Oracle® Hospitality Cruise AffairWhere

Security Guide
Release 2.2.5
E85968-01

April 2017

ORACLE

Contents

Figures

Tables

Preface

This document provides security reference and guidance for AffairWhere.

Audience

This document is intended for:

- System administrators installing AffairWhere
- End users of AffairWhere

Customer Support

To contact Oracle Customer Support, access My Oracle Support at the following URL:

https://support.oracle.com

When contacting Customer Support, please provide the following:

- Product version and program/module name
- Functional and technical description of the problem (include business impact)
- Detailed step-by-step instructions to recreate
- Exact error message received and any associated log files
- Screenshots of each step you take

Documentation

Oracle Hospitality product documentation is available on the Oracle Help Center at http://docs.oracle.com/en/industries/hospitality/

Revision History

Date	Description of Change
April 2017	• Initial publication

1 AffairWhere Security Overview

This chapter provides an overview of Oracle Hospitality Cruise AffairWhere security and explains the general principles of application security.

Basic Security Considerations

The following principles are fundamental to using any application securely:

- **Keep software up to date.** This includes the latest product release and any patches that apply to it.
- **Limit privileges as much as possible.** Users should be given only the access necessary to perform their work. User privileges should be reviewed periodically to determine relevance to current work requirements.
- **Monitor system activity.** Establish who should access which system components, and how often, and monitor those components.
- **Install software securely.** For example, use firewalls, secure protocols using TLS (SSL), and secure passwords.
- **Learn about and use the AffairWhere security features.**
- **Use secure development practices.** For example, take advantage of existing database security functionality instead of creating your own application security. See Security Considerations for Developers for more information.

Keep up to date on security information. Oracle regularly issues security-related patch updates and security alerts. You must install all security patches as soon as possible. See the Critical Patch Updates and Security Alerts website:
http://www.oracle.com/technetwork/topics/security/alerts-086861.html

Overview of AffairWhere Security

AffairWhere Architecture Overview

AffairWhere uses N-Tier Architecture and is a collection of applications and interfaces. They can be deployed anywhere. It is scalable and does not have to be deployed on a single machine.

Technology

AffairWhere product developed using industry standards. Every communication can be configured to use Secure Sockets Layer (SSL) if required. It also uses powerful encryption/hashing algorithms (Windows Data Protection Application Programming Interface (DPAPI), Password-Based Key Derivation Function 2 (PBKDF2)) to encrypt and store sensitive information like application user passwords, application configuration information, and Database user passwords.

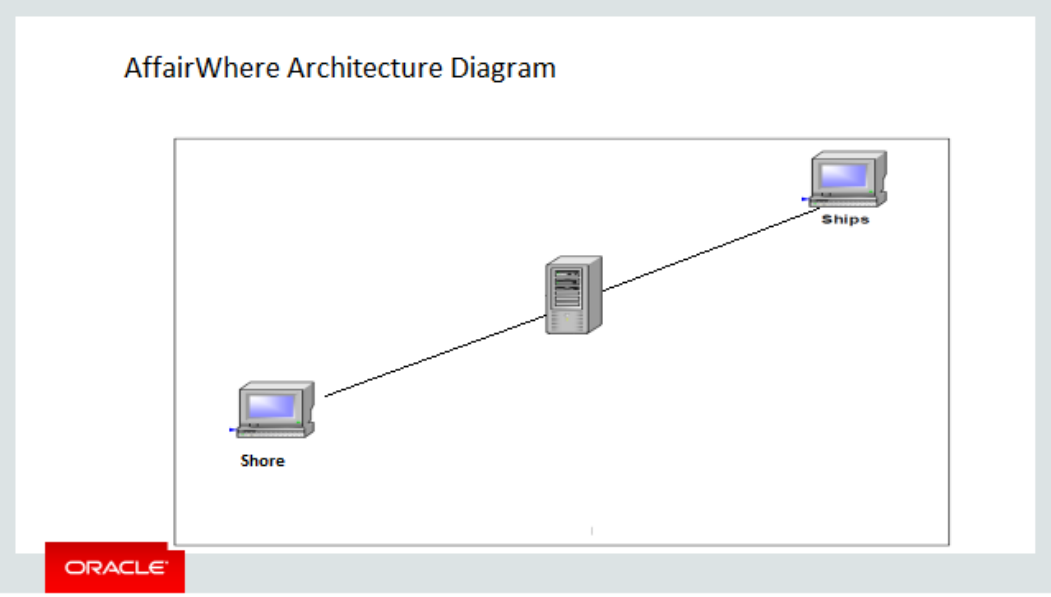

Figure 1 - AffairWhere Architecture Diagram

User Authentication

Overview

Authentication is the process of ensuring that people are who they say they are.

Client Authentication

All users' credentials of AffairWhere are stored in the database. Anyone who wishes to access the clients must provide a valid username and password. To ensure strict access control of the AffairWhere, always assign unique usernames and complex passwords to each user. Passwords must follow PCI-DSS guidelines, must be at least eight characters long, and include letters and numbers.

Database Users

AffairWhere works with both Oracle and Microsoft SQL Server databases.

Understanding the AffairWhere Environment

When planning your AffairWhere implementation, consider the following:

- **Which resources need to be protected?**
    - You need to protect customer data.
    - You need to protect internal data, such as proprietary source code.
    - You need to protect system components from being disabled by external attacks or intentional system overloads.
- **Who are you protecting data from?** For example, you need to protect your subscribers' data from other subscribers, but someone in your organization might need to access that data to manage it. You can analyze your workflows to determine who needs access to the data; for example, it is possible that a system administrator can manage your system components without needing to access the system data.

- **What will happen if protections on strategic resources fail?** In some cases, a fault in your security scheme is nothing more than an inconvenience. In other cases, a fault might cause great damage to you or your customers. Understanding the security ramifications of each resource will help you protect it properly.

Recommended Deployment Configurations

The AffairWhere product can be deployed on a single server or in a cluster of servers. The simplest deployment architecture is the one shown Figure 2.

This single-computer deployment may be cost effective for small organizations; however, it cannot provide high availability because all components are stored on the same computer. In a single server environment such as the typical installation, the server should be protected behind a firewall.

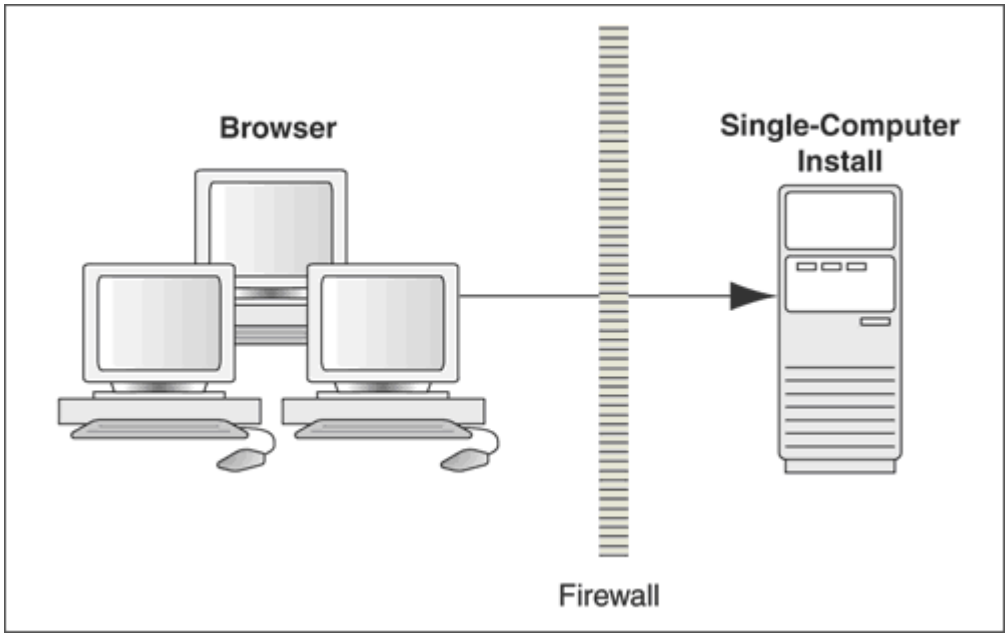

Figure 2 - Single Computer Deployment Architecture

The general architectural recommendation is to use the well-known and generally accepted Internet-Firewall-DMZ-Firewall-Intranet architecture shown in Figure 3 - Traditional DMZ View.

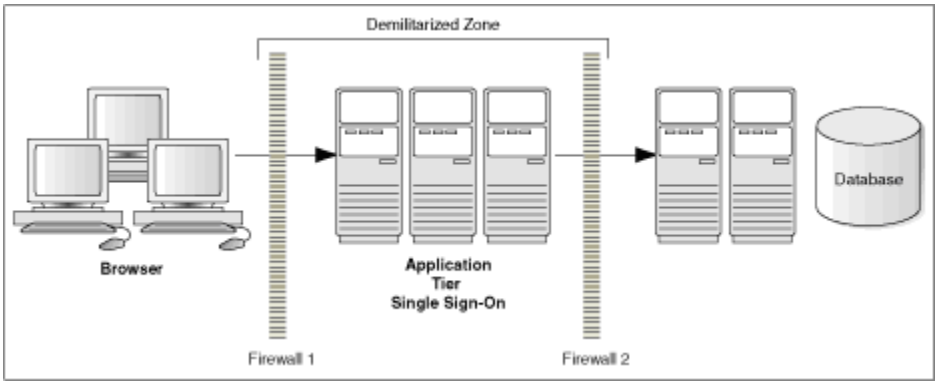

Figure 3 - Traditional DMZ View

The term demilitarized zone (DMZ) refers to a server that is isolated by firewalls from both the Internet and the intranet, thus forming a buffer between the two. Firewalls separating DMZ zones provide two essential functions:

- Blocking any traffic types that are known to be illegal
- Providing intrusion containment, should successful intrusions take over processes or processors

See AffairWhere Port Numbers.

Component Security

Operating System Security

Prior to installation of Cruise Fleet Management, it is essential that the operating system be updated with the latest security updates.

Refer to the following Microsoft TechNet articles for more information about operating system security:

• Windows Server 2012 Security

• Windows Server 2008 R2 Security

Oracle Database Security

Oracle Database

Refer to the Oracle Database Security Guide for more information about Oracle Database security.

Microsoft SQL Server

Refer to the Microsoft SQL Server 2012 Security Best Practices Whitepaper for more information about Microsoft SQL Server security.

2 Performing a Secure AffairWhere Installation

This chapter presents planning information for your AffairWhere installation. For information about installing AffairWhere, see the *AffairWhere Installation Guide*.

Pre-Installation Configuration

Prior to installation of AffairWhere, perform the following tasks:

- Apply critical security patches to the operating system
- Apply critical security patches to the database server application
- Create the required Oracle Database objects per the instructions in the *AffairWhere Installation Guide* located at http://docs.oracle.com
- Acquire SSL compliant security certificate from Certification Authority

AffairWhere Installation

You can perform a custom installation or a typical installation. Perform a custom installation to avoid installing options and products you do not need. If you perform a typical installation, remove or disable features that you do not need after the installation.

The installation requires the user running the installation to have administrator privileges. No other users have the required access to successfully complete the installation.

When creating a database, enter a complex password that adheres to the database hardening guides for all users.

The following Desktop applications are required for proper operation of the system:

- AffairWhere

The following interfaces are required for proper operation of the system:

- AffairWhere Import
- AffairWhere Export
- Database Installer

Post-Installation Configuration

This section explains additional security configuration steps to complete after AffairWhere is installed.

Operating System

Turn On Data Execution Prevention (DEP)

Turn on DEP if required. Refer to the Microsoft product documentation library at https://technet.microsoft.com/en-us/ for instructions.

Turning Off Auto Play

Turn off Auto Play if required. Refer to the Microsoft product documentation library at https://technet.microsoft.com/en-us/ for instructions.

Turning Off Remote Assistance

Turn off Remote Assistance if required. Refer to the Microsoft product documentation library at https://technet.microsoft.com/en-us/ for instructions.

Application

Software Patches

Apply the latest AffairWhere patches available on My Oracle Support if available any. Follow the deployment instructions included with the patch.

Passwords Overview

The configuration of AffairWhere product passwords is performed in the AffairWhere Administration module. Administrators are recommended to configure a strong password policy after initial installation of the application and review the policy periodically.

Maintaining Strong Passwords

Ensure that passwords adhere to the following strength requirements:

1. The password must be at least eight characters long.
2. The password must contain letters, numbers.
3. Must not choose a password equal to the last three passwords used.

Change Default Passwords

AffairWhere is installed with a default administrative user and password. Please change the default administrative user password in the AffairWhere, following the above guidelines, after logging in for the first time.

Configure User Accounts and Privileges

When setting up users of the AffairWhere application, ensure that they are assigned the minimum privilege level required to perform their job function. User privileges are described in Access Control.

3 Implementing AffairWhere Security

This chapter describes how to implement AffairWhere security features.

Authorization Privileges

Overview

Setting Authorization privileges establishes strict access control, explicitly enabling or restricting the ability to do something with a computer resource.

User authorization privileges are configured in the AffairWhere within the AffairWhere Administration module. AffairWhere uses simple authorization model.

Adding Users

1. Select **User ID Maintenance** under **Tools**.
2. On the left side pane, right-click **Add User** to add a user. Enter the user login, password, first name and last name, and select a user location from the **Ship/Shore** drop-down menu.

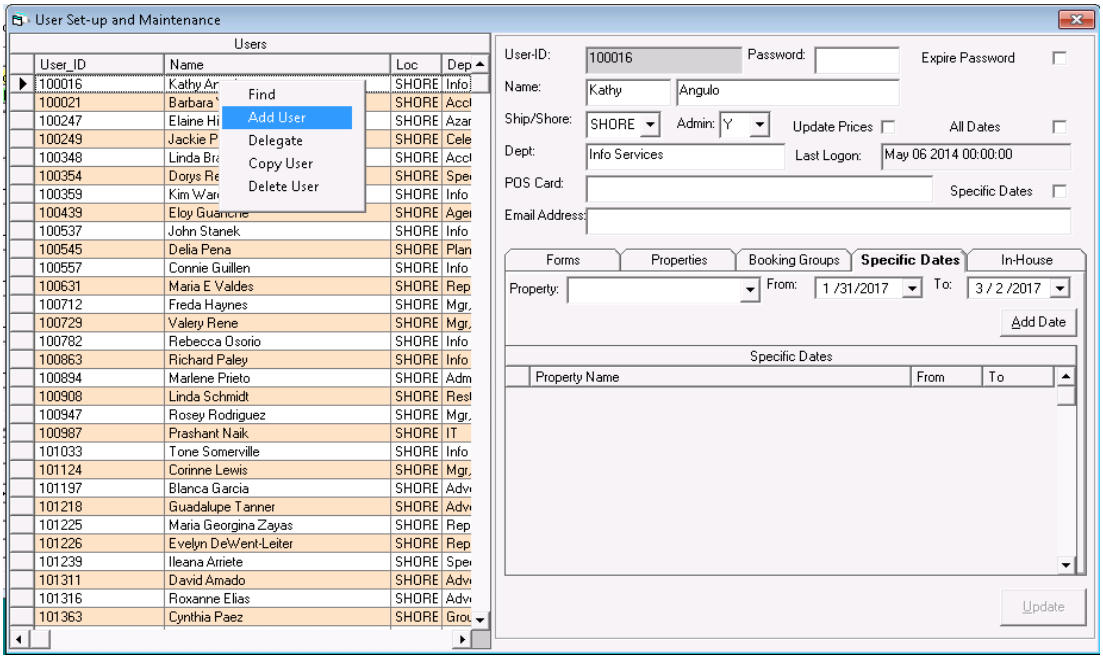

Figure 4 - Adding User

3. Click **Update**.

4 AffairWhere Port Numbers

Port Numbers

This is a list of port numbers that are used in AffairWhere. Open a port only if required for communication.

Table 1 - Service/Port Number

Service	Port Number
SFTP	22