Oracle® Hospitality Suites Management

Security Guide
Release 3.7
E87198-03

May 2017

ORACLE

Contents

Tables

Figures

Preface

This document provides security reference and guidance for Suites Management.

Audience

This document is intended for:

- Implementation specialists.
- System administrators installing Suites Management.
- End users of Suites Management.

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 re-create
- Exact error message received and any associated log files
- Screen shots of each step you take

Documentation

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

- Open Web Application Security Project (OWASP)
  http://www.owasp.org
- Center for Internet Security (CIS) Benchmarks (used for OS Hardening)
  https://Benchmarks.cisecurity.org/downloads/multiform/
- Refer to the *Suites Management Installation Guide* for information about installing the Suites application.
- Refer to the *Simphony First Edition Security Guide* for more information about hardening your system's security.

Revision History

Date	Description of Change
May 2017	• Initial publication

1 Suites Management Security

This chapter provides an overview of Oracle Hospitality Suites Management 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 all patches that apply to it.
- **Limit privileges as much as possible.** Users should be given only the access necessary to perform their work. Review user privileges periodically to determine relevance to current work requirements.
- **Monitor system activity.** Establish the appropriate system component users and frequency of access, and monitor those components.
- **Install software securely.** See Performing a Secure Suites Management Installation for more information about secure software installation.
- **Learn about and use the Suites Management security features.** See Suites Management Security for more information.
- **Use secure development practices.** For example, take advantage of existing database security functionality instead of creating your own application security.
- **Stay up-to-date on security information**. Oracle Hospitality regularly issues security-related patch updates and security alerts. You must install all security patches as soon as possible.
- **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 for more security update information.

Suites Management Architecture Overview

Suites Management is an add-on product for the Simphony product. The Suites Management application provides a web-based back office application for managing inventory, events, event ordering and pricing as well a limited financial reporting. Suites also includes a SuitesService which is an ASP.NET web service that works together with other Microsoft Windows based components to integrate with the Simphony point-of-sales (POS) workstations.

Technology

The Suites Management web application/portal connects to two separate Microsoft SQL Server databases for application security and for data storage. The Suites Management application communicates with Simphony Transaction Service for data exchange between the SuitesService and it's on premise components in order to facilitate interaction between the POS workstations and the location specific related data. Suites Management's application components use industry standard SOAP services running a web service for connectivity.

Suites Architecture and Data Flow

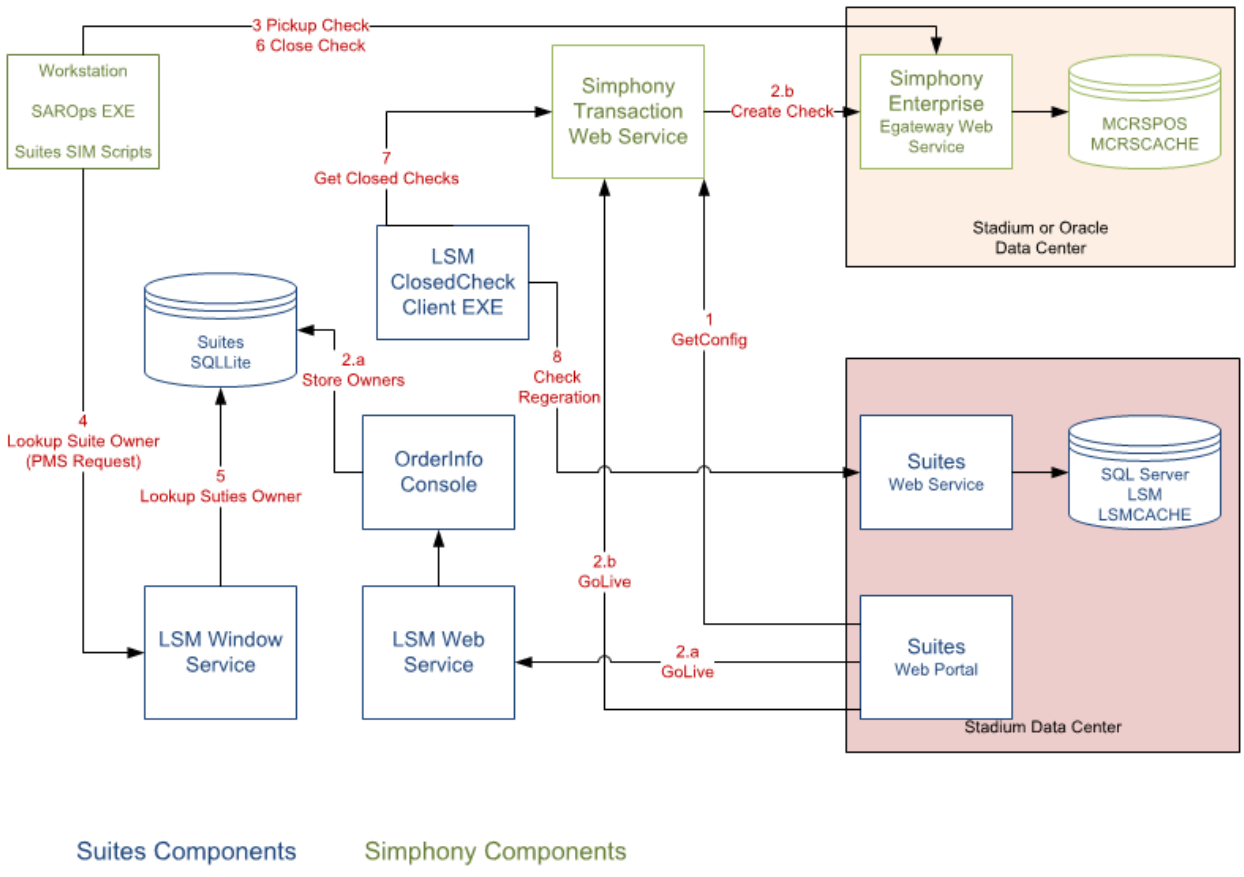

Figure 1-1 - SUITES Architecture \ Data Flow Diagram

Suites Web Services

The Suites Management application is an enterprise web application that can manage information related to events and activities that take place in multiple venues (stadiums, arenas, parks) in different geographical locations.

The first Suites Service (ConfigLSMService.asmx) is a web service component that gets installed in the venue (location level) for the purpose of linking the venue specific data to the POS workstations.

The second Suites Service (LSMWebService.asmx) is a very simple web service with a single function of capturing the sales data into the Suites Management application's database at the Enterprise level.

- During the GoLive process the first Suites Service (ConfigLSMService.asmx) receives the venue specific data in .xml format and engages a Microsoft Windows application (Order Info Console) for the purpose of storing the data in the SQLite on premise database.
- The data from SQLite database gets extracted (pulled) by the POS workstation through usage of a Microsoft Windows service (LSMWinService).
- During the CheckRegen process the 2nd Suites Service (LSMWebService.asmx) receives the sales data from a Microsoft Windows application (Closed Check Client) and inserts the received data into Suites Management application's database (LSM).

User Authentication

Authentication is the process of ensuring that people on both ends of the connection are who they say they are. This applies to both the entity trying to access a service, and to the entity providing the service.

Suites Management application Authentication

All users' logon credentials for Suites Management are stored in the central database. Anyone who has access to the Suites (back office) application must provide a login of a valid username/password. No two users can have the same username. To ensure strict access control of the Suites Management application, always assign unique username and complex passwords to each employee/user.

User Management

During the Suites Management application installation process the installer that performs the installation needs to provide a user name and password for an Administrative account that gets created inside the LSM database. The created account will be used for logging into the Suites Management application and for performing Suites administrative duties (e.g., creation of employees/users, and assigning roles, etc.).

Oracle Hospitality mandates that users have a unique, strong password. The password must be at least 8 characters long and include letters, numbers and special characters.

Database Access Management

The Suites Management installation program also prompts for the creation of a Microsoft SQL Server Login and a Database User for each of the two Suites databases: LSM and LSMCACHE.

Security Note

Database access credentials are stored on the Suites Management application server, protected by Microsoft Windows Server file permissions.

Suites Management Environment Considerations

When planning your Suites Management implementation, consider the following:

1. Which resources need to be protected?
    - Protect customer data, such as credit-card numbers
    - Protect internal data, such as employee names
    - Protect system components from being disabled by external attacks or intentional system overloads
2. Who are you protecting data from?

    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.
3. What happens 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

This section describes recommended deployment configurations for Suites Management.

Suites Management can be deployed on a single server or in a cluster of servers. The simplest deployment architecture is the one shown below.

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.

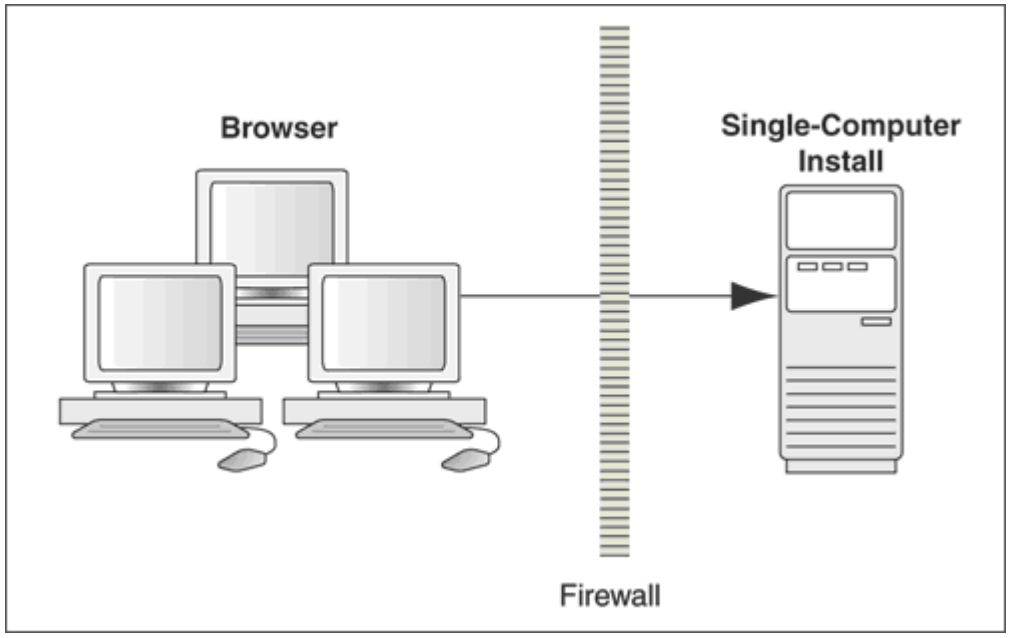

Figure 1-2 - Single Server Scenario

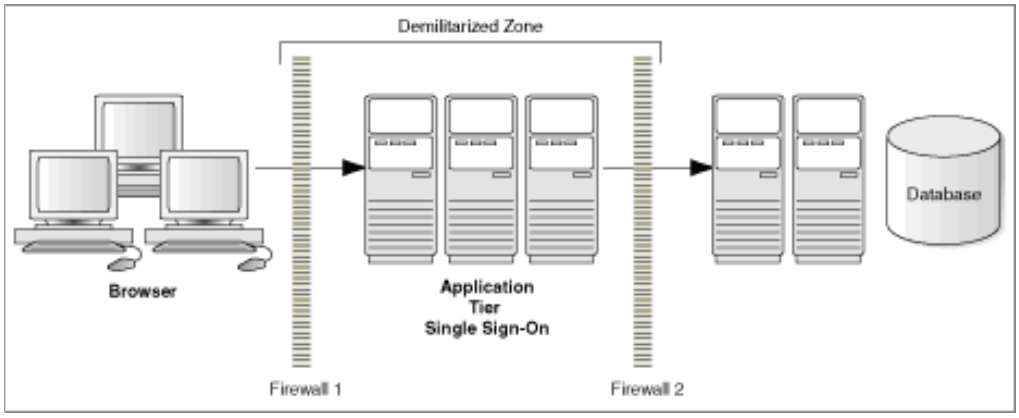

Figure 1-3 - Server Cluster Scenario

Suites Management Security

Operating System Security

Prior to installation of Suites Management application, it is essential that the operating system be updated with the latest Microsoft Windows security updates.

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

- Microsoft Windows Server 2008 R2 Security
- Microsoft Windows Server 2012 Security

Database Platform Security

Oracle Database

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

Microsoft SQL Server

Refer to the Microsoft MSDN website for more information about Microsoft SQL Server security.

Network Security

The Suites Management web site requires secure communications when transmitting data between the browser and a web service running on the application server. Oracle Hospitality recommends the use of Transport Layer Security (TLS) 1.1 (or higher) to provide secure network communications.

To ease the configuration, the installation program provides the necessary functionality to configure the required certificates for the Suites web site. It is recommended to use a certificate obtained from a trusted certificate authority (CA).

2 Performing a Secure Suites Management Installation

This chapter presents Suites Management installation planning information. For information about installing Suites Management, see the *Suites Management Installation Guide*.

Pre-Installation Configuration

Perform the following tasks before installing Suites:

- Apply critical security patches to the operating system
- Apply critical security patches to the database server application
- Ensure that connections to the database are restricted to a few trusted nodes using firewall rules or the Oracle listener invited nodes feature
- Review the *Oracle Hospitality MICROS Hardware Wireless Networking Best Practices Guide*
- Install a web service on the application server and configure it for Transport Layer Security (TLS) 1.1 or higher network communications.

Suites Management Installation Changes

The Suites Management installation application is now comprised of two components:

1. Suites Management Installer – Installs the Suites web application.
2. Suites Service Installer – Installs the Suites Web and Microsoft Windows services.

Remove or disable features that you do not require after the installation.

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

The Suites Management installation application disables the following operating system features:

- AutoPlay
- Remote Assistance
- Administrative Shares

A new Microsoft Windows group named SUITES_USERS is created during the Suites Management installation.

All Microsoft Windows services required to run Suites Management have been updated to run under this user group.

Access to the Suites Management installation folder is restricted to members of the SUITES_USERS group. Any user required to access the Suites folders needs to be added to the SUITES_USERS group by the system administrator.

When creating a new database, enter a complex password that adheres to the Oracle Database hardening guidelines for all users.

The following Suites Management web services are required for proper connectivity with Simphony:

- ConfigLSMService.asmx
- LSMWebService.asmx

The Suites Microsoft Windows LSMWinService is required for proper connectivity with point-of-sales (POS) workstations.

Post-Installation Configuration

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

Operating System

Turn On Data Execution Prevention (DEP)

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

Configuring the Microsoft Windows Idle Time Logout Setting

For additional security, configure Microsoft Windows to ensure that the Maximum Idle Time in Minutes setting is not greater than 15 minutes (default setting).

Refer to https://technet.microsoft.com/en-us/library/jj852253.aspx for more information about configuring the Maximum Idle Time in Minutes setting.

Application

Software Patches

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

Administrative Account and Database Connection Management in Suites

The **Database Configuration** utility stores connection information for establishing a connection to the database. These credentials are used by the Suites Management to connect to the application databases. The credentials are stored and protected using operating system encryption.

Database Connection

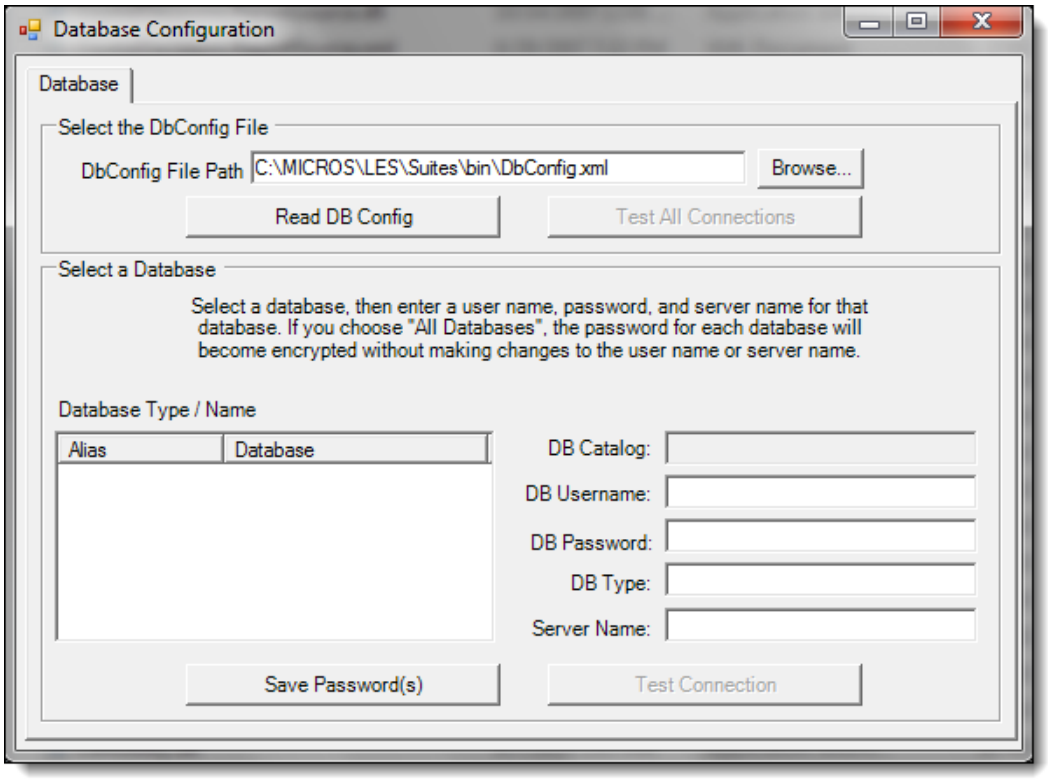

Figure 2-1 - Database Configuration - Database Connection

To establish a database connection, perform the following steps:

1. Navigate to the <*Drive letter*>:\MICROS\LES\Suites\bin folder, and open the **DatabaseConfig.exe** utility. The **Database** tab shows the folder in which Suites was installed.
2. Click the **Read DB Config** button to read the contents of the DBConfig.xml file.
3. If the DBConfig.xml file is not present, a message prompts you to create the default file.
4. If prompted, click **OK** to create the new file with the default settings. After the DB Config file has been read, all of the available connections in the Database Type / Name section appear. The first entry in the Database Type / Name section is **All Databases**.

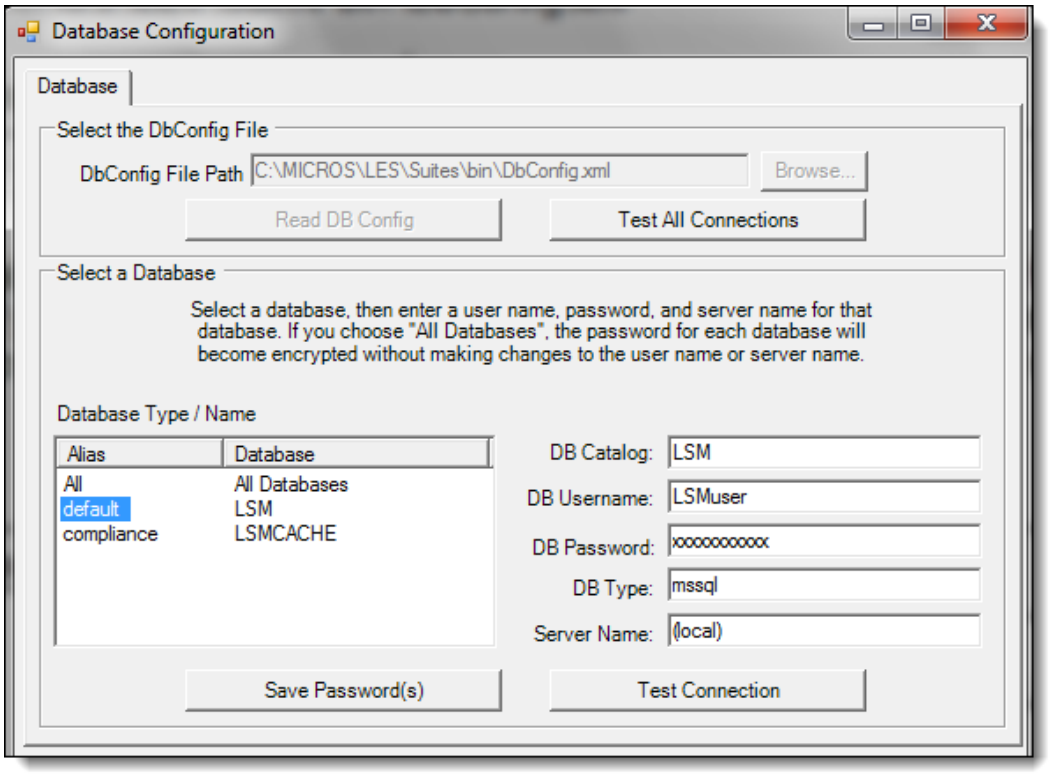

Figure 2-2 - Database Configuration - Testing DB Connections

1. Click **Test all Connection**s. The utility tests all available database connections.
2. When a specific connection is selected in the Database Type / Name section, the fields on the right populate with the connection's details.
    - When you click **Test Connection**, the connection to the database is initiated using the data contained in the populated text fields
    - If the connection fails, a message appears indicating the connection failure and provides an option to view the detailed exception. Re-enter the correct connection details (in the text fields on the right) for the tested connection, and retry clicking **Test Connection**.

Administrative Account

The Database Configuration utility has an Administrative Account tab page. This tab is only visible one time; after the connection to the LSM database is successfully tested and if the conditions for creation of a Suites Management application Administrative user account are met. The newly created Administrative account is used for logging into the Suites Management application and for performing various Suites administrative duties.

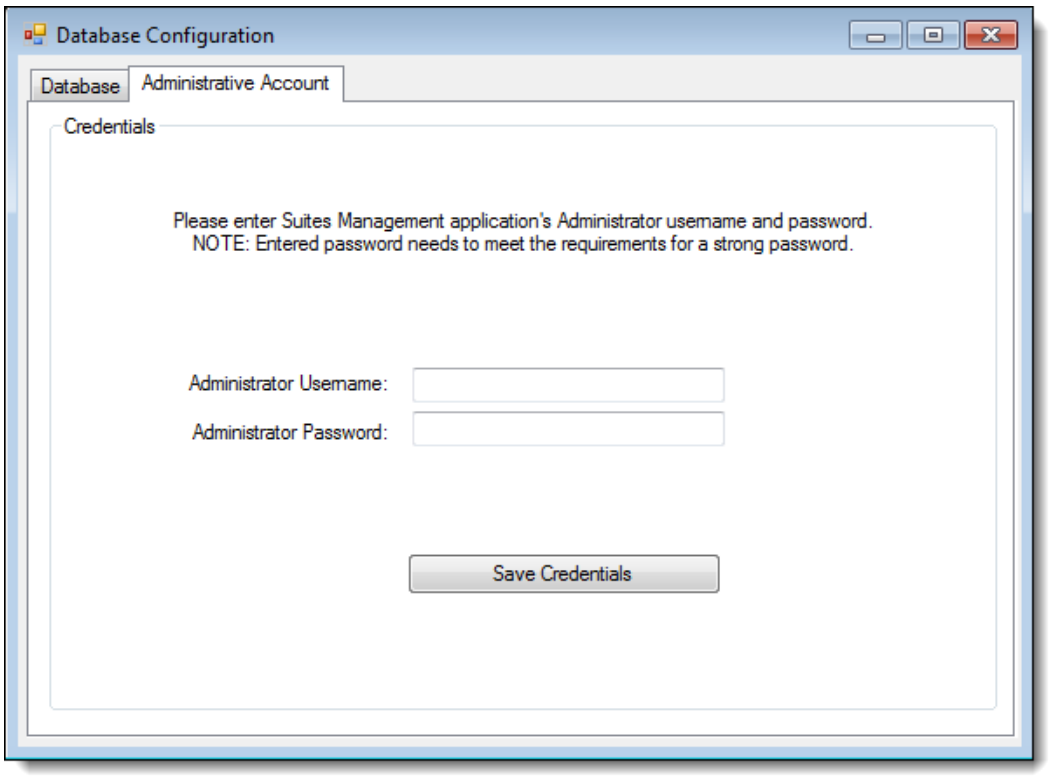

Figure 2-3 - Database Configuration - Administrative Account

Key Manager – Securing Sensitive Data

The purpose of the Suites Key Manger module is to allow the user to set an encryption pass phrase for Suites. The Key Manager is used to rotate the encryption key used to secure sensitive data stored in the Suites database.

Performing a Key Rotation

To access the Key Manger module the user must be associated with the Administrative role. Once granted this role, the user is required to enter a valid username and password to gain access to the utility.

Changing the Pass Phrase

The new pass phrase must:

- Contain at least 1 alphabetic character
- Contains at least 1 numeric character
- At least 1 special character from:!”$%&’()*+,-./:;⇔?@[\]^_`|~{}
- Must be a minimum of 16 characters long (up to 24)
- Must not contain any dictionary word
- The passphrase and confirmed pass phrases must match
- The database must be accessible

Caution: If the pass phrase is lost, the encrypted data in the database is unrecoverable. There are no backdoors!

Change the pass phrase following the directions below.

1. Login to the Key Manager Utility.
2. Enter the current (or new) Pass Phrase.
3. Re-enter the Pass Phrase to confirm it.

Figure 2-4 - LSM Key Manager

4. Click the **Update** button

5. A confirmation prompt appears. Click **Yes** to start the key rotation process. Do not perform a key rotation process if a database backup is in process. Backing up the database during the key rotation process can potentially cause the data in the backed-up database to become out-of-sync with Suites.

   Click **No** if a database backup is currently in progress and begin the key rotation process at a later time after the backup is finished.

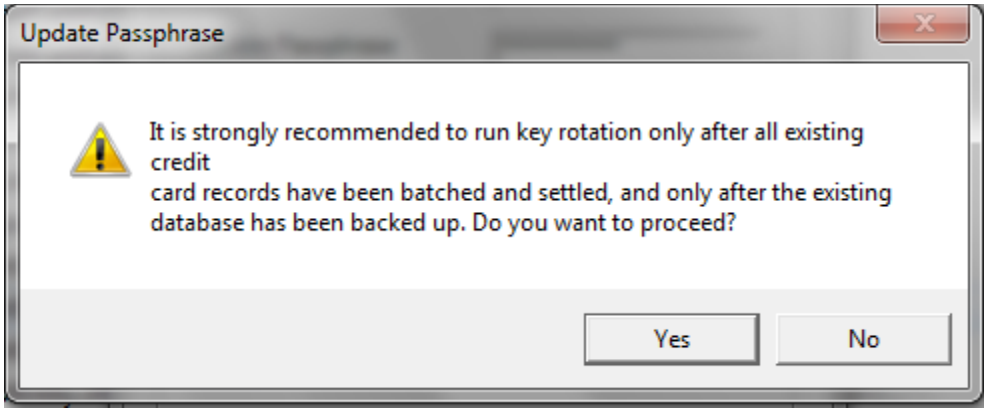

Figure 2-5 - Update Passphrase Prompt

6. A status box appears indicating the progress of the encryption. When the progress has reached 100%, click OK.

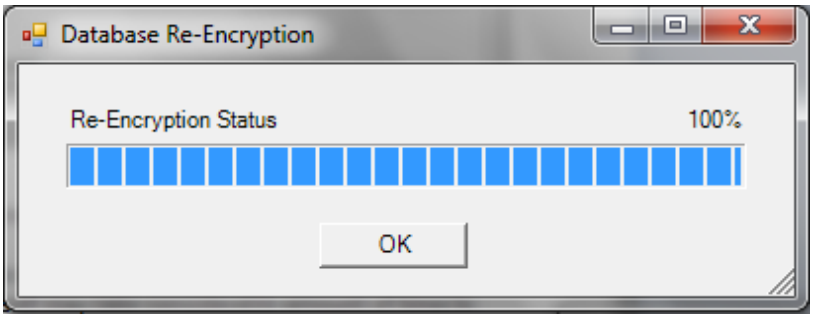

Figure 2-6 - Database Re-Encryption Status

7. Once the key rotation is finished, a message appears indicating that the operation was successfully completed. Click Yes to the close the window.

3 Implementing Suites Management Security

Passwords Policy Overview

Suites Management enforces a strong password policy by default. The following password requirements are enforced:

- The password must be at least 8 characters long and maximum 20 characters
- The password must contain letter(s), number(s), and punctuation character(s): ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~
- Users cannot choose a password equal to the last 4 previously used passwords
- The Maximum Allowed Failed Logins before a user account is locked out is 5
- Passwords expire every 90 days.

Authorization Privileges

Setting Authorization privileges establishes strict access control, explicitly enabling or restricting a user's system access and their performance of specific functions.

Suites User Authorization Management

All users' logon credentials for the Suites Management application are stored in the LSM database. Anyone who has access to the Suites Management software must provide a valid and unique login user name and password. To ensure strict access control of the Suites Management application, always assign unique user names and complex passwords to each account.

It is mandated that sites maintain proper configuration and adhere to privilege level restrictions based on a need-to-know basis. For security purposes, each user's activities are traced via an audit trail log file stored in the LSM database. The Suites Management database is installed with no pre-defined username and password.

Oracle Hospitality recommends not using any administrative accounts for any Suites Management application logins. The Suites Management installation automatically creates a SQL Server Login and a Database User with username and password specified at installation time. Before any code can execute SQL statements to the Microsoft SQL Server database, the database requires a username and password in the SQL string.

Suites Management Access Controls

Setting Authorizations/Privileges establishes strict access control, explicitly enabling or restricting a user's system access and their performance of specific functions.

- Access control for Suites Management application system services, web pages and reports is defined within the application, Employees, Employee Roles, Map Services button, Role-System Services mapping web page.
- User/Employee access control is defined within the application, Employees, Employee Setup, Employee Maintenance, Map Roles button, User Roles mapping dialog.

General Configuration

The System Services web page has a list of 43 pre-defined System Services covering all the available functions in the entire Suites Management system.

Understanding System Service Profiles

You can group employees according to the duties they perform, such as cashiers, managers, office clerks, and assign the same privilege and option settings to a role using corresponding System Service Profiles. For example, the Office Admin role is authorized to access, create and export the AR Data and other Historical reports. Without roles, each office clerk would be assigned individual authorizations, which can be a repetitive and time-consuming task. Roles are assigned to an employee within the Suites Management application, by going to Employees, Employee Setup, Employee Maintenance, Map Roles button, User Roles mapping dialog.

Working with Role Profiles

Roles limit access and determine how each securable item, including system services, web pages and reports, in Suites Management are used. A role grants the privileges needed to access, create, delete, or edit each securable item.

Adding or Removing Securable Item Authorizations

Suites Management application has a predefined set of 43 System Services that are incorporating the accessibility to the applications' menu options, functions, web pages and reporting tools. Currently the Suites Management application doesn't allow modification to these predefined System Services, so there is no UI that will allow adding or removing securable items to or from System Services.

Adding Roles

To add a new Role:

1. Access the Employees \ Employee Roles web page.
2. Click **New** and the Role Maintenance web page appears.
3. Enter the new Role information and click **Save**.

Deleting Roles

To delete an entire Role:

1. Access the Employees \ Employee Roles web page.
2. Select the role to be deleted from the Role List and click **Delete**.
3. Click **OK** when prompted.

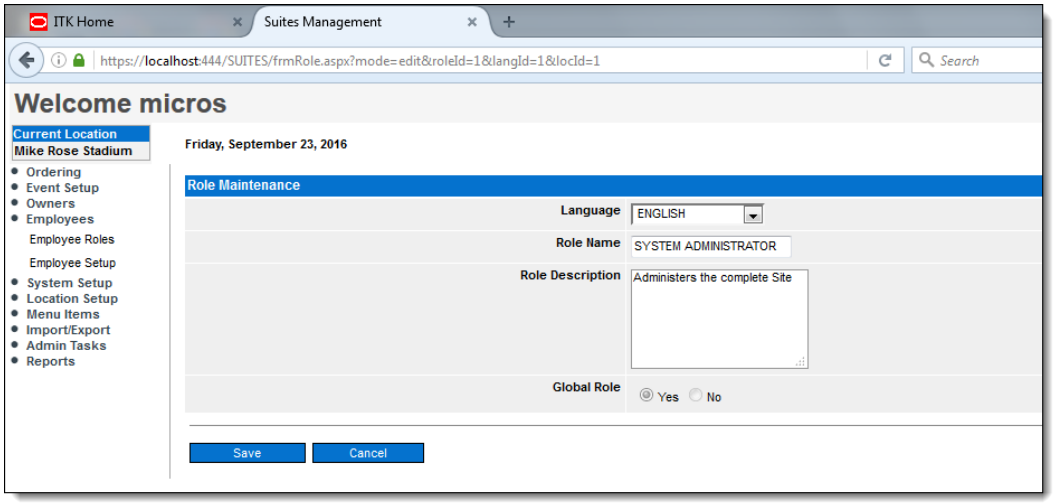

Figure 3-1 - Role Maintenance

Adding All Roles

To add all Roles at once:

1. Navigate to the Employee Maintenance web page and click **Map Roles**.
2. Check the checkbox next to Role Name (in the column header).
3. Select all Roles and click **Save**.

Removing a Role

To remove a Role:

1. Navigate to Employee Maintenance web page and click **Map Roles**.
2. Deselect the role to be removed from the employee /users' role mappings.
3. Click **Save**.

Understanding Suites User / Employee Profiles

Employee Profiles are used to grant different levels of access to securable items, including web pages and reports, through the assignment of Roles.

Creating New Users/Employees

Employee Maintenance web page is used to create a new employee.

To create a new employee (which is also a suites user):

1. Log onto the Suites Management application with a user that has an administrative role.
2. Navigate to the Employees \ Employee Setup web page
3. Click **New**.
4. Enter the Employee's **First** and **Last Name**.
5. Enter a unique **User ID** and a **Password**.
6. Select a **Location**.
7. Click **Save**.

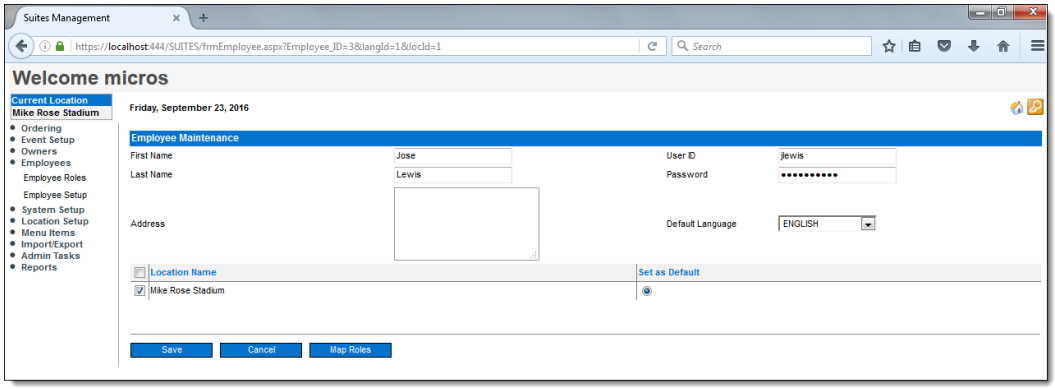

Figure 3-2 - Employee Maintenance

Deleting Users/Employees

The Employee Maintenance web page allows an employee record to be deleted.

To delete an employee (which is also a suites user):

1. Log into Suites management application with a user that has administrative role.
2. Navigate to Employees \ Employee Setup web page.
3. Select the **Employee**.
4. Click **Delete** button.

Locked User Accounts

If a user fails to login to the Suites application more than 5 times in a row the user account will become locked. The administrator can see locked accounts in the Employee List under the Blocked column. In the event that an Employees account becomes locked out, it will automatically be unlocked in 15 minutes. Alternatively, it can be unlocked immediately by the Administrator by going into the Employee List, selecting the employee, and clicking the **Unblock** button.

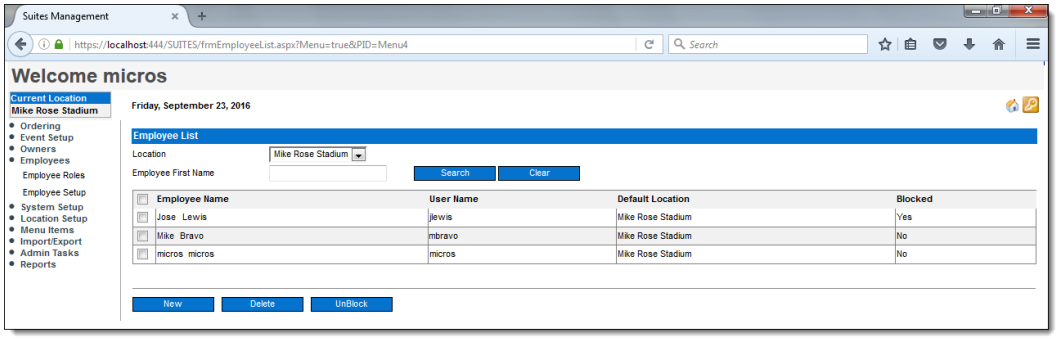

Figure 3-3 - Employee List Unblocking

Linking Employees to Roles

Employees are linked to roles within the Suites Management application. To map roles:

1. Navigate to Employees, and the Employee Setup web page.
2. Select an employee from the list by clicking on his/her name.
3. Once the Employee Maintenance web page appears, click **Map Roles**.

If there are unique employees among the staff who do not fit any of the general roles, create a role for them. For example, Sheila usually works as a Suite Staff, but occasionally fills in as a Suites Manager when necessary. She needs to be able to perform the duties of both roles (Suite Staff and Suites Manager). Create a role that combines the privileges required to perform as a staff and allows the authorizations required of a Suites Manager. Label this new class something like, Utility, or perhaps Sheila, and add this role only to her employee profile. The number of roles that can be created is limited only by the size of the system's memory.

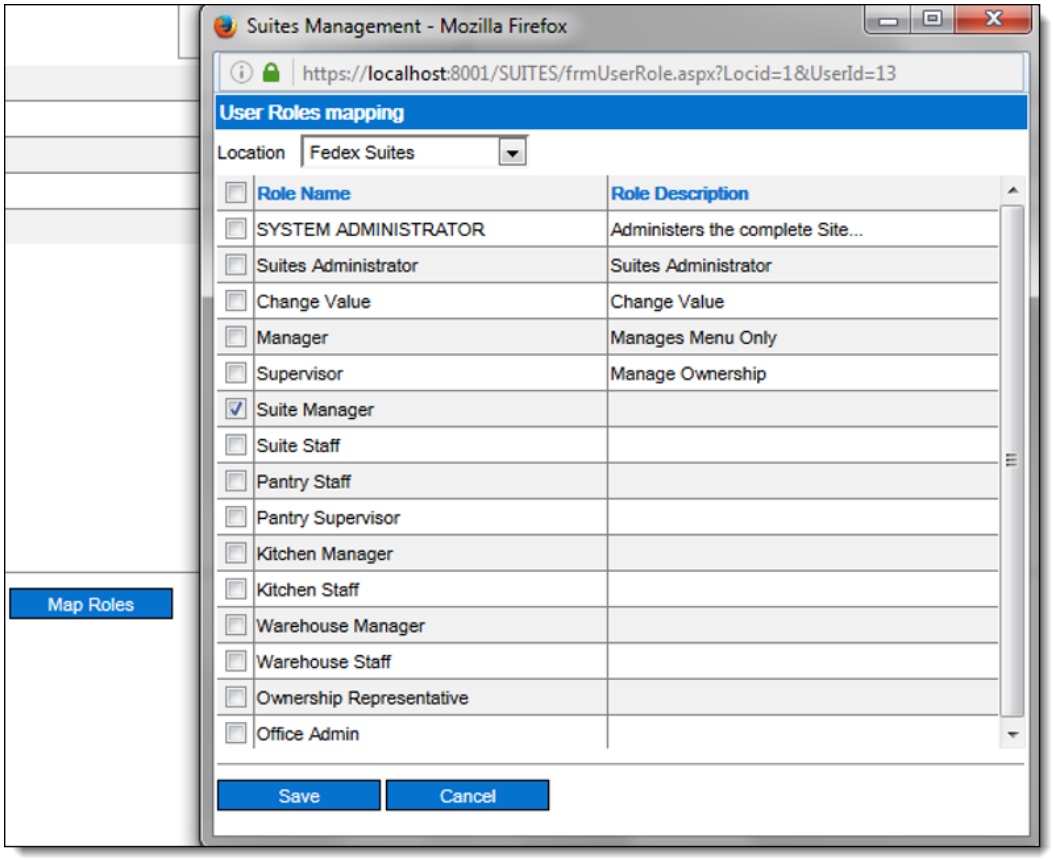

Figure 3-4 - User Roles Mapping

Tracking Suites Management application Configuration, Edits, Errors, and Access

Configuration and Edit Logging

The **LSMWeb.Log** file tracks configuration steps and edits performed within the Suites Management application.

Error Logging

Errors that have occurred in the Suites Management application are written to the **LSMWeb.Log** file. The file lists the date and time the error occurred, the error number, where the error occurred, and the error message.

Accessing the LSMWeb.Log file

To access and review the LSMWeb.Log file:

Navigate to <*Drive letter*>:\MICROS\LES\Suites\Logs\LSMWeb.Log and open the file using a text editor.

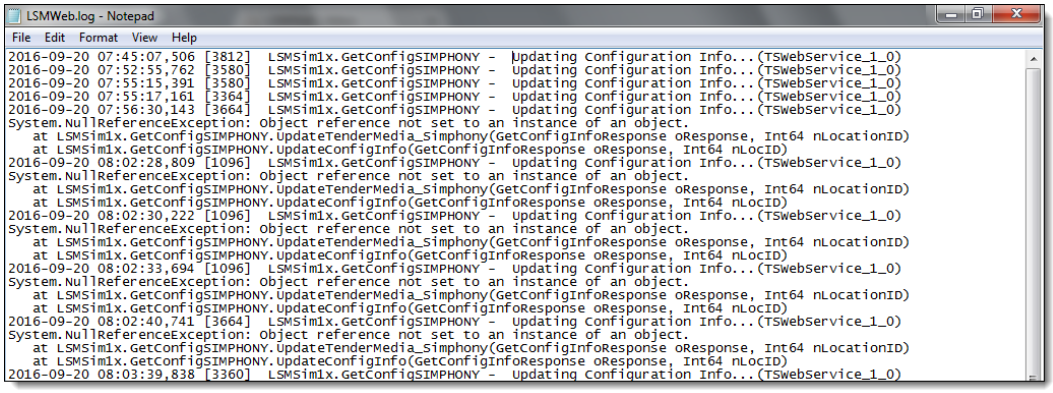

Figure 3-5 - LSMWeb.log File

Suites Management Access Logging – Audit Trail List

The logging of users accessing Suites tracks and records each login to the Suites Management application. The Audit Trail tracks:

- Login User ID
- Login User Name
- Login Date and Time
- Login Action
- Login Action Result
- Login Machine Name
- The log monitors successful and unsuccessful logins

Accessing the Suites Management Audit Trail List

To access and view the Audit Trail List:

1. Log in into the Suites Management application with a user that has administrative role.
2. On the menu expand the Admin Task and click the Audit Trail link.

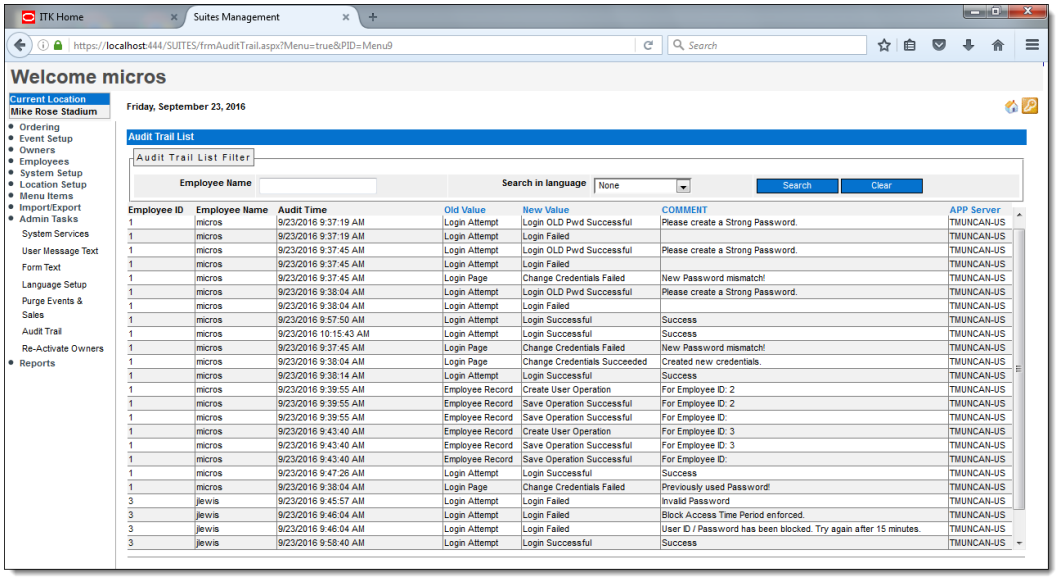

Figure 3-6 - Access Log - Audit Trail List

Appendix A Secure Deployment Checklist

The following security checklist includes guidelines that help secure your database:

- Install only what is required
- Lock and expire default user accounts
- Enforce password management
- Enable data dictionary protection
- Practice the principle of least privilege

Only grant the minimal amount of privileges to perform a job.

- Revoke unnecessary privileges from the PUBLIC user group.
- Restrict permissions on run-time facilities
    - Enforce access controls effectively and authenticate clients stringently
    - Restrict network access
    - Apply all security patches and workarounds
- Use a firewall
- Never poke a hole through a firewall
- Monitor who accesses your systems
- Check network IP addresses
- Encrypt network traffic
- Harden the operating system security

Appendix B Suites Port Numbers

Port Numbers

The following tables list port numbers that are used in Suites. Open only the minimum required ports based upon the installation type and deployment configuration.

Table 1 - Enterprise Ports

Service	Port Number	Configurable?
Default Database (Microsoft SQL Server)	1433	Yes
Suites Web application	8001	Yes

Table 2 - Property Ports

Service	Port Number	Configurable?
LSM Win Service	5009	Yes
Suites Web Service	8000	Yes