Oracle® Hospitality Simphony Venue Management
Security Guide

Release 3.11.0
E93650-01
May 2018

ORACLE®

Oracle Hospitality Simphony Venue Management Security Guide, Release 3.11.0

E93650-01

Contents

Preface

This document provides security reference and guidance for Simphony Venue Management (SimVen).

Audience

This document is intended for:

- Implementation Specialists

- System administrators for Simphony Venue Management

- End users of Simphony Venue 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

- 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/

For more information about securing your Simphony Venue Management database, see the *Simphony Venue Management Database Backup and Recovery Guide* on My Oracle Support (MOS) by searching Doc ID 2388284.1.

Revision History

Date	Description of Change
May 2018	Initial publication

1

Simphony Venue Management Security Overview

This chapter provides an overview of Oracle Hospitality Simphony Venue 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 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. See Performing a Secure Simphony Venue Management Installation for more information.

- Learn about and use the Simphony Venue Management security features. See Implementing Simphony Venue 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. 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 to access this information.

Overview of Simphony Venue Management Security

Architectural Overview

Simphony Venue Management is an add-on product to the Simphony Client Server\ service oriented architecture (SOA) that is a collection of loosely coupled self-contained modules. The core of the SimVen software is the Back Office application (SimVen Back Office). This application is Windows-based and communicates with supporting services.

Simphony Architecture vs. Single Server Systems

The Simphony Architecture leads to a more scalable and reliable system compared to server-based models as services are distributed and do not have to be located on a single machine

Technology

Simphony Venue Management SOA uses industry standard SOAP services that provide greater ability to work with third-party applications.

A Mertech Data Systems database driver is used to connect the SimVen Microsoft Windows application to the Microsoft SQL Server Database.

A Microsoft Windows Service facilitates communication to the point-of-sale (POS) workstations.

Figure 1-1 Basic Simphony Venue Management Topology
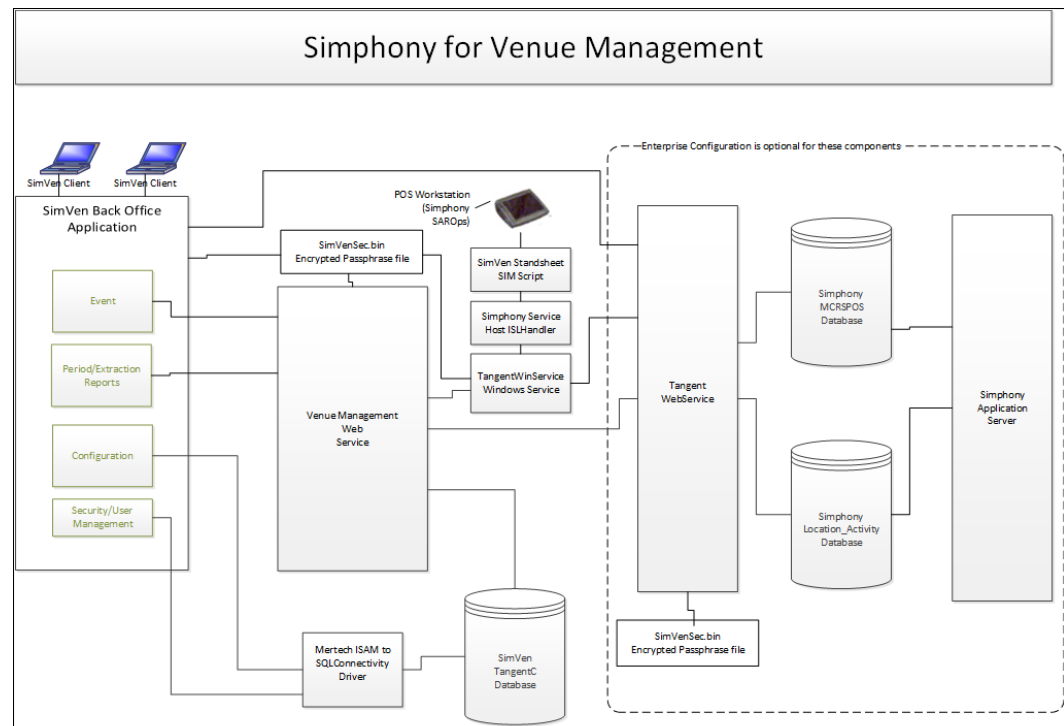
Understanding the Simphony Venue Management Services

The Simphony Venue Management back office application is a Microsoft Windows desktop application that resides behind a firewall on a property and is used to manage perpetual inventory, warehouse data and Event Management. The SimVen services include:

- The Venue Management web service provides a mechanism for extracting data related to inventory for specific events, and is also referred to as **Stand-Sheet** data

- The Tangent Web Services provides the interface to communicate with Simphony databases

The Tangent Windows Service interacts with the Tangent Web Service and also provides a mechanism to communicate with the POS workstations.

Simphony Venue Management Back Office 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.

Database User Management

The Simphony Venue Management sample database is installed with only one pre-defined username and password, the SimVen user that is created by the installer which allows access to SimVen's Security screen.

Oracle Hospitality mandates that users create a unique, strong password for the pre-defined SimVen user. The password must be at least 8 characters long and include letters and numbers.

SimVen's installation program also prompts for the creation of a Microsoft SQL Server Login and a Database User with a username and password that are created by the user in the installer. The same credentials are being used by the Mertech SQL Driver to log into the Microsoft SQL Server database at runtime.

> **NOTE:**
>
> Authentication Database credentials are stored in the configuration file on the SimVen application server, protected by Microsoft Windows Server file permissions.

Understanding the Simphony Venue Management Environment

When planning your Simphony Venue Management implementation, consider the following:

- **Which resources need to be protected?**

  - You need to protect customer data, such as credit-card numbers.

  - 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

This section describes recommended deployment configurations for SimVen.

The SimVen product can be deployed on a single server or in a cluster of servers.

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-Computer Deployment Architecture
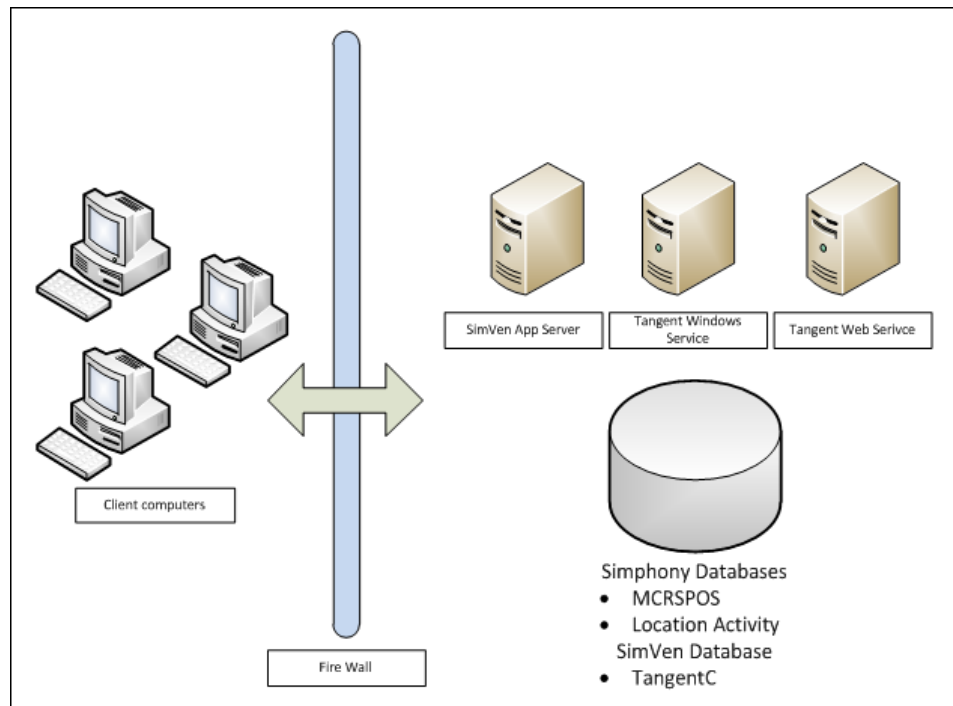
The general architectural recommendation is to use the well-known and generally accepted Internet-Firewall-DMZ-Firewall-Intranet architecture shown in Figure 1-3.

Figure 1-3 Traditional DMZ View
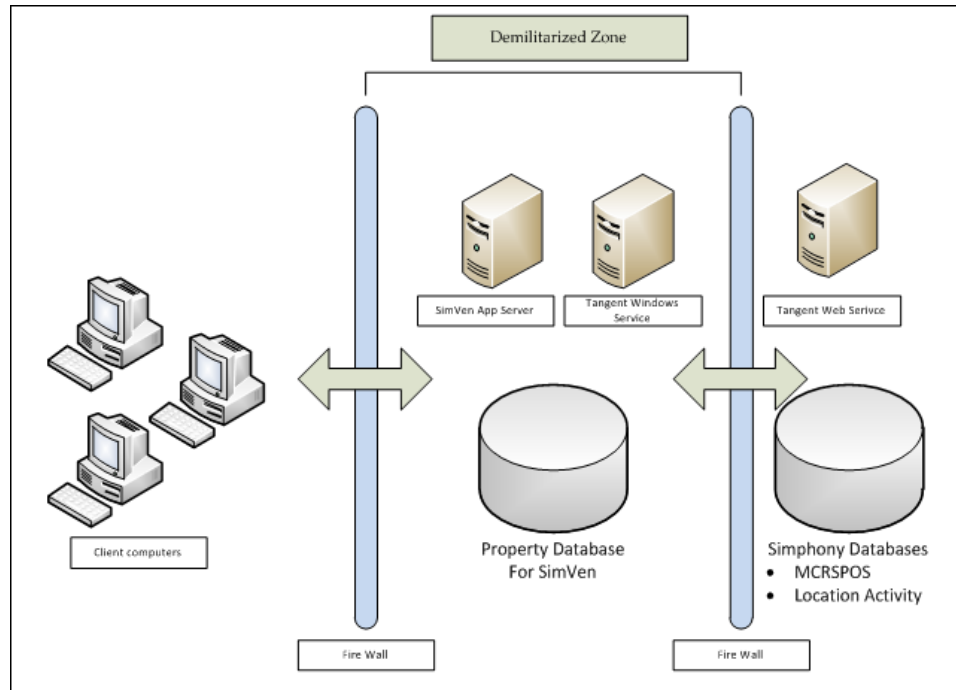
> ✏️ **NOTE:**
>
> The term demilitarized zone (DMZ) refers to a server that is isolated by firewalls from both the Internet and the intranet, thus forming a buffer between the two. Firewalls separating DMZ zones provide two essential functions:
>
> - Blocking any traffic types that are known to be illegal
>
> - Providing intrusion containment, should successful intrusions take over processes or processors

Refer to Enterprise Ports or Property Ports in Appendix B for more information about Simphony for Venue Management network port usage.

Simphony Venue Management Security

Operating System Security

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

1. 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

2. Perform the steps outlined in the How to disable 8.3 file name creation on NTFS partitions article on the SimVen application server.

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

Network Security

It is recommended that Simphony Venue Management is configured to use secure communications when transmitting data between the client application and Microsoft Internet Information Services (ISS) 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 Simphony Venue Management web services. It is recommended to use a certificate obtained from a trusted certificate authority (CA).

Authentication

All Microsoft Windows and Web Service requests are authenticated to ensure that the request comes from a trusted source. A token is stored in a protected file and read before transmitting a request to a Web Service. A token is transmitted with AES 256 bit SHA hash/ Salt combination in the SOAP header for each request. The Web Service compares the incoming token with the stored token to ensure authentication before accepting requests. The stored passphrase is encrypted with Microsoft Windows System encryption.

2

Performing a Secure Simphony Venue Management Installation

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

Pre-Installation Configuration

Perform the following tasks before installing Simphony Venue Management:

1. Apply critical security patches to the operating system.

2. Apply critical security patches to the database server application.

3. Review the Oracle Hospitality Enterprise Back Office Security Guide.

4. Review the Oracle Hospitality MICROS Hardware Wireless Networking Best Practices Guide.

5. Install Microsoft Internet Information Services (IIS) and configure it for Transport Layer Security (TLS) 1.1 (or higher) network communications.

6. Perform the steps outlined in the How to disable 8.3 file name creation on NTFS partitions article on the SimVen application server.

7. Ensure that connections to the database are restricted to a few trusted nodes using firewall rules.

Simphony Venue Management Installation

The Simphony for Venue Management Installation is comprised of two components:

1. SimVen Back Office Installer: Installs the Back Office applications.

2. SimVen Interface Installer: Installs the Windows and Web services.

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 new database, enter a complex username and password that adheres to the database hardening guides for all users.

The Simphony for Venue Management installation application disables the following operating system features:

- AutoPlay

- Remote Assistance

- Administrative Shares

A new Microsoft Windows user group named SIMVEN_USERS is created during the SimVen installation.

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

Access to the SimVen installation folder is restricted to members of the SIMVEN_USERS group. Any user required to access the SimVen folders needs to be added to the SIMVEN_USERS group by a system administrator.

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

- TangentService.asmx (Tangent Web Service)

- VenueManagementService.asmx (Venue Management Web Service)

The SimVen Microsoft Windows **Tangent Win Service** is required for proper connectivity with point-of-sales (POS) workstations.

Post-Installation Configuration

This section explains additional security configuration steps to complete after Simphony Venue Management 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 Simphony Venue Management patches available on My Oracle Support. Follow the deployment instructions included with the patch.

Passphrase and Database Connection Management in Simphony Venue Management
The **SimVen Crypt** utility stores connection information for establishing a connection to a database, and creates an encrypted pass phrase for the Authorization token. All Microsoft Windows and Web services use the **SimVenDbSettings.xml** file to store all user credentials that can connect to a database. The password entry for each connection in this .xml file is stored and encrypted with Microsoft Windows encryption.
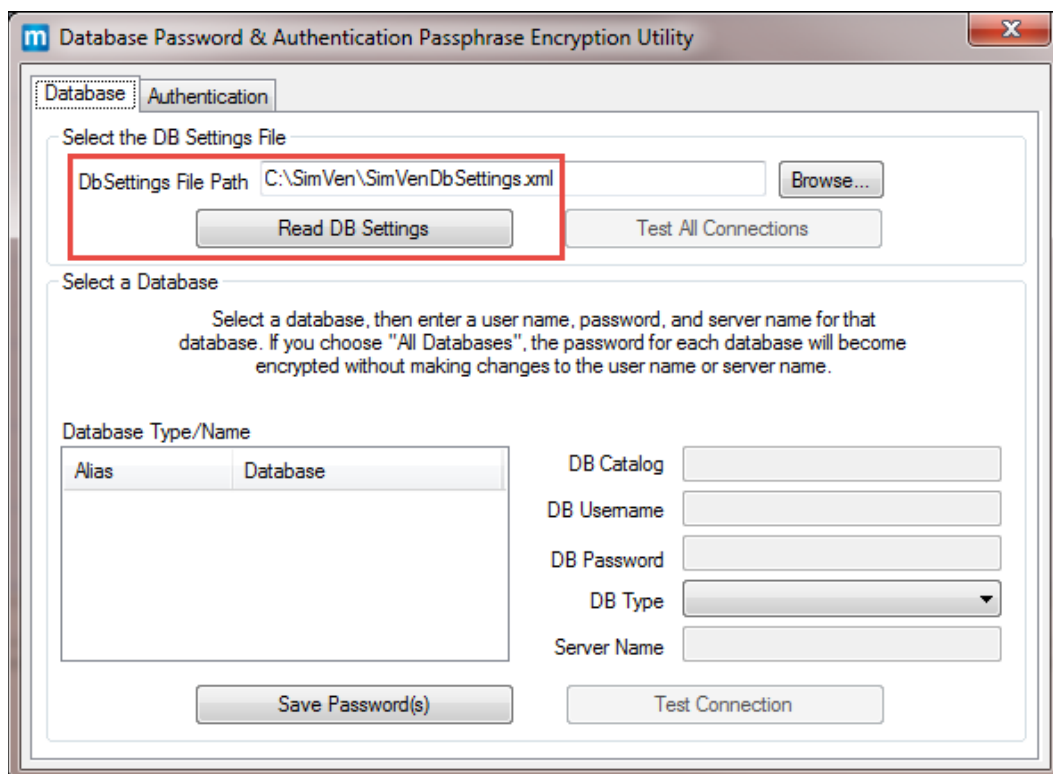
Database Connection
To establish a database connection, perform the following steps:

1. Navigate to the *<Drive>*:\SimVen\SimVenTools\Crypt folder, and open the **SimVenCrypt.exe** utility.

   The **Database** tab shows the folder in which SimVen was installed. This is the default location of the passphrase.

Figure 2-1 DB Password & Authentication Passphrase Encryption Utility – DB Settings

2. Click the **Read DB Settings** button to read the contents of the SimVenDBSettings.xml file.

3. If the SimVenDBSettings.xml file is not present, a message appears to have you create the default file.

   If the message appears, click **OK** to create the new file with the default settings. After the DB Settings file has been read, the screen shows all of the available connections in the **Database Type/Name** section as shown in the following figure.

Figure 2-2 Testing All Database Connections
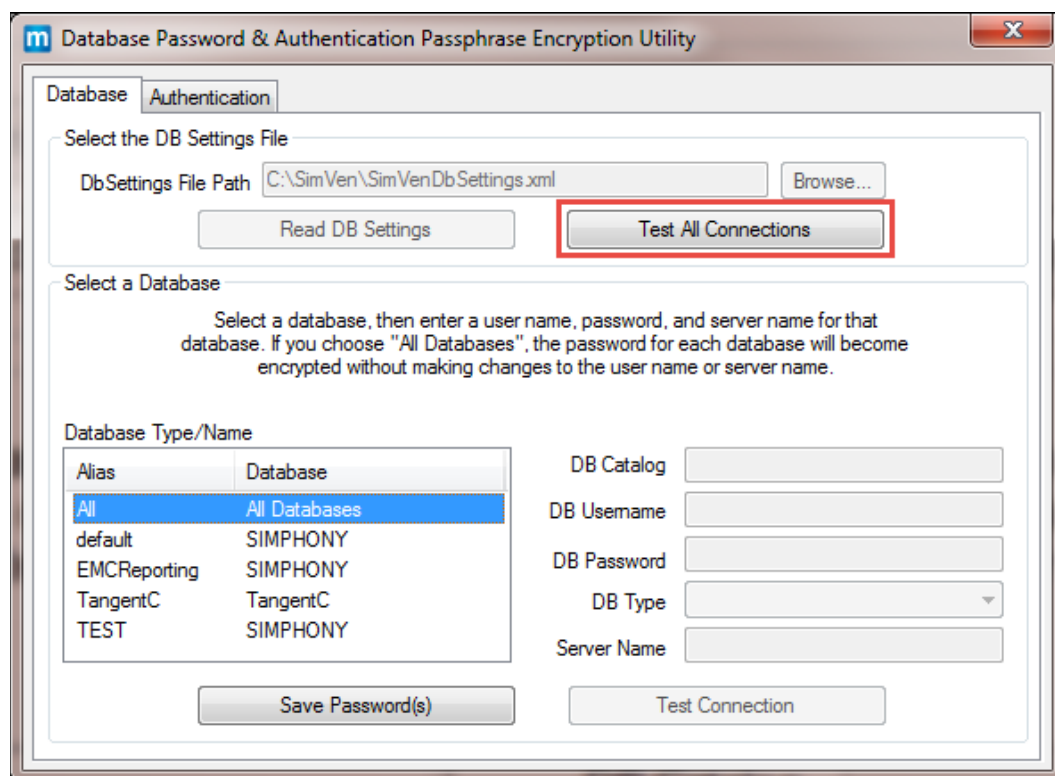
The first entry in the Database Type/Name section is **All Databases**.

4. Click the **Test all Connections** button to test all connections for all of the databases. The utility tests all available database connections and a message appears showing the results of the test for each connection.

**Figure 2-3 Connection Message Prompt**
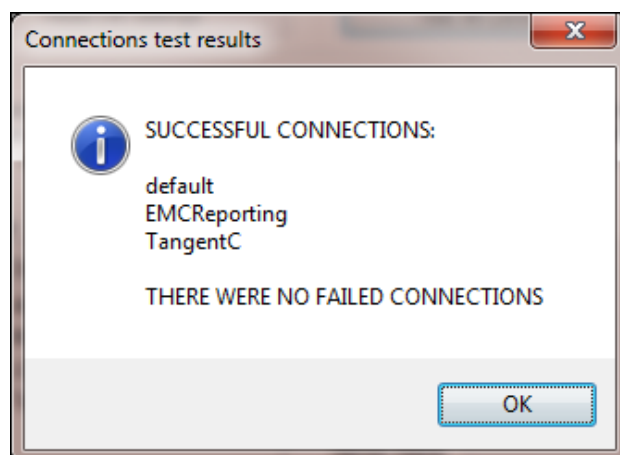
5. When a specific connection is selected in the Database Type/Name section, the fields on the right populate with the connection's details.

• 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**.

Figure 2-4 Testing Specific Database Connections
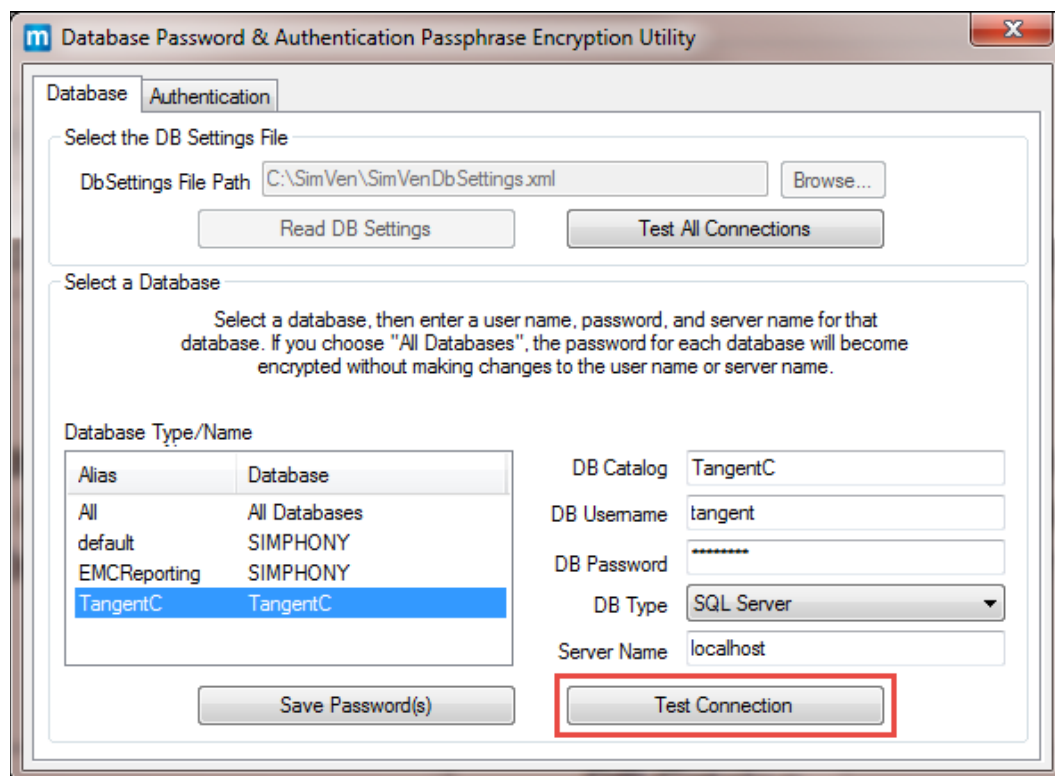
Creating a New Passphrase

Authentication in the Simphony Venue Management Crypt Utility
Passphrase data is managed by the **Authentication tab** of the SimVen Crypt utility. The passphrase is stored and encrypted using the AES 256 algorithm using the Microsoft data protection interface.
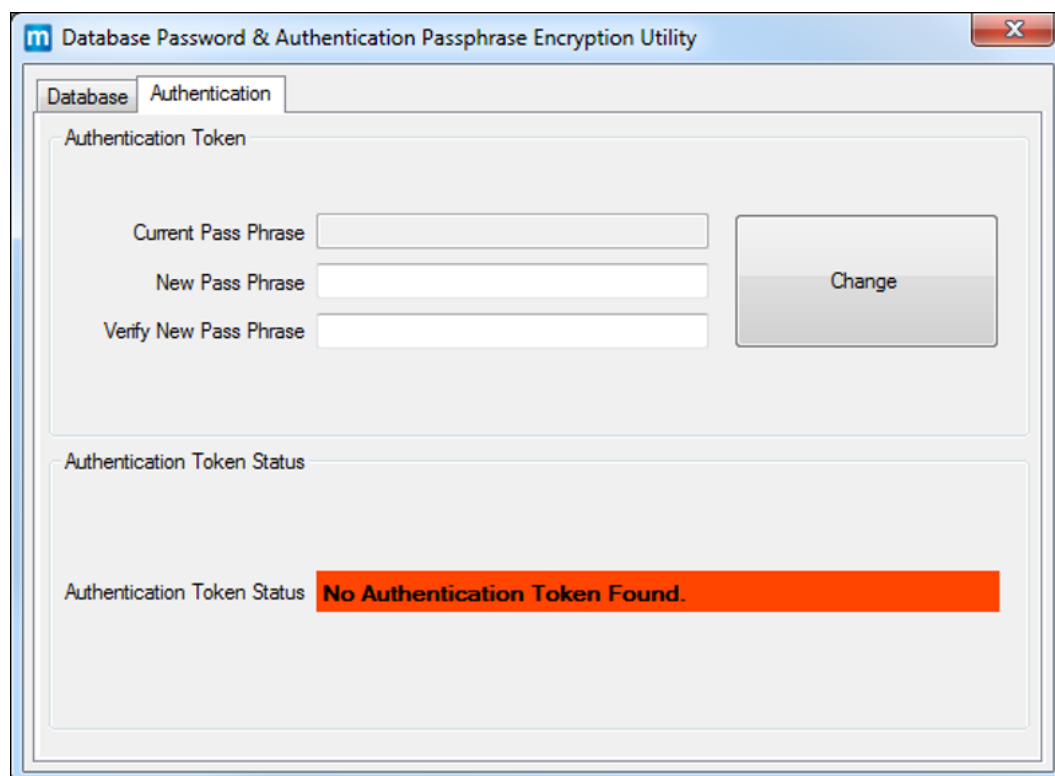
To create a new passphrase file:

1. Click the **Authentication** tab.

2. Enter a new passphrase between 8 and 14 characters in the **New Passphrase** field.

3. Re-enter the new passphrase in the **Verify New Passphrase** field.

4. Click **Change**. A message appears indicating that the passphrase was successfully created.

If the passphrase is not successfully created, repeat steps 1-4.

**Figure 2-5 Creating a New Authentication Token Passphrase**

Managing an Existing Passphrase

1. Enter the existing passphrase in the **Current Passphrase** field.

2. Enter a new passphrase in the **New Passphrase** field.

3. Re-enter the new passphrase in the **Verify New Passphrase** field and click **Change**.

A message indicating either success or failure appears. If successful, the new passphrase is encrypted and saved to the file.

Figure 2-6 Verifying the Status of a New or Existing Authentication Token Passphrase
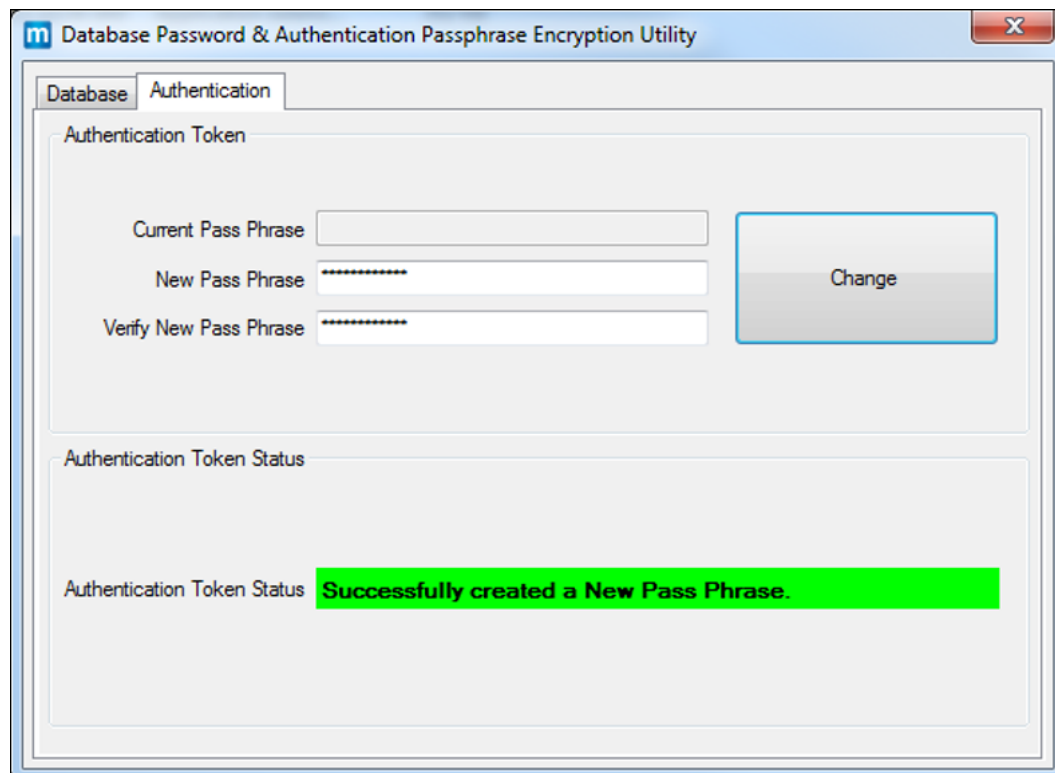

Changing Default Passwords

Previous releases of Simphony Venue Management installed a default administrator username and password. As a post-upgrade step of SimVen, Oracle Hospitality recommends that the default administrator password be changed to a strong password immediately upon logging on for the first time.

Security Configurations

The System Profile Management, System Profile tab contains fields that are related to SimVen password and access security and should be configured after initial installation.

- Global SYSTEM Lock

  - **System is Totally Locked** checkbox: When enabled, this option prevents all users from logging into SimVen until it is disabled

- Login and Password

  - **Password Timeout Period (in Days)** field: This value represents the number of days before passwords expire and all SimVen users must enter a new password

  - U**se SQL Login** checkbox: When enabled, this allows users to sign in to SimVen using their Microsoft SQL Server login credentials.
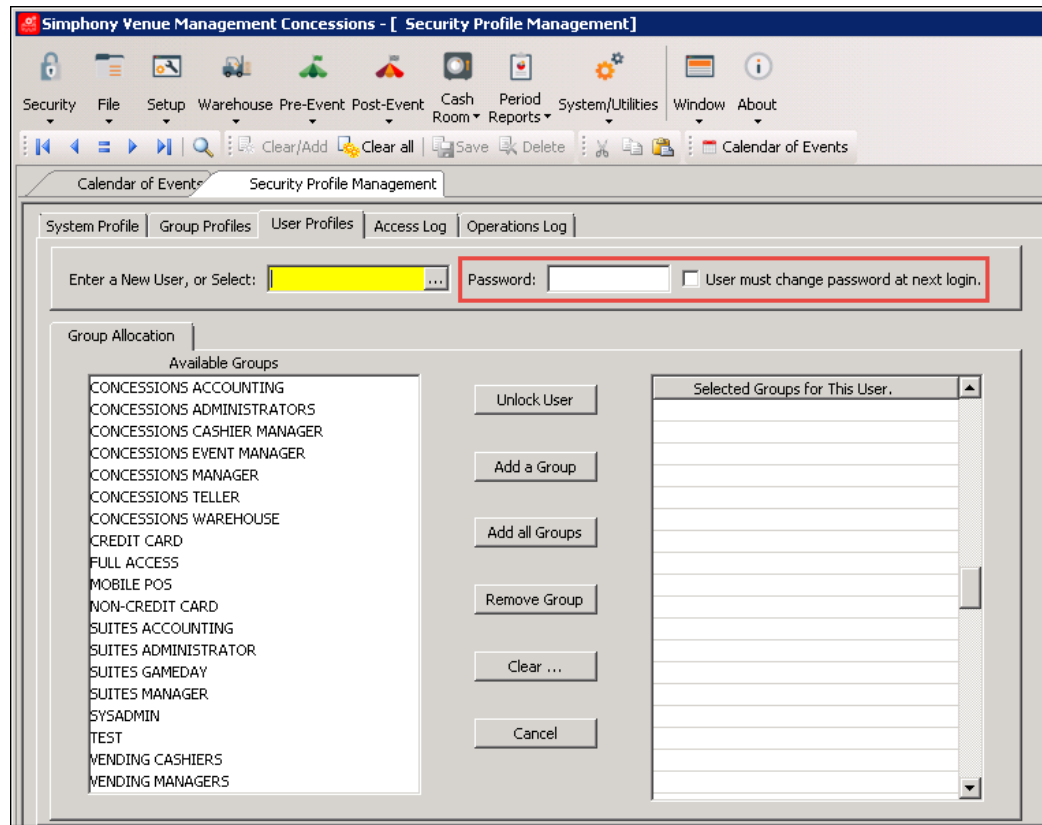
Figure 2-7 Security Profile Management – System Profile Tab
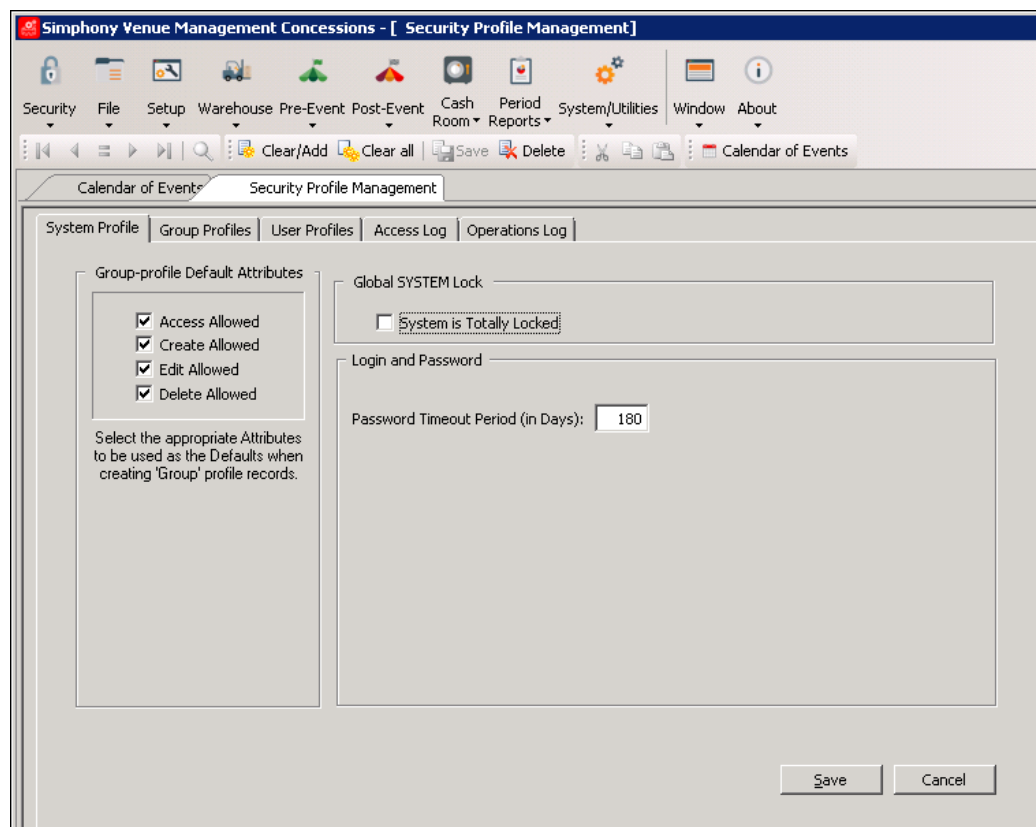
Configuring User Passwords

To configure a user's password:

1. Access **Security Profile Management** and select the **User Profiles** tab.

2. Select the user.

3. Enter the password in the **Password** field. Passwords are case-sensitive.

Figure 2-8 Security Profile Management – Setting SimVen User Passwords

Purging Data

Purging Simphony Venue Management data is not required for security purposes. Simphony Venue Management does not store any sensitive information such as credit card cardholder data.

3
Implementing Security

Passwords Policy Overview

Simphony Venue 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 5 previously used passwords

- The Maximum Allowed Failed Logins before a user account is locked out is 5

- Passwords expire based upon the policy configured in System Profile Management. This policy should be reviewed periodically

Inactivity Timeout

The SimVen application timeouts after 15 minutes of inactivity. After 15 minutes of inactivity all screens close and all unsaved work is discarded and a dialog appears to indicate an Activity Timeout.

Authorization Privileges

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

User Authorization Management

All users' logon credentials for the SimVen Back Office application are stored in the TangentC database. Anyone who has access to the SimVen Back Office software must provide a valid and unique login user name and password. No SimVen users can have the same username.

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 TangentC database. To ensure strict access control of the Simphony Venue Management Back Office application, always assign unique user names and complex passwords to each account. During installation, the SimVen Back Office installer prompts the user to configure the SimVen Back Office Administrator user, who is used to access the Back Office configurator.

The Simphony Venue Management Back Office' installation creates a SQL Server database user. During installation the user is prompted for a username and password to create the database user. This user is granted the minimum required permissions for the SimVen application to interface with the database. These credentials are used by the Mertech SQL Driver to connect to the Microsoft SQL Server database.

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 SimVen Back Office views and reports is defined within the Back Office, Security, User's Security Setup, Group Profiles tab

- User access control is defined within the Back Office, Security, User's Security Setup, User Profiles tab

General Configuration

The System Profile tab allows setting the default Group Profile attributes, locking out the entire system, and the default password timeout options.

Understanding Group Profiles

You can group employees according to the duties they perform, such as cashiers, managers, accounting clerks, and assign the same privilege and option settings to a group using Group Profiles. For example, the **Accounting** group is authorized to access, create, delete, and edit the **Chart of Accounts Maintenance** view. Without groups, each accountant would be assigned individual authorizations, which can be a repetitive and time-consuming task. Groups are assigned to an employee within the Back Office, Security, User's Security Setup, User Profiles tab.

Working with Group Profiles

Group Profiles limit access and determine how each securable item, including views and reports, in SimVen Back Office are used. A group grants the privileges needed to access, create, delete, or edit each securable item.

Adding or Removing Securable Item Authorizations

To create a group (or edit an existing group) and add or remove securable item authorizations to them, perform the following steps:

1. Navigate to the Back Office, Security, User's Security Setup, and click the **Group Profiles** tab.

2. Enter the name of the group in the **Enter a New Group or Select Existing Group** field.

   To edit an existing group, click the ellipses button (**…**), select the desired group from the Available Groups list window and click **OK**.

3. Select the view or report to be added to the group from the **Securable Items** list until it highlights. Views are highlighted green and reports are highlighted red (see Figure 3-1).

Table 3-1 – Adding or Removing Securable Item Authorizations To and From Groups

Action	Instructions
Adding an individual Securable Item Authorization to a group	1. Click **Add Item**. 2. Resume with step 4 below.
Adding All Securable Item Authorizations to a group	1. Click **Add All**. 2. Resume with step 4 below.
Removing an individual Securable Item Authorization from a group	1. Click **Remove Item**. 2. Resume with step 4 below.
Removing All Securable Item Authorizations from a group	1. Click **Remove All**. 2. Resume with step 4 below.

4. The item appears in the **Selected Item for this Group** table.

5. Select or deselect each authorization checkbox to allow or deny access, creation, deletion, or editing of the selected securable item.

6. Repeat steps 2 through 5 until all desired securable item authorizations are added or removed for the group.
7. Click **Save**.

Figure 3-1 Security Profile Management – Group Profiles
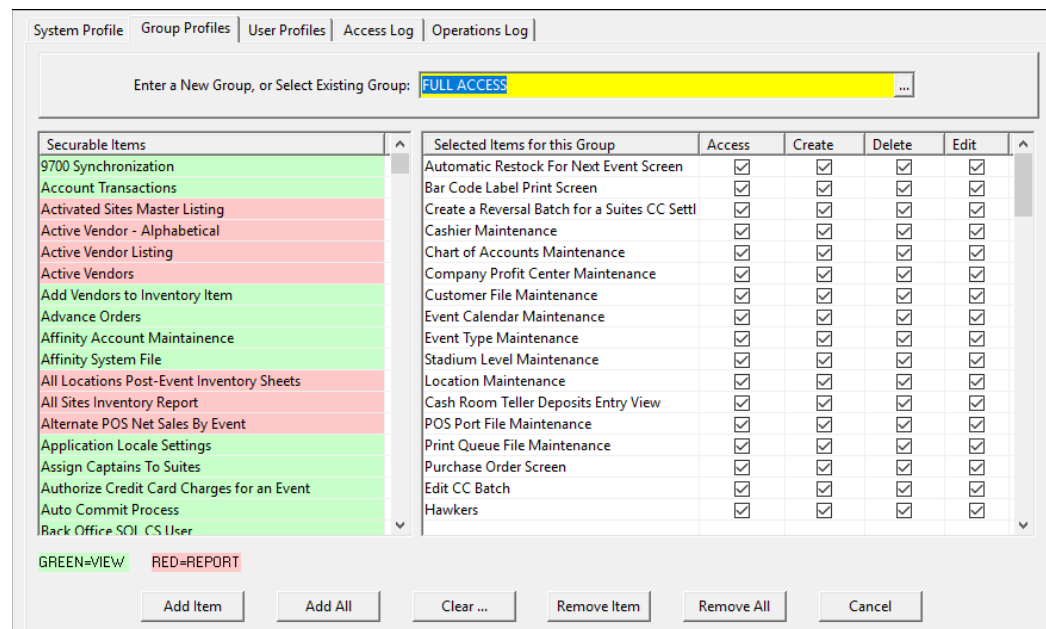
Deleting Groups

To delete an entire group:

1. In the **Enter New Group or Select Existing Group** field, click the ellipses button (**…**).

2. Select the group to be deleted from the Available Groups List window and click **OK**.

3. Click **Delete** and **Save**.

> ✏️ **NOTE:**
>
> You cannot delete a group when a user is associated with it. To successfully delete an entire group, first remove user associations with the group in the User Profiles tab.

Adding Individual Groups

To add a group:

1. Select or enter the employee in the **Enter a New User, or Select** field.

2. Select the desired group from the Available Groups list until the group highlights.

3. Click **Add a Group**. The group appears in the **Select Groups for This User** list.

4. Click **Save**.

Adding All Groups

To add all groups at once:

1. Select or enter the employee in the **Enter a New User, or Select** field.

2. Click **Add all Groups**. All groups appear in the **Select Groups for This User** list.

3. Click **Save**.

Figure 3-2 Security Profile Management – User Profiles

Removing a Group

1. Select or enter the employee in the **Enter a New User, or Select** field.

2. Select the group to be removed from the Available Groups list until the group highlights.

3. Click **Remove Group**. The group is removed from the **Select Groups for This User** list.

4. Click **Save**.

Understanding User Profiles

You can use the User Profiles to grant different levels of access to securable items, including views and reports, through the assignment of Group Profiles.

Creating New Users

The User Profile view is used to create a new user, create the user's password, and link groups to users.

1. Enter a unique username in the **Enter a New User, or Select field**

2. Enter a strong password in the **Password** field**.**

3. Click **Save**.

Figure 3-3 Security Profile Management – Creating New Users

Linking Employees to Groups

Employees are linked to groups within the Back Office, Security, User's Security Setup, User Profiles tab.

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

Tracking Simphony Venue Management Configuration, Edits, Errors, and Access
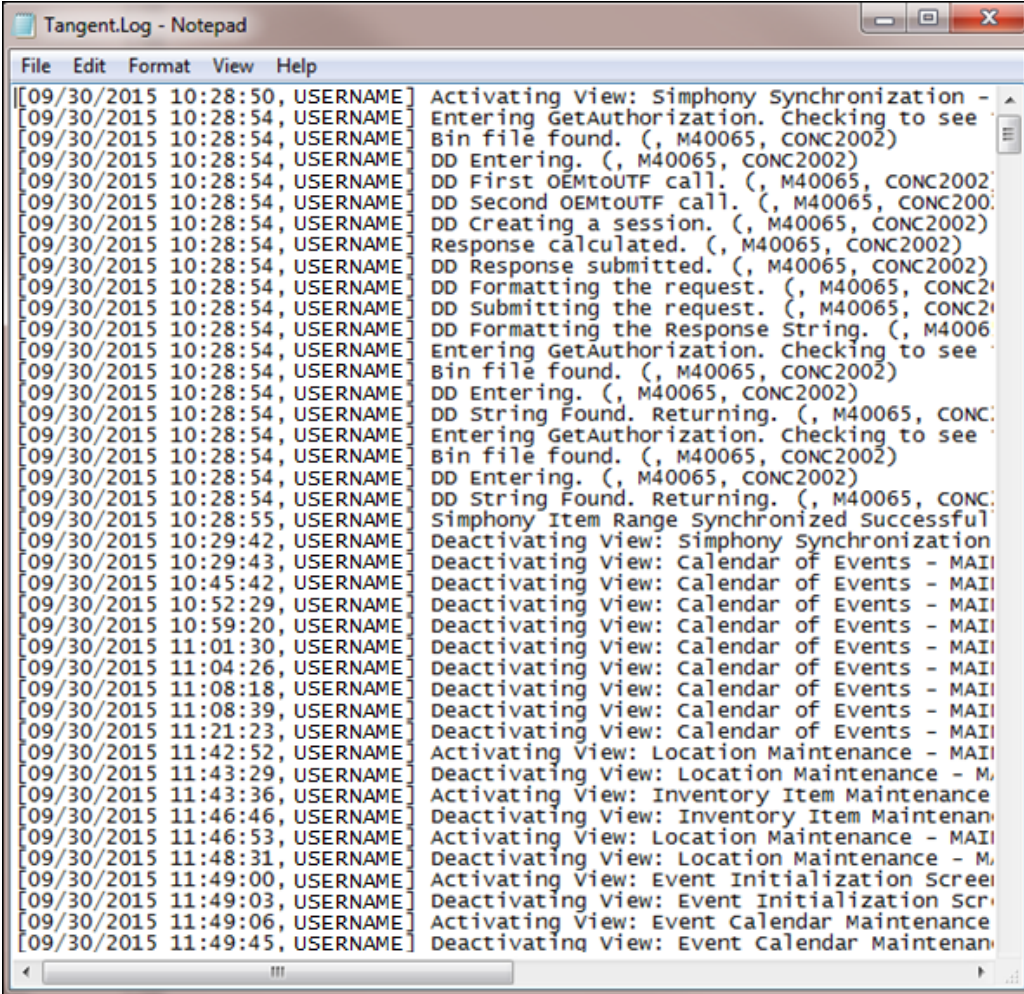
Configuration and Edit Logging

The **Tangent.Log** file tracks configuration steps and edits performed within SimVen.

Accessing the Tangent.Log file
To access and review the Tangent.Log file, navigate to
<*Drive*>:\SimVen\Data\Tangent.Log and open the file using a text editor.

**Figure 3-4 Tracking Configuration and Edits – Tangent.Log file**

Error Logging

Errors that have occurred in the SimVen Back Office application are written to the **TangetErr.Log** file. The file lists the date and time the error occurred, the error number, where the error occurred, and the error message as shown above.

Accessing the TangentErr.Log file

To access and review the TangentErr.Log file, navigate to
<Drive>:\SimVen\Data\TangentErr.Log and open the file using a text editor.

Figure 3-5 Tracking System Errors – TangentErr.Log
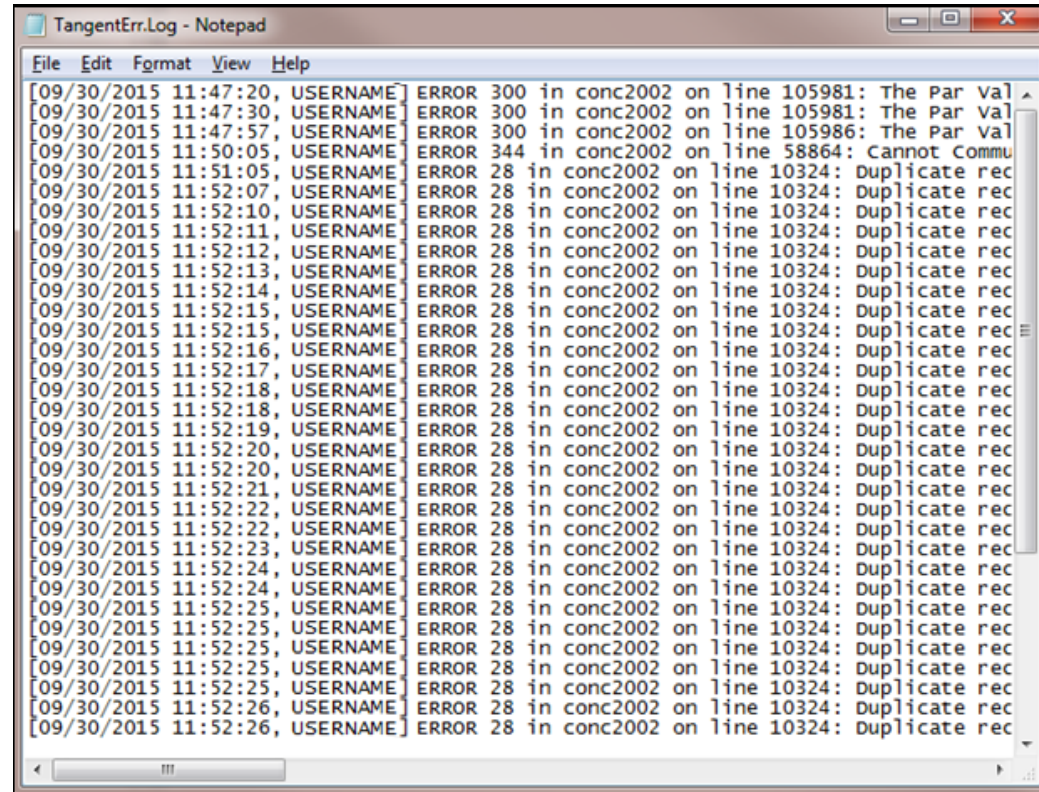
Operations Log

In addition to external log files that are created on the disk, a central operations log exists in the Security Panel and is available to users that are assigned to the System Administrators group.

Viewing the Operations Log

To access the Operations Log, navigate to the Back Office, Security, User's Security Setup, and click the **Operations Log** tab as shown in the following figure.

Figure 3-6 Operations Log

If Additional information is available to the specific line selected, the **Show Details** button is made available.

Operations Log Filter

Items can be filtered by clicking on the **Filter** button. This shows a new dialog in which the Operations log can be filtered. To activate a filter click on the checkbox to enable the filter and select or enter the specific data to be filtered as shown the following figure.

Figure 3-7 Operations Record Filter Options

Purging Operations Log

To manually purge the Operations Log, click the **Purge Log** button, for options. This allows you to purge items by a specific date range or to purge all items in the Operations Log file as shown in the following figure.

Figure 3-8 Operations Purging Options

In addition to manual purge options, the Operations Log can be set to automatically purge, by setting the **Num. of Days to Keep Logs** field in the System Maintenance screen under the **Venue Management Web Service** tab. Once the value is set, the Venue Management Web Service automatically purges the log entries that are older than the specified date range.

Figure 3-9 Main System Maintenance – Purging Logs Automatically

Access Log

The **Access Log** within SimVen Back Office tracks and records each login to the SimVen Back Office application. The Access Log tracks:
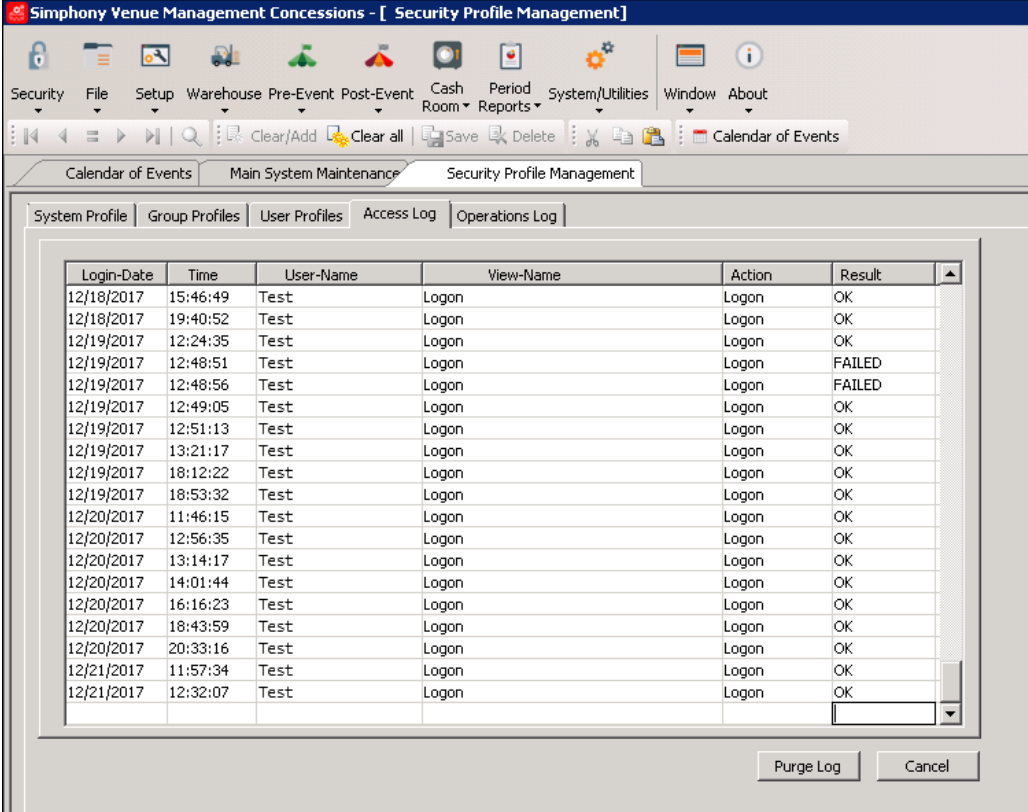
- Login Date

- Login Time

- Login User name

- Login View name

- Login Action

The Access Log also monitors unsuccessful logins.

Accessing the SimVen Access Log

To access and view the Access Log, navigate to the Back Office, **Security**, Security Profile Management, and click the **Access Log** tab.

Figure 3-10 Security Profile Management – Access Log Tab

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.

  - Grant necessary privileges only.

  - Revoke unnecessary privileges from the PUBLIC user group. iii. 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.

  - Protect the Oracle listener.

  - Monitor listener activity.

  - Monitor who accesses your systems.

  - Check network IP addresses.

  - Encrypt network traffic.

  - Harden the operating system.

Appendix B

Simphony Venue Management Port Numbers

The following tables list port number that are used in Simphony Venue Management. Open only the minimum required ports based on the installation type and deployment configuration.

Enterprise Ports

Table 3-2 – Enterprise Ports

Service	Port Number	Configurable?
Database Default (Oracle)	1521	Yes
Database Default (Microsoft SQL Server)	1433	Yes
Tangent Web Service	8081	Yes

Property Ports

Table 3-3 – Property Ports

Service	Port Number	Configurable?
Tangent Win Service	5050	Yes
Venue Management Web Service	8080	Yes