

Entrust GetAccess[™] 7.0 Technical Integration Brief for IBM WebSphere Portal 5.0

November 2004

www.entrust.com
1-888-690-2424

Entrust is a registered trademark of Entrust, Inc. in the United States and certain other countries. Entrust is a registered trademark of Entrust Limited in Canada. All other company and product names are trademarks or registered trademarks of their respective owners. The material provided in this document is for information purposes only. It is not intended to be advice. You should not act or abstain from acting based upon such information without first consulting a professional. ENTRUST DOES NOT WARRANT THE QUALITY, ACCURACY OR COMPLETENESS OF THE INFORMATION CONTAINED IN THIS ARTICLE. SUCH INFORMATION IS PROVIDED "AS IS" WITHOUT ANY REPRESENTATIONS AND/OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, BY USAGE OF TRADE, OR OTHERWISE, AND ENTRUST SPECIFICALLY DISCLAIMS ANY AND ALL REPRESENTATIONS, AND/OR WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, NON-INFRINGEMENT, OR FITNESS FOR A SPECIFIC PURPOSE.

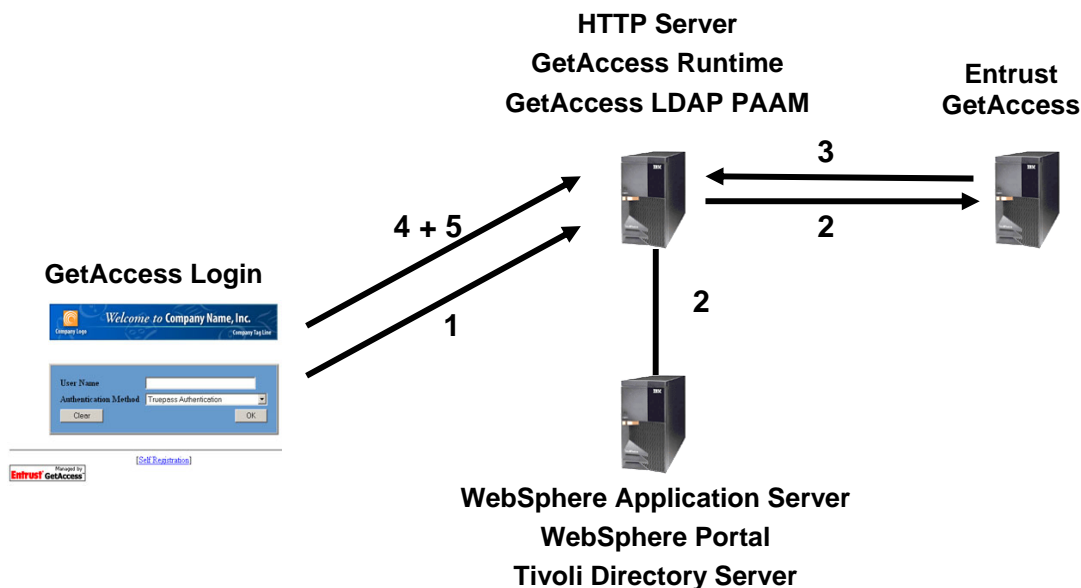
Entrust GetAccess™

Entrust GetAccess™ software provides a comprehensive, Web Access Control and Single Sign-On security solution that can help to enable organizations to move business processes online. The Entrust GetAccess portfolio delivers a single entry and access point for user authentication and authorization across Web portal applications. As such, Entrust GetAccess provides organizations with security, flexibility and performance to personalize the user experience of a Web portal.

Integration Overview

The integration of Entrust GetAccess products with the IBM WebSphere Portal can help enable enterprises to leverage the benefits, efficiency, and convenience of unified browser access to IBM and non-IBM applications employing the comprehensive centralized authentication and authorization services of Entrust GetAccess. This integration can provide the ability to securely extend the enterprise to employees, customers, partners, and suppliers helping to deliver increased access to information, improved efficiency, and cost reductions.

GetAccess and IBM WebSphere Portal Solution



Use Case Scenario

1. User access protected WebSphere Portal and login occurs
2. Entrust GetAccess validates the user against the WebSphere User Registry (IBM Tivoli Directory Server)
3. Entrust GetAccess creates a SSO token
4. User gains access to WebSphere and user mapping occurs
5. User is automatically logged into WebSphere Portal

Integration Details

The integration of Entrust GetAccess components with the IBM WebSphere Portal primarily consists of implementing a Trust Association Interceptor (TAI) to interact with the Entrust GetAccess system as a supported authentication mechanism for proof of potential Single Sign-On (SSO) operation.

Once a user is authorized by the Entrust GetAccess software, their account username (UID), is communicated to the portal in the HTTP header. The WebSphere Application Server Lightweight Third Party Authentication (LTPA) is configured to enable the integration TAI, which compares the user identifying HTTP header value against existing User Registry data sources and grants access to the portal upon finding a match. A WebSphere logon ticket is generated and stored in the user's browser to enable SSO in the portal.

The Entrust GetAccess LDAP Plug-able Authentication and Authorization Module (PAAM) is configured to authenticate and auto-enroll against the WebSphere User Registry LDAP. The WebSphere User Registry LDAP is IBM Tivoli Directory Server.

The user login model is as follows:

1. The user accesses the WebSphere Portal.
2. The Entrust GetAccess system authorizes portal users access and returns a user UID to the TAI as part of the HTTP header.
3. The WebSphere does not perform any additional authentication of the user.
4. A WebSphere token is generated and stored in the user's browser to enable Single Sign-On in the portal.

Configuring Entrust GetAccess System

The Entrust GetAccess Runtime must be installed on the IBM HTTP Server that is hosting the WebSphere Reverse Proxy Plug-in. The installation will configure IBM HTTP Server with the Entrust GetAccess directives required to protect server resources.

Configure the Entrust GetAccess Runtime to protect the WebSphere Portal URL. Using the Entrust GetAccess Administration Application, configure the installed Runtime to protect the following relative URL:

`/wps/myportal`

;and protect the follow item:

`/wps/*`

The GetAccess protected Portal Resource will require a Role assigned. Create an appropriate Role and assign it to the corresponding Portal Resource.

Configure Entrust GetAccess with the LDAP Plug-able Authentication and Authorization Module (PAAM) against the WebSphere configured LDAP User Registry. The LDAP PAAM will permit GetAccess to authenticate and auto-enroll users against the same User Registry WebSphere authenticates users against. The advantage is the user credentials required for authentication to both products will remain in-sync.

The LDAP PAAM will require additional configuration to statically or dynamically assign the GetAccess Role assigned to the Portal Resource. Please refer to the Entrust GetAccess documentation for further information regarding "Assigning roles and a user type automatically".

Configuring WebSphere Application Server and Portal

1. Move the accompanying Entrust TAI file `entrusttai70.jar` to the `<was_root>\classes` directory.
2. Login to the WebSphere Application Server Administrative Console.
3. Navigate to **Security > Authentication Mechanisms > LTPA**, then click the **Trust Association** link.
4. Check **Trust Association Enabled**.

The screenshot shows the 'LTPA > Trust Association' configuration page. At the top, there is a description: 'Enable Trust Association. Trust Association is used to connect reversed proxies to Websphere.' Below this is a 'Configuration' section with a 'General Properties' tab. In this tab, the 'Trust Association Enabled' checkbox is checked. There are buttons for 'Apply', 'OK', 'Reset', and 'Cancel'. Below the 'General Properties' is an 'Additional Properties' section with a link for 'Interceptors' and a description: 'Specifies a list of Trust Association Interceptor implementations.'

5. Click **Interceptors**.
6. Click **New**.
7. Enter the Interceptor Class name:
`com.wps.sso.EntrustGetAccessTruePassTrustAssociationInterceptor`

The screenshot shows the 'LTPA > Trust Association > Interceptors > New' configuration page. At the top, there is a description: 'Specifies trust information for reverse security proxy servers.' Below this is a 'Configuration' section with a 'General Properties' tab. In this tab, the 'Interceptor Classname' field contains the text `* truePassTrustAssociationInterceptor`. There are buttons for 'Apply', 'OK', 'Reset', and 'Cancel'.

8. Click **OK**.

9. Click **Custom Properties** and add the following required **Name** and **Value** pair.

Name	Value	Required?
entrust.integration	The TAI supported Entrust product to integrate with. <i>Ex: getaccess</i>	Yes

10. Click **Apply** and **Save** the changes.

11. Modify the file <was_root>\AppServer\installedApps\< node>\wps.ear\wps.war\WEB-INF\web.xml.

```
<login-config id="LoginConfig_1">
  <auth-method>FORM</auth-method>
  <realm-name>WPS</realm-name>
  <form-login-config id="FormLoginConfig_1">
    <form-login-page>myportal</form-login-page>
    <form-error-page>/error.html</form-error-page>
  </form-login-config>
</login-config>
```

12. Modify the file

<was_root>\PortalServer\shared\app\config\services\ConfigService.properties.

```
# Logout redirect parameters
#
# Default: false, false, <none>
redirect.logout      = true
redirect.logout.ssl  = <true:false>
redirect.logout.url  = <ga_AccessServer_Logout>
```

Change **redirect.logout.ssl** to **true** if IBM HTTP Server is configured for SSL communication.

Set **redirect.logout.url** to the GetAccess Access Server Logout servlet URL. For example:

<https://p2800-01.entrust.com/GetAccess/Logout>

13. Restart WebSphere Application Server and Portal.

System Behavior

When users access the portal, the Entrust GetAccess authentication dialog appears and users enter their Entrust GetAccess authentication information. Once the user has successfully been authorized to access the Portal URL, they will be transparently logged into WebSphere through the configured TAI. If the user has been previously authenticated into the Entrust GetAccess system, the user will be transparently logged into WebSphere without an authentication dialog.

The WebSphere Portal access URL is `http(s)://<hostname>/wps/myportal`.

For example:

`https://p2800-01.entrust.com/wps/myportal`

As a result of utilizing the GetAccess LDAP PAAM, existing WebSphere Portal users are capable of authenticating, changing profile and password settings, and transparently auto-enrolling into GetAccess.

The WebSphere admin account (wpsadmin) will auto-enroll to GetAccess through the LDAP PAAM initially, as will existing WebSphere users. Existing WebSphere user creation procedures apply as normal.

System Components

Entrust GetAccess 7.0	IBM WebSphere Portal 5.0
Entrust TruePass 7.0 SP1 - optional	IBM HTTP Server 2.0.47.1
Entrust Authority Security Manager 6.0 or 7.0 – optional	IBM Tivoli Directory Server 5.2
Self-Administration Server 7.0 – optional	
Entrust Authority Roaming Server – optional	

Please check PSIC for the latest supported version information at:

<https://www.entrust.com/support/psic/index.cfm>