Workbench Software

Customer Portal Security

By

Workbench Software, LLC

Creation Date:	January 2011
Last Updated:	May 2011
Version:	2.0

Contents

Workbench Software Security

Overview

Security is an important part and feature of the Workbench Customer Portal. The portal application was created specifically as a B2B enterprise class application. Security has been taken into consideration with every aspect of the portal.

This white-paper describes security considerations of the Customer Portal and Legacy System Interface.

Workbench Host Services

Workbench Software hosted applications are located on a dedicated private Server and Database hosted by Revion Solutions, Inc. We at Workbench Software strive to provide the highest quality products and services to our customers. Choosing a partner to host our applications and customer data was a key component of our offering. We took our time and did a lot of research including actual experience with multiple host providers to prove that our host partner will be the best solution for us and most importantly, our customers. Our final decision was to partner with Revion Solutions, Inc. a web hosting company based in New York, NY. Workbench Software started using Revion host services internally and for our customers in 2009. We could not be more pleased with Revion.

About Revion Solutions, Inc.

Revion Solutions, Inc (founded in June 1999) is a web hosting company based in New York, NY USA. Revion offers a complete suite of professional services. Revion is an Oracle Gold partner.

Revion customers include organizations such as

- United States Army
- United States Navy
- Department of Justice
- And more. For more examples visit http://www.revion.com/company/clients/

Data Center

Revion servers are located in New York & New Jersey, monitored and maintained by Microsoft® and Cisco® certified engineers. Our system-administrators strive to ensure that our servers are always up and running all the time. Their efforts guarantee that our servers are running the latest software versions, to prevent incompatibility or program error issues from occurrence. Our data center has:

• Connectivity to the Quality Technology International Backbone
• Redundant Power Feeds
• Uninterruptible Power Supply (UPS) systems
• Backup Diesel Generator Power
• 24 x 7 Monitored Security
• Environmental-control Units
• Fire-suppression Systems
• 24 x 7 system administrators on-site to monitor and maintain the data center infrastructure and client equipment.

Global Network Operations Center

The Quality Tech (Globix) Global Network Operations Center (GNOC), located in New York City, serves as the command, control and communications center for all Quality (former Globix) / network operations and customer support centers. Staffed 24 x 7 with teams dedicated to maintaining the highest quality of service, the GNOC utilizes state-of-the-art equipment and technology for monitoring and managing the network and identifying and resolving problems.


The Actual GNOC
Photo courtesy of Globix


A Server Room
Photo courtesy of Telecity Redbus

Data Center provide you with multiple security features, including video surveillance by both visible and hidden cameras, motion sensors, biometric identification systems, controlled photo ID key-card access and 24-hour security-guard patrols.

At all times, Security Personnel are on duty to ensure the safety of your systems and your employees. Security guards are stationed at every entrance to the site guaranteeing that entry is strictly limited to authorized personnel and to properly account for all equipment entering and leaving the facility. Each guard is supplied with up-to-the-minute access rights information that is linked to Internal Security tools to ensure complete security.

In addition to the security desk, Security personnel man a complex system of monitoring applications designed to oversee the security of the entire facility from data centers to generators. These controls ensure that your systems are protected from unwanted visitors and that access to critical systems is restricted.

In addition to electronic keycards, access to our secure data center facilities is restricted by biometric fingerprint scanners that ensure every user is who they claim to be. The scanners require that the thumb used on the sensor match the print in the system, be within a standard temperature range and have a detectable pulse.

Our very fast connections speed is made possible do to our OC-192 backbone Internet connections. Our servers are top of the line super fast servers all of which are at least Dual/Quad 2.8Ghz or faster with RAID configuration.

Workbench Server Hardware (Hosted by Revion)

Workbench Software has provisioned the following server hardware to host our applications. This is a dedicated server physically located in the Revion Data Center. Our environment is scalable and we plan to add servers as needed.

Workbench Server details:

Quad Core
RAID 1+0 hardware controller
24 GB memory

Workbench APEX Applications Architecture

The Customer Portal was developed with an Oracle product called APEX. Workbench Software hosts APEX applications on a dedicated Oracle Database following standard Oracle security and APEX architecture. This database is located on the Workbench server.

Virtual Private Database

Each Workbench Portal Customer is assigned to a virtual private database within the workbench apex database. APEX manages this using an APEX Workspace. See “About APEX Architecture” for more information about how this is managed by the APEX environment.

Workbench Software Implementation of APEX Architecture

Workbench Server

It is necessary to have a basic understanding of the APEX architecture to understand the Workbench Implementation and services. The following is a description of the APEX architecture taken from the APEX Developer Guide. In this section, look for highlighted comments specific to the Workbench Implementation.

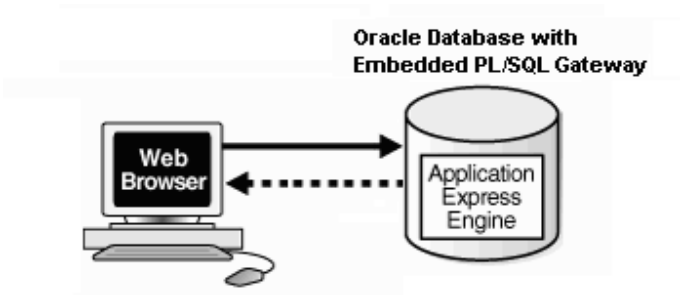
About APEX Architecture

Oracle Application Express installs with your Oracle database and is comprised of data in tables and PL/SQL code.

Whether you run the Oracle Application Express development environment or an application you built using Oracle Application Express, the process is the same. Your browser sends a URL request that is translated into the appropriate Oracle Application Express PL/SQL call. After the database processes the PL/SQL, the results are relayed back to your browser as HTML. This cycle happens each time you request or submit a page.

The application session state is managed in the database tables within Oracle Application Express. It does not use a dedicated database connection. Instead, each request is made through a separate database session, consuming minimal CPU resources.

- Workbench Software Oracle Database is 11g and implements the embedded PL/SQL gateway. The following graphic illustrates the two-tier architecture using the embedded PL/SQL gateway.



About the Oracle Application Express Environment

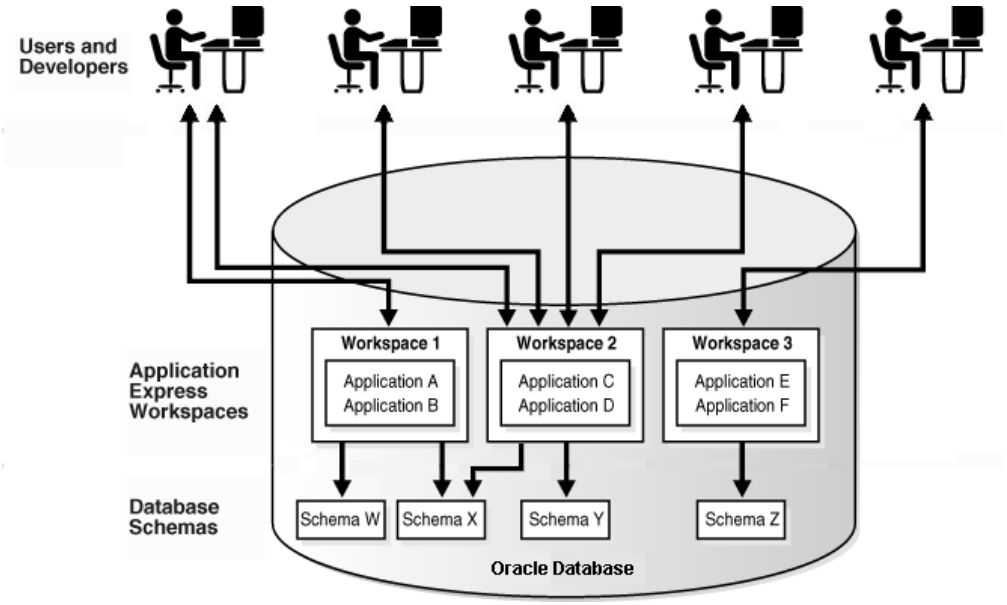
Oracle Application Express enables a single Oracle database to become a shared workgroup database service. Multiple users can access it using a Web browser without installing additional software.

About Workspaces

The area where you develop applications is called a workspace. A **workspace** is a virtual private database that enables multiple users to work within the same Oracle Application Express installation while keeping their objects, data, and applications private.

In a typical development environment, you might create a single workspace for all your developers to share. However, you can also create dedicated workspaces for specific developers or projects. Creating a dedicated workspace limits access to the workspace objects to only those users associated with the workspace.

The following illustration shows the relationship among users and developers, workspaces, and database schemas. Many users and developers can access the same workspace, and one user or developer can access several workspaces.



When you create a workspace, you associate it with a new or existing schema. A **schema** is a logical container for database objects such as tables, views, and stored procedures. A single schema can be associated with one or more workspaces.

All Workbench Customers are assigned to a dedicated workspace.

Although schemas can be associated with more than one workspace, Workbench Host services always dedicate a single schema to each workspace.

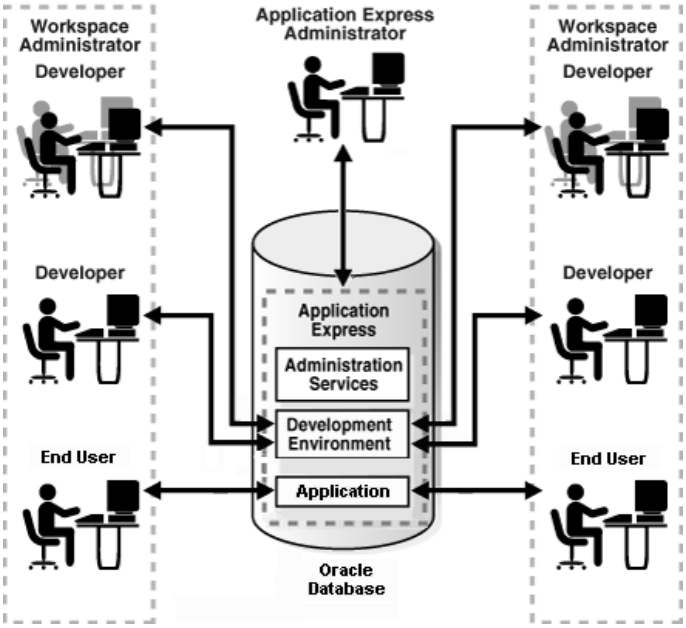
For example, Workbench Software will only configure workspaces and schemas like “Workspace 3” in the above illustration.

About Oracle Application Express User Roles

When setting up Application Express users at a large organization, you assign roles and privileges to specific users. The roles within Oracle Application Express include the following:

- **Workspace administrators** are users who perform administrator tasks specific to a workspace such as managing user accounts, monitoring workspace activity, and viewing log files. For this guide, you are acting as the workspace administrator when setting up the development environment.
- **Developers** are users who create and edit applications and modify database objects. Developers can have their own workspace or share a workspace.
- **End users** have no development privileges. You define end users so that they can access applications that do not use an external authentication scheme.
- **Instance administrators** are superusers that manage an entire hosted instance using the Application Express Administration Services application.

The following illustration shows multiple users with various roles accessing the Oracle Application Express development environment, Application Express Administration Services, and the published applications.



Workbench Support staff have Developer and Administrator Roles.

For security and control, Workbench Software Customers are only allowed End-User access (roles) to the application.

Workbench Legacy Application Interface

Legacy System to Portal Host Security Considerations

To keep the data in the host server database up-to-date with the Legacy System, data is transferred between systems. This data transfer is controlled by the workbench 'Portal Application Interface' product. The portal can be configured to interface with multiple legacy systems in a single implementation.

Legacy Server Security

All data transfers are initiated by the legacy system. The legacy system is never contacted by the web-host server. All control resides on the legacy server; therefore the legacy system does not need to be opened to insure security.

The data transfer function is controlled by a single script and database procedures. The script is installed on the legacy server and is scheduled using the operating system cron. The database procedures are installed into the legacy database (for example the Oracle eBusiness Suite database). These procedures export data and import customer orders and addresses created in the portal application.

Host Server Security

When the legacy system contacts the host server, it has limited access. It does not have access to the database. It is only allowed to do an FTP-Put and an FTP-Get to a single location on the server. Using this limited access method provides ability to secure the host server from all access except from the specified legacy host and is limited to this single ftp function to a pre-assigned location. No database access or execution of any script is allowed on the host server.

Data Transfer Process

Data transfers are scheduled. Data transfers can be scheduled to execute as often as needed by the implementation. The following is a summary of the data transfer process.

- Export data from the legacy database
- Establish communications with the Hosted server (workbench server at revion)
- Execute a single FTP-Put and a single FTP-Get to transfer data between the systems
- Terminate communication with the host
- Import data into the Legacy database

Portal Application Security

Security has been build into all aspects of the portal application. Because the portal is an Internet-based application, there are security features built into the application that are not normally found in a typical business database application. The following is a list of special application security features built into the portal application.

- Application authorization (and user id management processes)
- Role based security management - roles define application functions to authorize
- Page authorization
- Application has been programmed to specifically protect unauthorized access to data using the URL browser-address-line
- Application code to insure no unauthorized access to data such as Private Catalogs, Items, Prices, Attachments
- Application User-id management functions, processes, and security rules definition

Credit Card Information

By default the Portal and Interface application do not store or retain credit-card information. By default, only the following information is stored or transmitted to the legacy via the interface

- Last 4 digits of credit-card number
- Credit card expiration date
- Transaction authorization number
- Credit Card Billing Address

Denied Party Screening (option)

The portal application supports Denied Party Screening. Denied Party Screening is applicable to the selling of products and distribution of technical information via the portal. Denied Party Screening is accomplished using a real-time web-service. When turned on, the application will screen and flag the transaction as ‘Pass’ or ‘Fail’. If Pass, it is not a denied party and the transaction occurs as normal. If Fail, the transaction is flagged (along with the detailed reason) for manual intervention. The entire process is invisible to the customer. When a customer request is denied, the portal screens simply thank the user for the order/request and is informed that the order is in process. Flagged orders/requests are then reported to an administrator that can review the transaction and make the decision to allow or deny the transaction (and inform the customer accordingly).

SSL Certificate and Verification

Workbench Software requires all customers to use an active SSL certificate. Live validation is also required. Workbench Server configuration requires 128-bit encryption. All sessions (all screens) are encrypted (not just the credit-card screen that you may see on some sites).

SFTP User Access

Each workbench customer is assigned web-disk-space to use for temporary data storage and to store images to display on the web-site. An ftp site (user) is created for each customer. The site is secured and only the assigned customer and workbench support staff have access to the ftp site. Normal ftp is not allowed on the site. Only SFTP is allowed (Secured File Transfer Protocol).

Summary

Security is one of the most important aspects of implementing a B2B portal application. We have made every effort to insure our customer's data and processes are protected from unwanted access or disruption. We value your input on this topic. If you have suggestions or comments, please feel free to contact Workbench support to discuss security topics.