Oracle® Hospitality Simphony First Edition Venue Management

Security Guide
Release 3.8
Part Number: E69861-01

December 2015

ORACLE

Contents

Tables

Figures

Preface

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

Audience

This document is intended for:

- Implementation Specialists
- System administrators for Simphony First Edition Venue Management
- End users of Simphony First Edition 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
- Screen shots of each step you take

Documentation

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

- Refer to the *Simphony First Edition Venue Management Installation Guide* for information about installing the SimVen application.
- Refer to the *Simphony First Edition Security Guide* for more information about hardening your system's security.

Revision History

Date	Description of Change
December 17, 2015	• Initial publication

1 Simphony First Edition Venue Management Security Overview

This chapter provides an overview of SimVen security and explains the general principles of the application's 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 Simphony First Edition Venue Management Installation for more information about secure software installation.
- **Learn about and use the Simphony First Edition Venue Management security features.** See Implementing Simphony First Edition 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.
- **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.

  See the **Critical Patch Updates and Security Alerts** web site: `http://www.oracle.com/technetwork/topics/security/alerts-086861.html`

Overview of Simphony First Edition Venue Management Security

Architectural Overview

SimVen is an add-on product for the Simphony First Edition (FE) point-of-sale (POS) product. The SimVen application provides a Windows-based back office application for managing inventory, event pricing, cash room deposits, and financial reporting. SimVen also includes components that integrate with the Simphony FE POS client which enables inventory updates to the back office application.

Technology

The Simphony Venue Management components connect to a Microsoft SQL Server database for application data storage. A Microsoft Windows Service facilitates communication between the point-of-sale (POS) workstations and the back office application. Simphony Venue Management's application components use industry standard SOAP services running under Microsoft Windows Internet Information Server (IIS) for connectivity.

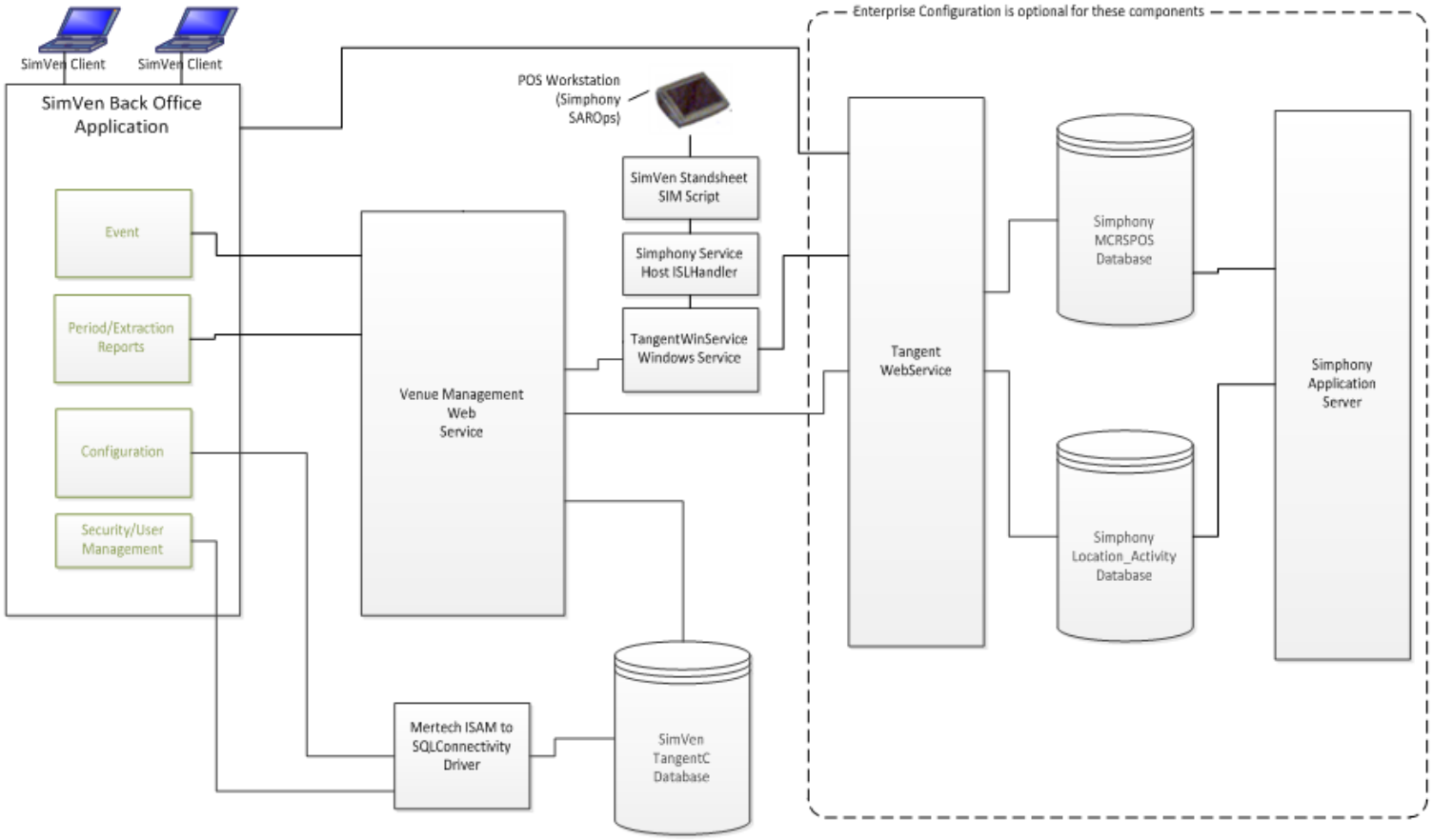


Figure 1 - Basic SimVen Topology

Understanding SimVen Services

The SimVen 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 services include:

- The Venue Management web service provides a mechanism for storing and extracting event based inventory data, also referred to as **Stand-Sheet** data.
- The Tangent Web Service provides the interface to communicate with the Simphony databases.
- The Tangent Windows Service provides a mechanism for the POS workstations to communicate with the back office application via the Venue Management Web Service.

User Authentication

Overview

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.

SimVen Authentication

All users' logon credentials for Simphony Venue Management are stored in the central database. Anyone who has access to the 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 SimVen application, always assign unique username and complex passwords to each account.

Database User Management

The SimVen database is installed with a pre-defined username and password, the SimVen user (SYSADMIN, sysadmin$1), 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 wizard also prompts for the creation of a Microsoft SQL Server Login and a Database User with default username (TANADMIN) and password. The same credentials are being used by the Mertech SQL Driver to log into the Microsoft SQL Server database at runtime.

Security 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 First Edition Venue Management Environment

When planning your Simphony First Edition 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?

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 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 SimVen.

The SimVen product can be deployed on a single server or in a cluster of servers. The simplest deployment architecture is the one shown in Figure 2 - Single-Computer Deployment Architecture.

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.

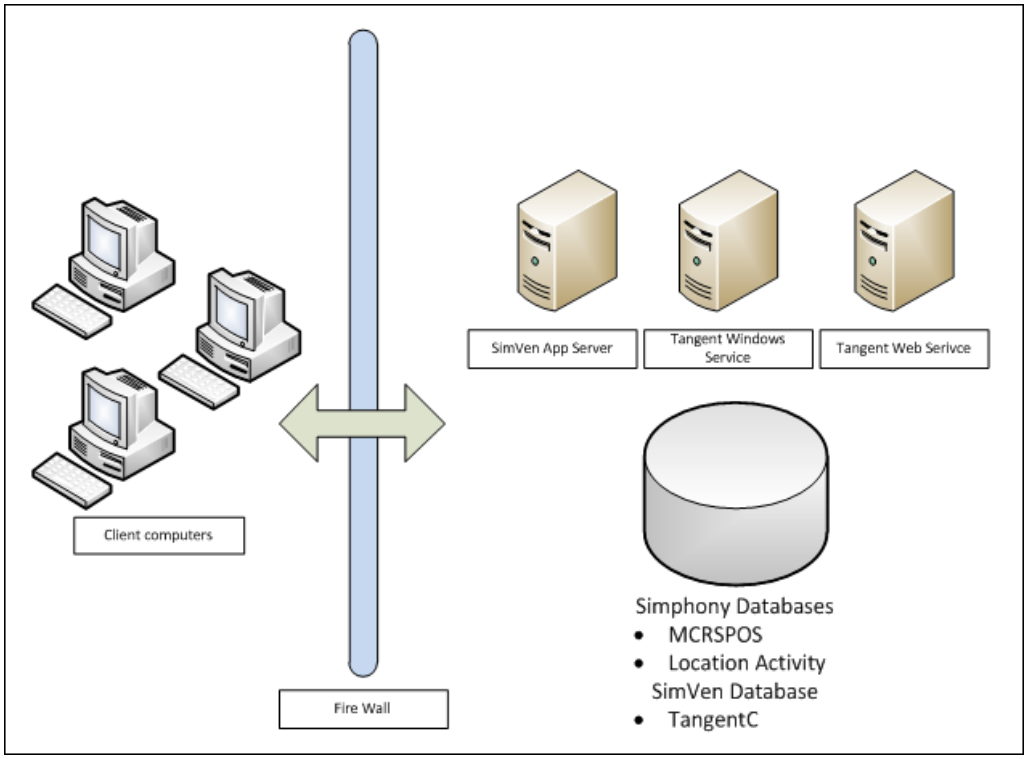


Figure 2 - Single-Computer Deployment Architecture

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.

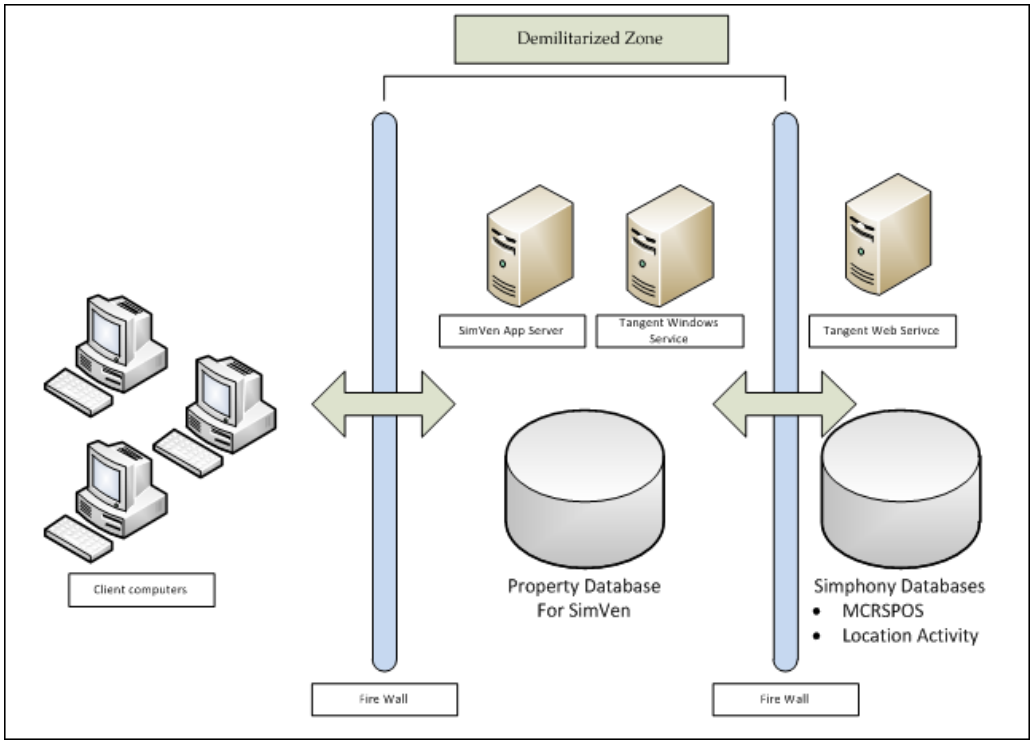


Figure 3 - Traditional DMZ View

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:

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

Refer to SimVen Port Numbers in Appendix B for more information about Simphony for Venue Management network port usage.

Simphony for 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.

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

Authentication

All SimVen Web Service requests are authenticated to ensure that the request comes from a trusted source. Any un-trusted Web service requests will be rejected.

2 Performing a Secure Simphony First Edition Venue Management Installation

This chapter presents SimVen 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 SimVen:

- Apply critical security patches to the operating system
- Apply critical security patches to the database server application
- Review the Oracle Hospitality MICROS Hardware Wireless Networking Best Practices Guide

Simphony for 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 password that adheres to the database hardening guides for all users.

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

- Tangent Web Service
- Venue Management Web Service

The following SimVen Microsoft Windows service is required for proper connectivity with the workstations:

- Tangent Win Service

Post-Installation Configuration

This section explains additional security configuration steps to complete after SimVen 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.

Turning Off Auto Play

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 SimVen patches available on My Oracle Support. Follow the deployment instructions included with the patch.

Passwords Overview

Oracle Hospitality recommends that administrators configure a strong password policy after the initial installation of the application and review the policy periodically. Passwords in SimVen are required to be strong.

Maintaining Strong Passwords

Ensure that passwords adhere to the following strength requirements:

- 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 should not choose a password equal to the last 5 previously used passwords

Configuring Passwords

To create a PCI compliant password, enter the password in the Password field following the guidelines outlined below:

- The **Minimum Password Length** is at least 8 characters
- The **Password Repeat Interval** is set to 5 by default
- The **Days Until Expiration** should be set to greater than 30 days
- The **Maximum Allowed Failed Logins** is 5

Change Default Passwords

SimVen is installed with a default master user name and password. Oracle Hospitality recommends changing the master user name and password after logging in for the first time. Refer to the *Simphony First Edition Venue Management Installation Guide* for information about default passwords.

Security Configurations

To configure your SimVen system's security access for users, navigate to the Security Profile Management module by:

1. Logging into SimVen.
2. Select the **Security** drop-down menu.
3. Select **Security Setup and Edit** and the Security Profile Management screen appears. See Figure 4 - Security Profile Management - System Profile tab.

   The **System Profile** tab contains fields that are related to passwords and SimVen access security. They are:

   - Global SYSTEM Lock
     - **System is Totally Locked** - When enabled, this option prevents all users from logging into SimVen.
   - Login and Password
     - **Password Timeout Period (in Days)** - This value represents the number of days before passwords expire and all SimVen users must enter a new password.
       - For example (see Figure 5 - Security Profile Management - Setting SimVen User Passwords), if a user's or Group profile does not have the **No Password Timeout** checkbox selected, then passwords will expire after 5 days.
       - If the **No Password Timeout** checkbox is selected for a user's or Group profile, the **Password Timeout Period (in Days)** set value is ignored by the system.
     - **Use SQL Login** - When enabled, this allows users to sign in to SimVen using their Microsoft SQL Server login credentials

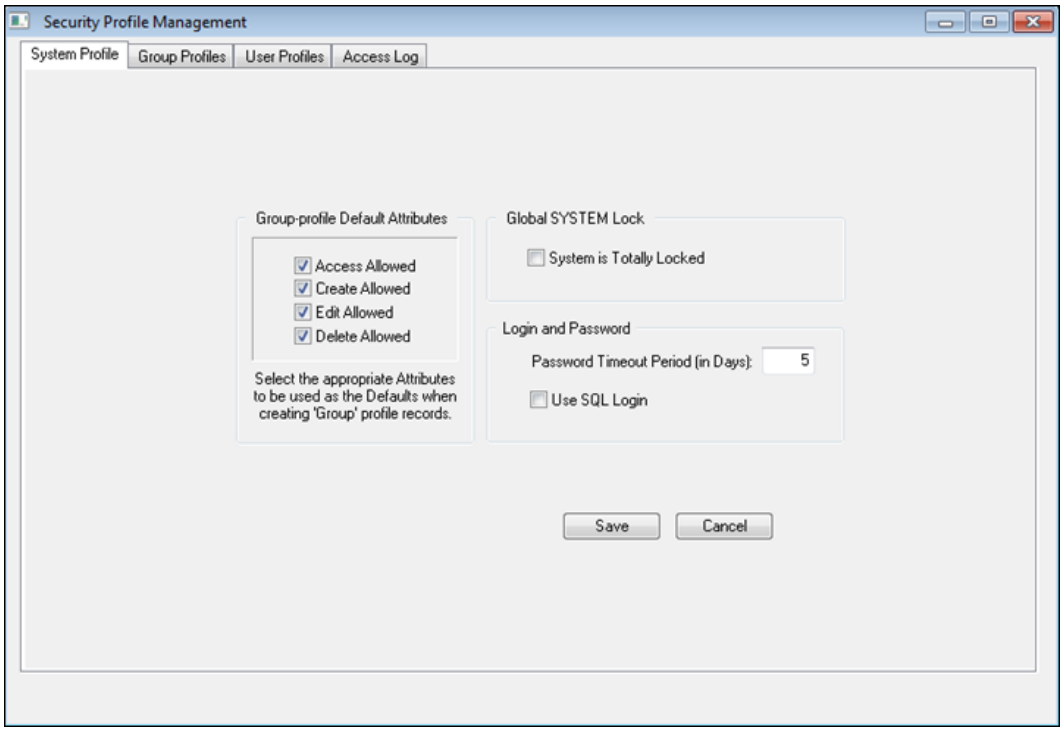


Figure 4 - Security Profile Management - System Profile tab

Configuring Passwords in SimVen

To configure SimVen user passwords:

1. Access the **Security View** and select the **User Profiles** tab.
2. Enter the password in the **Password** field. Passwords are case-sensitive.

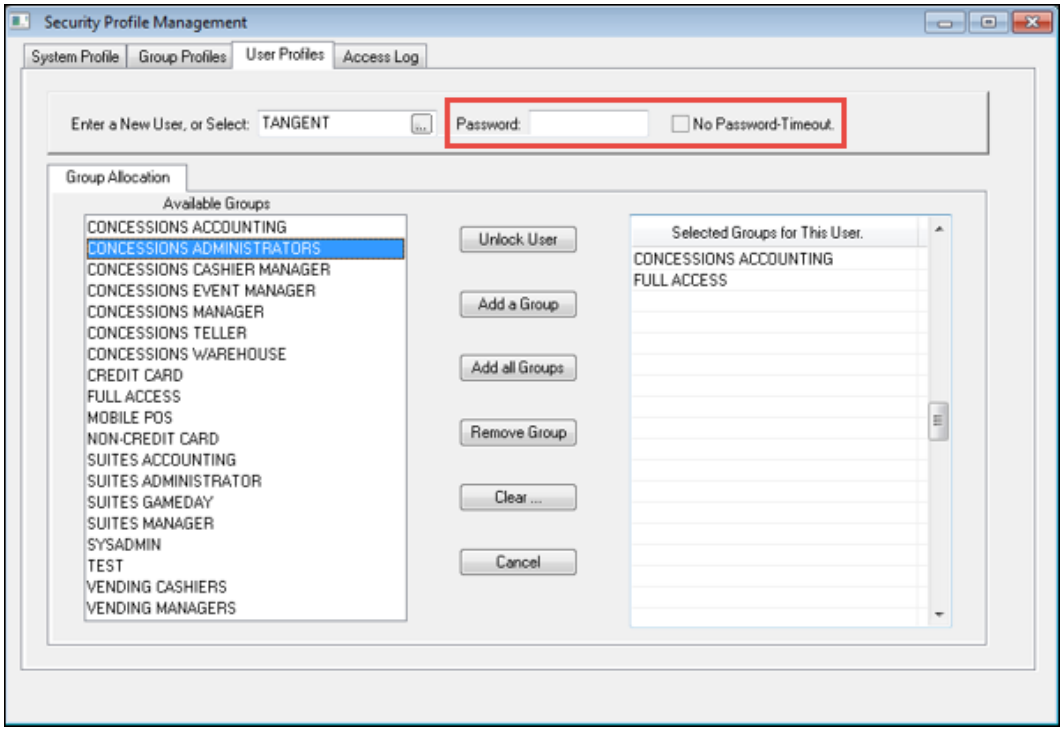


Figure 5 - Security Profile Management - Setting SimVen User Passwords

Pass Phrase and Database Connection Management in SimVen

The **SimVen Crypt** utility stores connection information for establishing a connection to the database. These credentials are used by the SimVen Web services to connect to the application databases. The credentials are stored and protected using operating system encryption.

Database Connection

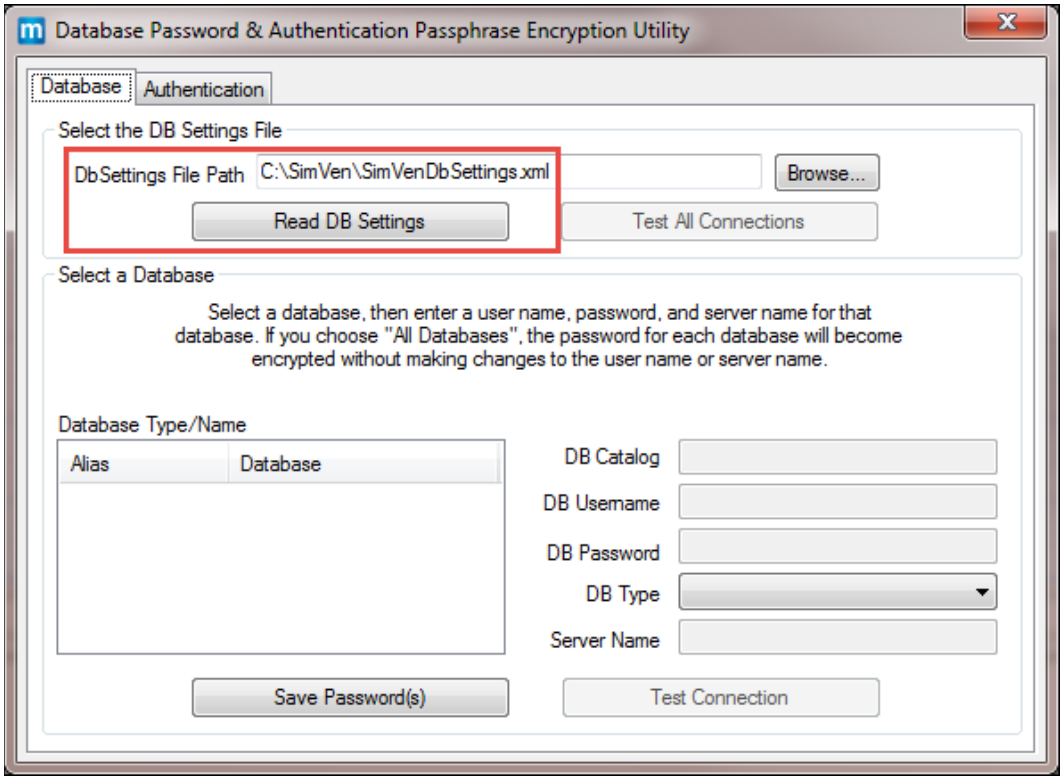


Figure 6 - DB Password & Authentication Pass Phrase Encryption Utility - DB Settings

To establish a database connection, perform the following steps:

1. Navigate to the <*Drive letter*>:\SimVen\SimVenTools\Crypt folder, and open the **SimVenCrypt.exe** utility.
    - The **Database** tab shows the folder in which SimVen was installed.
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 on Figure 7 - Testing All Database Connections.

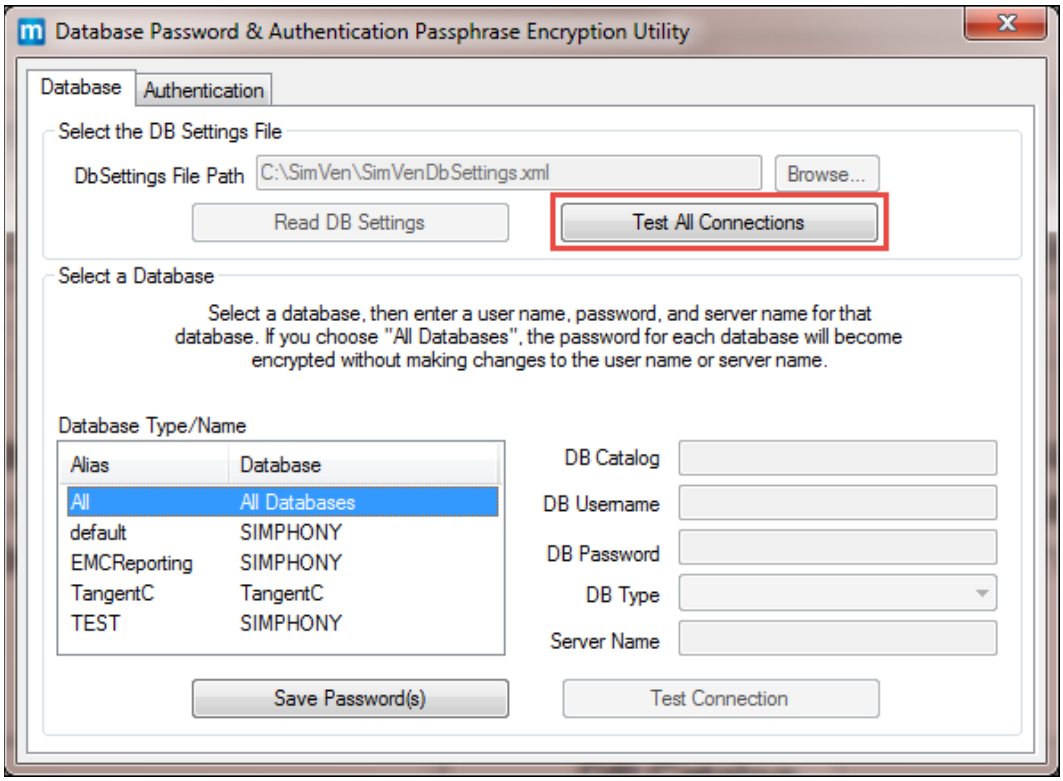
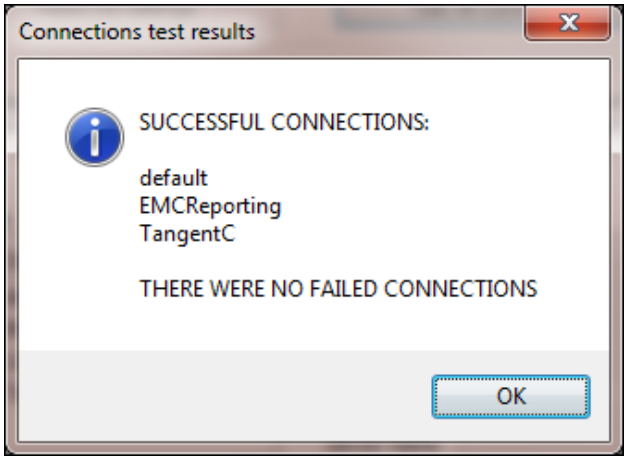


Figure 7 - Testing All Database Connections

The first entry in the Database Type/Name section is **All Databases**.

1. 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.



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

     See Figure 8 - Testing Specific Database Connections

   - 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**.

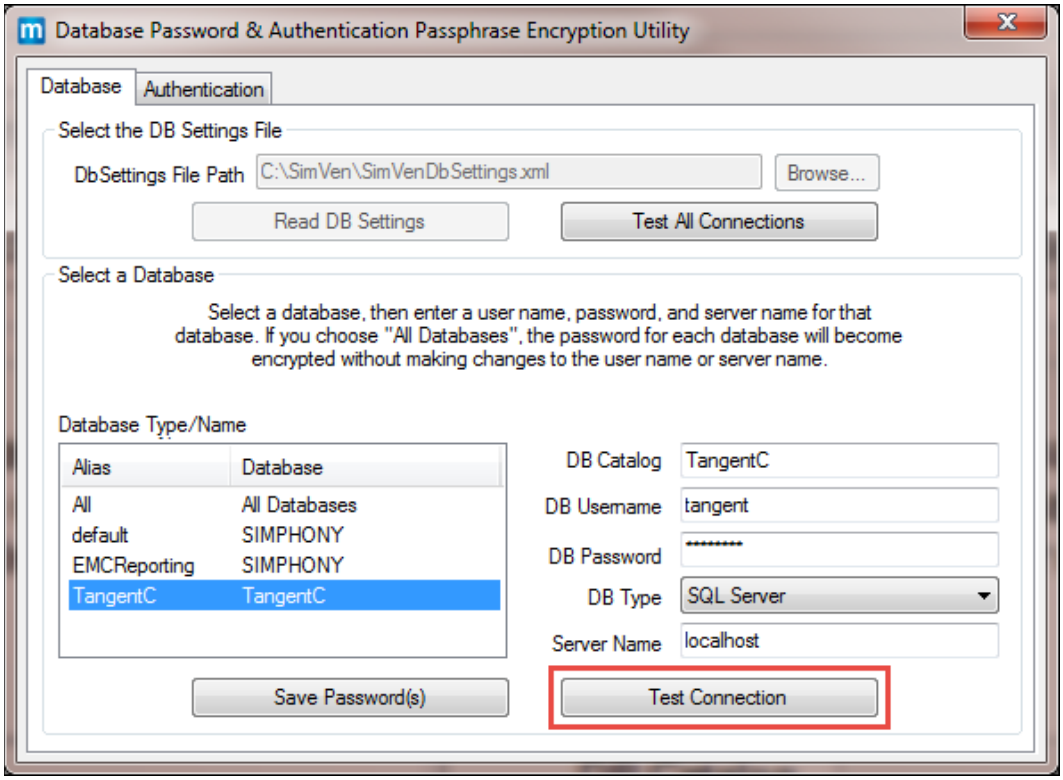


Figure 8 - Testing Specific Database Connections

Users Authentication

Overview

Authentication is the process of ensuring that people on both ends of the connection are who they say they are. Applicable to not only the entity trying to access a service, Authentication is also applicable to the entity providing the service.

Configuring Authentication using the SimVen Crypt Utility

Pass phrase data is managed by the **Authentication tab** of the SimVen Crypt utility.

To create a new pass phrase file:

1. Click the **Authentication** tab.
2. Enter a new pass phrase between 8 and 14 characters in the **New Pass Phrase** field.
3. Re-enter the new pass phrase in the **Verify New Pass Phrase** field.
4. Click **Change**. A message appears indicating that the pass phrase was successfully created.

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

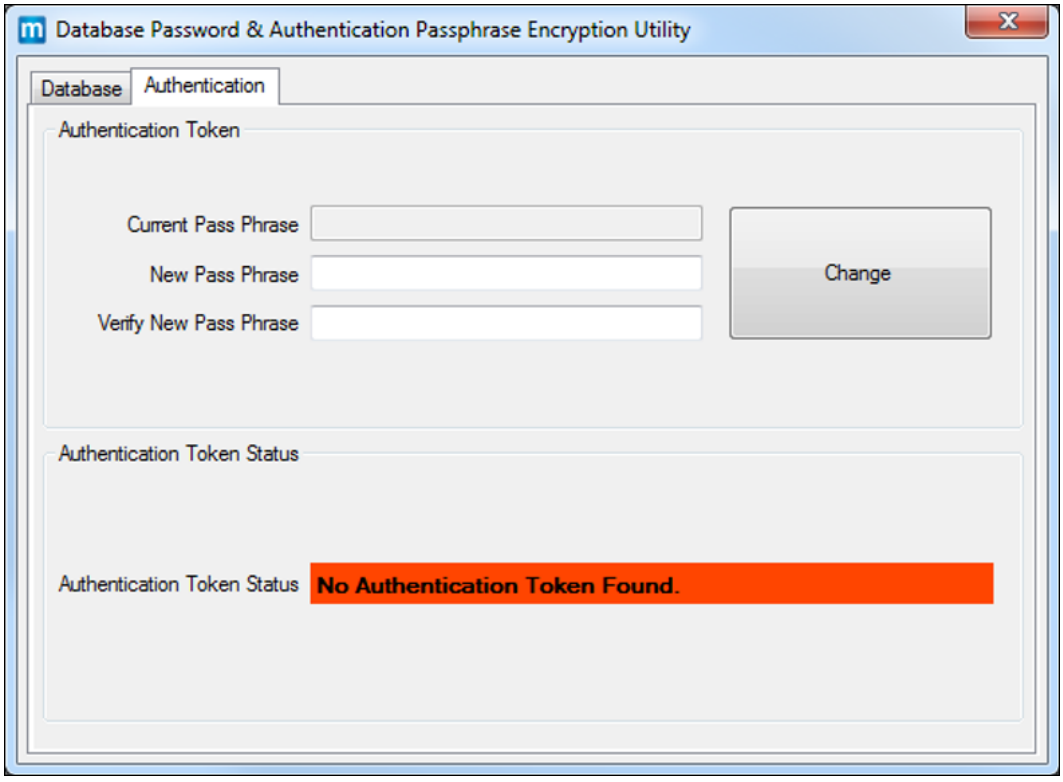


Figure 9 - Creating a new Authentication Token Pass Phrase

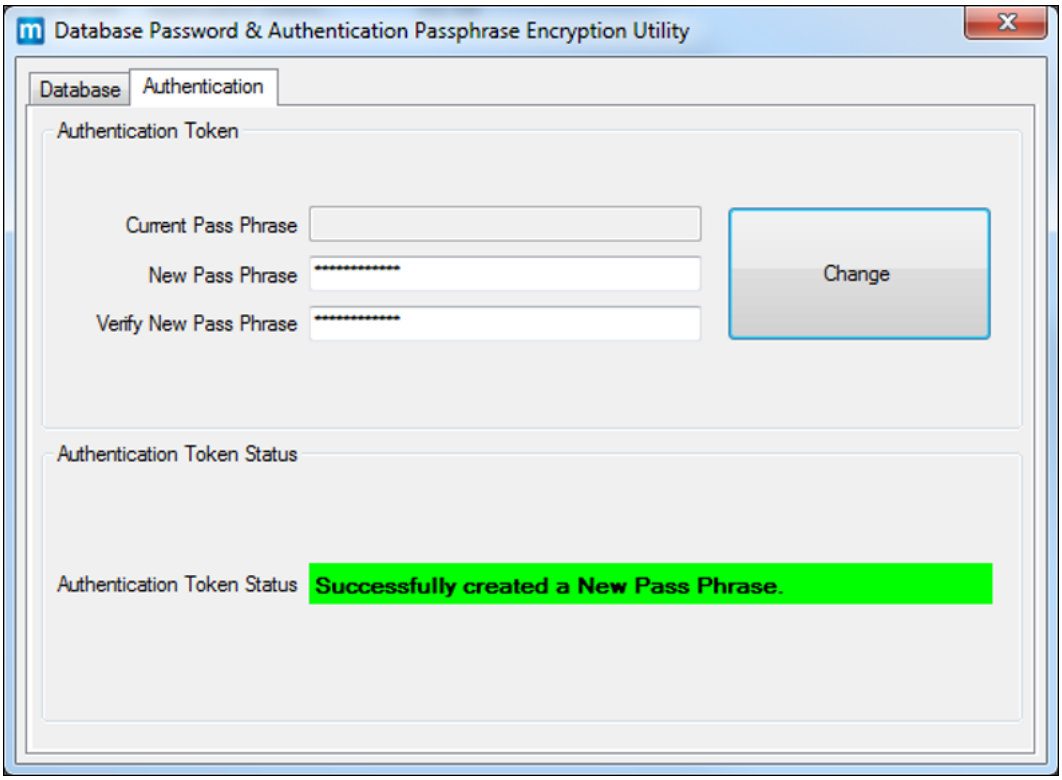


Figure 10 – Verifying the status of a new or existing Authentication Token Pass Phrase

Managing an Existing Pass Phrase

1. Enter the existing pass phrase in the **Current Pass Phrase** field.
2. Enter a new pass phrase in the **New Pass Phrase** field.
3. Re-enter the new pass phrase in the **Verify New Pass Phrase** field and click **Change**.
4. A message indicating either success or failure appears.

3 Implementing Simphony First Edition Venue Management Security

This chapter reviews the SimVen security features.

Authorization Privileges

Overview

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

SimVen 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 SimVen back office application, always assign unique user names and complex passwords to each account. The SimVen back office database is installed with only one pre-defined username and password, the SimVen back office User, (SYSADMIN), which allows access to the SimVen back office's configurator.

Oracle Hospitality recommends not using any administrative accounts for any SimVen back office application logins. It is strongly suggested that you create a different password for the pre-defined SimVen back office User within the back office, Security, User's Security Setup, and User Profile tab after logging into back office for the first time. The new password must be PCI compliant, containing at least 8 alphanumeric characters with both letters and numbers.

The SimVen back office' installation automatically creates a SQL Server Login and a Database User with username (TANADMIN) and password. The same credentials are being used by the Mertech SQL Driver to log into the Microsoft SQL Server database. Before any code can execute SQL statements to the Microsoft SQL Server database, the database requires a username and password in the SQL string.

SimVen Access Controls

Overview

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 11 - Security Profile Management - Group Profiles.

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

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

4. The item appears in the **Selected Items 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 2-5 until all desired securable item authorizations are added or removed for the group.
7. Click **Save**.

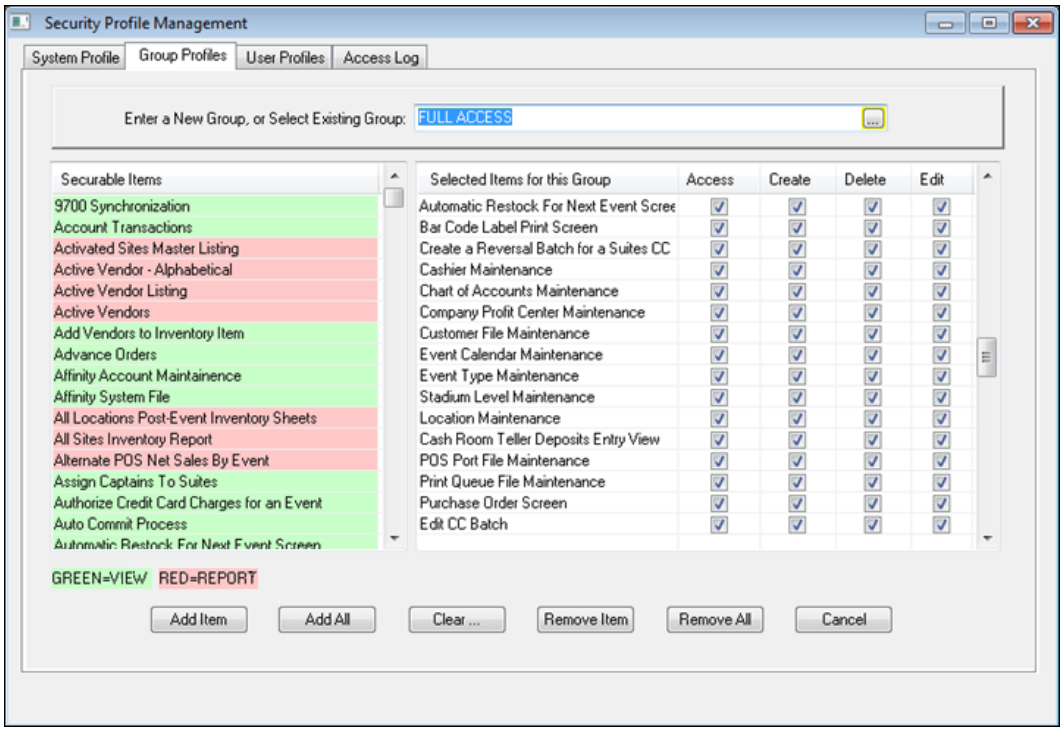


Figure 11 - Security Profile Management - Group Profiles

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 any 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**.

See Figure 12 - Security Profile Management - User Profiles.

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**.

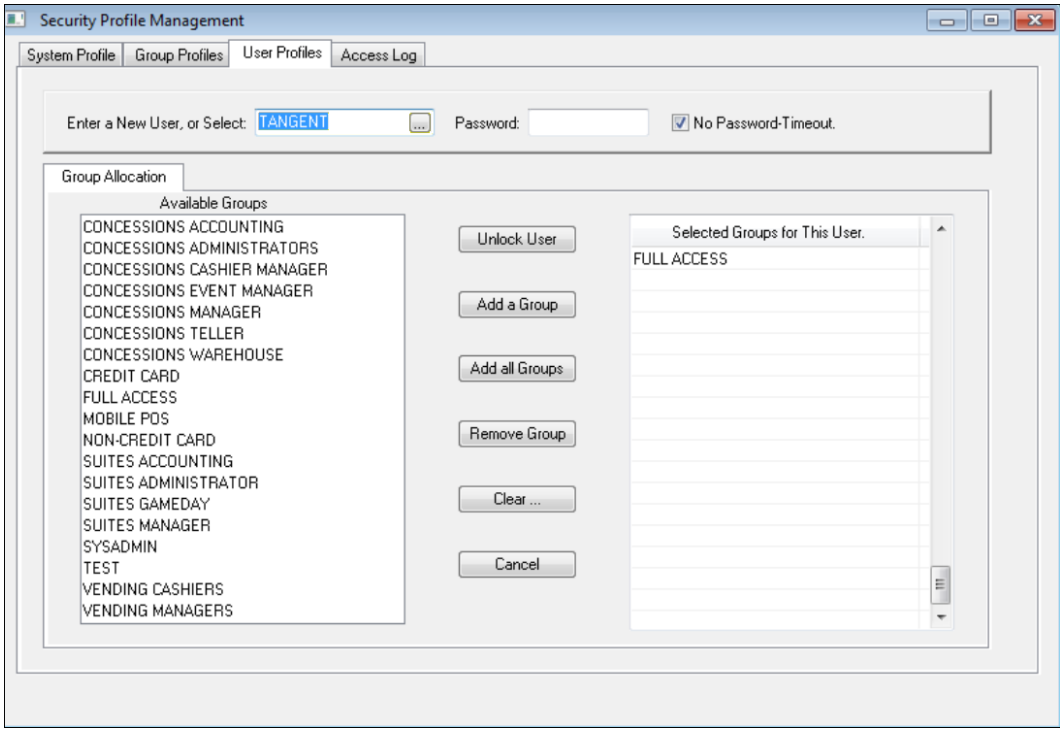


Figure 12 - Security Profile Management - User Profiles

Removing a Group

To remove 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

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

To create a new user:

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

See Figure 13 - Security Profile Management - Creating New Users.

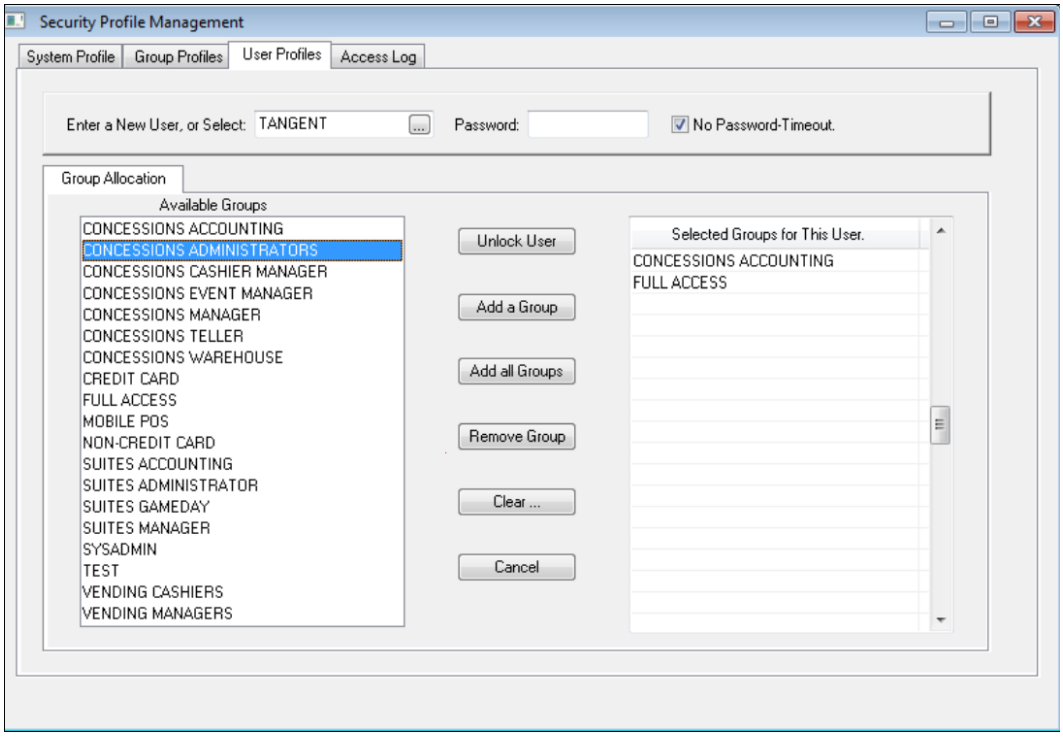


Figure 13 - Security Profile Management - Creating New Users

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 something like, Utility, or perhaps Sheila, and add this group in only her user profile. The number of groups that can be created is limited only by the size of the system's memory.

Tracking SimVen 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:

1. Navigate to <*Drive letter*>:\SimVen\Data\Tangent.Log and open the file using a text editor.

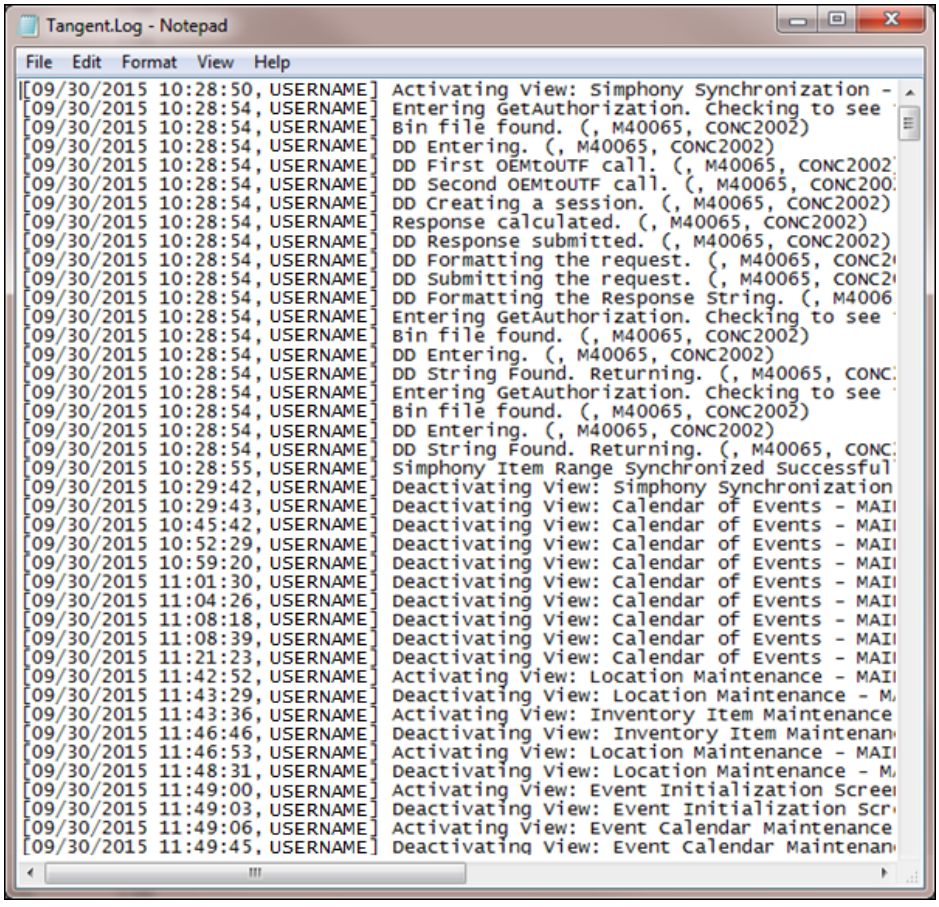


Figure 14 - Tracking Configuration and Edits - Tangent. Log file

Error Logging

Errors that have occurred in the SimVen back office application are written to the **TangetErr.Log** file. The file (as seen in **Figure 15 - Tracking System Errors - TangentErr.Log**) lists the date and time the error occurred, the error number, where the error occurred, and the error message.

Accessing the TangentErr.Log file

To access and review the TangentErr.Log file:

1. Navigate to <*Drive letter*>:\SimVen\Data\TangentErr.Log and open the file using a text editor.

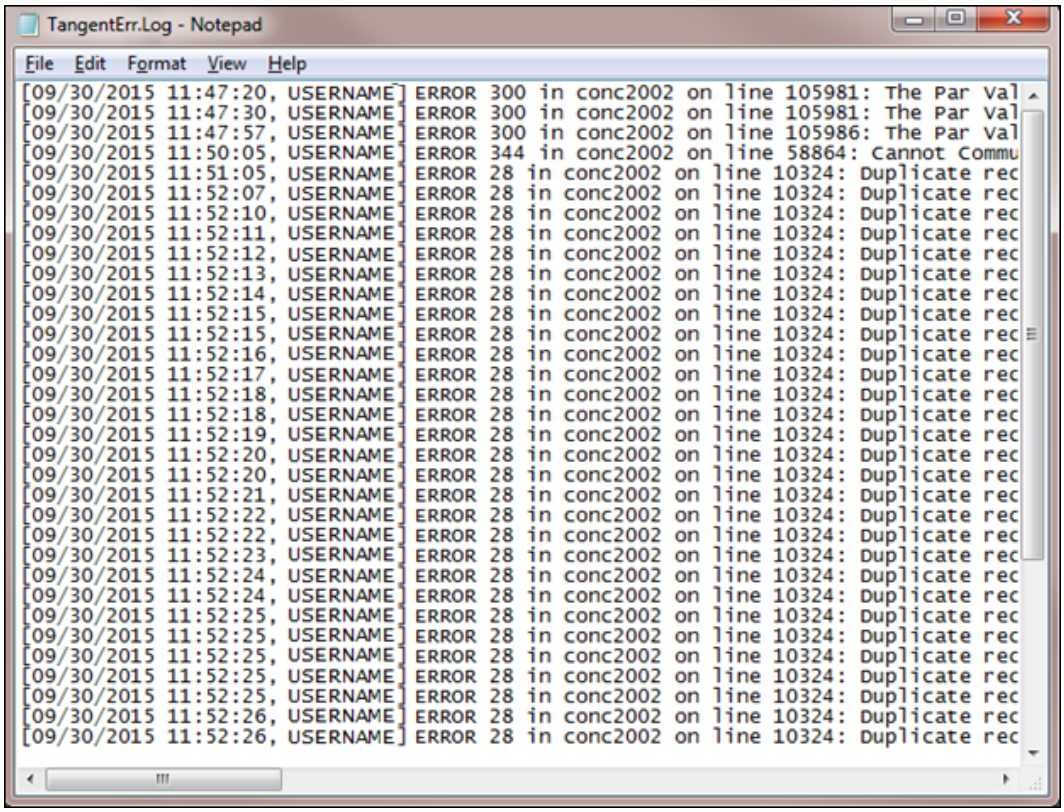


Figure 15 - Tracking System Errors - TangentErr.Log

SimVen Access Logging

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:

1. Navigate to the back office, Security, User's Security Setup, and click the **Access Log** tab.

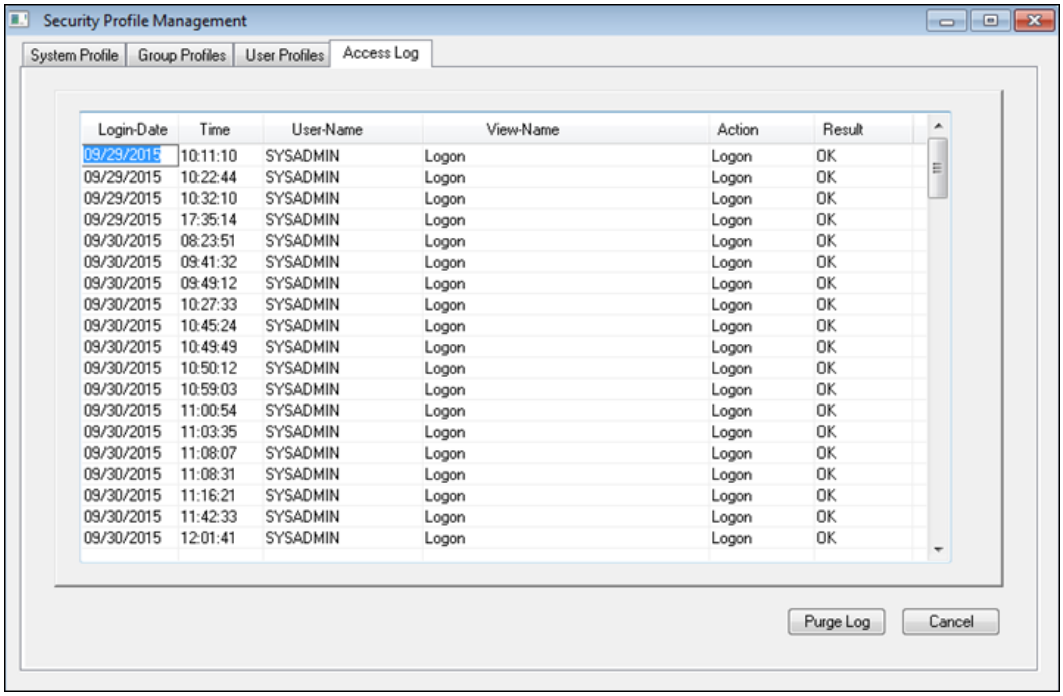


Figure 16 - Security Profile Management - Access Log tab

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
  - 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
  - Protect the Oracle listener
  - Monitor Oracle listener activity
  - Monitor who accesses your systems
  - Check network IP addresses
  - Encrypt network traffic
  - Harden the operating system security

Appendix B SimVen Port Numbers

Port Numbers

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

Enterprise Ports

Table 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 - Property Ports

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