BEA AquaLogic Enterprise Repository®

eTrust™ SiteMinder® Setup and Configuration Guide

Version 3.0 RP1
Document Revised: February 2008

Table of Contents

- Configure ALER for use with SiteMinder Authentication
  - Enable SiteMinder Integration System Properties
  - Modify Application Property Files
- Advanced Options
  - Creating/Assigning Default Roles for New Users
  - Create New Users/Allow Unapproved Users
  - Enable Unapproved/New User Login
  - New User Notification
  - Syncing Departments
  - Syncing Roles

Overview

The ALER **Advanced Container Authentication LoginModule** is used to accept user credentials passed by HTTP Request Headers (potentially populated by an SSO system). This feature allows integration with single-sign-on systems such as eTrust Siteminder.

Configure ALER For Use With SiteMinder Authentication

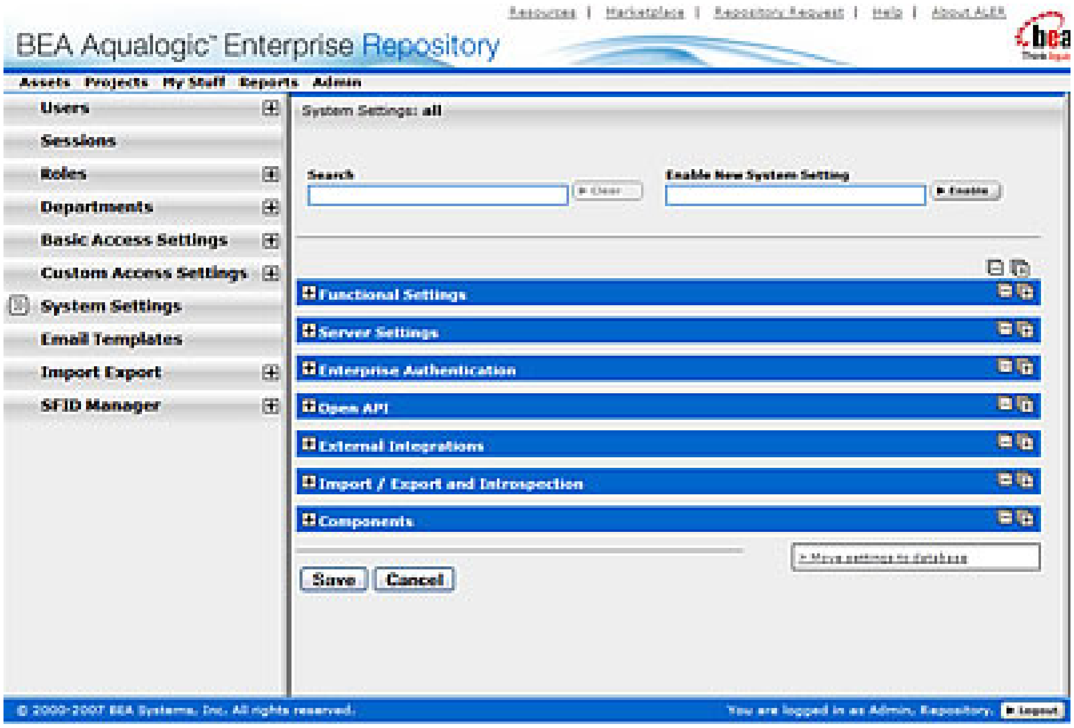
Access the following configuration properties requires **Access Administrator** rights.

Note about the SSO Soap Header Enhancement - This enhancement allows AdvancedContainerLogin Module to accept user information in SOAP Headers for the AuthtokenCreate REX API method. The username is passed in a SOAP Header with a name that is identified by the ALER system setting enterprise. container.auth.username and has a namespaceUri of www.bea.com/aler. The value of the SOAP Header is the username of the user. If the username is not passed within a SOAP Header then the ALER system setting enterprise.loginmodules.fallbackauthentication is used. If enterprise.loginmodules. fallbackauthentication is true, then the user is authenticated by the configured PluggableLoginModule for the specified username/password.

Enable SiteMinder Integration System Properties

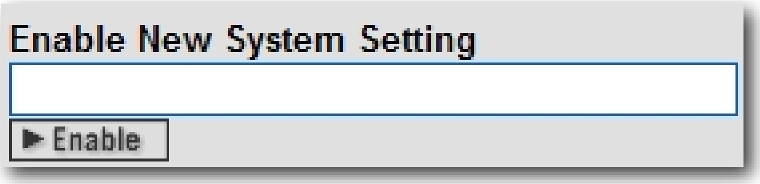
This procedure is performed on the ALER **Admin** screen. The SSO Integration is an Advanced Licensed feature.

1. Click **System Settings** in the left pane.


Resources | Marketplace | Repository Request | Help | About ALER
BEA Aqualogic™ Enterprise Repository
bea
Assets Projects My Stuff Reports Admin
Users
Sessions
Roles
Departments
Basic Access Settings
Custom Access Settings
System Settings
Email Templates
Import Export
SFID Manager
System Settings: all
Search
Clear
Enable New System Setting
Enable
Functional Settings
Server Settings
Enterprise Authentication
Open API
External Integrations
Import / Export and Introspection
Components
Move settings to database
Save
Cancel
© 2000-2007 BEA Systems, Inc. All rights reserved.
You are logged in as Admin, Repository.
Logout

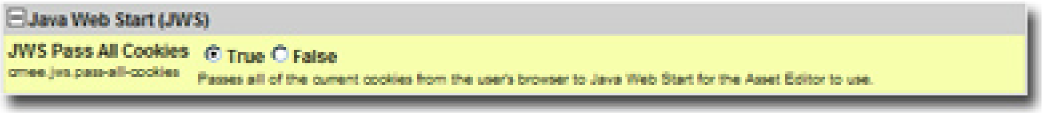
2. Enter **`enterprise.authentication.advancedcontainer.enabled`** into the Search box. Set the value to **True** and click Save.

3. Enter **`cmee.jws.pass-all-cookies`** in the **Enable New System Setting** text box.



4. Click **Enable**.

   JWS Pass All Cookies appears in the **Java Web Start (JWS)** section of the **Server Settings** group of system settings.



Java Web Start (JWS)

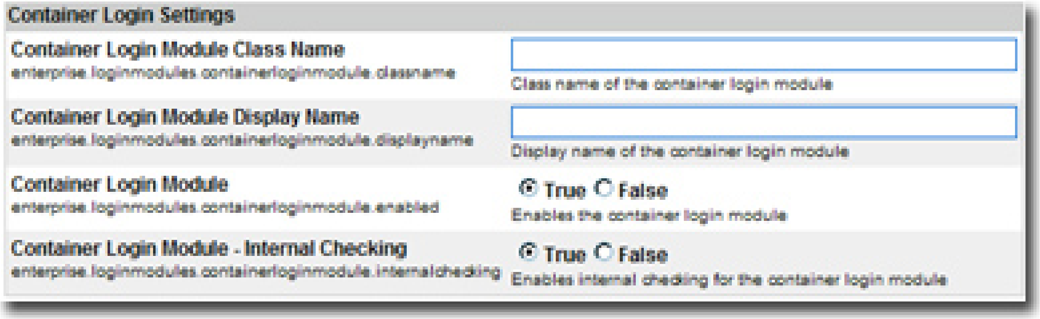
JWS Pass All Cookies ● True ○ False
cmee.jws.pass-all-cookies
Passes all of the current cookies from the user's browser to Java Web Start for the Asset Editor to use.

5. Make sure the property is set to **True**.

6. Click **Save**.

7. Enter `container login module` in the System Settings **Search** text box.

   The **Containter Login Module** section opens in the **Enterprise Authentication** group of system settings.



Container Login Settings	
Container Login Module Class Name enterprise.loginmodules.containerloginmodule.classname	Class name of the container login module
Container Login Module Display Name enterprise.loginmodules.containerloginmodule.displayname	Display name of the container login module
Container Login Module enterprise.loginmodules.containerloginmodule.enabled	● True ○ False Enables the container login module
Container Login Module - Internal Checking enterprise.loginmodules.containerloginmodule.internalchecking	● True ○ False Enables internal checking for the container login module

8. Modify the following properties as indicated:

    - **Container Login Module Class Name**
        - Enter `com.flashline.enterprise.authentication.server.loginmodule.AdvancedContainerLogin` in the text box.

    - **Container Login Module Display Name**
        - Enter `Advanced Container Login Module` in the text box.

    - **Container Login Module**
        - Set the property to **True**.

9. Supply SSO Header Values as indicated (these are often called Responses within the Policy Server):
    - **Username Header Name**
        - Set this property to the Header Name that will contain the user's UID value.

    - **Firstname Header Name**
        - Set this property to the Header Name that will contain the user's First Name value.

    - **Middlename Header Name**
        - Set this property to the Header Name that will contain the user's Middle Name value.

    - **Lastname Header Name**
        - Set this property to the Header Name that will contain the user's Last Name value.

    - **Status Header Name**
        - Set this property to the Header Name that will contain the user's Active Status value.

    - **Email Header Name**
        - Set this property to the Header Name that will contain the user's Email value.

    - **Phone Header Name**
        - Set this property to the Header Name that will contain the user's Phone Number value.

    - **Roles Header Name**
        - Set this property to the Header Name that will contain the user's Role(s) value.

    - **Department Header Name**

        - Set this property to the Header Name that will contain the user's Department(s) value.

10. Update the behavior of the SSO module with the following properties:
    - **Use Container passed Departments**
        - Set this value to True if you would like to synchronize the user's department from the policy server responses.

    - **Departments passed within single header**
        - Set this value to **True**.

    - **Department Delimiter**
        - Set this value to the character that will delimit multiple departments within the single department header. This field can accept Unicode notations such as \u0020 for a space.

    - **Use Container passed Roles**
        - Set this value to True if you would like to synchronize the user's roles from the policy server responses. (NOTE: Setting this value to true prior to verifying the correct configuration may render your ALER application unusable).

    - **Roles passed within single header**
        - Set this value to **True**.

    - **Role Delimiter**
        - Set this value to the character that will delimit multiple roles within the single roles header. This field can accept Unicode notations such as \u0020 for a space.

    - **Assign default roles to users**
        - Set this value to True so that users will have all roles marked as 'default' assigned to their user account.

    - **Auto create missing roles**
        - Set this value to True to allow ALER to create roles included within a user's role header that do not exist currently. This feature will create a role and assign the user to that role, but no roles will be assigned to the newly created role.

    - **Auto create missing departments**
        - Set this value to True to allow ALER to create departments included within a user's department header that do not exist currently. This feature will create a department and assign the user to that department, but will not assign that department to any project.

11. Enter `cookie login module` in the System Settings **Search** text box.

    The **Cookie Login Settings** section opens in the **Enterprise Authentication** group of system settings.

12. Set the **Cookie Login Module** property to **False**.

13. Enter `plug-in login` in the System Settings **Search** text box.

    The **Plugin Login Settings** section opens in the **Enterprise Authentication** group of system settings.

14. Enter `false` in the **Plug-in Login Module** text box.

15. Enter `unapproved user` in the System Settings **Search** text box.

    The **Unapproved User Login** property appears in the **General** section of the **Enterprise Authentication** group of system settings.

16. Set the **Unapproved User Login** property to **True**.

17. Click **Save**.

Using the ALER SSO Integration with Basic Authentication

If the SiteMinder installation uses **Basic Authentication**, additional property settings are required to allow the AquaLogic Enterprise Repository **Asset Editor** to function properly.

1. Using the process described above, enable the following property:
    - `cmee.jws.suppress-authorization-header`

2. Set the property to **True**.

3. Click **Save**

Modify Application Property Files Manually

- **Prerequisite:** Stop the application server.
    - Modifications to properties files may impact any applications running on the application server.

1. Edit the `containerauth.properties` file in `WEB-INF/classes`.

    This file contains a list of header names that are specific to the SiteMinder server. This information represents the Response Headers SiteMinder uses for replies, and should be acquired from your organization's SiteMinder Administrators/Architects.

    If SiteMinder responses do not provide the appropriate value for an **email** header, a blank "" can be substituted instead of a true header value. Other fields that are not supplied or populated by SiteMinder should be left null.

    (An asterisk <*> indicates a required field.)

    - Configure the Header variables that should be mapped to the appropriate AquaLogic Enterprise Repository user information:

        (**Note:** The values indicated below are examples only and **must** be replaced with the appropriate SiteMinder Response Header names defined by your SiteMinder system.)

- *enterprise.container.auth.username* = <UID>*
- *enterprise.container.auth.firstname* = <FIRST_NAME>
- *enterprise.container.auth.middlename* = <MIDDLE_NAME>
- *enterprise.container.auth.lastname* = <LAST_NAME>
- *enterprise.container.auth.status* = <STATUS>
- *enterprise.container.auth.email* = <MAIL>*
- *enterprise.container.auth.phone* = <PHONE>
- *enterprise.container.auth.roles* = <ROLES>
- *enterprise.container.auth.depts* = <DEPARTMENTS>
- *enterprise.container.auth.enable-synch-roles* = true
- *enterprise.container.auth.roles-single-header* = true
- *enterprise.container.auth.roles-delimiter* = \u0020
- *enterprise.container.auth.enable-synch-depts* = true
- *enterprise.container.auth.depts-single-header* = true
- *enterprise.container.auth.depts-delimiter* = \u0020

Note: The last six properties listed above are utilized when role and/or department synching is enabled, and more than one role or department is supplied in a single header. These additional properties can be disabled/ignored depending on the values supplied in the boolean parameters enable-synch-roles and enable-synch-depts. The delimiter field in this example uses the unicode space character; however, unicode is not required for any other delimeter character.

2. Most SiteMinder web agent applications are deployed against an HTTP server that is separate from the Application Server. In this scenario, an AJP type connector (**`mod_jk/mod_jk2`** for Apache HTTP Servers, **`mod_was_ap20_http`** for IBM HTTP Server, etc.) will link the HTTP server to the application server. Typically, the HTTP server runs on a seperate machine for performance or resource pooling reasons. In this scenario it is necessary to modify the **`cmee.properties`** file to reflect the new name for your application, as outlined below.

   - Edit the `cmee.properties` file in `WEB-INF/classes`.

     - Original Configuration (Tomcat with Coyote)
       - *cmee.server.paths.image=http\://tomcat.example.com\:8080/flashline-web/images*
       - *cmee.server.paths.jsp=http\://tomcat.example.com\:8080/flashline*
       - *cmee.server.paths.servlet=http\://tomcat.example.com\:8080/flashline*
       - *cmee.server.paths.jnlp-tool=http\://tomcat.example.com\:8080/flashline-web/webstart*
       - *cmee.server.paths.resource=http\://tomcat.example.com\:8080/flashline-web*
       - *cmee.enterprisetab.homepage=http\://tomcat.example.com\:8080/flashline/custom/home.jsp*
       - *cmee.assettab.asset-detail-page=http\://tomcat.example.com\:8080/flashline/cmee/index.jsp*

     - New configuration (Apache HTTP with mod_jk2 to Tomcat)
       - *cmee.server.paths.image=http\://apache.example.com/flashline-web/images*
       - *cmee.server.paths.jsp=http\://apache.example.com/flashline*
       - *cmee.server.paths.servlet=http\://apache.example.com/flashline*
       - *cmee.server.paths.jnlp-tool=http\://apache.example.com/flashline-web/webstart*
       - *cmee.server.paths.resource=http\://apache.example.com/flashline-web*
       - *cmee.enterprisetab.homepage=http\://apache.example.com/flashline/*

    custom/home.jsp
    - *cmee.assettab.asset-detail-page=http\://apache.example.com/flashline/cmee/index.jsp*

  - In this example the new URL to connect to the Repository will be: **`http://apache.example.com/flashline/index.jsp`**

3. Restart the ALER application.

Advanced SiteMinder Options

The following options add functionality for assigning default roles, new user creation/notification, syncing departments, and syncing roles.

Creating/Assigning Default Roles for New Users

With Advanced RBAC:

1. Click **Admin** on the ALER menu bar.
2. On the **Admin** screen, click **Roles**.
3. Click **Create New**.
4. Enter **Browse_Only** in the name field.
    - Check **Automatically assign to new users**
    - Add any existing users who fit this profile.
5. Click **Save**.
6. Click the role **1: Create/Submit**.
7. Click **Edit**
    - Uncheck **Automatically assign to new users**.
8. Click **Save**.
9. Click the role **User**
10. Click **Edit**.
    - Uncheck **Automatically assign to new users**. (**User** is the default role and automatically assigned to new users as shipped with the ALER.)
11. Click **Save**.
12. Click **Custom Access Settings**.
13. Click **Create New**.
14. Enter **Browse_Only** in the name field.
    - Check **Automatically assign to all new assets**.
    - Locate **Browse_Only** in the list of roles.
    - Check **View**.
15. Click **Save**.

16. Click **OK** to apply to all assets.

With Basic Access Settings:

1. Click **Admin** on the ALER menu bar.
2. On the **Admin** screen, click **Roles**.
3. Click **Create New**.
4. Enter **Browse_Only** in the name field.
    - Check **Automatically assign to new users**
    - Add any existing users who fit this profile.
5. Click the role **User**
6. Click **Edit**.
    - Uncheck **Automatically assign to new users**. (**User** is the default role and automatically assigned to new users as shipped with ALER.)
7. Click **Save**.

Create New Users/Allow Unapproved Users

The ALER SiteMinder authentication integration will automatically create new users within the ALER database once they are successfully authenticated. The specific access and permissions granted to new users is determined by the configuration of the default **New User Role(s)**, as described in the previous section. Upon approval by the access administrator, new users may be assigned to other roles with different access settings. However, if the SiteMinder integration is configured with role synchronization enabled, then the user will be assigned the roles provided by SiteMinder response headers.

Enable Unapproved/New User Login

When enabled, this option allows unapproved/new AquaLogic Enterprise Repository users to access the application after SiteMinder authentication. If disabled, new or unapproved users cannot access AquaLogic Enterprise Repository. This feature is particularly useful when a manual approval process is required before accessing the application.

- **Enable Unapproved User Login = true** (file: enterprise.properties)
    - enterprise.security.unapproveduser.allowlogin=true

New User Notification

When enabled, this property will notify the access adminstrator via email when a new user account is added to ALER via SiteMinder.

- **Enable New User Notification = true** (file: cmee.properties)
    - cmee.new.unapproved.users.notify=true

Syncing Departments

When enabled, this property will synchronize department names from SiteMinder response header values.

- **Enable Department Syncing = true** (file: *containerauth.properties*)
    - enterprise.container.auth.enable-synch-depts - Set to true if known departments are to be synchronized with users, set to false otherwise.
- **Enable Department Creation = true** (file: *containerauth.properties*)*
    - enterprise.container.auth.auto-create-missing-depts - Set to true if user's departments are to be automatically created at login, set to false otherwise.

Notes on Department Synchronization

The SiteMinder integration will **not** create new departments. It will only link users to departments that already exist within AquaLogic Enterprise Repository and have the same name as that provided in the SiteMinder response header value(s).

The ?SiteMinder server may be configured to pass multiple headers of the same name but different values for each department a user is assigned, or one header containing all of the departments that a user is assigned.

- Configuration 1 - A multiple headers of the same name, with a different value in each:

  enterprise.container.auth.enable-synch-depts= **true**
  enterprise.container.auth.depts-single-header= **false**
  enterprise.container.auth.depts-delimiter= **""**
  enterprise.container.auth.depts= **DEPT_HEADER_NAME**

DEPT_HEADER_NAME=DEPTA
DEPT_HEADER_NAME=DEPTB
DEPT_HEADER_NAME=DEPTC

and NOT

DEPT_HEADER_NAME=DEPTA DEPTB DEPTC ...

- Configuration 2 - One header with multiple values seperated by a delimeter:

  enterprise.container.auth.enable-synch-depts= **true**
  enterprise.container.auth.depts-single-header= **true**
  enterprise.container.auth.depts-delimiter= **"^"**
  enterprise.container.auth.depts= **DEPT_HEADER_NAME**

  DEPT_HEADER_NAME=DEPTA^DEPTB^DEPTC^ ...

  and NOT

  DEPT_HEADER_NAME=DEPTA
  DEPT_HEADER_NAME=DEPTB
  DEPT_HEADER_NAME=DEPTC

Syncing Roles

When enabled, this property will synchronize role names from SiteMinder response header values.

- **Enable Role Syncing = true** (file: containerauth.properties)
  - enterprise.container.auth.auto-create-missing-roles - Set to true if unknown roles are to be auto-created, set it to false otherwise.

Notes on Role Synchronization

The SiteMinder integration **can** create new roles. The integration will link users to roles that previously exist within the AquaLogic Enterprise Repository and have the same name as that provided in the SiteMinder response header value(s). In addition to linking to existing roles, the integration will also create roles found in the header values that do not already exist within the AquaLogic Enterprise Repository. Roles created in this way will have no rights assigned to them by default.

- **Enable Missing Role Creation = true** (file: containerauth.properties)
  - *enterprise.container.auth.auto-create-missing-roles* = ***true***

The Siteminder server may be configured to pass one header value for each role a user is assigned

- Configuration 1 - A multiple headers of the same name, with a different value in each:

  enterprise.container.auth.enable-synch-roles= **true**
  enterprise.container.auth.roles-single-header= **false**
  enterprise.container.auth.roles-delimiter= **""**
  enterprise.container.auth.roles= **ROLE_HEADER_NAME**

  ROLE_HEADER_NAME=ROLEA
  ROLE_HEADER_NAME=ROLEB
  ROLE_HEADER_NAME=ROLEC

  and NOT

DEPT_HEADER_NAME=ROLEA ROLEB ROLEC ...

- Configuration 2 - One header with multiple values seperated by a delimeter:

  enterprise.container.auth.enable-synch-roles= **true**
  enterprise.container.auth.roles-single-header= **true**
  enterprise.container.auth.roles-delimiter= **"^"**
  enterprise.container.auth.roles= **ROLE_HEADER_NAME**

  DEPT_HEADER_NAME=ROLEA^ROLEB^ROLEC^ ...

  and NOT

  ROLE_HEADER_NAME=ROLEA
  ROLE_HEADER_NAME=ROLEB
  ROLE_HEADER_NAME=ROLEC

Enable Debug Logging

Enable debug logging by appending the following line in the log4fl.properties file:

```
log4j.category.com.flashline.enterprise.authentication.client.LoginContext=debug, cmeeLog
```