BEA AquaLogic® Ensemble

Administrator Guide

Version 1.0
Document Revised: June 27 2007

Contents

4. Proxy Resources

5. Proxy Authentication

6. Credential Mapping

7. Policies and Rules

8. Experience Definitions

9. Pagelets

CHAPTER 1

Welcome to AquaLogic Ensemble

This book describes how to administer and use AquaLogic Ensemble.

This chapter describes the how to use this book and where to find other resources pertinent to Ensemble. It is divided into the following sections:

- "How to Use This Book" on page 1-1 describes the intended audience, organization, and typographical conventions of the book.
- "BEA Documentation and Resources" on page 1-3 describes other sources for Ensemble information and assistance.

How to Use This Book

This guide has been designed to be a reference for administrators of Ensemble. The following sections describe how to use this book:

Audience

This guide is written for users responsible for administering, configuring, and audting Ensemble and Ensemble resources.

Organization

This guide includes the following chapters:

- This chapter provides information on how to use this guide and describes other resources available to help install, deploy, upgrade, and administer Ensemble.
- Chapter 2, "Introduction to AquaLogic Ensemble" provides an introduction to the features, functionality, and architecture of AquaLogic Ensemble.
- Chapter 3, "The AquaLogic Ensemble Console" provides a high-level description of the AquaLogic Ensemble Console and Ensemble Console security and resource ownership.
- Chapter 4, "Proxy Resources" describes how to configure AquaLogic Ensemble resources.
- Chapter 5, "Proxy Authentication" describes resource access control using AquaLogic Ensemble proxy authentication.
- Chapter 6, "Credential Mapping" describes how to configure credential mapping for AquaLogic Ensemble resources.
- Chapter 7, "Policies and Rules" describes how to use policies and policy rules to control access to AquaLogic Ensemble resources.
- Chapter 8, "Experience Definitions" describes how to configure AquaLogic Ensemble user experiences.
- Chapter 9, "Pagelets" describes how to use AquaLogic Ensemble to create and deploy pagelets.
- Chapter 10, "Audit" describes how to configure and use the auditing functionality of AquaLogic Ensemble.
- Chapter 11, "Analytics" describes how to configure Aqualogic Analytics to accept and report on events from AquaLogic Ensemble.
- Chapter 12, "Extending AquaLogic Ensemble" describes ways to extend Ensemble, including customizing the user experience and developing web applications using Ensemble extensions.

Typographical Conventions

This book uses the following typographical conventions.

Table 1-1 Typographical Conventions

Convention	Typeface	Examples/Notes
• Items you need to take action on (such as files or screen elements)	**bold**	• Upload **Procedures.doc** to the portal. • To save your changes, click **Apply Changes**.
• User-defined variables • New terms • Emphasis • Object example names	*italic*	• The migration package file is located in *install_dir*\serverpackages. • *Portlets* are Web tools embedded in your portal. • The URI *must* be a unique number. • The example Knowledge Directory displayed in Figure 5 shows the *Human Resources* folder.

• Text you enter
• Computer generated text (such as error messages)
• Code samples
	`computer`	• Type `Marketing` as the name of your community.
		• This script may generate the following error: `ORA-00942 table or view does not exist`
		• Example:
		`<setting name="SSOCookieIsSecure">`
		`<value xsi:type="xsd:integer">0</value>`
		`</setting>`

• Environment variables	ALL_CAPS	• The default location of BEA_HOME is C:\bea.

BEA Documentation and Resources

This section describes other documentation and resources provided by BEA.

Table 1-2 BEA Documentation and Resources

Resource	Description
Installation Guide	This guide describes the prerequisites (such as required software) and procedures for installing AquaLogic Ensemble. It is available on edocs.bea.com.

Table 1-2 BEA Documentation and Resources

Resource	Description
Installation Worksheet	This worksheet allows you to record prerequisite information necessary for installing AquaLogic Ensemble. It is available on edocs.bea.com.
Release Notes	The release notes provide information about new features, issues addressed, and known issues in the release. They are available on edocs.bea.com and on the application CD.
Online Help	The online help is written for all levels of Ensemble users. It describes the user interface for Ensemble and gives detailed instructions for completing tasks in Ensemble. To access online help, click the help icon.
Developer Guides, Articles, API Documentation, Blogs, Newsgroups, and Sample Code	These resources are provided for developers on the BEA dev2dev site (dev2dev.bea.com). They describe how to build custom applications using AquaLogic User Interaction and how to customize AquaLogic User Interaction products and features.

Table 1-2 BEA Documentation and Resources

Resource	Description
AquaLogic User Interaction (ALUI) and AquaLogic Business Process Management (ALBPM) Support Center	The ALUI and ALBPM Support Center is a comprehensive repository for technical information on ALUI and ALBPM products. From the Support Center, you can access products and documentation, search knowledge base articles, read the latest news and information, participate in a support community, get training, and find tools to meet most of your ALUI and ALBPM-related needs. The Support Center encompasses the following communities: **Technical Support** Submit online service requests, check the status of your requests, search the knowledge base, access documentation, and download service packs and hotfixes. **User Group** Participate in user groups; view webinars, presentations, the CustomerConnection newsletter, and the Upcoming Events calendar. **Product Center** Download product updates, service packs, and patches; view the Product Interoperability matrix (supported third-party products and interoperability between products). **Developer Center** Download developer tools, view code samples, access technical articles, and participate in discussions. **Education Services** Review the available education options, then choose courses by role and delivery method (Live Studio, Public Classroom Training, Remote Classroom, Private Training, or Self-Paced eLearning). **Profile Center** Manage your implementation details, local user accounts, subscriptions, and more. If you do not see the Support Center when you log in to http://support.plumtree.com, contact ALUISupport@bea.com or ALBPMSupport@bea.com for the appropriate access privileges.

Table 1-2 BEA Documentation and Resources

Resource	Description
Technical Support	If you cannot resolve an issue using the above resources, BEA Technical Support is happy to assist. Our staff is available 24 hours a day, 7 days a week to handle all your technical support needs. E-mail: ALUISupport@bea.com or ALBPMSupport@bea.com Phone Numbers: USA, Canada +1 866.262.7586 or +1 415.263.1696 EMEA +44 1494 559127 Asia Pacific +61 2.9931.7822 Australia/NZ +61 2.9923.4030 Singapore +1 800.1811.202

CHAPTER 2

Introduction to AquaLogic Ensemble

This chapter provides an introduction to the features, functionality, and architecture of AquaLogic Ensemble, and is divided into the following sections:

- "About Ensemble" on page 2-1 describes the features and functionality of Ensemble.
- "The Ensemble Architecture" on page 2-4 describes the component architecture of Ensemble.

About Ensemble

This section describes the features and functionality of Ensemble.

The Ensemble Console

The Ensemble Console is a browser-based administration tool used to create and manage the various objects in your Ensemble deployment. From the Ensemble Console you can register web applications and pagelets with the Ensemble Proxy, configure authentication, manage the user experience, and configure auditing.

For more details on the Ensemble Console, see Chapter 3, "The AquaLogic Ensemble Console."

Resources

Resources are web applications registered with the Ensemble proxy. Registering a resource allows the Ensemble proxy to map internal applications to external URLs, manage authentication both at the proxy level (between user and resource) and at the resource level (between resource

and application), and transform applications using Ensemble adaptive tags and the AquaLogic Interaction IDK.

For details on proxy resources, see Chapter 4, "Proxy Resources."

Authentication of users is managed using two mechanisms: proxy authentication and credential mapping.

Proxy authentication is how a user authenticates with the proxy in order to access proxied resources. Multiple authentication sources can be configured as login resources with Ensemble. The relative strength of authentication sources is described using authentication levels. A user authenticated at an authentication level can access resources configured for that authentication level, plus any resources with lower authentication levels. Authentication sources for proxy authentication can be based on the AquaLogic Interaction portal database or third-party SSO providers such as CA SiteMinder or Oracle COREid.

For details on proxy authentication, see Chapter 5, "Proxy Authentication."

For details on how authentication sources are associated with users accessing resources, see Chapter 8, "Experience Definitions."

Credential mapping is how a resource authenticates with the proxied application. Credentials can be be static and defined within the resource configuration, can be stored in the user's profile in AquaLogic Interaction, or can be stored in the Credential Vault after the user has logged into the proxied application once.

For details on credential mapping, see Chapter 6, "Credential Mapping."

In addition to authentication, access to resources is controled by policies and rules. Policies determine who can access a resource and under what conditions. Conditions for access can include factors such as time of day, an IP address within a configured range, the user's browser, and other criteria.

For details on policies and rules, see Chapter 7, "Policies and Rules."

Pagelets

A pagelet is a sub-component of a web page, accessed through the Ensemble proxy, and able to be injected into any proxied application. Any application on an Ensemble resource that returns text can be registered as a pagelet.

You can pass data to pagelets using pagelet parameters or the pagelet payload. The former passes name-value pairs to the pagelet application, while the latter is any text, including XML.

Parameters can even be configured to be sent using transport types that mimic AquaLogic Interaction parameter transport, which allows you to port ALI portlets to be Ensemble pagelets.

For details on pagelets, see Chapter 9, “Pagelets.”

Audit and Analytics

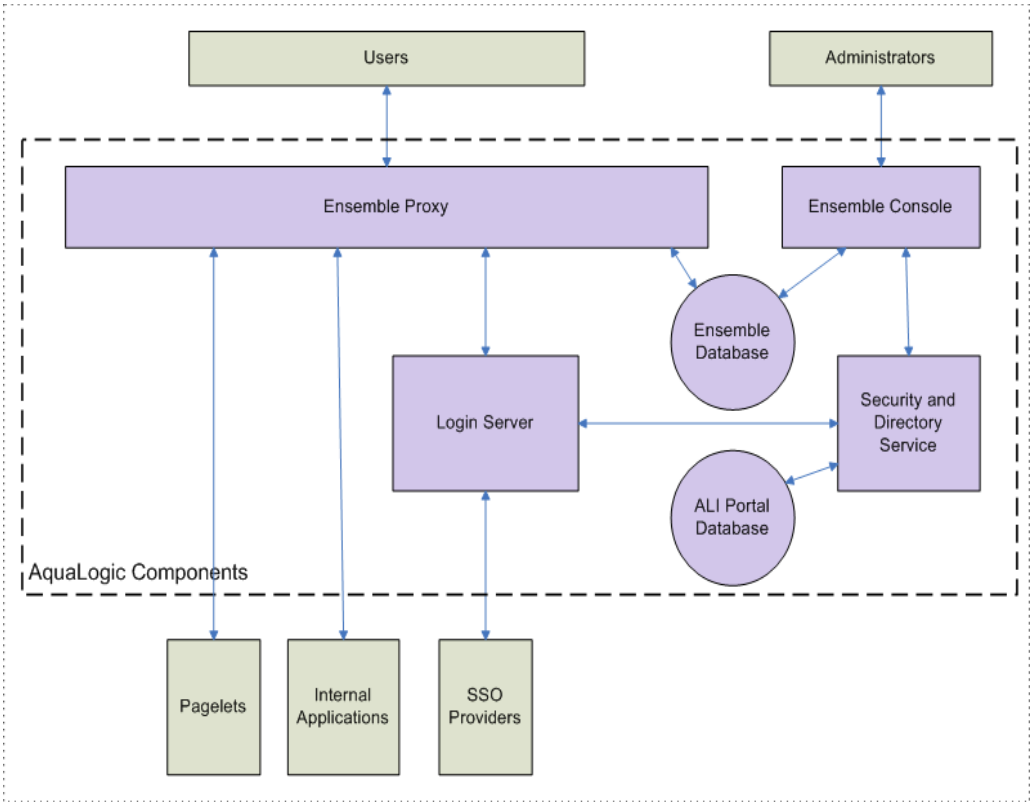
You can access usage information for Ensemble proxied applications and the Ensemble Console by using the Ensemble audit system and the Ensemble integration with AquaLogic Analytics.

For details on Ensemble audit features, see Chapter 10, “Audit.”

For details on using Ensemble with Analytics, see Chapter 11, “Analytics.”

The Ensemble Architecture

The following diagram illustrates the architecture of an AquaLogic Ensemble deployment.



- The Ensemble Proxy provides users with external access to internal resources including login resources, internal applications, and pagelets.
- The Ensemble Console allows administrators to configure resources, pagelets, access, and auditing features of Ensemble.
- The Login Server interfaces with the security and directory service and SSO providers to provide authentication services to the Ensemble Proxy.
- The security and directory service uses the AquaLogic Interaction portal database to authenticate users in both the Ensemble Console and the Ensemble Proxy via the Login Server.

CHAPTER 3

The AquaLogic Ensemble Console

This chapter provides a high-level description of the AquaLogic Ensemble Console and Ensemble Console security and resource ownership. It is divided into the following sections:

- "About the Ensemble Console" on page 3-1 provides an overview of what the Ensemble Console does and where to find more information on configuration of Ensemble objects.
- "Launching the AquaLogic Ensemble Console" on page 3-2 describes how to access the Ensemble Console.
- "AquaLogic Ensemble Console Roles" on page 3-2 describes how Ensemble Console roles allow you to control how users access the Ensemble Console.

About the Ensemble Console

The Ensemble Console is a browser-based administration tool used to create and manage the objects in your Ensemble deployment. From the Ensemble Console:

- Developers register resources and pagelets and configure credential mapping for remote applications. For details, see:
  - Chapter 4, "Proxy Resources."
  - Chapter 6, "Credential Mapping."
  - Chapter 9, "Pagelets."
- IT configures proxy authentication and manages experience definitions and interstitial pages. For details, see:

  - Chapter 5, “Proxy Authentication.”
  - Chapter 8, “Experience Definitions.”
- Users edit policy sets and manage resources that they own. For details, see:
  - Chapter 7, “Policies and Rules.”
- Auditors enable and disable auditing for remote applications. For details, see:
  - Chapter 10, “Audit.”

Launching the AquaLogic Ensemble Console

You access the Ensemble Console via a supported web browser. By default, the Ensemble Console is located:

`http://<host>:20070/ensembleadminui/`

where <host> is the server on which you installed the Ensemble Console.

AquaLogic Ensemble Console Roles

Ensemble Console roles control which parts of the Ensemble Console users can access and what actions they can perform. The following table summarizes the Ensemble Console roles, the tabs each role can access, and the actions each role can perform:

Table 3-1

Role	Accessible Tabs	Available Actions
Administrators	• All	• All actions
Managers	• Applications • Policies • Experiences • Proxy Authentication	• Any action on accessible tabs.
Resource Owners	• Applications	• Edit resources the user owns. • Edit pagelets associated with resources the user owns. • Create pagelets associated with resources the user owns.

Table 3-1

Role	Accessible Tabs	Available Actions
Policy Set Owners	• Policies	• Edit policy sets the user owns. • Create policy rules in the rule library.
Auditors	• Audit	• Enable or disable auditing on any resource.

Configuring Administrators, Managers, and Auditors

You configure *Administrators*, *Managers*, and *Auditors* by adding or deleting users or groups in each role.

To add users to the Administrators, Managers, or Auditors roles:

1. Launch the Ensemble Console.
2. Click the **ADMINISTRATION** tab.
3. Click the **Administrators**, **Managers**, or **Auditors** sub-tab.
4. To display the user and group picker, click **Add**.
5. Select one or more users or groups.
6. Click **Add selected items**.
7. Click **OK**.
8. Click **Save**.

To remove users from these roles:

1. Launch the Ensemble Console.
2. Click the **ADMINISTRATION** tab.
3. Click the **Administrators**, **Managers**, or **Auditors** sub-tab.
4. Select one or more users or groups to remove.
5. Click **Remove**.
6. Confirm that you want to delete these users or groups by clicking **OK**.
7. Click **Save**.

Configuring Resource and Policy Set Owners

The *Resource Owners* and *Policy Set Owners* roles are granted to a user when the user is made owner of a resource or policy set. To change the owner of a resource or policy set:

1. Launch the Ensemble Console.
2. Click the **ADMINISTRATION** tab.
3. Click the **Resource Owners** or **Policy Set Owners** sub-tab.
4. Click the name of the resource or policy set you want to edit.
5. To display the user picker, next to the **New Owner** box, click **Select**.
6. Select the user whom you want to make owner of the resource or policy.
7. Click **OK**.
8. To replace all instances of the **Current Owner** with the **New Owner**, select the check-box next to **Replace all ownership instances assigned to this user**.
9. Click **Save**.

CHAPTER 4

Proxy Resources

This chapter describes how to configure AquaLogic Ensemble resources. It is divided into the following sections:

- "About Ensemble Resources" on page 4-1 describes what an Ensemble resource is.
- "Registering a Resource" on page 4-2 describes how to create a basic Ensemble resource.
- "Advanced Resource Configuration" on page 4-3 describes additional configurations of Ensemble resources, including URL rewriting, resource roles, the AquaLogic Interaction login token, and authentication.

About Ensemble Resources

Ensemble resources are web applications registered in Ensemble. A registered resource maps an internal URL, accessible by Ensemble, to an external URL, accessible by end users. Any web application can be registered as a resource.

Registering a web application as an Ensemble resource allows Ensemble to do the following:

- Proxy internal web applications to external addresses.
- Manage authentication, both at the proxy level (Ensemble controls access to resources using Ensemble policies and roles) and at the resource level (Ensemble provides credentials to proxied web applications).
- Transform proxied web applications, including URL-rewriting and the use of Ensemble and AquaLogic Interaction adaptive tags.

- Customize the user experience through custom login, logout, interstitial, and error pages.

Registering a Resource

You register a resouce in Ensemble using the Ensemble Console. The simplest Ensemble resource has three configured properties:

- Name.
- Internal URL prefix, which is the URL of the application to be proxied.
- External URL prefix, which is the URL that end users will use to access the application.

Once configured, all URLs starting with the Internal URL prefix are accessible via the External URL prefix. For example, if the Internal URL prefix is

`http://internalServer/foo`

and the External URL prefix is

`http://externalServer/bar`,

the external path

`http://externalServer/bar/index.jsp` will map to
`http://internalServer/foo/index.jsp`,

and

`http://externalServer/bar/baz/index.jsp` will map to
`http://internalServer/foo/baz/index.jsp`.

To register a simple resource in Ensemble:

1. Launch the Ensemble Console.
2. Click the **APPLICATIONS** tab.
3. Click the **Resources** sub-tab.
4. To create a new resource, click **Create new**.
5. On the General page, in the **Name** box, type the name of the resource.
6. On the Connections page, in the **Internal URL prefix** box, type the URL to the internal web application to be proxied. For example, `http://internalServer/foo/`.

7. In the **External URL prefixes** box, type the URL to be used to access the resource. This URL must be on the Ensemble Proxy server. You may specify a fully-qualified URL or a path relative to the Ensemble Proxy server. For example, `http://externalServer/bar/` or just `/bar/`.

   Note: A fully-qualified External URL prefix must include the same port used by the Ensemble Proxy server.

8. Click **Save**.

Advanced Resource Configuration

This section describes advanced configuration options for Ensemble resources. It is divided into the following sub-sections:

URL Rewriting and DNS

When you enable URL rewriting, the Ensemble Proxy rewrites URLs in the proxied application that begin with the internal URL prefix so that they point to the external URL prefix. Ensemble enables URL rewriting by default.

It is strongly recommended that you disable URL rewriting, especially for production deployments. Disabling URL rewriting has the following benefits:

1. Ensemble will not rewrite links between Ensemble resources. For example, if you have two applications behind Ensemble, *http://foo.company.com/* and *http://bar.company.com*, links to bar.company.com within the foo.company.com application will not be rewritten. Users clicking these links will be taken to the link destination outside of the context of Ensemble.
2. Ensemble will not rewrite URLs formed on the client using client-side scripting.
3. The performance of the application improves.

There are two cases where you should disable URL rewriting:

1. The internal URL prefix and external URL prefix are identical.

   In this case, the user's DNS must resolve the URL to the Ensemble Proxy server, and the Ensemble Proxy server's DNS must resolve the URL to the internal resource. Because DNS only resolves IP and not port, both servers must listen to the same port. This method is strongly recommended.

2. All links in the application are relative URLs.

   In this case, the internal URL prefix path and the external URL prefix path must be identical. For example, if the internal URL prefix is `http://internal_server/bar/` the external URL prefix path must be `/bar/` or `http://proxy_server/bar/`.

To disable URL rewriting:

1. Launch the Ensemble Console.
2. Click the **APPLICATIONS** tab.
3. Click the **Resources** sub-tab.
4. Click the resource you want to edit.
5. On the General page, uncheck the box next to **Enable URL Rewriting**.
6. Click **Save**.

Roles

You can configure Ensemble to send role information to proxied applications. You define the roles available for Ensemble to send to the proxied application within the resource configuration. Policies determine which of these roles Ensemble sends for a given user.

For details on policies and how they map to roles, see Chapter 7, "Policies and Rules."

Ensemble sends roles in the HTTP header and are accessed by the proxied application using the Proxy IDK. For details on using the Proxy IDK, see the AquaLogic Interaction IDK documentation.

To configure roles to send to a proxied application:

1. Launch the Ensemble Console.
2. Click the **APPLICATIONS** tab.
3. Click the **Resources** sub-tab.

4. Click the resource you want to edit.
5. On the Roles page, type the names of the role or roles. Click **Add** to create additional roles.
6. Click **Save**.

The roles entered on the Roles page are the values that Ensemble can send to the proxied application, based on what policy or policies are associated with the user.

Proxy Authentication

Proxy Authentication describes how users log into Ensemble resources. Ensemble can facilitate authentication using a variety of methods, including basic authentication, HTML form-based authentication, and integration with third-party SSO products.

For details on Proxy Authentication, see Chapter 5, "Proxy Authentication."

Credential Mapping

Credential mapping allows Ensemble to automatically supply credentials to proxied applications. The credentials can be a static set used for all users, credentials specific to the user and stored in the user's ALI user profile, or credentials used once by the user and captured and stored by Ensemble in the Credential Vault. The Credential Vault allows users to authenticate once and then be logged in automatically by Ensemble in future accesses to the proxied resource.

For details on credential mapping, see Chapter 6, "Credential Mapping."

The AquaLogic Interaction Login Token

The AquaLogic Interaction login token allows the Ensemble resource to access the AquaLogic Interaction IPortletContext object. By default, the AquaLogic Interaction login token is not passed to the proxied resource.

To pass the login token to the proxied resource:

1. Launch the Ensemble Console.
2. Click the **APPLICATIONS** tab.
3. Click the **Resources** sub-tab.
4. Click the resource you want to edit.
5. On the CSP page, select **Send login token**.

6. Click **Save**.

CHAPTER 5

Proxy Authentication

This chapter describes resource access control using AquaLogic Ensemble proxy authentication. It is divided into the following sections:

- "Authentication Levels" on page 5-1 describes how Ensemble uses authentication levels to control access to resources.
- "Configuring Authentication Levels" on page 5-2 describes how to configure authentication level associated with each authenticator.
- "SSO Integration" on page 5-3 describes how to configure Ensemble to use SiteMinder, Oracle COREid, and SPNEGO SSO products.

Authentication Levels

There are two factors that control access to a resource: authentication levels and policies. Before any policy is evaluated for a given resource, the user must first be authenticated with an *authenticator* that has an authentication level equal to or greater than the authentication level of the resource. If an authentication level does not have an authenticator associated with it, the next higher authenticator is used to authenticate.

Authentication levels range from 0 to 10. An authenticator cannot be assigned level 0; authentication level 0 is reserved for anonymous access. For details on anonymous access, see "Configuring Anonymous Access" on page 7-4.

An authenticator is a method for authentication. HTML form-based authentication and third-party SSO providers are examples of authenticators.

When a user attempts to access a resource without credentials appropriate for the resource's authentication level, the following happens:

1. Ensemble evaluates experience rules to determine which experience definition is appropriate for the user.
2. Ensemble passes the authenticator associated with the experience definition to the authentication stack.
3. If the authenticator is equal to or greater than the resource's authentication level, Ensemble uses the authenticator associated with the experience definition to authenticate the user.

   If the authenticator is lower than the resource's authentication level, Ensemble uses the authenticator associated with the resource's authentication level.
4. Once the user is authenticated, Ensemble evaluates the policies for the resource. If one or more policies evaulate to true, the user is granted access to the resource.

For details on experience rules and experience definitions, see Chapter 8, "Experience Definitions."

For details on policies, see Chapter 7, "Policies and Rules."

Configuring Authentication Levels

You configure the authentication level is associated with an authenticator in the Ensemble Console. You configure each authenticator with a numerical level between 1 and 10. Two authenticators cannot have the same authentication level.

To configure authentication levels:

1. Launch the Ensemble Console.
2. Click the **PROXY AUTHENTICATION** tab.
3. Select the authentication level from the **Level** drop-down next to the authenticator you are configuring.

Note: Changing authentication levels for authenticators will not change authentication levels associated with policy sets. The authentication level will remain the same and the authenticator will change.

SSO Integration

This section describes how to configure Ensemble to authenticate users with one of the supported third-party SSO systems: Siteminder, COREid, or Active Directory via SPNEGO. The following subsections describe each configuration in detail:

- "Integrating with Computer Associates SiteMinder" on page 5-3
- "Integrating with Oracle COREid" on page 5-5
- "Integrating with Microsoft Active Directory via SPNEGO" on page 5-7

In addition, configuring Ensemble to log users out of an SSO system is described in "SSO Logout" on page 5-11.

Note: For all SSO integrations, the user name used to authenticate to the SSO software must also exist as an Ensemble user name. To add users to Ensemble, add users to your AquaLogic Interaction installation.

Integrating with Computer Associates SiteMinder

This section provides details about integrating Ensemble with Computer Associates SiteMinder, and is divided into the following sections:

- "Overview" on page 5-3 describes how the SiteMinder integration works.
- "Configuring Ensemble and SiteMinder" on page 5-4 describes how to integrate Ensemble with SiteMinder.

Overview

Configuring Ensemble to authenticate users with SiteMinder involves protecting a special Ensemble resource, **sso.aspx**, with SiteMinder. Ensemble uses this resource to authenticate a user with SiteMinder when the user attempts to access any resource with an authentication level that requires SiteMinder.

The process flow is as follows:

1. The user attempts to access a resource proxied by Ensemble.
2. Ensemble determines the user needs to authenticate with SiteMinder.
3. Ensemble redirects the user to sso.aspx. Since sso.aspx is protected by SiteMinder, the user is asked to authenticate to SiteMinder.

4. On successful authentication, the user accesses sso.aspx, which redirects the user to Ensemble marked as authenticated.
5. Ensemble redirects the user to the resource he initially attempted to access.

The redirects between sso.aspx and Ensemble are transparent to the user. The user experiences attempting to access the resource, being authenticated by SiteMinder, and then accessing the resource.

Configuring Ensemble and SiteMinder

To configure Ensemble for use with SiteMinder, first install **sso.aspx** and configure SiteMinder to protect it:

1. Create a virtual directory on IIS and protect it with SiteMinder.
2. Copy **sso.aspx** and **sso.aspx.cs** to the virtual directory you created. There are versions of these files for .NET v1.1 and .NET v2.0. In a default installation, the files are located under the **NET v1.1 aspx** or **NET v2.0 aspx** directory in:

   C:\bea\alui\loginserver\1.0\webapp\loginserver\ssointegration\siteminder
3. Verify that the files are installed and SiteMinder is correctly configured. Attempt to access sso.aspx via IIS. You are prompted to log into SiteMinder and then are presented with a page of header information. (The result from sso.aspx is not intended to be human-readable.)

Once you have correctly **sso.aspx,** you must configure Ensemble to access sso.aspx via IIS. To configure Ensemble:

1. Launch the Ensemble Console.
2. Click the **APPLICATIONS** tab.
3. Click the **Resources** sub-tab.
4. Click the **CA SiteMinder sample login resource**.
5. On the **Connections** page, edit the **Internal URL prefix** to point to the location of **sso.aspx.** For example:

   http://siteminder.company.com:80/ensembleIntegration/

   Do not include the file name sso.aspx.
6. Retrieve the **shared secret key** from the AquaLogic Interaction portal database. In the PTSERVERCONFIG table, the shared secret key is VALUE where SETTINGID=65. For example:

```
select VALUE from PTSERVERCONFIG where SETTINGID=65;
```

7. Update the shared secret key using the Configuration Manager. In the Configuration Manager, browse to **ENSEMBLE | SSO Login** and update the **Shared Key** setting.
8. Restart the BEA ALI Security Service, the BEA AL Ensemble Administrative UI, and the BEA AL Ensemble Proxy.
9. Verify that the login resource is correctly configured. Create a resource and policy to protect it with your SiteMinder authentication level and configure your experience rules to request SiteMinder authentication when a user accesses the resource.
   - For details on creating resources, see Chapter 4, "Proxy Resources."
   - For details on configuring policies, see Chapter 7, "Policies and Rules."
   - For details on configuring authentication levels, see "Configuring Authentication Levels" on page 5-2.
   - For details on configuring experience rules, see Chapter 8, "Experience Definitions."

Integrating with Oracle COREid

This section provides details about integrating Ensemble and Oracle COREid. It is divided into the following sections:

- "Overview" on page 5-3 describes how the COREid integration works.
- "Configuring Ensemble and SiteMinder" on page 5-4 describes how to integrate Ensemble and CoreID.

Overview

Configuring Ensemble to authenticate users with COREid involves protecting a special Ensemble resource, **sso.aspx**, with COREid. Ensemble uses this resource to authenticate a user with COREid when the user attempts to access any resource with an authentication level that requires COREid.

The process flow is as follows:

1. The user attempts to access a resource proxied by Ensemble.
2. Ensemble determines that the user needs to authenticate with COREid.

3. Ensemble redirects the user to sso.aspx. Since sso.aspx is protected by COREid, the user is asked to authenticate to COREid.
4. On successful authentication, the user accesses sso.aspx, which redirects the user to Ensemble marked as authenticated.
5. Ensemble redirects the user to the resource he initially attempted to access.

The redirects between sso.aspx and Ensemble are transparent to the user. The user experiences attempting to access the resource, being authenticated by COREid, and then accessing the resource.

Configuring Ensemble and COREid

To configure Ensemble for use with COREid, first install **sso.aspx** and configure COREid to protect it:

1. Create a virtual directory on IIS and protect it with COREid.
2. Copy **sso.aspx** and **sso.aspx.cs** to the virtual directory you created. There are versions of these files for .NET v1.1 and .NET v2.0. In a default installation, the files are located under the **NET v1.1 aspx** or **NET v2.0 aspx** directory in:

   C:\bea\alui\loginserver\1.0\webapp\loginserver\ssointegration\coreid
3. Verify that the files are installed and that COREid is correctly configured. Attempt to access sso.aspx via IIS. You are prompted to log into COREid and then are presented with a page of header information. (The result from sso.aspx is not intended to be human-readable.)

Once you have correctly installed **sso.aspx**, you must configure Ensemble to access sso.aspx via IIS. To configure Ensemble:

1. Launch the Ensemble Console.
2. Click the **APPLICATIONS** tab.
3. Click the **Resources** sub-tab.
4. Click the **Oracle COREid sample login resource**.
5. On the **Connections** page, edit the **Internal URL prefix** to point to the location of **sso.aspx.** For example:

   http://coreid.company.com:80/ensembleIntegration/

   Do not include the file name sso.aspx.

6. Retrieve the **shared secret key** from the AquaLogic Interaction portal database. Open the PTSERVERCONFIG table. The shared secret key is VALUE where SETTINGID=65. For example:

   ```
   select VALUE from PTSERVERCONFIG where SETTINGID=65;
   ```

7. Add the shared secret key to the Ensemble configuration.xml. On the Ensemble server, configuration.xml is located by default at:

   C:\bea\alui\settings\runner\configuration.xml

   In configuration.xml, verify that the value of the following setting is your shared secret key:

   ```
   <setting name="runnersso:ssologin:sharedSecretKey">
      <value xsi:type="xsd:string">[Your shared secret key]</value>
   </setting>
   ```

8. Restart the BEA ALI Security Service, the BEA AL Ensemble Administrative UI, and the BEA AL Ensemble Proxy.

9. Verify that the login resource is correctly configured. Create a resource and policy to protect it with your COREid authentication level and configure your experience rules to request COREid authentication when the user accesses the resource.
   - For details on creating resources, see Chapter 4, "Proxy Resources."
   - For details on configuring policies, see Chapter 7, "Policies and Rules."
   - For details on configuring authentication levels, see "Configuring Authentication Levels" on page 5-2.
   - For details on configuring experience rules, see Chapter 8, "Experience Definitions."

Integrating with Microsoft Active Directory via SPNEGO

Configuring Ensemble for SPNEGO authentication is a complex process involving configuration of the Active Directory server in addition to the creation of Ensemble configuration files and Ensemble configuration within the Ensemble Console.

To complete the Ensemble / SPNEGO integration, complete the instructions of each of the following sub-sections in the order provided:

1. "Configuring Microsoft Active Directory" on page 5-8
2. "Configuring the Ensemble Server" on page 5-8

3. "Verifying the Ensemble / SPNEGO Integration" on page 5-11

Configuring Microsoft Active Directory

Ensemble requires an Active Directory account with which to query the Active Directory. To configure this account:

1. Create a new Active Directory user. Record the OU because you will need it when configuring Kerberos on the Ensemble server. For example, if the user is in:

   `CN=Users,DC=ensemble,DC=mydomain,DC=com`

   Ensemble will need to use the *ensemble.mydomain.com* realm.

2. Verify that the user account is Kerberos enabled:
   - Turn on **Use DES encryption types for this account**.
   - Verify that **Do not require Kerberos pre-authentication** is not selected.

3. Enable Ensemble to access Active Directory as a service by using the Windows utility **setspn** to create an SPN for Ensemble. For example:

   setspn -a HTTP/ensembleserver.mydomain.com ensembleuser

   where *ensembleserver.mydomain.com* is the fully qualified domain name of your Ensemble server, and *ensembleuser* is the user you just created in Active Directory.

4. Create a keytab file for the SPN you created using **ktab**. This file will be used on the Ensemble server to authenticate Ensemble to the Active Directory server. For example:

   ktab -k mykeytab -a HTTP/ensembleserver.fakedomain.com

   will create a keytab file, *mykeytab*.

5. Put a backup copy of the keytab file in a secure location. Then copy the keytab file to the Ensemble server.

Configuring the Ensemble Server

To configure the Ensemble server to access Active Directory:

1. Copy the keytab file you created in Configuring Microsoft Active Directory to a location on your Ensemble server. For example:

   C:\SPNEGO\mykeytab

2. Create a new text file named *jaas.conf*. For example:

C:\SPNEGO\jaas.conf

3. Copy the following into **jaas.conf**:

```
com.sun.security.jgss.initiate {
   com.sun.security.auth.module.Krb5LoginModule required debug=true
   principal="host/ensembleserver.mydomain.com" useKeyTab=true
   keyTab="c:\\SPNEGO\\mykeytab" storeKey=true;
};
com.sun.security.jgss.accept {
   com.sun.security.auth.module.Krb5LoginModule required debug=true
   principal="host/ensembleserver.mydomain.com" useKeyTab=true
   keyTab="c:\\SPNEGO\\mykeytab" storeKey=true;
};
```

   where *host/ensembleserver.mydomain.com* is your SPN and *c:\\SPNEGO\\mykeytab* is your keytab file.

   Note: Use *host/* instead of *HTTP/* for the SPN.

4. Configure the Ensemble Proxy server **wrapper.conf** to refer to your jaas.conf. By default, the Ensemble Proxy server wrapper.conf is located at:

   C:\bea\alui\ensembleproxy\1.0\settings\config

   Add the following lines to wrapper.conf, replacing *C:\SPNEGO\jaas.conf* with the location of your jaas.conf. You must add the lines near the top of the wrapper.conf, in the section titled *Additional -D Java Properties*. You must number the **wrapper.java.additional.#** properties consecutively in ascending order, starting with wrapper.java.additional.8. The wrapper.java.additional.8 property will already exist. Add the following lines:

```
wrapper.java.additional.9=-Djava.security.auth.login.config=C:\SPNEGO\jaas.conf
wrapper.java.additional.10=-Djavax.security.auth.useSubjectCredsOnly=false
wrapper.java.additional.11=-Dsun.security.krb5.debug=true
```

5. Create a **krb5.ini** file in your Windows directory. For example:

   C:\windows\krb5.ini

6. Copy the following into the krb5.ini file you created:

```
[libdefaults]
udp_preference_limit = 1
default_realm = ENSEMBLE.MYDOMAIN.COM
default_tkt_enctypes = des-cbc-crc
default_tgs_enctypes = des-cbc-crc
ticket_lifetime = 600

[realms]
ENSEMBLE.MYDOMAIN.COM = {
kdc = ADSERVER.MYDOMAIN.COM
admin_server = ADSERVER.MYDOMAIN.COM
default_domain = ENSEMBLE.MYDOMAIN.COM
}

[domain_realm]
. ENSEMBLE.MYDOMAIN.COM = ENSEMBLE.MYDOMAIN.COM
ENSEMBLE.MYDOMAIN.COM = ENSEMBLE.MYDOMAIN.COM

[appdefaults]
autologin = true
forward = true
forwardable = true
encrypt = true
```

7. Edit the krb5.ini file so that:
   - ENSEMBLE.MYDOMAIN.COM is the realm (OU) of the server user account you created on your Active Directory server.
   - ADSERVER.MYDOMAIN.COM is the fully qualified domain name of your Active Directory server.
8. Retrieve the **shared secret key** from the AquaLogic Interaction portal database. Open the PTSERVERCONFIG table. The shared secret key is VALUE where SETTINGID=65. For example:

```
select VALUE from PTSERVERCONFIG where SETTINGID=65;
```

9. Add the shared secret key to the Ensemble configuration.xml. On the Ensemble server, configuration.xml is located by default at:

   C:\bea\alui\settings\runner\configuration.xml

   In configuration.xml, ensure the value of the following setting is your shared secret key:

```
<setting name="runnersso:ssologin:sharedSecretKey">
   <value xsi:type="xsd:string">[Your shared secret key]</value>
</setting>
```

10. Restart the BEA ALI Security Service, the BEA AL Ensemble Administrative UI, and the BEA AL Ensemble Proxy.

Verifying the Ensemble / SPNEGO Integration

Verify the login resource is correctly configured. Create a resource and policy to protect it with your SPNEGO authentication level and configure your experience rules to request SPNEGO authentication when the user accesses the resource.

- For details on creating resources, see Chapter 4, "Proxy Resources."
- For details on configuring policies, see Chapter 7, "Policies and Rules."
- For details on configuring authentication levels, see "Configuring Authentication Levels" on page 5-2.
- For details on configuring experience rules, see Chapter 8, "Experience Definitions."

Note: For SPNEGO authentication to work from the client side, the user must be logged into Windows into the appropriate Active Directory domain. In addition, Internet Explorer must be configured so that the Ensemble server is in the *Local Intranet* zone and integrated Windows authentication must be enabled.

SSO Logout

A user may be accessing multiple resources under a single SSO authentication. When a user logs out of an Ensemble proxied resource, Ensemble can prompt the user to log out of only that application or all applications.

For Ensemble to capture logout attempts, you must configure one or more internal logout patterns for each resource. To configure SSO log out patterns:

1. Launch the Ensemble Console.
2. Click the **APPLICATIONS** tab.
3. Click the **Resources** sub-tab.
4. Click the name of the resource you want to edit.
5. On the SSO Log Out Settings page, type the regular expression pattern that matches your log out page into the **Internal log out URL patterns** box.
6. To add more patterns, click **Add**.
7. To delete patterns, click **Delete**.
8. When you are done configuring SSO Log Out Settings, click **Save**.

CHAPTER 6

Credential Mapping

This chapter describes how to configure credential mapping for AquaLogic Ensemble resources. It is divided into the following topics:

- "About Credential Mapping" on page 6-1 describes what credential mapping is and how it can be used.
- "Configuring Credential Mapping" on page 6-2 provides details on how to configure credential mapping.

About Credential Mapping

Credential mapping allows Ensemble to supply credentials to proxied applications automatically. The credentials used by Ensemble to log in to the application can come from:

- The Credential Vault. When the user logs into the proxied resource, her credentials are stored in the Credential Vault. Subsequent access to that resource is authenticated using the stored credentials.
- The user's AquaLogic Interaction profile. Credentials for specific applications can be stored in the user's profile and used by Ensemble to automatically log the user into proxied applications.
- Static credentials. The Ensemble resource can be configured with static credentials that are used for every user with access to the resource.

Configuring Credential Mapping

Ensemble can automatically log in to resources through HTML forms and basic authentication.

The following sections describe how to configure credential mapping for authentication:

- "Configuring Credential Mapping for HTML Forms" on page 6-2 describes how to configure a resource to log in automatically to a resource that prompts for authentication with an HTML form.
- "Configuring Credential Mapping with Basic Authentication" on page 6-3 describes how to configure a resource to log inautomatically to a resource that prompts for authentication with basic authentication.
- "Authentication Field Sources" on page 6-4 describes the static, user profile, and credential vault authentication field sources.

Configuring Credential Mapping for HTML Forms

This section describes how to configure credential mapping for a resource that prompts for authentication with an HTML form.

To configure a resource for HTML form credential mapping:

1. Launch the Ensemble Console.
2. Click the **APPLICATIONS** tab.
3. Click the **Resources** sub-tab.
4. Click the name of the resource you want to edit.
5. On the Credential Mapping page, select **HTML Form** from the **Type** drop-down.
6. Create a new login form mapping by clicking **Create new.**
7. Type a **Name** for the login form mapping.
8. Set the login form by typing a **Page URL,** or select **Detect log in page with pattern**.
   - If the login form is located at a static URL, type the URL into the **Page URL** box.
   - If the login form is dynamic, select the **Detect log in page with pattern**. Type the regular expression pattern into the **Pattern** box.
9. Set the login form action by typing an **Action URL**, or select **Use pattern for action URL**.

- If the login form action is a static URL, type the URL into the **Action URL** box.
- If the login form is dynamic, select the **Detect log in page with pattern**. Type the regular expression pattern into the **Pattern** box.

10. To submit the login form data as an HTTP POST, select **Submit action as post**. Otherwise, login form data will be submitted as an HTTP GET.
11. Map one or more field values to authentication field sources.
    a. Type the name of the HTML form input in the **Field Name** box.
    b. For details on how to configure the Source and Mapped Value properties, see "Authentication Field Sources" on page 6-4.
    c. To automatically detect and populate field mappings, click **Detect Form Fields**.
    d. To add additional field mappings, click **Add**.
    e. To delete field mappings, click the  icon.

Configuring Credential Mapping with Basic Authentication

This section describes how to configure credential mapping for a resource that prompts for authentication with basic authentication.

To configure a resource for basic authentication credential mapping:

1. Launch the Ensemble Console.
2. Click the **APPLICATIONS** tab.
3. Click the **Resources** sub-tab.
4. Click the name of the resource you want to edit.
5. On the Credential Mapping page, select **Basic** from the **Type** drop-down.
6. Enter values for **Basic Auth Username** and **Basic Auth Password.** For details on how to configure the Source and Mapped Value properties, see "Authentication Field Sources" on page 6-4.

Authentication Field Sources

Authentication field sources map values to login fields. The following table describes each of the authentication field source values in the **Source** drop-down:

Table 6-1 Authentication Field Sources

Source	Description
Static	Use the static source when the authentication field is the same for all users accessing the resource. Type the static value in the **Mapped Value** box.
Masked Static	The masked static source is like the static source, except that the value typed into the **Mapped Value** box is obscured in the Ensemble Console UI. Use this source to protect the values of passwords and other sensitive fields.
User Profile	The user profile source uses properties from the user's AquaLogic Interaction profile to supply credential data for authentication. For each form field with a user profile source, select the profile property from the picker.
Credential Vault	With the Credential Vault source, Ensemble prompts the user for credentials the first time she accesses the resource. The supplied credentials are stored in the credential vault, and each subsequent access to that resource is authenticated with the stored credentials.

CHAPTER 7

Policies and Rules

This chapter describes how to use policies and rules to control access to AquaLogic Ensemble resources. It is divided into the following sections:

- "About Policies and Rules" on page 7-1 provides an overview of how policies and rules control access to an Ensemble resource.
- "Policies" on page 7-2 describes policies in depth, including how to create policies and configure policy sets.
- "Rules" on page 7-5 describes rules in depth, including what kinds of rules can be created and how to create them.

About Policies and Rules

Each non-login resource has an associated *policy set*. A policy set is a collection of *policies* that control access to a resource. Each policy grants access to a resource based on two criteria:

- Users and Groups. A user must be among the users or groups configured in the policy.
- Rules. A set of rules, one or all of which must evaluate to true for the user to have access.

For details on creating and configuring policies, see "Policies" on page 7-2.

Rules describe a set of criteria that must be met. If the criteria are met, the rule evaluates to true. For example, a rule could restrict access to business hours or evaulate to true when the user's client is a specific browser. For details on creating and configuring rules, see "Rules" on page 7-5.

In addition to controlling access to a resource, policies associate a *role* with the user. Role information is sent to the proxied application, allowing the application to determine the correct access level for the user. Since more than one policy can be granted for a given user on a given resource, more than one role can be associated with a user. Roles are created with the resource configuration. For details on configuring roles, see "Roles" on page 4-4.

Policies

When you create a resource, Ensemble creates a default policy for that resource. Policy sets map to resources 1:1. The name of the policy set is the same as the name of the resource and cannot be changed.

When Ensemble creates the policy, it creates a default policy for that policy. The default policy grants the Administrator user access to the resource. You can edit or delete this policy, and you can add new policies.

Creating a New Policy

To create a new policy:

1. Launch the Ensemble Console.
2. Click the **POLICIES** tab.
3. Click the **Policy Sets** sub-tab.
4. Click the name of the policy set associated with the resource you are configuring.
5. On the Policies page, click **Add policy**.

Configuring a Policy

A policy consists of four properties:

- A name.
- The resource role the policy maps to. Roles are configured in the resource configuration. For details, see "Roles" on page 4-4.
- One or more rules that describe the conditions for access.
- Zero or more users or groups that are allowed access by this policy.

At minimum, a policy must have a name, a mapped resource role, and an associated rule.

To configure a policy:

1. Launch the Ensemble Console.
2. Click the **POLICIES** tab.
3. Click the **Policy Sets** sub-tab.
4. Click the name of the policy set associated with the resource you are configuring.
5. On the Policies page, expand the policy you want to configure by clicking the ▶ icon.
6. Type a **Name** for the policy.
7. Associate a role with the policy. In the **Maps to Resource Role** drop-down list, select a role.
8. Associate one or more rules with the policy:
   a. Click **Add Rule**.
   b. Select the rule or rules you want to add.
   c. Click **Add selected items**.
   d. Click **OK**.
   e. Select **ANY** or **ALL**. When ANY is selected, and one or more rule evaluates to true, the policy will evaluate to true (provided any users and groups restrictions are satisfied). When ALL is selected, all rules must evaluate to true.
9. Restrict the policy to specific users or groups (optional).
   a. Click **Add User or Group**.
   b. Select the users or groups you want to add.
   c. Click **Add selected items**.
   d. Click **OK**.

To delete users, groups, or rules, highlight the item to be deleted and click **Delete**.

Authentication Levels

Authentication levels determine the minimum credential level required to access a resource. Ensemble checks the authentication level of a policy set before it evaluates any policies. If the

user is not logged in, or is logged in with credentials lower than the set authentication level, he is challenged with the authentication method.

For details on authentication, see Chapter 5, “Proxy Authentication.”

Configuring Anonymous Access

Anonymous access allows user to access a resource without providing credentials. This is useful for resources such as login resources, where the user is not expected to be authenticated prior to accessing the resource.

To configure anonymous access:

1. Launch the Ensemble Console.
2. Click the **POLICIES** tab.
3. Click the **Policy Sets** sub-tab.
4. Click the name of the policy set associated with the resource you want to configure for anonymous access.
5. Set the authentication level to Anonymous. In the **Minimum Credential Level** drop-down, select *0 (Anonymous)*.
6. When prompted, create an anonymous policy. Select a resource role from the drop-down and click **Create anonymous policy**.
7. Click **Save**.

A new policy, *Anonymous policy*, is created. This policy always evaluates to true for any user.

Rules

Rules are defined by one or more *rule types*. A rule type is a single condition that evaluates to true or false. The rule is configured so that either any or all of the rule types must evaluate to true for the rule to evaluate to true. The following table describes the available rule types:

Table 7-1 Rule Types

Rule Type	Description
Client IP	Evaluates to true if this value matches the user's IP. You can configure the Client IP rule to match a range of IP addresses by using regular expressions.
Date	You can set the Date rule to be equal to, greater than, less than, greater than or equal to, or less than or equal to a given date. You can combine two Date rule types to provide access over a range of dates.
User	Evaluates to true if this value is the current user.
Secure connection	Evaulates to true of the connection is secure (HTTPS).
Time	You can set the Time rule to be equal to, greater than, less than, greater than or equal to, or less than or equal to a given time. You can combine two Time rule types to provide access over a period of time.
Browser	Evaluates to true if this value matches the user's browser type.
Group membership	Evaluates to true if this value is a group of which the user is a member.
Non-secure connection	Evaulates to true of the connection is not secure (HTTP).
Day of Week	Evaulates to true if this value is equal to the current day of the week.
Locale	Evaluates to true if this value matches the user's locale.
User property	Evaluates to true if this value matches the user's property value.
Always true	Always evaluates to true.
Always false	Always evaluates to false.

Creating and Editing Rules

You create rules in the rule library. To create a new rule:

1. Launch the Ensemble Console.
2. Click the **POLICIES** tab.
3. Click the **Rule Library** sub-tab.
4. To create a new rule, click **Create new**.
5. On the General page, in the **Name** box, type the name of the rule.
6. Type a **Description** of the rule.
7. On the Definition page, click **Add**.
8. Either select the rule type to create or click on an existing rule.

   Existing rules can be added as rule types. This allows compound rules to be formed. For example, a rule might evaluate to true if any of three users is accessing the resource from a secure connection. A rule type is created that evaluates to true for *any* of the three uses. That rule type is added to a rule type where it *and* the Secure connection rule type must evaluate to true.
9. Add the rule type by clicking **OK**.
10. Click **Add** to add another rule type or finish creating the rule by clicking **Save**.

Published Rules

You can configure a rule to be published or not published. You are able to add a published rule to a policy. You are able use an unpublished rule only as as a rule type for other rules.

To publish a rule, from the rule's General page, select **Is published**. To unpublish the rule, clear the check box next to **Is published.**

Note: If the rule is currently being used in a policy, it cannot be unpublished.

CHAPTER 8

Experience Definitions

This chapter describes how to configure AquaLogic Ensemble user experiences. It is divided into the following sections:

- "About Experience Definitions" on page 8-1 provides an overview of how experience definitions control aspects of the user experience.
- "Configuring Experience Definitions" on page 8-2 describes how to create and configure experience definitions.
- "Configuring Experience Rules" on page 8-2 describes how to create and configure experience rules.
- "Login Resources and Interstitial Pages" on page 8-5 describes how login resources and interstitial pages are used in the login and logout process.

About Experience Definitions

An *experience definition* describes the following aspects of the user experience:

- The authenticator used to authenticate the user.
- The login, logout, error, and other interstitial pages displayed to the user.

Ensemble employes a set of *experience rules* to determine which experience definition to associate with a user. Each experience rule evaulates to true if its set of conditions is satisfied. Experience rules are evaluated in order, and the first rule to evaluate to true determines the experience definition is associated with the user.

Configuring Experience Definitions

To configure an experience definition:

1. Launch the Ensemble Console.
2. Click the **EXPERIENCES** tab.
3. Click the **Definitions** sub-tab.
4. Click the experience definition you want to edit, or to create a new resource, click **Create new**.
5. On the General page, type a **Name** and **Description** for the experience definition.
6. On the Log In Settings page, configure the login resource and interstitial pages. For details, see "Login Resources and Interstitial Pages" on page 8-5.
7. On the Authentication Settings page, select an **Authentication method** from the drop-down.

   Caution: Ensemble uses the authentication method set in the experience definition if it meets or exceeds the authentication level required by the resource being accessed. If the resource requires a greater authentication level, Ensemble uses the authentication method appropriate for that authentication level.

8. Click **Save**.

Configuring Experience Rules

The experience definition that Ensemble chooses depends on a set of experience rules that Ensemble evaluates in a specified order. You configure experience rules by first adding or editing rules in the Rule Library. You then set the precedence of rules in the Rule Order.

Rules are defined by one or more *rule types*. A rule type is a single condition that can be evaluated as true or false. You can configure the rule so that any or all of the rule types must evaluate to true for the rule to evaluate to true. The following table describes the available rule types:

Table 8-1 Rule Types

Rule Type	Description
Client IP	Evaluates to true if this value matches the user's IP. You can configure the Client IP rule to match a range of IP addresses by using regular expressions.
Date	You can set the Date rule to be equal to, greater than, less than, greater than or equal to, or less than or equal to a given date. You can combine two Date rule types to provide access over a range of dates.
User	Evaluates to true if this value is the current user.
Secure connection	Evaulates to true of the connection is secure (HTTPS).
Time	You can set the Time rule to be equal to, greater than, less than, greater than or equal to, or less than or equal to a given time. You can combine two Time rule types to provide access over a period of time.
Browser	Evaluates to true if this value matches the user's browser type.
Group membership	Evaluates to true if this value is a group of which the user is a member.
Non-secure connection	Evaulates to true of the connection is not secure (HTTP).
Day of Week	Evaulates to true if this value is equal to the current day of the week.
Locale	Evaluates to true if this value matches the user's locale.
User property	Evaluates to true if this value matches the user's property value.
Always true	Always evaluates to true.
Always false	Always evaluates to false.

Creating and Editing Rules in the Rule Library

1. Launch the Ensemble Console.
2. Click the **EXPERIENCES** tab.
3. Click the **Rule Library** sub-tab.
4. Click **Create new**.
5. On the General page, in the **Name** box, type the name of the rule.
6. Type a **Description** of the rule.
7. On the Definition page, click **Add**.
8. Either select the rule type to create or click on an existing rule.

   You can add existing rules as rule types. This allows compound rules to be formed. For example, you might create a rule that evaluates to true if any of three users is accessing the resource from a secure connection. To do this, you create rule type that evaluates to true for *any* of the three users. You then add that rule type to a rule type where it *and* the Secure connection rule type must evaluate to true.
9. Add the rule type by clicking **OK**.
10. Click Add to add another rule type, or finish creating the rule by clicking **Save**.

Published Rules

You can configure a rule to be published or not published. You are able to add a published rule to a policy. You are able use an unpublished rule only as as a rule type for other rules.

To publish a rule, from the rule's General page, select **Is published**. To unpublish the rule, clear the check box next to **Is published.**

Note: If the rule is currently being used in the Rule Order, it cannot be unpublished.

Rule Order

The Rule Order sub-tab associates experience rules with experience definitions and provides the order in which Ensemble evaluates the rules. When determining the experience definition, Ensemble first checks the first (lowest numbered) rule in the Rule Order. If the experience rule evaluates to true, Ensemble associates the experience definition with the user. If the experience

rule evaluates to false, the next rule in the order is checked, and so on, until an experience rule evaluates to true and Ensemble can associate an experience definition with the user.

To change the order of rules, adjust the numbers in the **Order** column.

To create a new rule in the Rule Order:

1. Launch the Ensemble Console.
2. Click the **EXPERIENCES** tab.
3. Click the **Rule Order** sub-tab.
4. Click **Add Rule**.
5. On the General page, in the **Name** box, type the name of the rule.
6. Type a **Description** of the rule.
7. On the Settings page, next to **Condition**, click **Select**.
8. Select the rule. Click **OK**.
9. Next to **Experience definition**, click **Select**.
10. Select the experience definition to be assigned if this rule is selected. Click **OK**.
11. Click **Save**.

Login Resources and Interstitial Pages

The experience definition associated with a user determines, in part, the specifics of the user's login and logout experience. On the **Log In Settings** page of the experience definition configuration you can supply the login resource and login, logout, error, and other interstitial pages.

The login resource is a proxied application server used to host the various pages associated with the experience definition.

To create a login resource, create a resource and select **Is Login resource** on the General page.

For details on creating a resource, see Chapter 4, "Proxy Resources."

The following table describes the various pages that you can associate with an experience definition.

Table 8-2 Login, Logout, and Interstitial Page Settings

Setting	Definition
Pre-log in page	Ensemble displays this page to the user prior to attempting to authenticate the user.
Login page	This page provides the form for login when the authenticator is HTML form-based login. Ensemble displays this page after the Pre-log in page and before the Post-log in page.
Post-log in page	Ensemble displays this page to the user after successful authentication and before the user accesses the resource.
Error page	Ensemble displays this page if there is an error in the login process.
Post-log out page	Ensemble displays this page after the user logs out of the resource.

For details on customizing the login, logout, error, and other interstitial pages, see "Custom Login Resources" on page 12-1.

Caution: Ensemble uses the login, logout, error, and interstitial page settings in the experience definition regardless of the final authenticator used to access the resource. Ensemble uses an authenticator other than the authenticator configured with the experience definition if the resource being access requires a higher authentication level. If the required authenticator uses a login page and there is no login page configured in the experience definition, the user is presented with a blank page and is unable to authenticate.

CHAPTER 9

Pagelets

This chapter describes how to use AquaLogic Ensemble to create and deploy pagelets. It is organized into the following sections:

- "About Pagelets" on page 9-1 describes what pagelets are.
- "Registering a Pagelet" on page 9-2 describes how you register a pagelet with Ensemble.
- "Adding a Pagelet to a Web Page" on page 9-3 describes how to add a pagelet to an application proxied by Ensemble.
- "Configuring Pagelet Consumers" on page 9-3 describes how to restrict the resources that can use a pagelet.
- "Configuring Pagelet Parameters and Transport Type" on page 9-4 describes how to pass parameters to your pagelets.
- "Accessing Pagelet Discovery for Developers" on page 9-7 describes the Ensemble pagelet discovery UI.

About Pagelets

A *pagelet* is a fragment of HTML that describes a self-contained, reusable UI element. With a portal system, a portlet is a self-contained UI element that can be used in the portal. A pagelet is like a portlet that you can easily insert into any web page proxied by Ensemble.

Registering a Pagelet

A pagelet is an application hosted on an Ensemble resource. Before registering a pagelet in Ensemble, a you must create a resource and configure it to point to the application server where the pagelets are hosted. For details on creating resources, see Chapter 4, "Proxy Resources."

To register a new pagelet:

1. Launch the Ensemble Console.
2. Click the **APPLICATIONS** tab.
3. Click the **Pagelets** sub-tab.
4. To create a new pagelet, click **Create new**.
5. On the General page, type the **Name** of the pagelet.
6. Select a parent resource. Next to **Parent resource**, click select. From the **Select a resource** picker, select the resource your pagelet is hosted on and click **OK**.
7. Type the **Library** to associate this pagelet with. This can be any text value. The library setting is a user-defined way of grouping pagelets together within the pagelet documentation. This setting is optional.
8. Type a **Description**.
9. On the Location page, type the **URL suffix**. The Internal URL prefix (taken from the parent resource) appended to the URL suffix forms the URL to the pagelet.
10. Click **Save**.

Once you save the pagelet, sample code for inserting the pagelet into a web page is available on the General page of the pagelet configuration. For details on inserting pagelets into web pages, see "Adding a Pagelet to a Web Page" on page 9-3.

Ensemble can restrict the resources that can insert each pagelet into its web pages. For details, see "Configuring Pagelet Consumers" on page 9-3.

Parameters can be configured to be passed to the pagelet. For details, see "Configuring Pagelet Parameters and Transport Type" on page 9-4.

Adding a Pagelet to a Web Page

You can add a pagelet to any web page that is proxied by Ensemble. Sample code for adding a pagelet to a web page is provided on the General page of the pagelet configuration. The basic format of the pagelet injection code is:

```
<pt:ensemble.inject pt:name="library:pagelet" />
```

Library is the library name and *pagelet* is the pagelet name, as entered in the Ensemble pagelet configuration.

Any data passed to the pagelet is also included in the pagelet injection code. For details on configuring pagelet parameters, see "Configuring Pagelet Parameters and Transport Type" on page 9-4.

Note: You must define the namespace prefix 'pt' in the web page as `xmlns:pt='http://www.plumtree.com/xmlschemas/ptui/`

Configuring Pagelet Consumers

By default, pagelets can be consumed by any Ensemble proxied application. To restrict which resources can consume a pagelet:

1. Launch the Ensemble Console.
2. Click the **APPLICATIONS** tab.
3. Click the **Pagelets** sub-tab.
4. Click the name of the pagelet you want to configure.
5. Restrict all resources from consuming the pagelet. On the Consumers page, clear the **Allow all consumers** check box.
6. Add resources able to consume the pagelet by clicking **Add**.
7. Select one or more resources to add.
8. Click **Add selected items**.
9. Click **OK**.

To remove a resource from the list of consumers, select the resource to remove and click **Delete**.

Configuring Pagelet Parameters and Transport Type

This section describes how to use pagelet parameters to pass data to pagelets. It is divided into the following sections:

- "Passing Data with Pagelet Parameters" on page 9-4 describes how to use *pagelet parameters* to pass data to the pagelet.
- "Passing Data with the Pagelet Payload" on page 9-5 describes how to use the *pagelet payload* to pass data to the pagelet.
- "Configuring Pagelet Parameter Transport Type" on page 9-6 describes how the pagelet parameter transport type allows you to port AquaLogic Interaction portlets to work as pagelets within Ensemble.

Passing Data with Pagelet Parameters

You configure the pagelet parameters that can be passed to the pagelet in the pagelet configuration in the Ensemble Console. You include pagelet parameter values in the pagelet injection code that is added to a web page. This section is divided into the following sub-sections:

- "Configuring Parameters in the Ensemble Console" on page 9-4
- "Setting Parameter Values in Pagelet Injection Code" on page 9-5

Configuring Parameters in the Ensemble Console

To configure parameters for a pagelet in the Ensemble Console:

1. Launch the Ensemble Console.
2. Click the **APPLICATIONS** tab.
3. Click the **Pagelets** sub-tab.
4. Click the name of the pagelet you want to configure.
5. On the Parameters page, type a **Name**, **Description**, and **Type** for the parameter.

   Note: The **Description** and **Type** fields are used for pagelet documentation and are optional. Pagelet documentation is automatically created and can be viewed in the Pagelet Discovery UI. For details on the Pagelet Discovery UI, see "Accessing Pagelet Discovery for Developers" on page 9-7.

6. To make the parameter mandatory, select the check-box under **Mandatory**.

7. To add the parameter, click **Add**.
8. Click **Save**.

To delete a parameter, select the checkbox to the left of the parameter and click **Delete**.

The **Pagelet Parameter Transport Type** setting is provided for porting AquaLogic Interaction portlets to Ensemble pagelets. For details, see "Configuring Pagelet Parameter Transport Type" on page 9-6.

Setting Parameter Values in Pagelet Injection Code

You set pagelet parameter values in the pagelet injection code using the parameter names configured in the Ensemble Console. For example:

```
<pt:ensemble.inject pt:name="library : pagelet"
   param1="foo"
   param2="bar"
/>
```

In this example, Ensemble passes the pagelet *library*:*pagelet* two parameters: *param1* with a value of *foo*, and *param2* with a value of *bar*.

Passing Data with the Pagelet Payload

Any text data can be passed to the pagelet by including it within the `<pt:ensemble.inject>` tag. For example:

```
<pt:ensemble.inject pt:name="library:pagelet">
   This is the payload.
</pt:ensemble.inject>
```

In this example, Ensemble passes the text *This is the payload* to the pagelet as the pagelet payload.

The pagelet retrieves the payload through the Ensemble Proxy API. In addition to extracting the payload as raw text, the Proxy API provides methods to extract an XML payload as an XML document.

For more information on the Proxy API, see the following documentation:

- Proxy API tutorials in Java.
- Proxy API tutorials in .NET.

Ensemble allows you to configure a payload schema URL to point to an XML schema that can validate an XML payload. Ensemble only supplies the URL to the pagelet; it is up to the pagelet to use the schema to validate the XML payload.

To configure the payload schema URL:

1. Launch the Ensemble Console.
2. Click the **APPLICATIONS** tab.
3. Click the **Pagelets** sub-tab.
4. Click the name of the pagelet you want to configure.
5. On the Parameters page, type the schema URL in the **Payload schema URL** textbox.

Configuring Pagelet Parameter Transport Type

Pagelet parameter transport type allows you to port AquaLogic Interaction portlets to work as pagelets within Ensemble. AquaLogic Interaction portlets may require Administrator, CommunityPortlet, or Community level preference settings.

For details on portlet settings and preferences, see the ALUI developer documentation for Portlet Settings.

To supply these preferences from Ensemble:

1. Launch the Ensemble Console.
2. Click the **APPLICATIONS** tab.
3. Click the **Pagelets** sub-tab.
4. Click the name of the pagelet you want to configure.
5. On the Parameters page, select the appropriate **Pagelet Parameter Transport Type** from the drop-down.
   - To supply Administrator preferences, select **Global - Admin Prefs.**
   - To supply Community preferences, select **Realm - Community Prefs**.
   - To supply CommunityPortlet preferences, select **Pagelet Realm - Community Pagelet Prefs**.
6. Add parameters, using the same name as the preferences in the portlet. For details on adding parameters, see "Configuring Parameters in the Ensemble Console" on page 9-4.

7. Define the parameters in your pagelet injection code. For details on setting parameter values, see “Setting Parameter Values in Pagelet Injection Code” on page 9-5.

Accessing Pagelet Discovery for Developers

Pagelets configured Ensemble are automatically documented in the Ensemble Pagelet Discovery UI. To access the pagelet discovery UI:

1. Launch the Ensemble Console.
2. Click the **APPLICATIONS** tab.
3. Click the **Pagelet Docs** sub-tab.

Audit

This chapter describes how to configure and use the auditing functionality of AquaLogic Ensemble. Auditing provides information about the creation, modification, and deletion of Ensemble resources and policies from within the Ensemble Console, along with usage information for resources proxied by Ensemble.

This chapter is divided into the following sections:

- "Enabling Audit" on page 10-1 describes how audit is enabled for Ensemble resources and policies.
- "Generating Audit Reports" on page 10-2 describes how to use the Ensemble database to generate audit reports.

Enabling Audit

Auditing data is automatically recorded when Ensemble resources and policies are created, modified, or deleted.

You can enable and disable auditing of usage for each proxied resource. When you create a resource, its audit status defaults to disabled.

To change the audit status of a resource:

1. Launch the Ensemble Console.
2. Click the **AUDIT** tab.
3. Click the name of the resource you want to configure.

4. To enable or disable auditing, next to **Audit Status,** select Enabled or Disabled.
5. Click **Save**.

Generating Audit Reports

Audit information is stored in the Ensemble database. You can generate audit reports using SQL queries. The following sections provide sample SQL scripts and describe the data returned by the queries:

Auditing Access to Proxied Resources

Audit information regarding access to proxied resources is stored in the **ACCESSAUDITRECORDS** table in the Ensemble database.

Example SQL Queries

The following query displays all accesses to any resource by a specific *username*. Replace *owner* with the database owner of the ACCESSAUDITRECORDS table.

```
select ID, CREATE_DATE, USERNAME, USERTYPE, SERVICENAME, RESOURCE_ID,
RESOURCENAME, ACCESSSUCCESS, ACCESSURL, ACCESSPRIMAUTHENTICATIONMETHOD,
ACCESSRESAUTHENTICATIONMETHOD
from owner.ACCESSAUDITRECORDS
where USERNAME='username';
```

The following query displays all accesses by a specific *username* to a specific *resource*. Replace *owner* with the database owner of the ACCESSAUDITRECORDS table.

```
select ID, CREATE_DATE, USERNAME, USERTYPE, SERVICENAME, RESOURCE_ID,
RESOURCENAME, ACCESSSUCCESS, ACCESSURL, ACCESSPRIMAUTHENTICATIONMETHOD,
ACCESSRESAUTHENTICATIONMETHOD
from owner.ACCESSAUDITRECORDS
where USERNAME='username' and RESOURCENAME='resource';
```

You should create custom queries to meet your reporting needs.

Schema Description

The following table describes the ACCESSAUDITRECORDS schema.

Table 10-1 ACCESSAUDITRECORDS

Column	Description
ID	A unique identifier for the audit record in this table.
CREATE_DATE	The date and time the audit event was created.
USERNAME	The name of the user accessing the resource.
USERTYPE	A comma-delimited list of roles. Roles are assigned by the experience definition associated with the user when the resource is accessed.
SERVICENAME	The fully-qualified domain name of the Ensemble proxy server.
ACCESSSUCCESS	1 if the resource is successfully accessed. 0 if access to the resource fails. **Note:** Access to the resource fails if the HTTP request from the proxy service to the proxied resource fails, or if the user does not have a role required to access the resource. If the user does not authenticate with Ensemble, no audit event is generated.
ACCESSURL	The URL the user used to access the resource.
ACCESSIPADDRESS	The user's IP address.

Table 10-1 ACCESSAUDITRECORDS

Column	Description
ACCESSPRIMAUTHENTICATIONMETHOD	The authentication method used to authenticate the user. Possible values include: • **Basic authentication:** [class com.plumtree.runner.authentication.integrated.BasicAuthIntegratedAuthenticator] • **Form authentication**: INTERACTIVE • **Oracle COREid authentication:** Oracle COREid Autenticator • **SPNEGO authentication**: SPNEGO • **SiteMinder authentication:** CA SiteMinder Authenticator
ACCESSRESAUTHENTICATIONMETHOD	The authentication method used by Ensemble to access the proxied resource. Possible values are: • Autologin Disabled • Basic • Form • None Selected

Auditing Creation, Modification, and Deletion of Ensemble Resources

Audit information regarding the creation, modification, and deletion of Ensemble resources is stored in two tables in the Ensemble database: **RESOURCECONFIGAUDITRECORDS** and **RESOURCECONFIGDATA**.

RESOURCECONFIGAUDITRECORDS stores information about who modifies which resources, and when.

RESOURCECONFIGDATA stores snapshot of the properties of the resource. This allows you to see how the resource changes with each modification.

Example SQL Queries

The following query displays all creation, modification, or deletion of resources by a specific *username*. Replace *owner* with the database owner of the RESOURCECONFIGAUDITRECORDS table.

```
select ID, CREATE_DATE, USERNAME, USERTYPE, OWNERNAME, POLICYOWNERNAME,
ENABLED_FLAG, SERVICENAME, RESOURCE_ID, RESOURCENAME, ACTIONTYPE
from owner.RESOURCECONFIGAUDITRECORDS
where USERNAME='username';
```

The following query displays the details of how a specific *resource* was modified.

```
select owner.RESOURCECONFIGDATA.record_id,
owner.RESOURCECONFIGDATA.pageNumber,
owner.RESOURCECONFIGAUDITRECORDS.USERNAME,
owner.RESOURCECONFIGAUDITRECORDS.RESOURCENAME,
owner.RESOURCECONFIGDATA.properties
from owner.RESOURCECONFIGAUDITRECORDS, owner.RESOURCECONFIGDATA
where
owner.RESOURCECONFIGAUDITRECORDS.ID=owner.RESOURCECONFIGDATA.record_id
and owner.RESOURCECONFIGAUDITRECORDS.RESOURCENAME='resource';
```

You should create custom queries to meet your reporting needs.

Schema Description

The following table describes the RESOURCECONFIGAUDITRECORDS schema.

Table 10-2 RESOURCECONFIGAUDITRECORDS

Column	Description
ID	A unique identifier for the audit record in this table.
CREATE_DATE	The date and time the audit event was created.
USERNAME	The name of the user creating, modifying, or deleting the resource.
USERTYPE	The highest administrative role of the user that allows him to make the resource configuration change. Possible values, from highest to lowest, are: 1. Administrators 2. Managers 3. Resource Owners
OWNERNAME	GUID of the resource owner.
POLICYOWNERNAME	GUID of the policy owner of the policy associated with this resource.
SERVICENAME	The fully-qualified domain name of the Ensemble proxy server.

Table 10-2 RESOURCECONFIGAUDITRECORDS

Column	Description
RESOURCE_ID	The ID of the resource in the RESOURCES table.
RESOURCENAME	The name of the resource.
ACTIONTYPE	An integer from 0-2 that indicates what has been done to the resource: • 0: Resource created. • 1: Resource modified. • 2: Resource deleted.

Note: OWNERNAME and POLICYOWNERNAME GUIDs come from the AquaLogic Interaction portal database. These values are stored in the PTMIGRATION table, which can be joined with the PTUSERS table to match user names with GUIDs.

The following table describes the RESOURCECONFIGDATA schema:

Table 10-3 RESOURCECONFIGDATA

Column	Description
record_id	Associates this entry with a record in RESOURCECONFIGAUDITRECORDS.
properties	A CR-delimited string of name/value pairs that provides a snapshot of the resource's configured values.
pageNumber	The properties column may require multiple rows. In cases where multiple rows are required, pageNumber is incremented for each additional row for a given record_id.

Auditing Creation, Modification, and Deletion of Ensemble Policies

Audit information regarding the creation, modification, and deletion of Ensemble policies is stored in two tables in the Ensemble database: **AUTHORIZATIONCONFIGAUDITRECS** and **AUTHORIZATIONCONFIGDATA**.

AUTHORIZATIONCONFIGAUDITRECS stores information about who modifies which policies, and when.

AUTHORIZATIONCONFIGDATA stores snapshot of the properties of the policy. This allows you to see how the policy changes with each modification.

Example SQL Queries

The following query displays all creation, modification, or deletion of policies by a specific *username*. Replace *owner* with the database owner of the AUTHORIZATIONCONFIGAUDITRECS table.

```
select ID, CREATE_DATE, USERNAME, USERTYPE, OWNERNAME, POLICYOWNERNAME,
ENABLED_FLAG, SERVICENAME, RESOURCE_ID, RESOURCENAME, ACTIONTYPE
from owner.AUTHORIZATIONCONFIGAUDITRECS
where USERNAME='username';
```

The following query displays the details of how a specific policy *policy* was modified.

```
select owner.AUTHORIZATIONCONFIGDATA.record_id,
owner.AUTHORIZATIONCONFIGDATA.pageNumber,
owner.AUTHORIZATIONCONFIGAUDITRECS.USERNAME,
owner.AUTHORIZATIONCONFIGAUDITRECS.RESOURCENAME,
owner.AUTHORIZATIONCONFIGDATA.properties
from owner.AUTHORIZATIONCONFIGAUDITRECS, owner.AUTHORIZATIONCONFIGDATA
where
owner.AUTHORIZATIONCONFIGAUDITRECS.ID=owner.AUTHORIZATIONCONFIGDATA.record
_id
and owner.AUTHORIZATIONCONFIGAUDITRECS.RESOURCENAME='policy';
```

Custom queries should be created to meet your reporting needs.

Schema Description

The following table describes the AUTHORIZATIONCONFIGAUDITRECS schema.

Table 10-4 AUTHORIZATIONCONFIGAUDITRECS

Column	Description
ID	A unique identifier for the audit record in this table.
CREATE_DATE	The date and time the audit event was created.
USERNAME	The name of the user creating, modifying, or deleting the resource.

Table 10-4 AUTHORIZATIONCONFIGAUDITRECS

Column	Description
USERTYPE	The highest administrative role of the user that allows him to make the resource configuration change. Possible values, from highest to lowest, are: 1. Administrators 2. Managers 3. Resource Owners
OWNERNAME	GUID of the resource owner this policy is associated with.
POLICYOWNERNAME	GUID of the policy owner of the policy set.
SERVICENAME	The fully-qualified domain name of the Ensemble proxy server.
RESOURCE_ID	The ID of the policy set in the POLICIES table.
RESOURCENAME	The name of the policy set.
ACTIONTYPE	An integer from 0-2 that indicates what has been done to the resource: • 0: Policy set created. • 1: Policy set modified. • 2: Policy set deleted.

Note: OWNERNAME and POLICYOWNERNAME GUIDs come from the AquaLogic Interaction portal database. These values are stored in the PTMIGRATION table, which can be joined with the PTUSERS table to match user names with GUIDs.

The following table describes the AUTHORIZATIONCONFIGDATA schema:

Table 10-5 AUTHORIZATIONCONFIGDATA

Column	Description
record_id	Associates this entry with a record in AUTHORIZATIONCONFIGAUDITRECS.
properties	A CR-delimited string of name/value pairs that provides a snapshot of the policy set's configured values.
pageNumber	The properties column may require multiple rows. In cases where multiple rows are required, pageNumber is incremented for each additional row for a given record_id.

CHAPTER 11

Analytics

This chapter describes how to configure Aqualogic Analytics to accept and report on events from AquaLogic Ensemble. This involves the following steps:

1. Configure AquaLogic Analytics to accept Ensemble events. For details, see

Link to Analytics Install Guide, Ensemble section.

2. Configure Ensemble to send events to Analytics. For details, see "Configuring Ensemble for AquaLogic Analytics" on page 11-1.

Configuring Ensemble for AquaLogic Analytics

You configure Ensemble to send events to Analytics by using the Configuration Manager.

To configure Ensemble to send events to Analytics, on the Ensemble host:

1. Launch the BEA AquaLogic Configuration Manager.
2. Under AquaLogic Ensemble, click **ALI Analytics.**
3. Select **Enabled.**
4. Type the **Server** and **Port** of your Analytics installation.

CHAPTER 12

Extending AquaLogic Ensemble

This chapter describes ways to extend Ensemble, including customizing the user experience and developing web applications using Ensemble extensions, and is divided into the following sections:

Custom Login Resources

What the user sees when she logs in and out of Ensemble resources is controlled by customizing login resources. Based on the experience definition associated with the user, different pages can be delivered to the user at different times in the login or logout process. The following sections describe login resources and how to use them to communicate with Ensemble.

For details on using experience definitions to determine which login resource is used with a given user, see Chapter 8, "Experience Definitions."

About Login Resources

A login resource hosts pages associated with a user's experience authenticating with Ensemble. The following table describes the types of pages that can be delivered by a login resource:

Table 12-1 Login Resource Pages

Page	Definition
Pre-login page	This page is displayed to the user prior to prompting the user for authentication the user.
Login page	This page is only applicable when form authentication is being used, and provides the form for login.
Post-login page	This page is displayed to the user after successful authentication and before the resource is accessed.
Error page	This page is displayed if there is an error in the login process.
Post-logout page	This page is displayed after the user logs out of the resource.

A web page on the login resource can be specified for any or all of these settings using experience definitions. For details on configuring experience definitions, see "Login Resources and Interstitial Pages" on page 8-5.

Communicating With Ensemble

Login resource pages communicate with Ensemble by using HTTP headers. The following table lists the available headers and describes how and when they are used in the login or logout process.

Table 12-2 Login Resource Headers

Page	Header	Values
Pre-login	runner_pre_interstitial_complete	• **true -** indicates that the Pre-login page has completed successfully. The page is not displayed and Ensemble proceeds to the login page. • **false** - Ensemble does nothing when the header is set to false or if the header is not present. The pre-login page is displayed.
Login	runner_username	• The username Ensemble uses to authenticate the user.
Login	runner_password	• The password Ensemble uses to authenticate the user.
Login	runner_authentication_provider	• The provider for authentication. For AquaLogic Ensemble 1.0 the only valid value is **portal**. If the header is not present, the provider defaults to **portal**.
Login	runner_portal_authentication_source	• The authentication source to authenticate the user against. This is the same as the authentication source the user would use to log in to the portal.
Post-login	runner_post_interstitial_complete	• **true -** indicates that the Post-login page has completed successfully. The page is not displayed and Ensemble proceeds to the login page. • **false** - Ensemble does nothing when the header is set to false or if the header is not present. The post-login page is displayed.

Note: Error and Logout pages are considered terminal pages and do not communicate with Ensemble using headers. Ensemble does provide information to these pages using Ensemble Adaptive tags. For details, see "Ensemble Adaptive Tags" on page 12-4.

Ensemble Adaptive Tags

Ensemble Adaptive Tags allow you to insert data and logic into your proxied web application. Ensemble transforms tags included in proxied web applications before the page is delivered to the user.

For details on Ensemble Adaptive Tags, see the topic on Ensemble Adaptive Tags in the AquaLogic developer documentation.