are commonly identical, and in the form of <code>http://image_server/imageserver.</code>		
X	– Base URL	The base URL of the ALI Image Service. For example: <code>http://image_service_host:image_service_port/imageserver.</code> This URL must be accessible to clients. Do not use local machine name aliases like <i>localhost</i> . It is best to use a fully qualified hostname in this URL.		

Table 2 Configuration Worksheet

Must Config	Setting	Description and Notes	Default Value	Your Value
X	– Secure URL	<p>The Secure URL of the ALI Image Service. For example:</p> <pre>https://secure_image_service_host:secure_image_service_port/imageserver.</pre> <p>This URL must be accessible to clients. Do not use local machine name aliases like <i>localhost</i>. It is best to use a fully qualified hostname in this URL.</p>		
X	– Connect URL	<p>The URL for the portal to access the ALI Image Service. This setting is used at startup in situations where security settings would deny access to the Base URL. If the Base URL is accessible at startup, this setting should be the same as the Base URL.</p> <p>This URL must be accessible to clients, and hence do not use local machine name aliases like <i>localhost</i>. It is best to use a fully qualified hostname in this URL.</p>		
	– Timeout	<p>The amount of time to wait for the ALI Image Service, in milliseconds. -1 indicates no timeout.</p> <p>Must not be changed.</p>	-1	

Table 2 Configuration Worksheet

Must Config	Setting	Description and Notes	Default Value	Your Value
	<ul style="list-style-type: none"> Proxy Server 	Settings for connecting to the AquaLogic Ensemble Proxy Server. In most cases, the proxy is configured to listen on standard HTTP/S ports (i.e. 80 or 443). In this configuration, both URL rewriting and non-rewriting (transparent mode) are supported. If other ports are specified, URL rewriting will be required for all resources. The recommended ports to use instead of 80 and 443 are 20050 and 20051 respectively. Please be careful when choosing the port number. Changing the port number after installation requires a multi-step process.		
	– Hostname	The fully-qualified domain name of the computer on which the Proxy Server is installed.	[autodetect]	
X	– Port	The connection port used by the Ensemble Proxy Server. The port entered here controls where Ensemble expects itself to be found but does not control the physical port, which is configured under application settings. The port specified here must match the HTTP port specified under Ensemble Proxy Application Settings .		

Table 2 Configuration Worksheet

Must Config	Setting	Description and Notes	Default Value	Your Value
X	– Secure Port	The secure connection port used by the Ensemble Proxy Server. The port entered here controls where Ensemble expects itself to be found but does not control the physical port, which is configured under application settings. The port specified here must match the HTTP port specified under Ensemble Proxy Application Settings .		
	• Login Server	Settings for connecting to the AquaLogic Ensemble Login Server.		
	– Base URL	<p>The base URL for the Ensemble Login Server. This cannot be in the same container instance as the Ensemble proxy. A default login server <i>Ensemble Login Server</i> is bundled with the Ensemble installer.</p> <p>The port specified in this URL must match up with the port that the Login Server runs on. If you customize the port Ensemble Login Server service runs on (by changing the port number under Ensemble Login Server Application Settings HTTP port), verify that the URL here refers to the correct customized port. If no changes are made, the supplied default URL can be retained. Note that changing the login server port after initial startup will require updating your seed data manually.</p>	http://localhost:20060/loginserver /	

Table 2 Configuration Worksheet

Must Config	Setting	Description and Notes	Default Value	Your Value
	<ul style="list-style-type: none"> Portal Server 	Setting for connecting to the AquaLogic Interaction Portal Server. For example: <code>http://portal_server:11905/ptapi/services/QueryInterfaceAPI</code>		
X	<ul style="list-style-type: none"> – SOAP API URL 	The URL of the AquaLogic Interaction Portal SOAP API (PTAPI) Service. This is sent to remote resources in the CSP headers. This URL can be found on the Portal URL Manager page of the Portal Settings Utility in portal administration. For example: <code>http://portal_server:11905/ptapi/services/QueryInterfaceAPI</code>		
	<ul style="list-style-type: none"> Security and Directory Service Login 	Settings for authenticating with the Security and Directory Service. The user must be a portal administrator.		
X	<ul style="list-style-type: none"> – User Name 	The user name of an administrative user for AquaLogic Interaction. This is normally "Administrator" but might be customized in your portal installation.		
X	<ul style="list-style-type: none"> – Password 	The password of an administrative user for AquaLogic Interaction.		
	<ul style="list-style-type: none"> Security and Directory Service 	Settings for connecting to the Security and Directory Service.		

Table 2 Configuration Worksheet

Must Config	Setting	Description and Notes	Default Value	Your Value
	– Host	The fully-qualified domain name of the computer on which the Security and Directory Service is installed.	localhost	
	– Port	<p>The port number that the Security and Directory Service runs on. This controls the port number the SDS client will attempt to connect to in order to reach the SDS service. This setting does not control the physical port the SDS service runs on.</p> <p>The value entered here must match with the value entered in Security and Directory Service Application Settings HTTP port</p>	20040	
	– Override host name and port with this URL	<p>Overrides the above settings. Ignored if blank. For example: <code>http://localhost:20040/securityservice/services/SecurityAPI</code></p> <p>Note: Secure installations may wish to use this override to cause SDS client to use HTTPS to connect to SDS server for transport security. If doing so, be sure to change both the protocol (http: to https:) and the port number to match the correct HTTPS port of SDS.</p>		
	• SSO Login	Settings for configuring Single Sign On Login.		

Table 2 Configuration Worksheet

Must Config	Setting	Description and Notes	Default Value	Your Value
	– Standard Cookie Timeout	<p>Timeout value of cookie in seconds. A positive value means that the cookie will be set to expire after that many seconds have passed. This cookie will be able to restore a session regardless if there are any active HTTP sessions.</p> <p>A negative value means that no cookie will be stored on the hard disk. For environments which need to be extremely secure, use a negative value to effectively disable the storage of this cookie on the harddisk. For environments which want convenience over security, this value may be kept at the default value.</p> <p>This cookie will then be used to log users into Ensemble, and will be stored on the user's harddisk.</p>	604800	
	– Session-linked Cookie Timeout	Timeout value of cookie in seconds. This cookie is different from the standard cookie in that it will only restore a session if there are still valid http sessions for this user. If all http sessions have expired, this cookie will not restore a session, even if the timeout value has not been reached.	604800	
	– Shared Key	The shared key for SSO	(default exists)	
	– Spnego Redirect URL	The redirect URL for SPNEGO	/spnego/Spnego Servlet	

Table 2 Configuration Worksheet

Must Config	Setting	Description and Notes	Default Value	Your Value
	– Oracle CORE Redirect URL	The redirect URL for Oracle COREid	/OracleCOREid/OracleCOREidServlet	
	– Site Minder Redirect URL	The redirect URL for CA SiteMinder	//siteminder/sso.aspx	
	• Ensemble Database	Settings for connecting to the Ensemble Database.		
X	– Vendor	Choose the database vendor.		
X	– Host	The name of the database server.		
X	– User Name	The name of the database user.		
X	– Password	The password for the database user.		
X	– Port	The port number on which the database services requests.		
X	– Database Name	The name of the database.		
For Oracle	– SID	The system ID of the Oracle database instance. Visible only when database vendor setting is Oracle.		
	• Logging	Settings for enabling communication with ALI Logging Utilities.		

Table 2 Configuration Worksheet

Must Config	Setting	Description and Notes	Default Value	Your Value
	– Server	<p>The application name that will uniquely identify log messages sent from this application. ALI Logging Utilities uses this string to determine the location from which log messages originate. The application name must be a string that meets the following criteria:</p> <ul style="list-style-type: none"> • It must not be empty • It must not exceed 128 in length • It may only contain non-white-space visible ASCII characters and the space character. <p>Most ALI products follow the naming convention [product-name].[machine-name]. [user-name].</p>	Autopopulated by default with a string of the form ensemble.machine_name.username	
	– Local Only	Select to limit broadcast of this application's logging messages to only the computer on which this application is installed. Changing this could impact performance.	yes	
ENSEMBLE PROXY				

Table 2 Configuration Worksheet

Must Config	Setting	Description and Notes	Default Value	Your Value
	<ul style="list-style-type: none"> Application Settings 	Application Server settings for Ensemble Proxy. In most cases, the proxy should be configured to listen on standard HTTP/S ports (i.e. 80 or 443). In this configuration, both URL rewriting and non-rewriting (transparent mode) are supported. If other ports are specified, URL rewriting will be required for all resources. The recommended ports to use instead of 80 and 443 are 20050 and 20051 respectively. Please be careful when choosing the port number since changing it after installation requires a multi-step process.		
	– HTTP Enabled	Select if HTTP should be used for the application's web protocol.	yes	
X	– HTTP Port	Specify the port on which the application listens for HTTP requests. This controls the physical port on which the Ensemble Proxy will run.	No default; however, port 80 is strongly recommended.	
	– HTTPS Enabled	Select if HTTPS should be used for the application's web protocol. Enable if you plan to use Ensemble Proxy with HTTPS without a SSL accelerator front end. That is, you want the local container to provide a SSL version of Ensemble Proxy.	no	

Table 2 Configuration Worksheet

Must Config	Setting	Description and Notes	Default Value	Your Value
For HTTPS	– HTTPS Port	Specify the port on which the application listens for HTTPS requests. This controls the physical port on which the Ensemble Proxy will run.	No default; however, port 443 is strongly recommended.	
	– AJP/1.3 Enabled	Select if AJP/1.3 should be used for the application's web protocol	no	
For AJP	– AJP/1.3 Port	Specify the port number on which the application should listen for AJP/1.3 requests.	3002	
ENSEMBLE LOGIN SERVER				
	• Application Settings	<p>Application Server settings for Ensemble Login Server.</p> <p>Note: If the Login Server port is changed, seed resources that are created by Ensemble when it starts for the first time will stop working and need to be manually updated.</p>		
	– HTTP Enabled	Select of HTTP should be used for the application's web protocol.	yes	
	– HTTP Port	Specify the port on which the application listens for HTTP requests. This controls the physical port on which the login server will run at. Changing this port after install requires updating seed data entries manually.	20050	

Table 2 Configuration Worksheet

Must Config	Setting	Description and Notes	Default Value	Your Value
	– HTTPS Enabled	Select if HTTPS should be used for the application's web protocol.	no	
	– HTTPS Port	Specify the port on which the application listens for HTTPS requests. This controls the physical port on which the Login Server will run.	20051	
	– AJP/1.3 Enabled	Select if AJP/1.3 should be used for the application's web protocol	no	
	– AJP/1.3 Port	Specify the port number on which the application should listen for AJP/1.3 requests.	3002	
	SECURITY AND DIRECTORY SERVICE	Settings for enabling communication with the Portal database.		
	• Portal Database			
X	– Vendor	Choose the database vendor.		
X	– Host	The name of the database server.		
X	– User Name	The name of the database user.		
X	– Password	The password for the database user.		
X	– Port	The port number on which the database services requests.		
X	– Database Name	The name of the database.		
For Oracle	– SID	The system ID of the Oracle database instance. Visible only when database vendor setting is Oracle..		

Table 2 Configuration Worksheet

Must Config	Setting	Description and Notes	Default Value	Your Value
	<ul style="list-style-type: none"> Token Settings 	Setting for configuring expiration settings for the Security and Directory Service's security token.		
	<ul style="list-style-type: none"> – Token Expiration Time 	The token expiration time, in minutes. Enter -1 for no expiration.	10080	
	<ul style="list-style-type: none"> Portal Settings 	Connection data for the Security and Directory Service.		
	<ul style="list-style-type: none"> – Portal Version 	The major version of the portal that you are running. Valid values are 5 and 6.	6	
	<ul style="list-style-type: none"> Logging 	Settings for enabling communication between the Security and Directory Service and ALI Logging Utilities.		

Table 2 Configuration Worksheet

Must Config	Setting	Description and Notes	Default Value	Your Value
	– Server	<p>The application name that will uniquely identify log messages sent from this application. ALI Logging Utilities uses this string to determine the location from which log messages originate. The application name must be a string that meets the following restrictions:</p> <ul style="list-style-type: none"> • It must not be empty • It must not exceed 128 in length • It may only contain non-white-space visible ASCII characters and the space character <p>Most ALI products follow the naming convention [product-name].[machine-name].[user-name].</p>	autopopulated by default with a string of the form sds.machine_name.username	
	– Local Only	Select to limit broadcast of this application's logging messages to only the computer on which this application is installed. Changing this could impact performance.	yes	
	• Application Settings	Application Server settings for Ensemble Security and Directory Service.		
	– HTTP Enabled	Select if HTTP should be used for the application's web protocol.	yes	
	– HTTP Port	Specify the port on which the application listens for HTTP requests. This controls the physical port at which SDS service runs.	20050	

Table 2 Configuration Worksheet

Must Config	Setting	Description and Notes	Default Value	Your Value
	– HTTPS Enabled	Select if HTTPS should be used for the application's web protocol.	no	
	– HTTPS Port	Specify the port on which the application listens for HTTPS requests. This controls the physical port at which SDS service runs.	20051	
	– AJP/1.3 Enabled	Select if AJP/1.3 should be used for the application's web protocol	no	
	– AJP/1.3 Port	Specify the port number on which the application should listen for AJP/1.3 requests.	3002	