Oracle® MICROS Simphony
Security Guide

Release 19.1
F15062-03
December 2020

Oracle MICROS Simphony Security Guide, Release 19.1

F15062-03

Copyright © 2010, 2020, Oracle and/or its affiliates.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or "commercial computer software documentation" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government’s use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

Preface

1 Simphony Security Overview

Basic Security Considerations 1-1
Service-Oriented Architecture (SOA) 1-2
Authentication 1-2
- EMC Authentication 1-3
- Workstation Authentication 1-3
- User Authentication 1-4
- Running a Workstation Securely with Windows Standard Users 1-4
- Database User Management 1-4

Understanding the Simphony Environment 1-4
Recommended Deployment Configurations 1-5
Operating System Security 1-6
Database Security 1-6
- Oracle Database 1-6
- Database Engine Not Present on Workstations (Windows-based Workstations only) 1-6
- Database Engine Exists on Workstations (Windows-based Workstations only) 1-7
- Database on Linux for MICROS Workstations 1-7

2 Performing a Secure Simphony Installation

Pre-Installation Configuration 2-1
Simphony Installation 2-1
Multi-Factor Authentication 2-2
Simphony MFA Configuration Prerequisite Requirement 2-2
Simphony MFA Configuration During the Installation of Simphony 2-3
Accessing the Simphony EMC Using MFA for the First Time 2-3
Assigning MFA EMC Access Privileges 2-4
Enrolling Users MFA Email Addresses and Passwords 2-5
Setting the Max Allowed Failed Logins for EMC Access 2-6

Configuring the SMTP and Backup SMTP Servers in the EMC 2-7
Configuring Workstation Database Passwords in the EMC 2-8
Post-Installation Configuration 2-10
Operating System 2-11
Application 2-11
Database Platform 2-11
Passwords Overview 2-12
Changing Default Passwords 2-13
Forgotten Password Recovery 2-13
Resetting Passwords from the Simphony Web Portal 2-14
User Profile Page 2-15
Configuring Security Questions 2-16
Configuring User Accounts and Privileges 2-16
Encryption Keys 2-16
Integrity Keys 2-17
Changing Database Passwords 2-17
Data Purging 2-19

3 Implementing Simphony Security

Authorization Privileges 3-1
Roles 3-6
EMC Configuration 3-7
Employee IDs 3-11
Employee Levels 3-12
Employee Levels and Roles 3-13
Employee Level Configuration Best Practices 3-13
Employee Groups 3-14
Configuration of Employee Groups 3-14
Job Code Overrides 3-15
Configuring Job Code Overrides 3-15
Workstation Security 3-16
Assigning Privileges to Allow Installing and Authenticating Workstation Clients 3-16
Hardening Security for Workstation USB Ports 3-16
Audit Trail 3-17
Audit Trail Search Parameters 3-18
Audit Trail Search Results 3-21
Other Audit Trail Considerations 3-23
Audit Trail Purging 3-25
Encryption 3-26

4 Appendix A: Simphony Port Numbers

Port Numbers 4-1
Enterprise Ports 4-1
Property Ports 4-1
Traffic Note 4-2
Interface Ports 4-2
iCare/Loyalty Ports 4-3
Oracle Component Ports 4-3

5 Appendix B: Module Accessibility

6 Appendix C: Key Manager Manual

General Information 6-1
About the Simphony Encryption Key Manager Module 6-1
D-Secure Key Practices 6-1
Key Manager Security Enhancements 6-1
The Encryption Scheme 6-2
Operational Considerations 6-2
Periodic Key Rotation 6-2

7 Appendix D: Key Manager Module

Operating Conditions 7-1
Authorizations 7-1
Key Manager Module 7-2
Changing the Pass Phrase 7-2

8 Appendix E: Simphony Payment Interface

Configuration Requirements for PSP using Transport Layer Security (TLS) in EMC 8-1
No TLS Support 8-1
TLS Server Certificate Support 8-1

Preface

Oracle MICROS Simphony is a cloud-based Point-of-Sale (POS) solution that provides business management capabilities using a single tool with vast integration capabilities to property management systems, paperless kitchen display systems, credit card interfaces, and reporting applications.

Purpose

This document provides security reference and guidance for Simphony.

Audience

This document is intended for:

- System administrators installing Simphony
- End users of Simphony

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

Product documentation is available on the Oracle Help Center at https://docs.oracle.com/en/industries/food-beverage/pos.html.

Revision History

Date	Description of Change
January 2020	Initial publication.
April 2020	Conversion of the document to HTML format.

Date	Description of Change
December 2020	• Added the **Configuring Workstation Database Passwords in the EMC** topic to Chapter 2. • Updated the **Changing Database Passwords** section of **Post-Installation Configuration** topic in Chapter 2.

1

Simphony Security Overview

This chapter provides an overview of Oracle MICROS Simphony security and explains the general principles of application security.

- Basic Security Considerations
- Service-Oriented Architecture (SOA)
- Authentication
- Understanding the Simphony Environment
- Recommended Deployment Configurations
- Operating System Security
- Database 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 Installation for more information.
- Learn about and use the Simphony security features. See Implementing Simphony Security for more information.
- Use secure development practices. For example, take advantage of existing database security functionality instead of creating your own application security.
- 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, located at http://www.oracle.com/technetwork/topics/security/alerts-086861.html to access this information.
- Testing is performed regularly with Simphony along with the latest Oracle and Microsoft software patches.

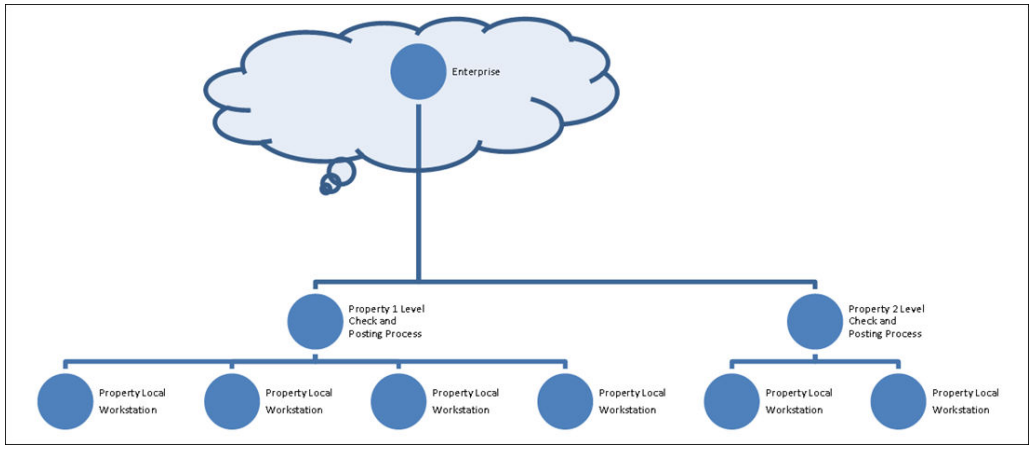
Service-Oriented Architecture (SOA)

Simphony uses a Service-Oriented Architecture (SOA) that is an essentially a collection of loosely coupled services. Rather than stand-alone applications, all application pieces in Simphony are services that can be deployed anywhere in the enterprise, limited only by network topology.

The Simphony architecture leads to a more scalable and reliable system compared to server-based models since services are distributed and do not have to be located on a single machine; if web services are running on application servers and the servers can communicate with the database, the workstations function in online mode.

Simphony's SOA uses industry standard SOAP services that provide greater ability to work with third-party applications. The SOA also controls the way that workstations interface with other applications or devices. Interfaces become services that can run centrally or locally.

Figure 1-1 Simphony Server-Oriented Architecture



See the Oracle MICROS Simphony Installation Guide, specifically the **Implementation Deployment Scenarios** section for more information.

Authentication

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.

- EMC Authentication
- Workstation Authentication
- User Authentication
- Running a Workstation Securely with Windows Standard Users
- Database User Management

EMC Authentication

All users' credentials of Simphony are stored in the central database. Anyone who has access to the Enterprise Management Console (EMC) must provide a login of a valid username/password. No two Simphony users can have the same username. Provided client site maintains proper configuration and adheres to privilege level restrictions based on a need-to-know basis, each user's activities are traced via the Audit Trail. To ensure strict access control of the Simphony application, always assign unique usernames and complex passwords to each account. Refer to the *Simphony PA DSS Implementation Guide* for more information about creating complex passwords.

Workstation Authentication

Simphony architecture supports both the server side and client side of authentication. Server authentication is accomplished via configuring the HTTPS connection by installing a TLS 1.2 compliant certificate on the server issued by Certification Authority. Client side authentication is required for Simphony operations and cannot be disabled.

> **Note:**
>
> Simphony security does not use the Windows Login on Windows-based workstations.

In order for the Simphony workstation to be able to communicate to a Simphony application server, it has to be authenticated first. The process of authentication is accomplished during initial workstation installation by the Client Application Loader (CAL). When CAL starts, it prompts users to enter credentials when configuring workstations. In order to configure, download, and install software, users must be authorized using the Enterprise Management Console (EMC). To add this privilege, see Assigning Privileges to Allow Installing and Authenticating Workstation Clients.

The username and password entered on the service host are the same as the one used to access the EMC. If a user does not have the privilege assigned to their Role, the process fails and the user is prompted to enter a valid username and password again.

When upgrading a workstation (from Simphony release 2.8 or later), the existing authentication continues to work, however when prompted, the new EMC credentials should be provided. Credentials are transmitted over an encrypted TLS channel to the application server. After the application server validates the credentials, an authentication token is issued that is returned to an encrypted channel back to the client. The token is stored by the client in an encrypted format inside its protected storage. All subsequent messages from the client to the server contain a security header that is encrypted with the public half of the key contained within the authentication token. The server stores a private key for each authenticated client in the database and can verify authenticity of an incoming request. With the Simphony version 2.9.1 release and later, a kitchen display system (KDS) Display now requires an initial authentication. Previously, KDS Displays they were not authenticated.

User Authentication

In addition to a workstation authenticating itself on a Simphony network, a user must authenticate themselves through the workstation by signing in using a unique employee ID number or an employee magnetic card.

Running a Workstation Securely with Windows Standard Users

On workstations running Microsoft Windows, workstations can be configured with Microsoft Windows standard user credentials, instead of using an administrative user. However, in order to successfully install the CAL client, users need to provide administrative credentials when using a Microsoft Windows standard user. After a successful installation and configuration of a service host (Ops), workstations can be run with Microsoft Windows standard user. Using as standard user minimizes the risk of remote code execution and other exploits.

On workstations running Linux for Micros, the application operating system users are preconfigured. During setup an additional support user is created with an administrator entered password. This user is intended to be used for support purposes only and the password should be kept secure. Daily operations do not require an explicit operating system user login, and Simphony runs under a preset standard user.

See the *Oracle MICROS Simphony Configuration Guide* for more information about installing CAL clients.

Database User Management

Oracle Food and Beverage mandates that users create a different, strong password for the pre-defined Simphony user within the EMC's Enterprise Level, Personnel, and Employees module. The password must be at least 8 characters long and include letters and numbers. Simphony's installation wizard prompts for a unique System Administrator username and password to begin the installation. The System Administrator is used to log into the Oracle Database. Simphony's installation wizard also prompts for the creation of a System Database User. Simphony's uses the database user credentials to access the database during communication with services. Oracle Food and Beverage mandates using a unique username and a complex password consisting of more than eight characters including alphanumeric and special characters.

Security Note

Database authentication credentials are stored in the configuration file (DBSettings.xml) on the Simphony application server, protected by Microsoft Windows Server file permissions. No applications, except for the application server, need access to the database directly. After the initial authentication, the application server performs a check of the authorization for the given user to perform the requested action.

Understanding the Simphony Environment

When planning your Simphony 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 happens if protections of 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 helps you protect it properly.

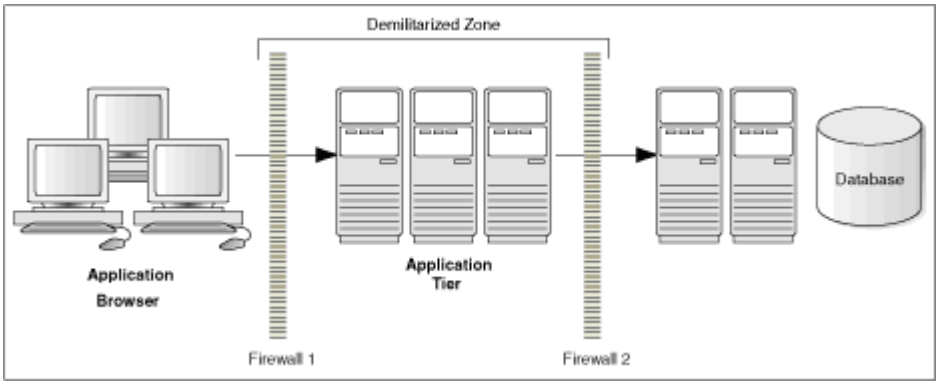
Recommended Deployment Configurations

This section describes recommended deployment configurations for Simphony.

The Simphony product is deployed on a cluster of servers. The simplest deployment architecture is the Server-Oriented Architecture (SOA) shown in Overview of Simphony Security.

The general architectural recommendation is to use the well-known and generally accepted Internet-Firewall-DMZ-Firewall-Intranet architecture shown in the following figure.

Figure 1-2 Traditional DMZ



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

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

See Port Numbers in Appendix A for more information about Simphony network port usage.

Operating System Security

Prior to Simphony installation, it is essential that the operating system be updated with the latest security updates. See the Oracle Food and Beverage Compatibility Matrix for more information about supported operating systems.

See the following Microsoft TechNet site for more information about operating system security: Microsoft Windows Server Security.

Database Security

- Oracle Database
- Database Engine Not Present on Workstations (Windows-based Workstations only)
- Database Engine Exists on Workstations (Windows-based Workstations only)
- Database on Linux for MICROS Workstations

Oracle Database

Transparent Data Encryption

The Oracle Database versions supported by Simphony 19.1.x, include Oracle Database 18c, Oracle Database 12c Release 2, and Oracle Database 12c Release 1. Each version provides Transparent Data Encryption (TDE) capabilities. TDE protects data at rest by way of automatically encrypting/decrypting sensitive data that is stored in tables and tablespaces used by Simphony. Oracle MICROS strongly recommends enabling TDE at the Oracle Database. More information about TDE can be found at:

Introduction to Transparent Data Encryption for 12c

Oracle Database Advanced Security Guide for 18c

See the Oracle Database Security Guide for more information about Oracle Database security.

Database Engine Not Present on Workstations (Windows-based Workstations only)

Install the supported Microsoft SQL Server version service packs level of the full version of Microsoft SQL Server Express.

- **Windows POSReady 2009**: SQL Server 2008 R2 SP2 – Express Edition
- **Microsoft Windows 7 or later**: Microsoft SQL Server 2012 SP4 Express (x86)

Database Engine Exists on Workstations (Windows-based Workstations only)

Best Practices

On an installed instance of Microsoft SQL Server Express on the workstation, Oracle Food and Beverage recommends that you apply the latest security updates and critical updates including general distribution releases (GDRs), service packs (SPs), and cumulative updates (CUs).

Applying Updates

Microsoft SQL Server updates are available through **Microsoft Updates** (MU), **Windows Server Update Services** (WSUS) and the **Microsoft Download Center**. Security and Critical updates for Microsoft SQL Server are available through Microsoft Updates, and to be able to view these updates, you need to opt-in to MU through the Microsoft Windows Updates applet from the **Control Panel**.

When you receive an update through Microsoft Updates, the system updates all Microsoft SQL Server features to the latest version in an unattended mode.

Source

See Install SQL Server Servicing Updates for Microsoft recommendations.

Additional Microsoft SQL Server Information

Table 1-1 Microsoft SQL Server 2008 R2

Latest Service Pack	Source
Microsoft SQL Server 2008 R2 Service Pack 3 (extended support ends on July 9, 2019)	Microsoft SQL Server 2008 R2 Service Pack 3 - EOL Microsoft SQL Server 2008 R2 Service Pack 3 - Release Notes

Table 1-2 Microsoft SQL Server 2012

Latest Service Pack	Source
Microsoft SQL Server 2012 Service Pack 4 (extended support ends on July 12, 2022)	Microsoft SQL Server 2012 Service Pack 4 - EOL Microsoft SQL Server 2012 Service Pack 4 – Release Notes

Database on Linux for MICROS Workstations

The database is automatically installed during installation of the application on workstations running on Linux for MICROS. Oracle makes security updates available via the Simphony Enterprise system, and it is important that such updates are taken and deployed.

2

Performing a Secure Simphony Installation

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

- Pre-Installation Configuration
- Simphony Installation
- Multi-Factor Authentication
- Simphony MFA Configuration Prerequisite Requirement
- Simphony MFA Configuration During the Installation of Simphony
- Accessing the Simphony EMC Using MFA for the First Time
- Assigning MFA EMC Access Privileges
- Enrolling Users MFA Email Addresses and Passwords
- Setting the Max Allowed Failed Logins for EMC Access
- Configuring the SMTP and Backup SMTP Servers in the EMC
- Configuring Workstation Database Passwords in the EMC
- Post-Installation Configuration

Pre-Installation Configuration

Prior to installation of Simphony, perform the following tasks:

- Apply critical security patches to the operating system.
- Apply critical security patches to the database server application.
- Review the Oracle Hospitality Enterprise Back Office Security Guide.
- Review the Oracle MICROS Hardware Wireless Networking Best Practices Guide.
- Create Oracle Database Tablespaces per the instructions in the Oracle MICROS Simphony Installation Guide. Tablespace requirements may vary based on the customer's specifications.
- Acquire TLS 1.2 compliant security certificate from a valid Certification Authority (CA).

Simphony Installation

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

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

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

Beginning with Simphony release 2.9.1, Simphony security requires installing a digital certificate. Oracle Food and Beverage recommends acquiring a certificate from a Certificate Authority (CA) prior to performing a Simphony software upgrade. Internet connectivity is a prerequisite for Simphony to successfully validate digital certificates.

Required Websites and Services for Simphony

The following Simphony websites and services are required for proper operation of the system:

- EGateway
- WCC
- WS
- API
- SimphonyApp
- ImportExportAPI
- EngagementApp
- EngagementAPI
- HMC

The following Simphony services are required for proper operation of the system:

- Data Posting Service (DPS)
- Data Transfer Service (DTS)
- Sequencer Service
- Data Request Processing System (DRPS)

Multi-Factor Authentication

In Simphony release 18.1 and later, Multi-factor Authentication (MFA) is enabled by default.

You can configure Simphony to provide users a one-time password through email in two ways:

1. During the installation of the Simphony software.
2. After the installation of the Simphony software, using the Simphony EMC.

Simphony MFA Configuration Prerequisite Requirement

For MFA implementation, you must install and make network accessible, two separate Simple Mail Transfer Protocol (SMTP) email servers (each to be designated as either a Primary or Backup server). This allows you to receive a one-time-password (OTP) via email, each time you attempt to log onto the EMC. An SMTP Backup server is

required to provide EMC access redundancy in the event that the Primary SMTP server fails for any reason.

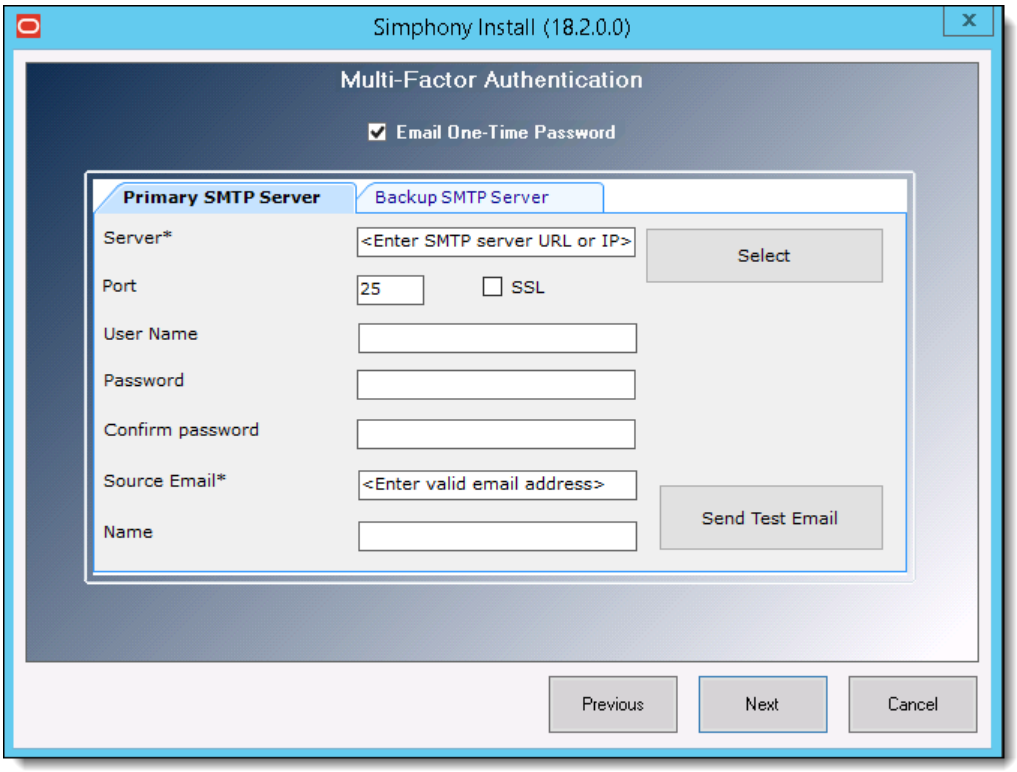
Simphony MFA Configuration During the Installation of Simphony

When running the Simphony 18.2 installation application, you are prompted to configure MFA. Your choices are:

1. To bypass the MFA SMTP server's configuration until after Simphony has been installed, deselect the **Email One-Time Password** check box, and then click **Next**.
2. To configure MFA SMTP servers at this time, see Configuring the SMTP and Backup SMTP Servers in the EMC for configuration instructions.

It is important to note that if you are performing a Simphony Standard Cloud Service installation, the MFA configuration that is completed during the installation of Simphony is duplicated for each enterprise. After Simphony has been installed, you can go back and make edits in the EMC for individual enterprises (or organizations) that might have differing SMTP servers or settings from each other.

Figure 2-1 Simphony Install MFA Configuration



Accessing the Simphony EMC Using MFA for the First Time

To configure MFA on your Simphony system:

1. When first attempting to log on to the Simphony EMC, when prompted, enter your user name in the **User Name** field, and enter your email address in the **Email Address** field.
2. Re-enter your email address in the **Confirm Email Address** field and then click **Register**.

   Your registered email address is written to your EMC employee record. This email address is used to send you the one-time-password (OTP) each time you attempt to log on to the EMC.
3. Access the email account you registered in step 1 and open the email containing the OTP.
4. Enter the temporary password in the **One-Time Password** field and then click **Enter**.

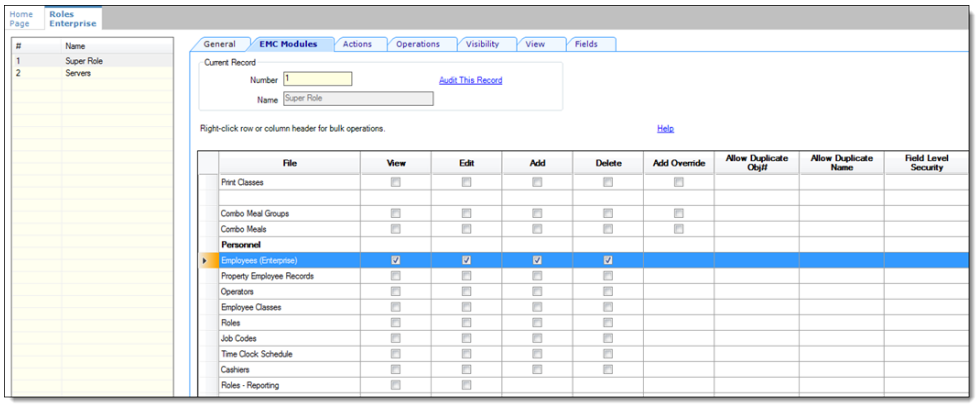
   Newly generated OTP passwords expire and become invalid after five minutes. If the OTP's five minute threshold is exceeded, you are required to log in again to the EMC to generate another OTP. After entering a valid OTP, the EMC opens.

Assigning MFA EMC Access Privileges

To access and configure MFA security for other users on your system, you need to be assigned the correct privileges in the EMC.

1. Select the **Enterprise** level, click **Configuration**, and then click **Roles**.
2. Click the **EMC Modules** tab and scroll to the Personnel section.
3. Select the check boxes for the **Employees (Enterprise)** access privileges for each of the following columns:
   - View
   - Edit
   - Add
   - Delete

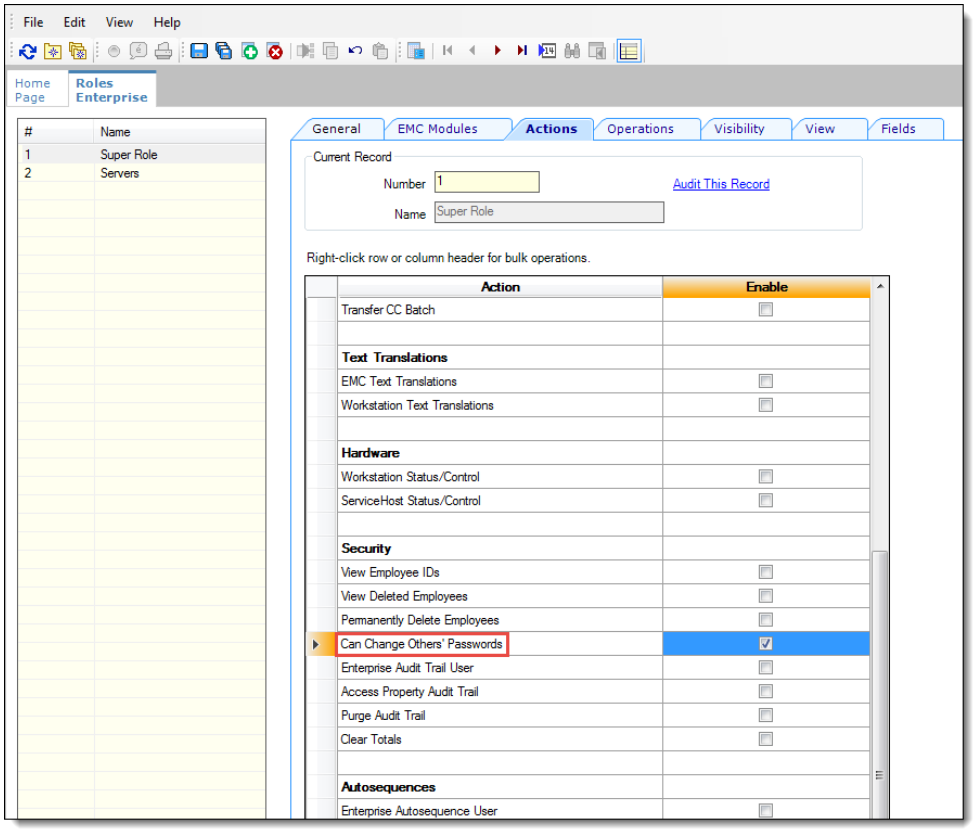
Figure 2-2 Roles Options for Assigning MFA Privileges



4. Click **Save**.

5. Click the **Actions** tab, scroll through the Action column until you reach the Security section, select the **Can Change Others' Passwords** check box, and then click **Save**.

Figure 2-3 Roles Option for Changing Other's Passwords



6. Ensure that all users requiring MFA configuration permissions are assigned a Role that have these access privileges enabled.

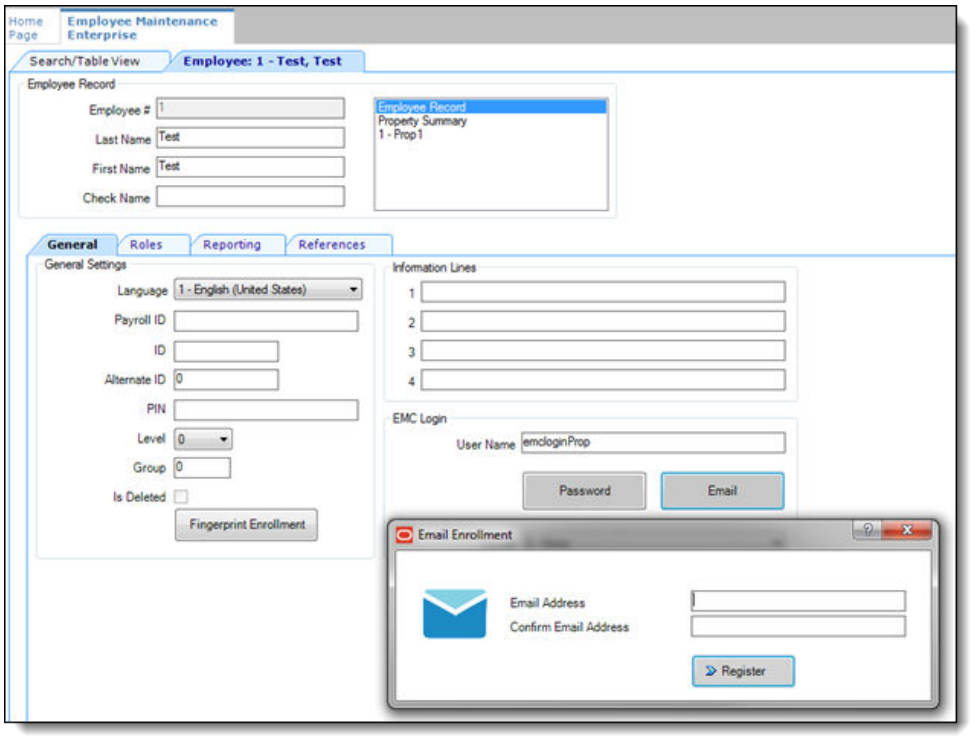
Enrolling Users MFA Email Addresses and Passwords

After installing or upgrading to Simphony release 18.1 or later, every user with access to the EMC is prompted to enter and register their email address during their first attempt to log on to the EMC. If the system detects that your email address has already been registered (by another privileged user), you simply need to enter your EMC user name and password and the system will email your OTP to the email address that was provided.

To enroll a user's email address using the EMC:

1. Select the **Enterprise** level, click **Configuration**, and then click **Employee Maintenance**.
2. Search for the employee record that requires editing.
3. Click the **Email** button and enter the user's email address in the **Email Address** field. Re-enter the email address in the **Confirm Email Address** field and click **Register**.

Figure 2-4 Email Enrollment



4. If a user's email address changes, click the **Email** button and enter the user's **Current Email Address** (that is already registered on the system), new **Email Address**, and then re-enter the address in the **Confirm Email Address** field and click **Register**.

Setting the Max Allowed Failed Logins for EMC Access

MFA adheres to the following EMC account lock out setting:

1. Select the **Enterprise**, click **Setup**, click **Enterprise Parameters**, and then click the **Login** tab.
2. From the Options section, set the value for the **Maximum Allowed Failed Logins** field.

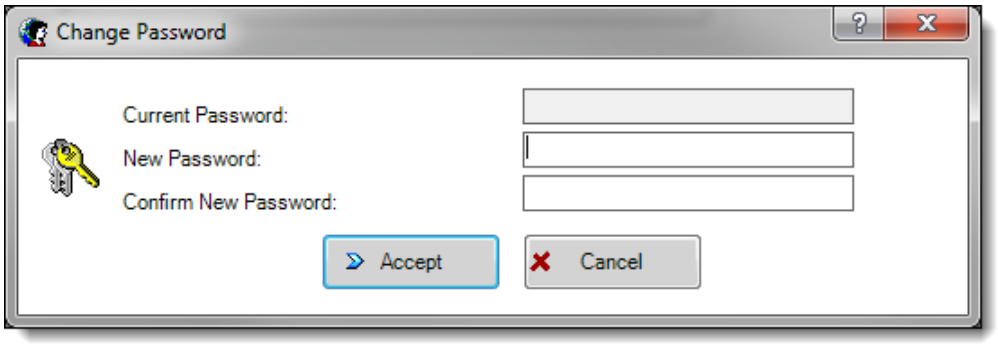
After reaching the failed login threshold (based on entering an invalid EMC user or OTP password), users are notified that their login was rejected by the system and that their account is currently locked out.

To assign a new user's EMC password (or to reset a password due to an account being locked out):

1. Select the **Enterprise** level, click **Configuration**, and then click **Employee Maintenance**.
2. Search for the employee record that requires editing.
3. Click the **Password** button and enter a password in the **New Password** field. Re-enter the email address in the **Confirm Password** field and click **Accept**.

   No entry is required in the **Current Password** field, as it is inaccessible.

Figure 2-5 Change Password



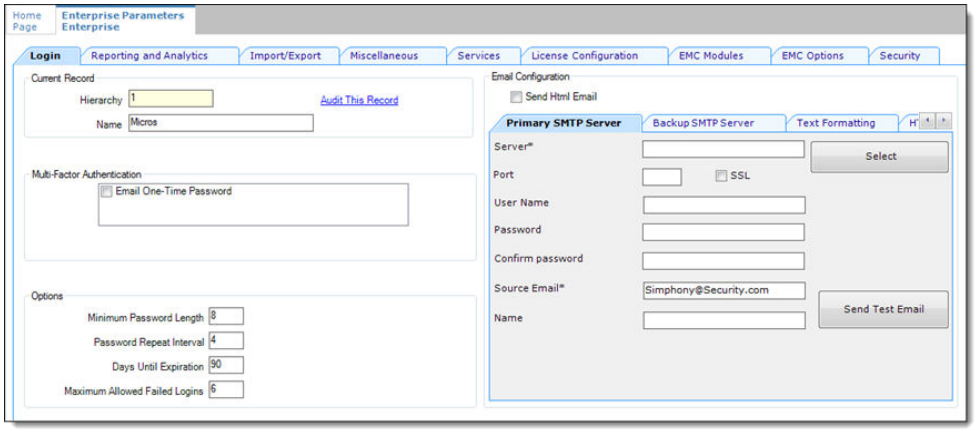
When the user attempts their next EMC login, the system prompts them to enter a new password (known only to that user).

Configuring the SMTP and Backup SMTP Servers in the EMC

SMTP and Backup SMTP server settings are configured and saved at the Enterprise level. To configure the SMTP servers, navigate the EMC as follows:

1. Select the Enterprise level, click **Setup**, click **Enterprise Parameters**, and then click the **Login** tab.
2. Within the Multi-Factor Authentication section, select **Email One-Time Password**.

Figure 2-6 Enterprise Parameters SMTP Server Settings



3. From the Email Configuration section, select the **Primary SMTP Server** subtab and enter the settings in the fields listed below (an asterisk * denotes a required field setting):
   - (Required) **Server***: Enter either the IP address or the name of your site's Primary SMTP server.
     - If you do not have a SMTP email server available to you, click the **Select** button to choose a publicly accessible email provider, and then click **OK**.

  - When you select a public email provider, the **Server** field auto-populates with an SMTP server name that includes the selected email provider's naming convention (for example, SMTP.GMAIL.COM).
- **Port**: Enter a port number for the SMTP server or utilize the defaults.
- **SSL**: Select to require secure Internet communication using HTTPS.
- **User Name**: Enter a user name of the email address that sends the OTP.
- **Password**: Enter the password associated with the email User Name and re-enter it in the **Confirm password** field for verification.
- (Required) **Source Email***: Enter the full email address. This email address is shown as the sender of all OTP emails.
- (Optional) **Name**: Enter an alternate (alias) name for the Source Email sender.

4. Click the **Backup SMTP Server** subtab and enter the IP address or server name of the Backup SMTP server.
5. Enter information in the fields as listed above for the SMPT Backup server.
6. Click **Save**.
7. On the **Primary SMTP Server** tab, click the **Send Test Email** button to confirm the SMTP server's configuration and that the OTP email is received. Repeat this step on the **Backup SMTP Server** tab to confirm the functionality.

Configuring Workstation Database Passwords in the EMC

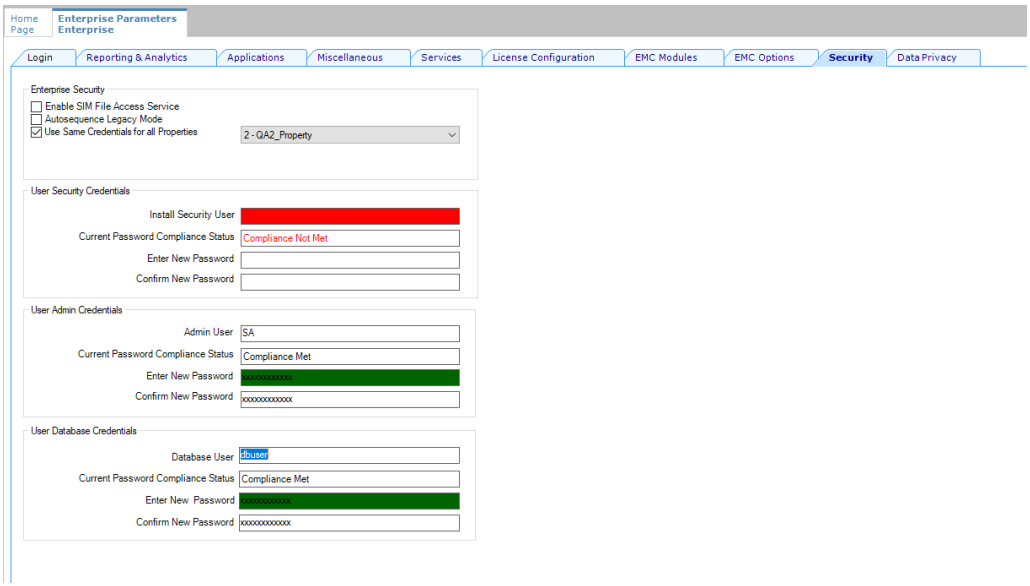
To maintain workstation database access control, you must assign unique usernames and complex passwords in the Simphony EMC. This is a required pre-installation step that ensures workstation security.

Simphony allows EMC administrators to configure strong passwords for workstation local databases at either the Enterprise or Property level before installation.

At the Enterprise Level

1. Select the Enterprise, click **Setup**, click **Enterprise Parameters**, and then click the **Security** tab.
2. In the **Enterprise Security** section, enable the **Use Same Credentials for all Properties** checkbox and select any arbitrary property from the drop-down list.
3. In the **User Admin Credentials** section, enter a username and a desired password that complies with your password complexity policy.
4. In the **User Database Credentials** section, enter a username and a desired password that complies with your password complexity policy.
5. Save changes.

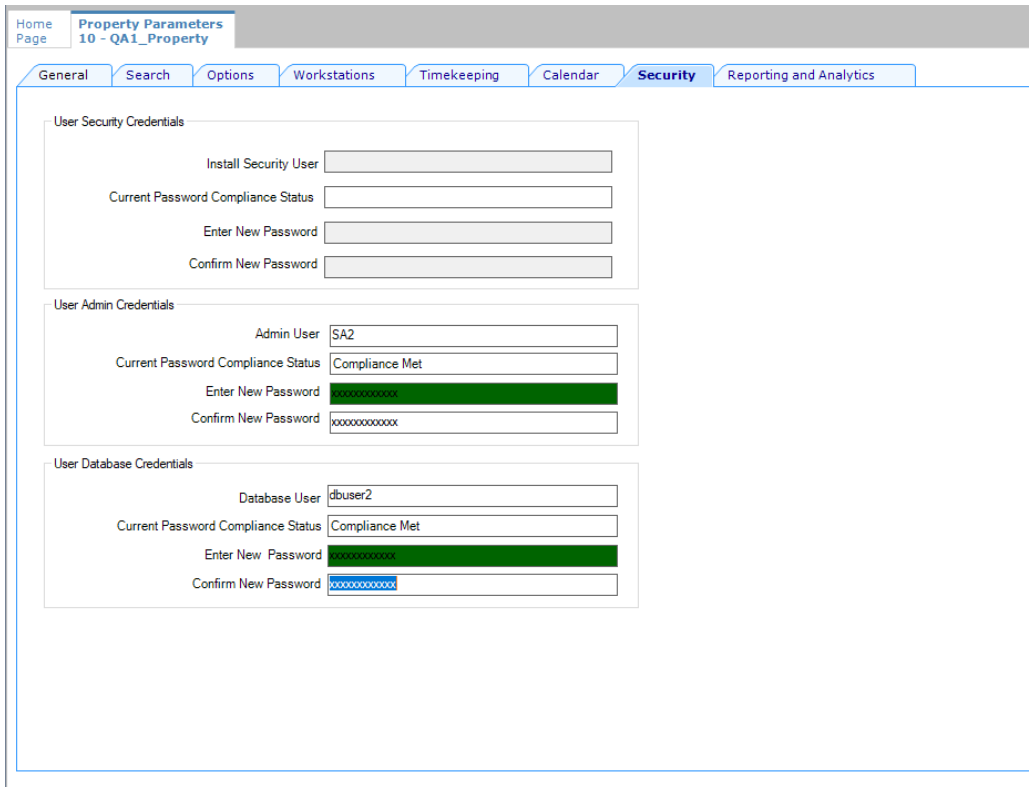
Figure 2-7 Enterprise Level Configuration



At the Property Level

1. Select the Property level, click **Setup**, click **Property Parameters**, and then click the **Security** tab.
2. In the **User Admin Credentials** section, enter a username and a desired password that complies with your password complexity policy.
3. In the **User Database Credentials** section, enter a username and a desired password that complies with your password complexity policy.
4. Save changes.

Figure 2-8 Property Level Configuration



Post-Installation Configuration

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

- Operating System
- Application
- Database Platform
- Passwords Overview
- Changing Default Passwords
- Forgotten Password Recovery
- Resetting Passwords from the Simphony Web Portal
- User Profile Page
- Configuring Security Questions
- Configuring User Accounts and Privileges
- Encryption Keys
- Integrity Keys
- Changing Database Passwords
- Data Purging

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.

Turning Off Remote Assistance

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

Browser Security

The Simphony solution requires the use of a web browser for some parts of the application. Users should configure the security settings for the web browser to disable features that are not required or that could cause security vulnerabilities.

Here are the commonly used browsers, and a link to the documentation that describes the security settings of each browser.

- **Internet Explorer**: http://windows.microsoft.com/en-us/internet-explorer/ie-security-privacy-settings
- **Mozilla Firefox**: https://support.mozilla.org/en-US/products/firefox/privacy-and-security
- **Google Chrome**: https://support.google.com/chrome#topic=3421433

Application

Software Patches

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

Security Certificates

It is required that Transport Layer Security (TLS) 1.2 (and higher) must be configured either on the load balancer or in Internet Information Server (IIS) for communication to Simphony Enterprise servers. The TLS 1.2 configuration process requires the use of a certificate generated by a trusted certificate authority. Refer to the *Oracle MICROS Simphony Installation Guide* for information about the installation of secure certificates.

Database Platform

Ensure that database login auditing is enabled.

Passwords Overview

The configuration of Simphony Enterprise passwords is performed in the EMC. Administrators are recommended to configure a strong password policy after initial installation of the application and to review the policy periodically.

Maintaining Strong Passwords

Ensure that passwords adhere to the following strength requirements:

1. The password must be at least 8 characters long and a maximum of 20 characters.
2. The password must contain letters, numbers, and special characters:

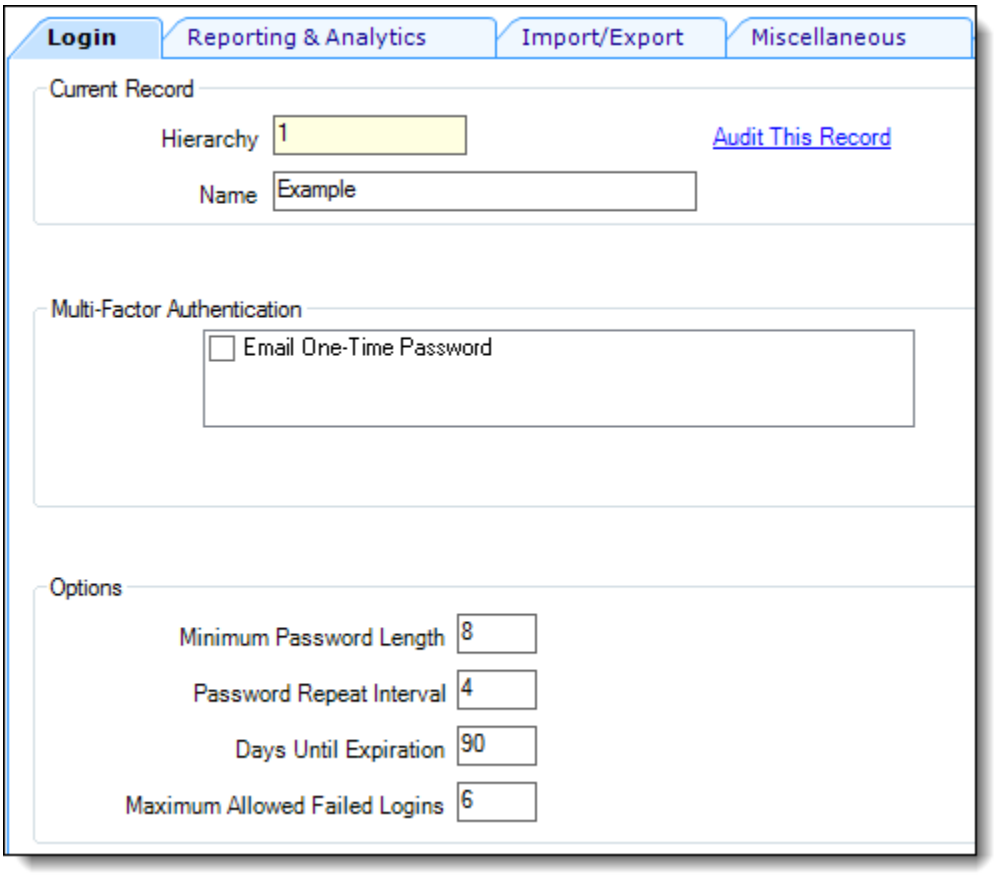
   ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~
3. The user must not choose a password equal to the last 4 passwords used.

Configuring Passwords for Simphony

In the EMC, **Enterprise Parameters** module, **Login** tab, **Enhanced Password Security** tab, configure the password policy options as follows:

1. Ensure that the **Minimum Password Length** is at least 8 characters.
2. Ensure that the **Password Repeat Interval** is at least 4.
3. Ensure that the **Days Until Expiration** is not greater than 90.
4. Ensure that the **Maximum Allowed Failed Logins** is not greater than 6.

Figure 2-9 Enhanced Password Security



Changing Default Passwords

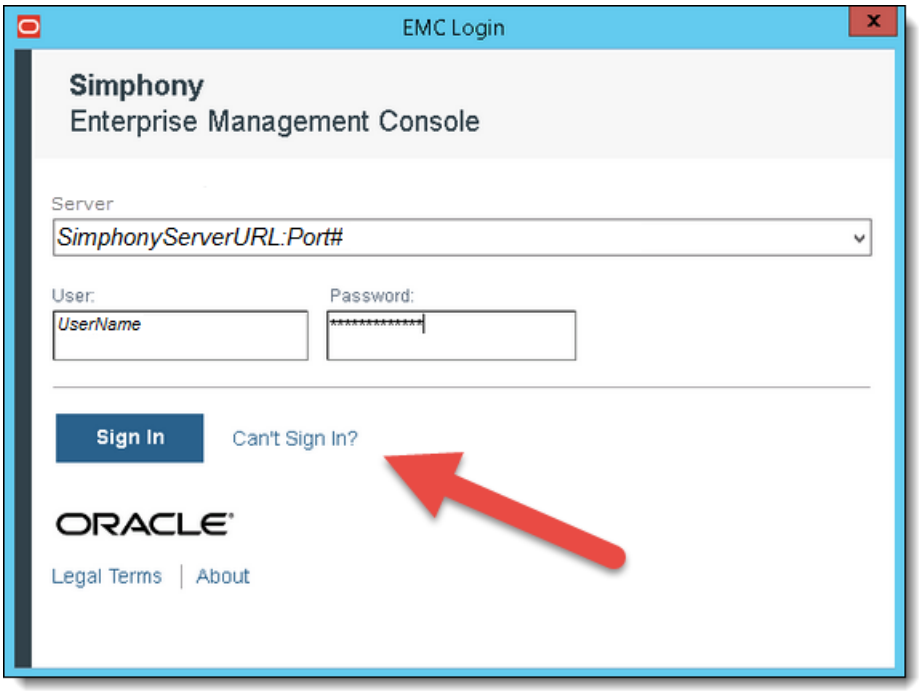
Oracle Food and Beverage mandates changing your master username and password in the EMC, following the guidelines above, after logging in for the first time.

Forgotten Password Recovery

In Simphony release 19.1 and later you can reset your own password. You are provided an option to reset the password using a **Can't Sign In?** link on the EMC sign-in screen. All privileged (and fully configured) users can initiate the resetting of their own password as well as for others. However, if you do not meet the following prerequisites, you must request to have a privileged supervisor initiate recovering your password:

- You do not have a valid email address configured within your employee record
- You have not configured your security questions and answers

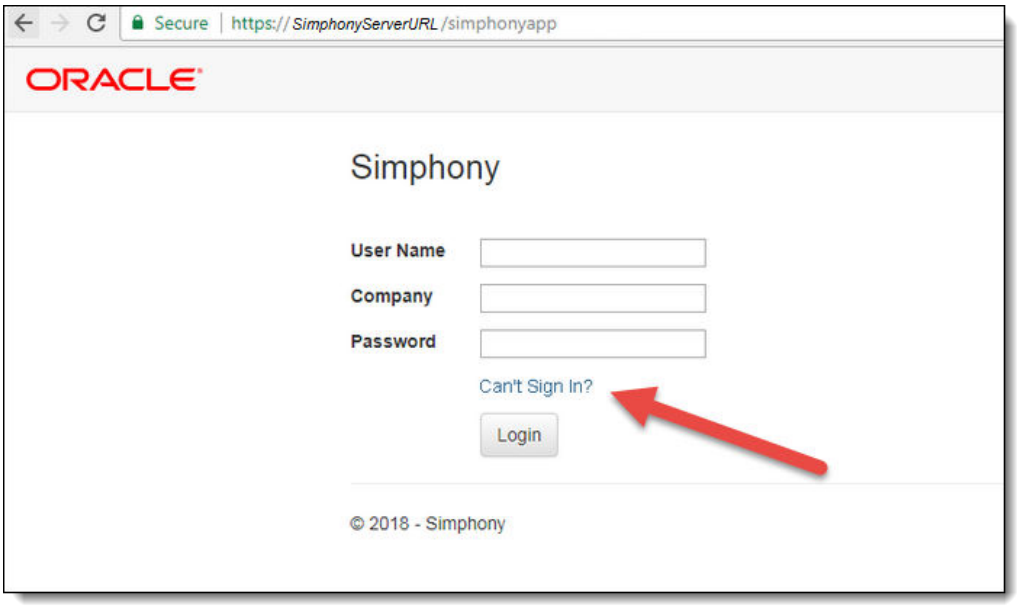
Figure 2-10 EMC Login Can't Sign In? Link



Resetting Passwords from the Simphony Web Portal

From the Simphony Web Portal logon window, enter your **Username** and click the **Can't Sign In?** link. You are provided with a One-Time Password (OTP) via email.

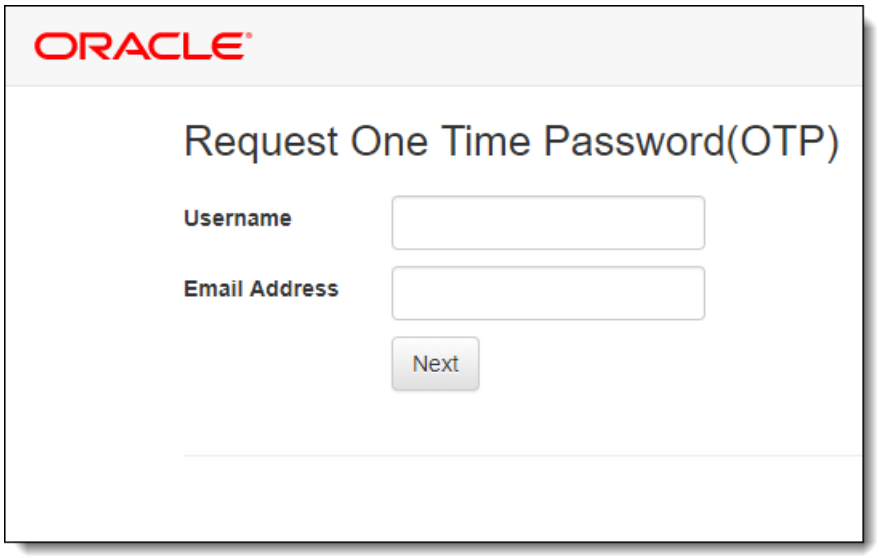
Figure 2-11 Simphony Web Portal Can't Sign In? Link



From here the following prerequisites are validated:

- In the Request One Time Password (OTP) window, you are asked to provide your registered user name and registered email address.

Figure 2-12 Simphony Request OTP



- This information is validated and you are sent to a details page where you must correctly answer your security questions as configured in the system.
- You must have a valid SMTP email server configured for the Enterprise to send you an email.

Upon entering your validated logon and security question responses, a OTP token is sent to your email account, and you are redirected to the Forgot Password page. You are prompted to enter your new password and the OTP received via email. The screen below shows the Simphony Web Portal page that is used to send a OTP to your registered email address.

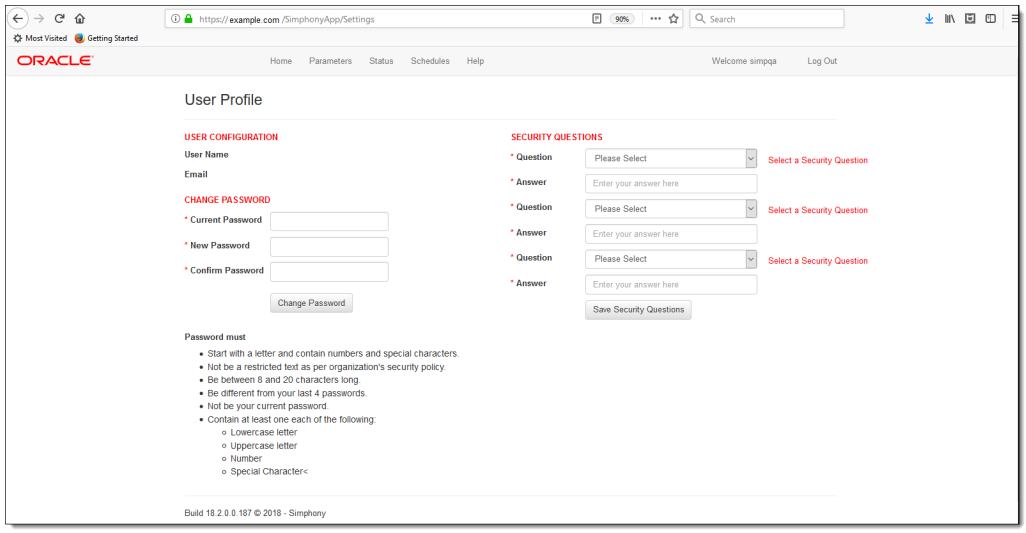
When you click the **Can't Sign In?** link from the EMC Sign-in screen, the system redirects you to the **Request One Time Password (OTP)** window of the Simphony Web Portal in a browser.

1. Enter your User Name.
2. Enter your email address.
3. Click **Next**.

User Profile Page

From the Simphony Web Portal, you can change your password and update your security questions. The following figure shows the default User Profile page.

Figure 2-13 User Profile Page

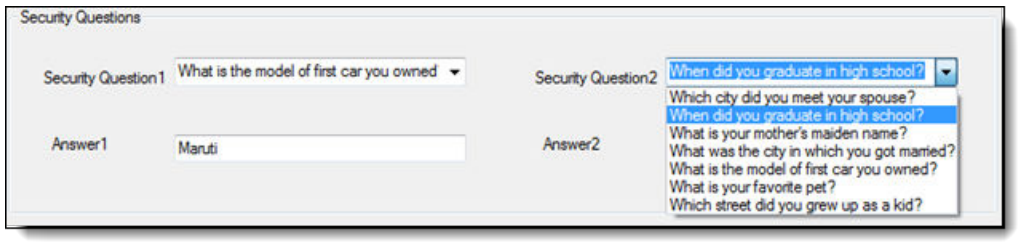


Configuring Security Questions

After you successfully log on to the EMC or to the Simphony Web Portal, if your security questions or email address have not yet been configured, you are prompted to configure them. The message prompt window contains a link to the User Profile page of the Import/Export application, which opens in a browser.

The following figure shows samples of the security questions that are available for you to provide responses as you configure the User Profile section.

Figure 2-14 Security Questions



Configuring User Accounts and Privileges

When setting up users of the Simphony application, ensure that they are assigned the minimum privilege level required to perform their job function. User privileges are described in the EMC Configuration section.

Encryption Keys

Simphony installs an encryption key using a default passphrase. Administrators need to rotate the encryption key on a regular interval. See Appendix C: Key Manager Manual for more information.

Integrity Keys

Simphony employs RSA 2048-bit keys to protect the integrity of certain sensitive files, such as SIM scripts. This allows workstations to ensure that the sensitive files have not been tampered with before executing them. Oracle Food and Beverage recommends that you rotate these keys at least once a year. See Appendix C: Key Manager Manual for more information.

Changing Database Passwords

Application Server

Crypt is a database credential management tool for the Simphony application. Crypt allows you to manage database users and their passwords, which are used to connect to the databases required for the proper operation of Simphony. For privileged users, the utility helps you:

- Test database connections
- Change database passwords
- Encrypt database passwords

> **Note:**
>
> The Crypt utility updates new passwords for the Simphony configuration files, but does not change passwords on the actual database platform. If you do not change the passwords for the database platform or if you enter incorrect passwords while using the Crypt utility, the database connection to the Simphony application fails.

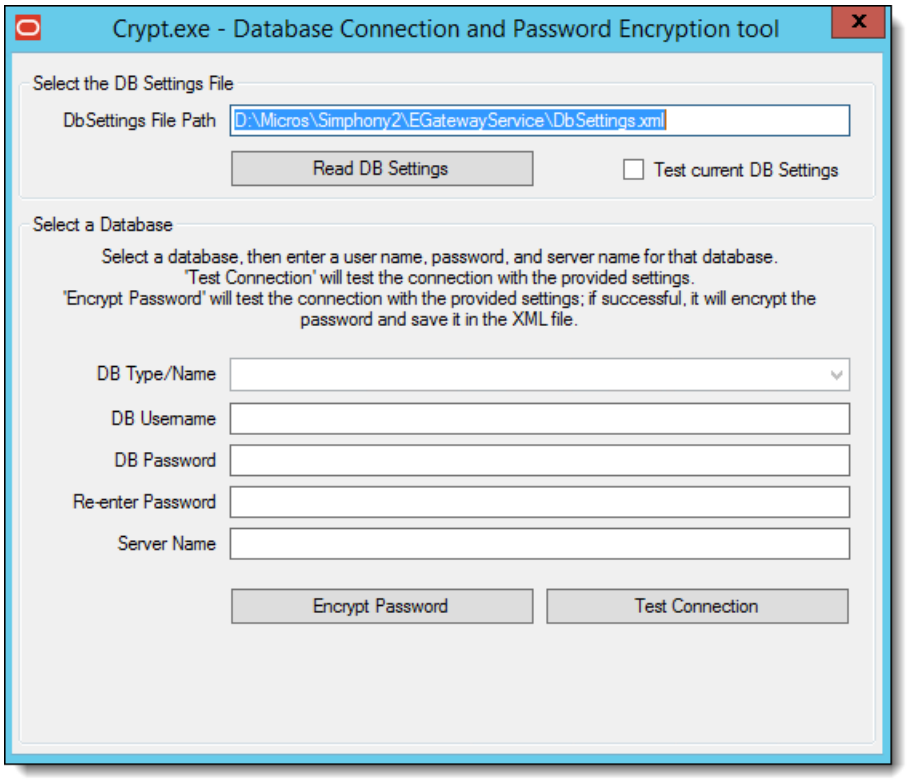
To ensure strict access control of the Simphony application, always assign unique usernames and complex passwords to each account (even if they won't be used), and then disable or do not use the accounts. Oracle Food and Beverage mandates applying these guidelines to not only Simphony passwords but to any applicable operating system passwords as well. Furthermore, Oracle Food and Beverage advises users to control access, via unique usernames and complex passwords, to any PCs, servers, and databases.

See the Oracle MICROS Simphony Post-Installation or Upgrade Guide, specifically the **Updating Property Administrator and Database Logon Credentials** section for more information about configuring strong passwords.

To access the Crypt utility:

1. Sign on to the Simphony application server.
2. Access the `[Drive letter]:\Micros\Simphony\Tools\` folder and double-click the **Crypt** executable. This utility edits the Simphony Database authentication credential stores in the configuration file (DBSettings.xml).

Figure 2-15 Crypt Database Password Encryption Tool



3. To change database passwords using the Crypt utility:
   a. Select the database.
   b. Enter your username in the **DB Username** field.
   c. Enter a new password in the **DB Password** field.
   d. Confirm the password in the **Re-enter Password** field.
   e. Enter the Simphony application server name in the **Server Name** field.
   f. Click the **Encrypt Password** button.
   g. Click the **Test Connection** button to verify that the Simphony application DB Passwords match the database passwords.
4. To encrypt database passwords using the Crypt utility:
   a. Select the database.
   b. Click the **Encrypt Passwords(s)** button.
   c. Click the **Test Connection** button.
5. To test database connections using the Crypt utility:
   a. To test the currently selected database settings, select the **Test current DB Settings** check box and then click the **Text Connection** button.
   b. To test other database connections, select the database from the **DB Type/ Name** drop-down list and then click the **Text Connection** button.

Workstation

If you did not configure unique usernames and complex passwords for the workstation database as part of the pre-installation process, you must do it now. It is paramount to maintain workstation database access control. You must assign these unique usernames and complex passwords in the Simphony EMC.

For more information on how to configure workstation database passwords, refer to the Configuring Workstation Database Passwords in the EMC topic.

Data Purging

Review the database purging configuration settings to ensure that and sensitive data is only stored for the minimum required time period.

3
Implementing Simphony Security

This chapter reviews Oracle MICROS Simphony security features.

- Authorization Privileges
- Employee Groups
- Job Code Overrides
- Workstation Security
- Hardening Security for Workstation USB Ports
- Audit Trail
- Encryption

Authorization Privileges

Setting Authorization privileges establishes strict access control, explicitly enabling or restricting the ability to do something with a computer resource. User authorization privileges are configured in the EMC.

- Select the Enterprise level and then click the **Roles** module.
- Workstation services also have their own privilege configuration settings within the EMC. Select the property level and then click the **Workstations** module.

Roles

A role is a group of privilege options defining what an employee can do. Employee roles determine the EMC modules a user may access, and they also determine what types of transaction behavior a workstation operator has (for example, permission to perform voids or open the cash drawer). A single role may be configured for all locations in the enterprise, or a role may be active in selected locations (zone, property, or revenue center). In addition, multiple roles may be assigned to a single employee, making the configuration of roles a task-based procedure. A role may include permissions that only allow a user to edit menu items (for example, see more in the best practices section). Also, job codes may be associated with employee roles, restricting clocked-in employees to a single set of permissions for the duration of a shift.

EMC Configuration

To open the Roles module in the EMC, select the Enterprise level, click **Configuration**, and then click **Roles**.

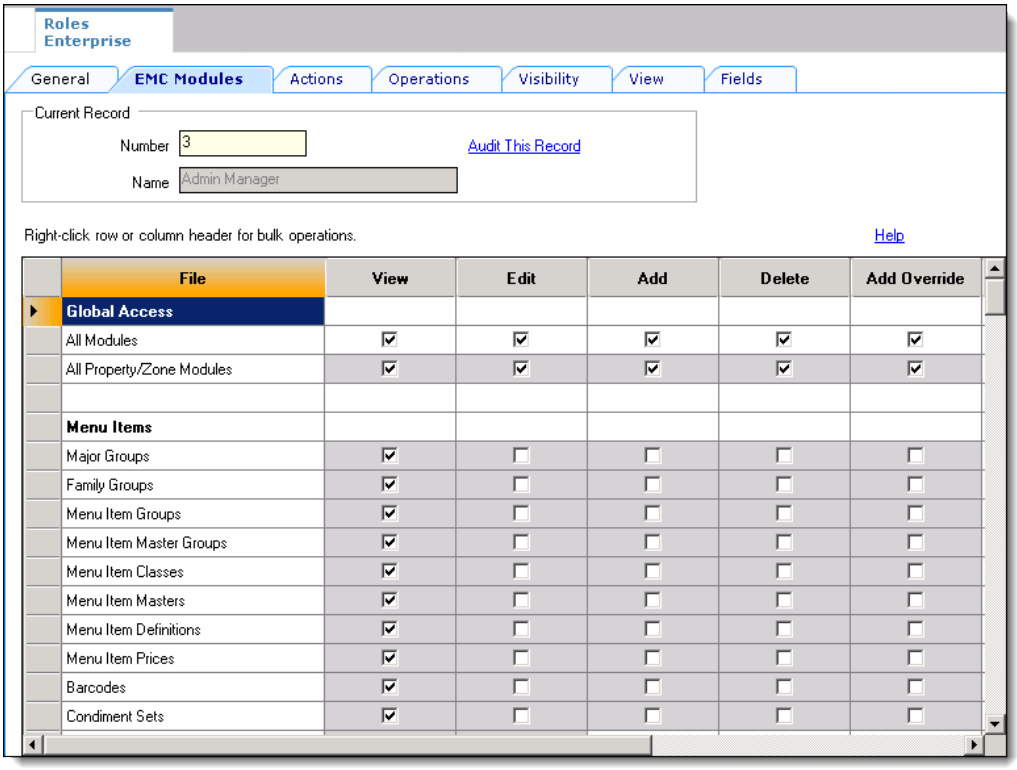
General Tab

- **Name**: Enter the name of the role. Up to 64 characters are allowed.
- **Comment**: Enter a comment describing this role. Up to 2000 characters are allowed; this field is not translatable.

- **Level**: This field is a level of security; it was created to prevent EMC users from creating employee records more powerful than themselves.

EMC Modules Tab

Figure 3-1 Roles EMC Modules Tab



In the EMC Modules tab, roles are configured to allow access to various modules of the EMC. From this tab, a user may be given permissions to:

- **View** a module (open it)
- **Edit** a module (to update fields or records within the module)
- **Add** records (to insert records where applicable)
- **Add Override** records allows for the creation of records or override existing records in differing levels. For example, property menu item records can override Enterprise menu item records when a role has this privilege enabled. **Add Override** is available only for zoneable modules.

Add Override also controls the ability to delete an override in single-record modules. In these modules, there are multiple fields to change, but all the changes are for a single record. Users cannot insert additional records into single-record modules.

> **Note:**
>
> Users must be assigned **View** access to a module to open it. If a user is assigned the privilege to edit, add, and delete a module, but not to view it, they are unable to open the module. When an employee does not have access to view a module, the module appears as grayed out on the EMC Enterprise home page.

In some modules, such as Enterprise Parameters, RVC Parameters or Order Devices, there is not an **Add** or **Delete** option because individual records cannot be added or deleted.

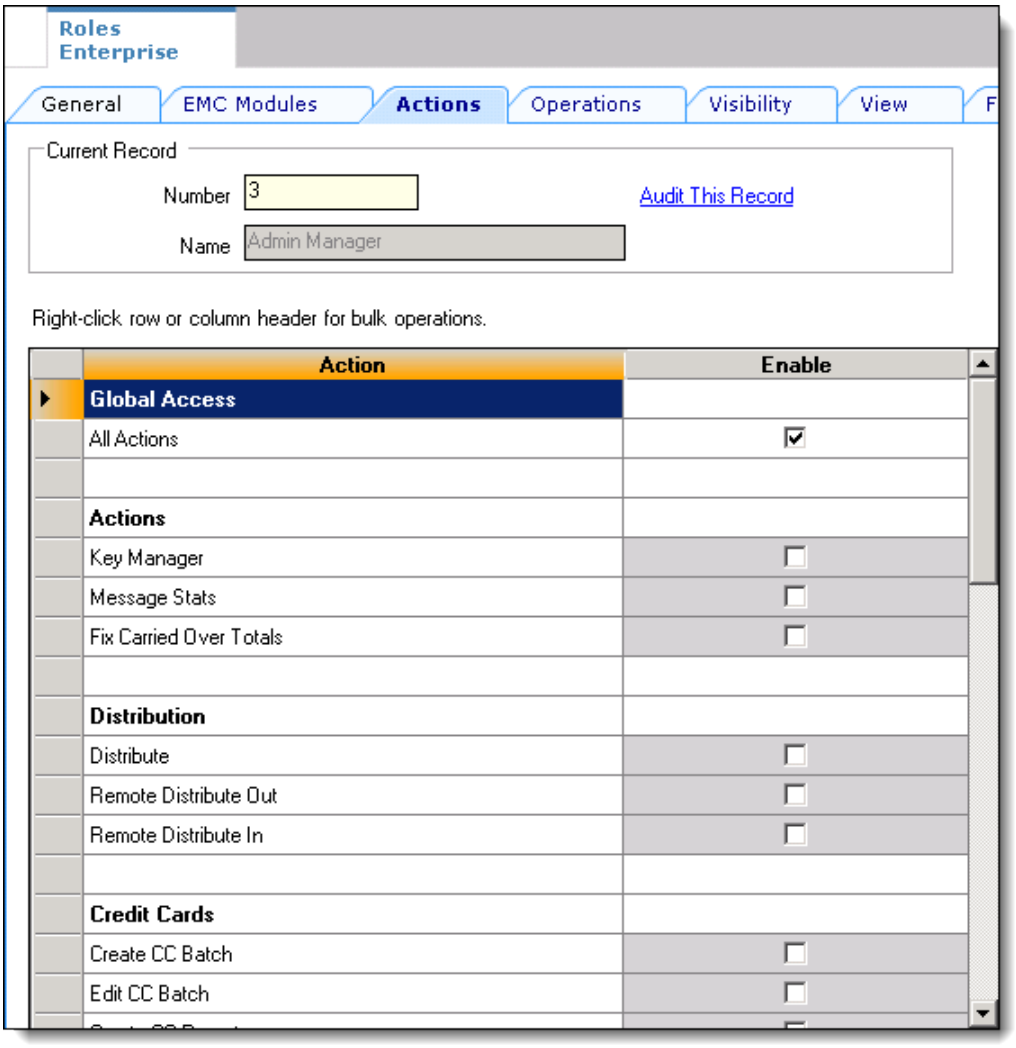
Global Access

The **All Modules and All Property/Zone Modules** check boxes are available so that a role may be easily configured to view, edit, add, or delete every module without having to individually check each box. Furthermore, this check box allows access to new modules that are created in the future. For example, if a new module “voice ordering” is created and released in a new version, an employee with “Global Access” for **View** will be able to access this module without having a specific check box for the “voice ordering” module. Oracle Food and Beverage recommends that administrator-type roles have the **All Modules** option checked, so that administrators are always able to access every module in the system.

Actions Tab

In the Actions tab, roles are granted access to specific actions that can be performed in the EMC.

Figure 3-2 Roles Actions Tab



Actions Global Access

Similar to the options on the EMC Modules tab, selecting the **All Actions** check box grants users associated with this role, permission to perform all actions. Oracle Food and Beverage recommends that administrator-type roles have this option checked, so that administrators are always able to perform all types of actions, including future actions that are not currently in the system.

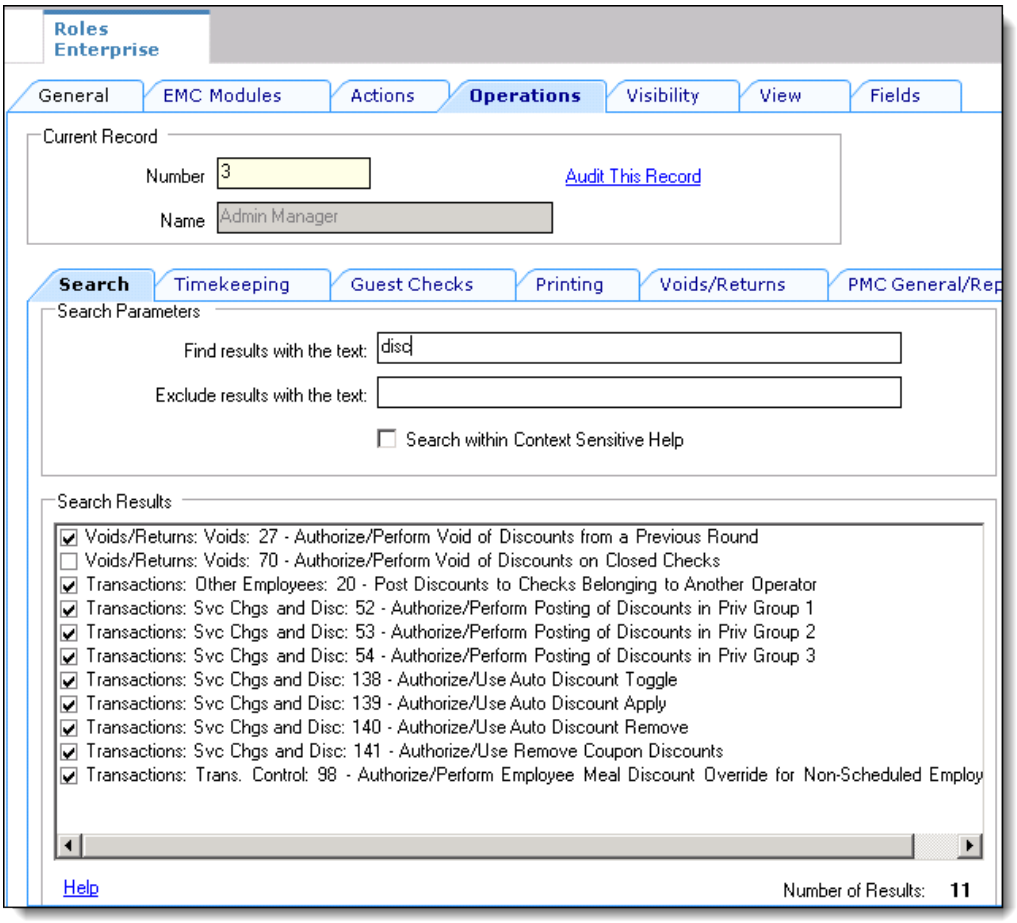
Security

A user who does not have a role assigned is not able to access any Enterprise level modules.

Operations Tab

There are over 200 operational options, so it could be difficult to find an option by searching on the various tabs. To quickly find options, use the Search tab to perform a Context Sensitive Help text comparison. The example figure above shows a search for discount options.

Figure 3-3 Roles Operations Tab



The Operations tab contains all of the options related to workstation functionality. The Operations tab is divided into sub-tabs based on similar functionality: Timekeeping, Voids, and the PMC.

Visibility Tab

On the properties tab, the role is assigned to specific locations or assigned to the Enterprise. In many situations, a role is assigned to the Enterprise — it is likely that a Server or Bartender role is the same for all properties. This tab consists of a grid that allows the administrator to add and delete locations, and to set the check box, [Propagate to Children], for each location.

The check box allows a role to be visible in the selected zones/locations and all its children; if it is unchecked, the role is visible in the selected zone/location only, but not its children.

View Tab

The View tab contains one option that controls the revenue centers that users can view: **Enable Revenue Center-Level Security**. This option relates to workstation behavior only. Employees associated with a role that has this option enabled are only able to view revenue centers in which they are an operator.

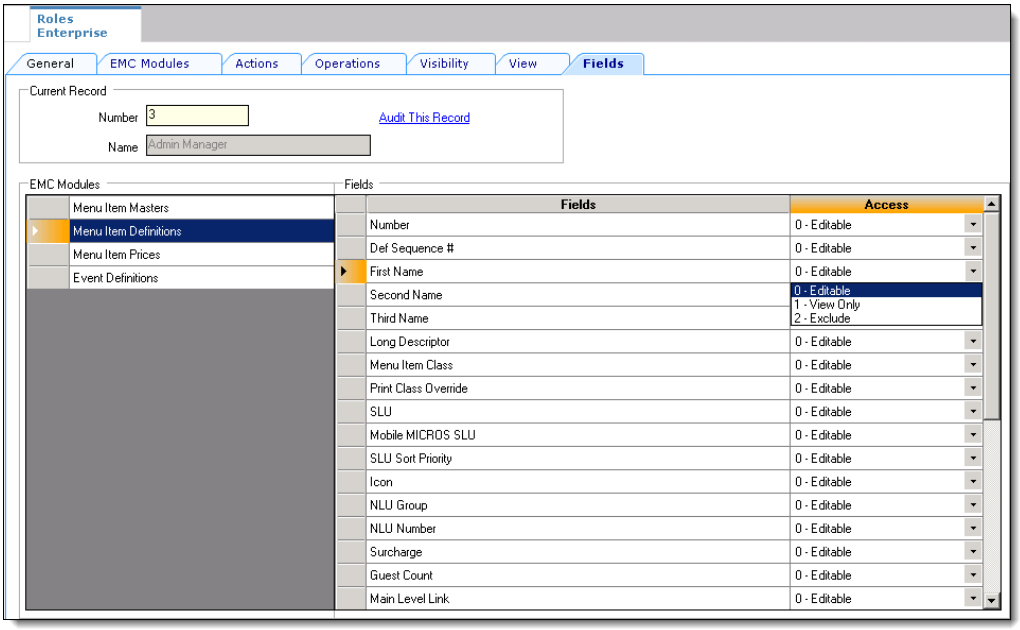
Employees can be set as an operator in a revenue center in the Employee Edit Form. When an employee is associated with a role with this option enabled, the employee is unable to add new revenue centers, even if the user is associated with a role with the **Add Revenue Centers** option enabled.

Fields Tab

The Field tab allows you to control specific field access for users in several EMC modules. Access control includes three privileges:

- **Editable**: You are able to view and edit the field
- **View Only**: You are only able to see the field (no editing allowed)
- **Exclude**: You cannot view or access the field at all

Figure 3-4 Roles Fields Tab



- Roles
- EMC Configuration
- Employee IDs
- Employee Levels
- Employee Levels and Roles
- Employee Level Configuration Best Practices

Roles

A role is a group of privilege options defining what an employee can do. Employee Roles determine the EMC modules a user may access, and they also determine what types of transaction behavior an operator has (permission to do voids or open the cash drawer, for example). A single Role may be configured for all locations in the enterprise, or a role may be active in selected locations (Zone/Property/RVC). In

addition, multiple Roles may be assigned to a single employee, making the configuration of roles a task-based procedure (a role may include permissions that only allow a user to "edit menu items", for example; see more in the best practices section). Also, job codes may be associated with employee roles, restricting clocked-in employees to a single set of permissions for the duration of a shift.

EMC Configuration

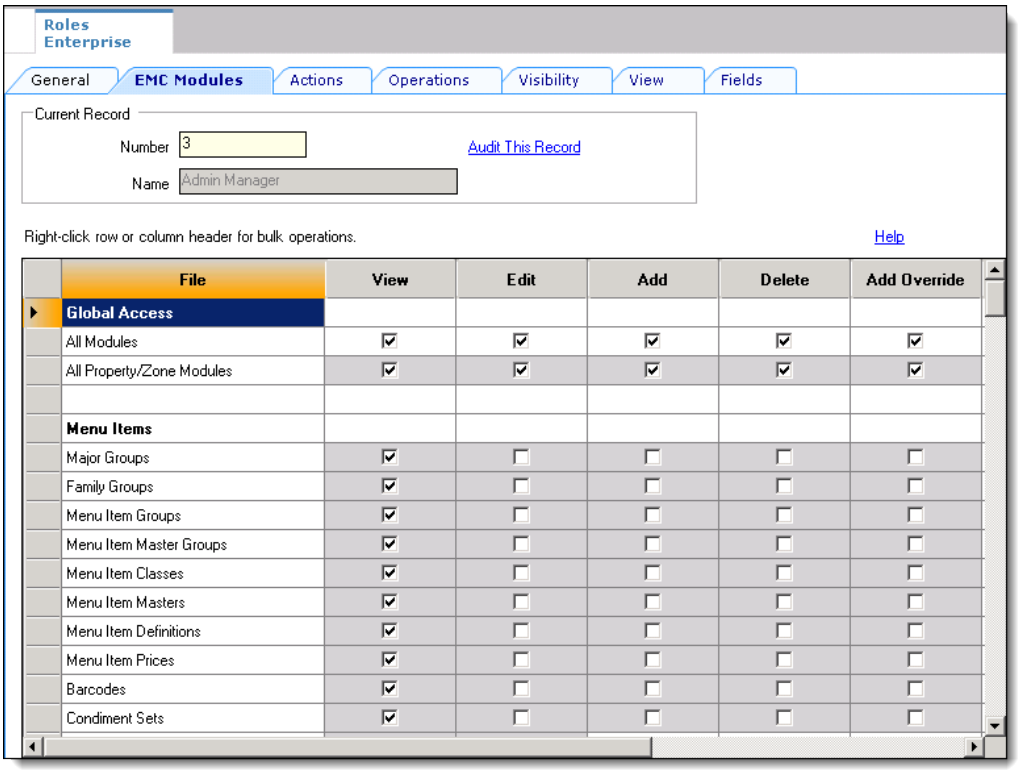
The Roles module is opened from the Enterprise level of the EMC.

General Tab

- **Name**: Enter the name of the role. Up to 64 characters are allowed.
- **Comment**: Enter a comment describing this role. Up to 2000 characters are allowed; this field is not translatable.
- **Level**: This field is a level of security; it was created to prevent EMC users from creating employee records more powerful than themselves.

EMC Modules Tab

Figure 3-5 Roles EMC Modules Tab



From the EMC Modules tab, roles are configured to allow access to various modules of the EMC. From this tab, a user may be given permissions to:

- **View** a module (open it)
- **Edit** a module (to update fields or records within the module)

- **Add** records (to insert records where applicable)
- **Add Override** records allows for the creation of records or override existing records in differing levels. For example, property menu item records can override Enterprise menu item records when a role has this privilege enabled. **Add Override** is available only for zoneable modules.

Add Override also controls the ability to delete an override in Single-Record modules. In these modules, there are multiple fields to change, but all the changes are for a single record. Users cannot insert additional records into Single-Record modules.

> **Note:**
>
> Users must be assigned View access to a module to open it. If a user is assigned the privilege to Edit, Add, and Delete a module, but not View it, they are unable to open the module. When an employee does not have access to View a module, the module appears as grayed out on the EMC Enterprise home page.

In some modules, such as Enterprise Parameters, RVC Parameters or Order Devices, there is not an Add or Delete option because individual records cannot be added or deleted.

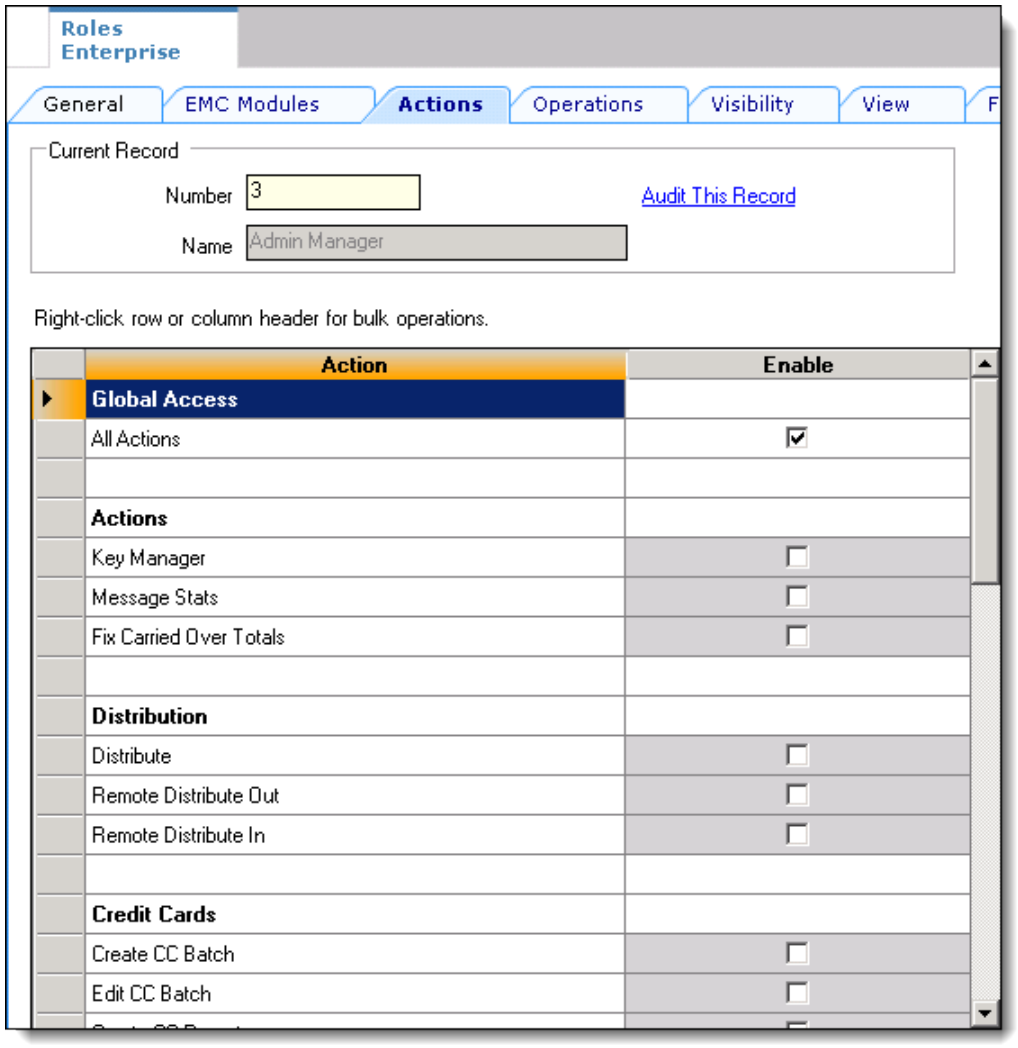
Global Access

The **All Modules and All Property/Zone Modules** checkboxes are available so that a role may be easily configured to **View**, **Edit**, **Add**, or **Delete** every module without having to individually check each box. Furthermore, this checkbox allows access to new modules that are created in the future. For example, if a new module “voice ordering” is created and released in a new version, an employee with **Global Access** for **View** will be able to access this module without having a specific checkbox for the “voice ordering” module. Oracle Food and Beverage recommends that administrator-type roles have the **All Modules** option checked, so that administrators are always able to access every module in the system.

Actions Tab

From the Actions tab, roles are granted access to specific actions that can be performed in the EMC.

Figure 3-6 Roles Actions Tab



Actions Global Access

Similar to the options on the EMC Modules tab, selecting the **All Actions** checkbox grants users associated with this role, permission to perform all actions. Oracle Food and Beverage recommends that administrator-type roles have this option checked, so that administrators are always able to perform all types of actions, including future actions that are not currently in the system.

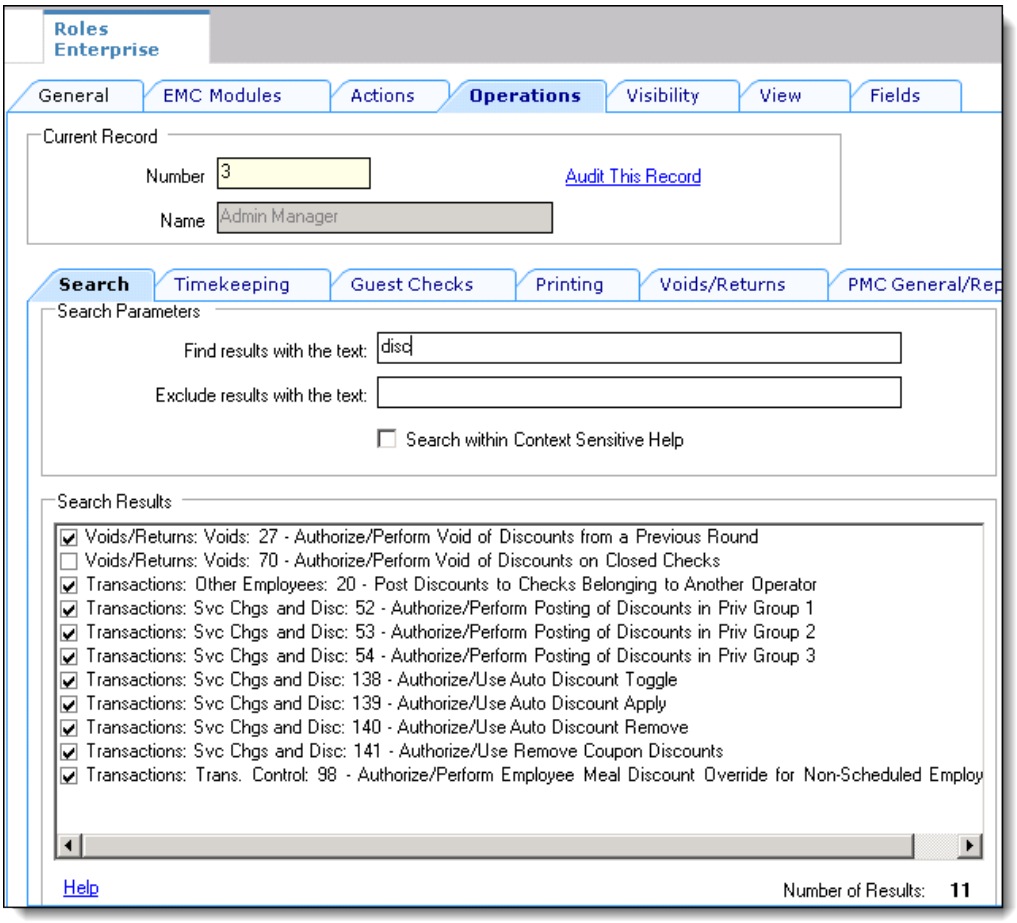
Security

A user who does not have a role assigned is not able to access Enterprise level modules.

Operations Tab

There are over 200 operational options, so it may be difficult to find an option by searching on the various tabs. To quickly find options, use the **Search** tab to perform a Context Sensitive Help text comparison. The following figure shows an example search for discount options.

Figure 3-7 Roles Operations Tab



The **Operations** tab contains all of the options related to workstation functionality. The **Operations** tab itself is divided into sub-tabs based on similar functionality: Timekeeping, Voids, and the PMC.

Visibility Tab

On the properties tab, the role is assigned to specific locations or assigned to the Enterprise. In many situations, a role is assigned to the Enterprise — it is likely that a Server or Bartender role is the same for all properties. This tab consists of a grid that allows the administrator to add/delete locations, and to set the checkbox, [Propagate to Children], for each location.

The checkbox allows a role to be visible in the selected zones/locations and all its children; if it is unchecked, the role is visible in the selected zone/location only, but not its children.

View Tab

The View tab contains one option that controls the revenue centers that users can view: **Enable Revenue Center-Level Security**. This option relates to workstation behavior only. Employees associated with a role that has this option enabled are only able to view revenue centers in which they are an operator.

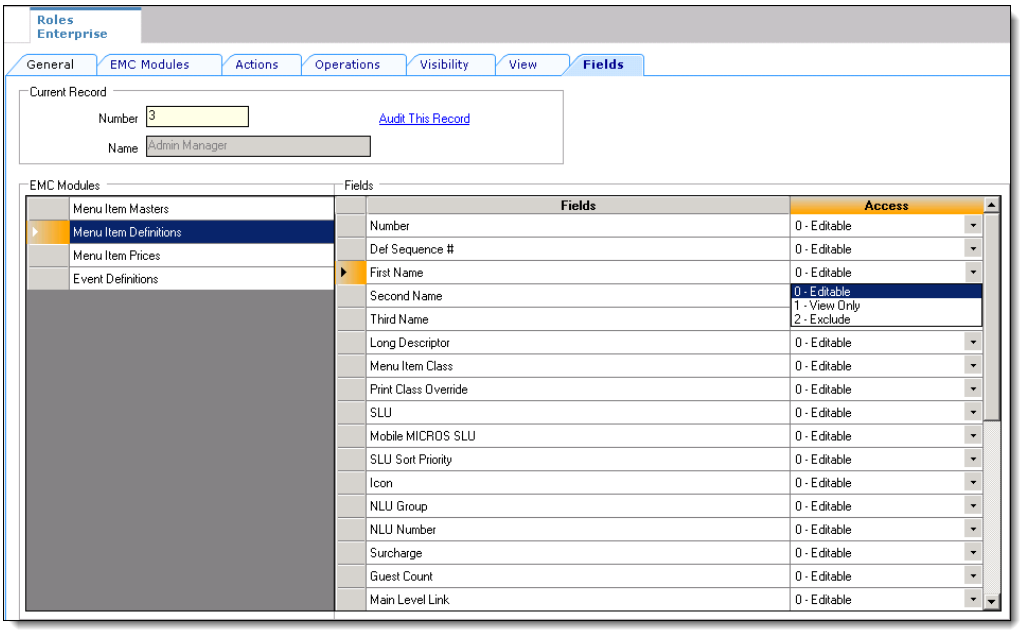
Employees can be set as an operator in a revenue center in the Employee Edit Form. When an employee is associated with a role with this option enabled, the employee is unable to add new revenue centers, even if the user is associated with a role with the **Add Revenue Centers** option enabled.

Fields Tab

The Field tab allows you to control specific field access for users in several EMC modules. Access control includes three privileges:

- **Editable**: You are able to view and edit the field
- **View Only**: You are only able to see the field (no editing allowed)
- **Exclude**: You cannot view or access the field at all

Figure 3-8 Roles Fields Tab



Employee IDs

An Employee ID refers to the number that an employee uses to sign into a workstation. An employee ID is often a Magnetic (Mag) card, which is a credit card-like swiping device that stores a 10-digit card number. An employee ID can also be just a number, such as a PIN, that the user types into the workstation.

Some function keys prompt for employee number or Employee ID, based on an option setting somewhere in the EMC. Every employee has an employee number, but not all employees have an Employee ID.

EMC Viewing

In the EMC, Employee IDs are editable in the Employee Maintenance module. A user can see the ID number of other employees only when the user is associated with a role that has the **View Employee ID** option enabled.

Workstation Option

In the EMC, when the Workstation module option **Mag Card Entry Required** for Employee ID is enabled, a user cannot type a number to sign in to the device.

Employee Levels

Each employee in a Simphony system is associated with an Employee Level, programmed in EMC's Employee Maintenance module or via the Property Management Console (PMC). This field is a layer of security; it controls how employees interact with other employees by preventing some employees from accessing other employee records. Also, it gives EMC user's access to some Employee Roles, but not others.

Configuration

This setting allows a one-digit entry, where 0 offers an employee the most access and 9 offers the employee the least access. This field controls access to other employee records in EMC and PMC, but the functionality is slightly different.

PMC and EMC Usage

> **Note:**
>
> In EMC's Employee Maintenance, if the Employee Level of the logged-in user is not 0, the list of Employee Levels is restricted to only levels that a user may access. For instance, if the logged-in employee's level is 2, the drop-down list shows 3-9.

Employee Level Setting is 0

When the Employee Level field for an employee is set to 0, the functionality is the same for both the EMC and PMC. Employees at this setting can view all other employees including themselves.

Employee Level Setting is non-0: EMC

When the Employee Level field for an employee is set to a value other than 0, the EMC prevents that employee from seeing other employees at the same level or levels with higher access. By higher access, this means having a lower numerical value. For example:

- Employee A's Employee Level is set at 2
- Employee A logs into EMC and enters Employee Maintenance
- Employee A can see all employees at levels 3–9
- Employee A cannot see employees at levels 0–2, including himself

Because the employee cannot see themselves, there is no way to change his level or other privileges.

PMC Security Setting is non-0: PMC

The PMC security settings are similar to the EMC security settings with one exception: the employee can access his own record. This has been made possible so that the employee can change his/her workstation ID or mag card. For example:

- Employee A's Employee Level is set at 2

- Employee A opens the PMC enters the employee procedure
- Employee A can see all employees at levels 3–9
- Employee A cannot see employees at levels 0–2. However, the employee can see himself, with access to only these fields:
  - First Name
  - Last Name
  - Check Name
  - Revenue Center
  - Assign ID
  - Assign Mag Card
  - Increment Shift

Because the employee cannot change their own level, there is no way for this employee to view additional employees.

Employee Levels and Roles

Each Employee Role and Enterprise Role is associated with a level. The Role Level field is designed to prevent an EMC user from modifying Employee Records to have greater permissions than the EMC user has. Consider the following example:

- An EMC user, Henley Nelson, has an Employee Level of 2. Henley can therefore see all employees in Levels 3–9.
- The database was programmed in a proper manner as the administrator configured the system so that super privilege roles have a level of 0, but other less-powerful roles (like Bartender or Floor Manager) have a Role Level of 3.
- Henley is able to Edit and Add employee records.

  In this situation, when Henley uses Employee Maintenance, the Employee's Roles tab prevents Henley from adding 0-Level Roles (also 1, and 2-Level Roles) to other Employee Records. Thus, Henley cannot create a user who is more powerful than himself.

  In the rare instance that an employee is programmed incorrectly, (a 0-Level EMC user assigns a 2-Level role to a 4-Level Employee) the EMC prevents other employees from modifying this Role. Following our example with Henley, he is able to see the 4-Level employee, but the 2-Level Role assigned to the employee is disabled, and Henley is not be able to modify it.

Employee Level Configuration Best Practices

The following table demonstrates a well-configured database. Notice that levels for roles are configured with gaps that allow flexibility for assigning levels in the future for different types of users.

Table 3-1 Employee Level Example Settings

Level Number	Type of User/Role
0	System Administrators. Typically, only a handful of employees are System Administrators in any given Enterprise.
1	Enterprise Programmers. These users are often able to perform the same tasks as System Administrators. However, some EMC modules are generally off-limits, such as Roles, Enterprise Roles, and Enterprise Parameters.
2	
3	
4	Property-Level Programmers. These users are often able to work in EMC modules that change frequently, such as Employee Maintenance, Menu Item Maintenance, and possibly Order Devices.
5	
6	Property Floor Managers. The term Floor Manager in this instance refers to an employee who does not have EMC access. Floor Managers provide operational assistance (for example, voids) to workstation users. Typically, these users have PMC access to Order Devices and perhaps Menu Item Availability.
7	
8	The typical Bartender, Cashier, or Server user is in this level. By placing these employees into Level 8, all EMC users and Floor Managers are able to view these records.
9	

Employee Groups

Each employee in a Simphony system is associated with an Employee Group, configured in the EMC's **Employee Maintenance** module. This field is a layer of security that controls how employees interact with other employees by preventing some employees from accessing other employee records. While useful, this field is quite restrictive; the Employee Level field is more commonly used.

- Configuration of Employee Groups

Configuration of Employee Groups

This setting allows a three-digit entry, where 0 allows employees to view all employee records, and any other value restricts the employee to viewing only employees who are also in the same group.

EMC and PMC Behavior

In the Employee Maintenance module, if the Employee Group of the logged-in user is not 0, employee records appear with the Employee Group field as disabled. This prevents the logged-in user from changing a record to a group that the logged-in user

cannot access. In the EMC and PMC, an employee can view only employees in the same group, or the employee can view all other employees if the value is 0. To summarize:

- Employee's Group is 0. The employee can see all other employees.
- Employee's Group is 17. The employee can see only other employees in Group 17.

POS Operations Behavior

During workstation operations, the **Employee Group** field controls which employees may perform authorizations (such as voids) for other employees. Consider the following table. The manager can perform authorizations only when his employee group is 0 or if it is the same as the employee who needs the authorization:

Table 3-2 Employee Group Numbers

Server's Employee Group	Manager's Employee Group	Ability to Authorize?
0	0	Yes
0	91	No
17	91	No
91	0	Yes
91	91	Yes
91	17	No

When an employee from Group 17 attempts to perform an authorization for an employee in Group 91, an `Authorizing employee is not in the correct employee group` error appears on the workstation.

Job Code Overrides

When a job code is linked to an employee role, employees who are clocked in to that job code inherit the permissions of the job code for the duration of the shift. This situation is ideal when two job codes exist: Server and Floor Manager. By linking both of these to appropriate roles, a user who is clocked-in as a Floor Manager has privileges to perform voids, but when that same user is clocked-in as a server, they do not. To summarize, there are two methods for configuring job codes:

- When the **Role** field is set to **0-None**, the workstation operator has privileges based on the role(s) assigned in the EMC.
- When the **Role** field is not **0-None**, the workstation operator's privileges from EMC do not apply. Only the privileges associated with the role from this field are active for the duration of the Clock-in Cycle.
- Configuring Job Code Overrides

Configuring Job Code Overrides

For companies that use Simphony's timekeeping features and require all hourly employees to clock in, the following configuration provides optimal security with the least amount of configuration:

- Configure an employee role that allows users to clock in. This role could be named **Ability to Clock In**, and it would be configured with the following options enabled:
  - **Clock in at Rate 1** (through 8, as appropriate)
  - **Clock in at Rates 9-255** (if appropriate)
- Every employee in the enterprise who clocks in should be associated with the **Ability to Clock In** role and *no other* roles
- Every job code is linked to an employee role. Here are examples:
  - A Bartender job code is associated with a role (probably also called bartender) that allows the ability to open cash drawers and to perform fast transactions
  - A Server job code is associated with a role that allows the ability to begin tables
  - An Hourly Manager job code is associated with a role that allows the ability to perform voids and other authorizations
- Other employees (those who are on salary) do not clock in. These employees could have one or more employee roles assigned within EMC.

Workstation Security

For information about enabling point-of-sale (POS) workstations security, refer to the *Oracle MICROS Simphony Configuration Guide*, specifically the **Configuring Workstation Security** section.

- Assigning Privileges to Allow Installing and Authenticating Workstation Clients

Assigning Privileges to Allow Installing and Authenticating Workstation Clients

The ability to download software, install and authenticate point of sales (POS) clients and service hosts using CAL, is controlled by employee Role option **10065 - Download Software, Install and Authenticate Clients and Service Hosts Using CAL**.

When enabled, the User Security Credentials configured in the Property Parameters module become inactive, allowing employees to use their EMC login credentials as the Installer Username and Installer Password when setting up POS clients.

The *Oracle MICROS Simphony Configuration Guide* contains more information on enabling employee role privileges.

Hardening Security for Workstation USB Ports

Here are instructions for hardening the security for various workstation USB ports.

Workstation 600 Series

1. Press the **F2** key while the workstation is starting up to enter the BIOS/Setup screen.
2. Navigate to and select the **Advanced** tab.
3. Scroll down and select **Special Configuration**.

4. Scroll down to the desired USB port.
5. Press **ENTER**, scroll up to **DISABLED**, and then press **ENTER** to select it.
6. Press **F10** to **Save and Exit**.

Workstation 310

1. Press the **F2** key while the workstation is starting up to enter the BIOS/Setup screen.
2. Use the touch screen BIOS and then select the **Advanced** option.
3. Select **Special Configuration** from the menu.
4. Select the desired USB port from the drop-down list and select **DISABLED**.
5. Click or touch **Save**.
6. Confirm **YES** from the Setup Confirmation prompt.

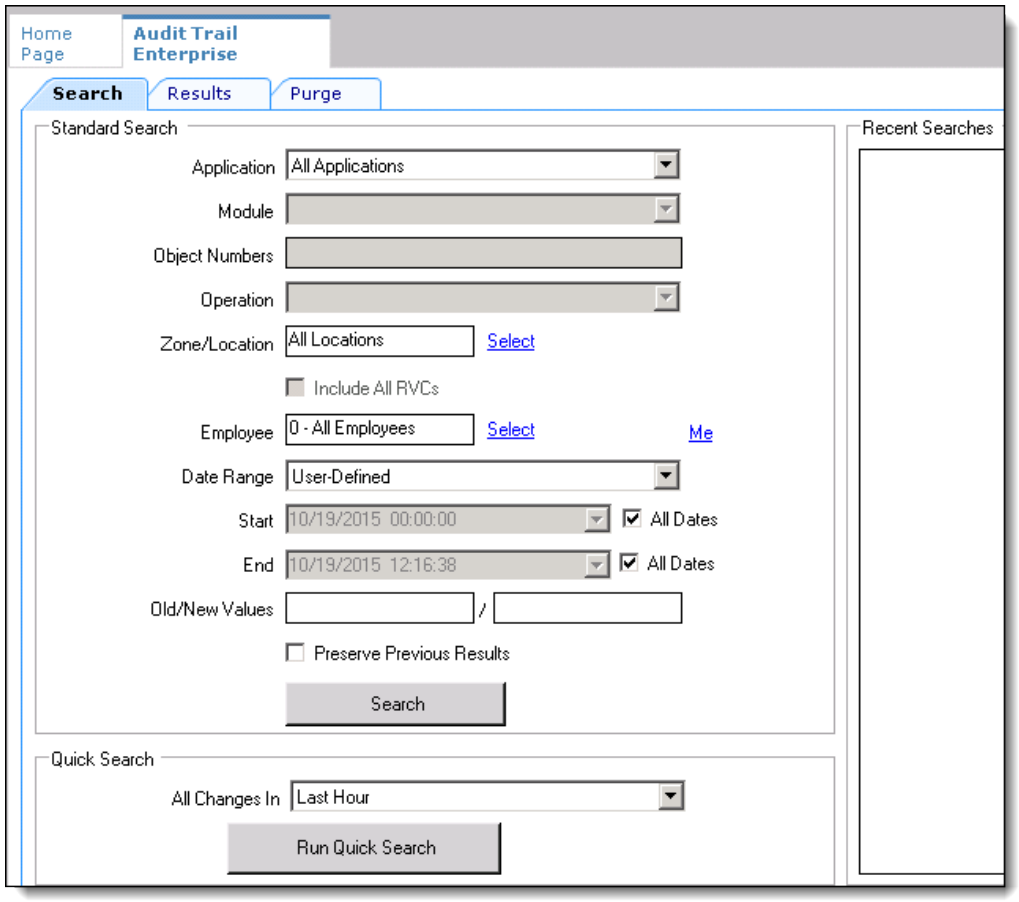
Workstation 5A

1. Press the **DELETE** key while the workstation is starting up to enter the BIOS/Setup screen.
2. Press the **RIGHT** arrow key until you reach the **ODM** tab (this tab appears after the Video tab and is not visible until you scroll over).
3. Scroll down to the desired USB Port, and use the + - key to select the **Enabled** or **Disabled** option.
4. Navigate to the **Exit** screen and select **Save Settings and Restart**.

Audit Trail

Audit Trail is the EMC module that displays changes made to the Simphony system. All changes, additions, and deletions made in the EMC and PMC Procedures are recorded and reportable in Audit Trail. In addition, Audit Trail reports on successful/failed logins to the EMC, users taking PMC Reports and Audit Trail Reports, Key Manager activity, Audit Trail purges, activity from credit card modules, and even activity from the DbProcs utility.

Figure 3-9 Audit Trail Search Tab



The Audit Trail module is located on the Enterprise level and the property level of the EMC. Two privileges determine a user's ability to enter the module:

- To use the Enterprise Audit Trail, a user must be associated with an Enterprise Role with the action **Enterprise Audit Trail User** enabled.
- To use the Property Audit Trail, a user must be associated with the Enterprise Role privilege mentioned above, or with an employee role with the privilege **Access Property Audit Trail** enabled.

- Audit Trail Search Parameters
- Audit Trail Search Results
- Other Audit Trail Considerations
- Audit Trail Purging

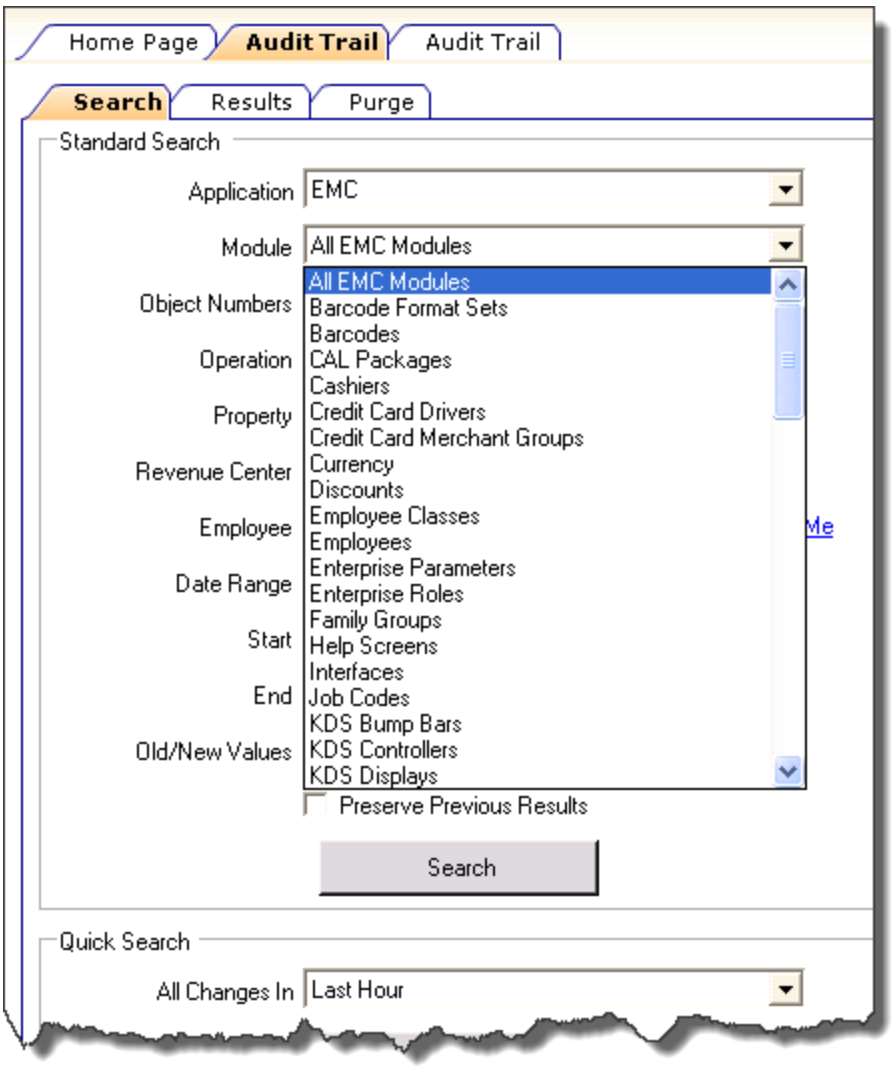
Audit Trail Search Parameters

Standard Search

The Audit Trail search tab displays a number of fields that help the user create queries.

- **Application**: Select an application or choose **All Applications**. This drop-down displays All Applications followed by an alphabetized list of available applications. When this field is changed, its setting may enable the Module field. For example, if EMC is selected, the Module drop-down menu shows a list of EMC Modules.
- **Module**: Select an EMC module or choose **All EMC Modules**. This drop-down displays All EMC Modules followed by an alphabetized list of available modules; this drop-down is enabled only when the Application selection allows a choice of modules. When this field is changed, its setting may enable the Object Numbers field. For example, if **EMC** is the Application and **Discounts** is selected as the Module, the Object Numbers field is enabled.

Figure 3-10 Audit Trail Standard Search



- **Object Numbers**: Enter an Object Number or Object Number Range to retrieve results based on specific records only. If this field is blank, all object numbers are considered.

- **Operation**: Select an Operation or choose **All Operations**. This field is enabled based on a combination of the Application and Module drop-downs. This drop-down displays All Operations, followed by an alphabetized list of the valid operations.
- **Property**: Select a property or choose **All Properties**. This field is enabled only when Audit Trail is opened from the Enterprise level.
- **Revenue Center**: Select a revenue center or choose **All RVCs**. This field is enabled only when a specific property is selected.
- **Employee**: Select an employee or choose **All Employees**. When a specific employee is selected, only changes made by that employee are included in the list. If me is selected, this field changes to the logged-in employee.
- **Date Range**: Select a predefined date range that is used to query the Audit Trail, or select “User-Defined” to enable the start/end fields. The predefined date ranges are:
  - Last Hour
  - Last Two Hours
  - Today
  - Last 24 Hours
  - Last 48 Hours
  - Last Week
  - Last Two Weeks
- **Start**: Select a Start date/time or choose **All Dates**. This field lets a user narrow a query to a specific date or date range.
- **End**: Select an End date/time or choose **All Dates**. This field lets a user narrow a query to a specific date or date range.

  While a search using text fields may return the specific Audit Record you want, a search of the module of the item, returns results more quickly.
- **Old/New Values**: Enter text that is used to query the **OldValue** and/or **NewValue** columns of the Audit Trail table. These text boxes can be useful to find a specific change to a record, such as, “When was the item Hamburger renamed to Cheeseburger?”
- **Preserve Previous Results**: If this box is checked, the search results are merged with the previous search results instead of overwriting them. If this box is not checked, the search results include only the data of the most recent search.

Recent Searches

Each time the user presses the **Search** or **Run Quick Search** buttons, this box lists the search information that was used to obtain the Audit Trail results. When **Preserve Previous Results** is checked, the latest search information is added to the box. If the option is not checked, previous information in this box is erased, and only the latest search information appears in the box.

Quick Search

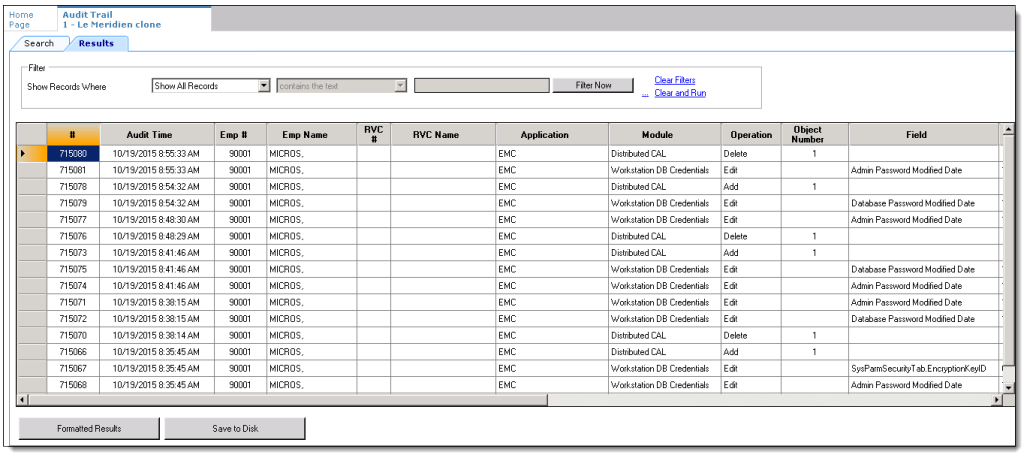
In this box, select a predefined date range and run a search. When this is used, the **Standard Search** criterion is ignored; only the date range selected is used.

Running a Search

When **Search** or **Run Quick Search** is clicked, the Audit Trail first checks the database to get an estimate on the number of records that are returned. (It is an estimate because changes may be in progress at the time of the query.) If the number of results that are returned exceeds the pre-configured thresholds for Audit Trail results, the user is prompted to confirm the action. The prompts occur when more than 10,000, 50,000, 100,000, 500,000, and 1,000,000 records are returned. These prompts are meant to confirm that the search criterion being used is desired. With these prompts, the user is prompted three times (10,000, 50,000, and 100,000) to confirm that the Audit Trail runs a query that returns the expected results of more than 101,000 records.

Audit Trail Search Results

Figure 3-11 Audit Trail Search Results Tab



After running a search, the Results tab becomes active and the results of the search are displayed. The records display in a Table View-like grid, allowing sorting and filtering. By default, the grid displays the most recent changes at the top of the list.

The following columns appear:

- #: This column displays the Audit Trail Record ID of each Audit Trail Entry
- **Audit Time**: This column displays the time of the change or activity
- **Emp #**: This column displays the employee number of the employee who made the change. If the change was made by an employee who is now deleted, a “0” is assigned to that record.
- **Emp Name**: This column displays the name of the employee who made the change. If the change was made by an employee who is now deleted, the database **ID 1234** appears (where 1234 is the Database ID of the deleted employee).
- **Prop #**: This column displays the Property number, if any, where the change was made. If the Property of the change is deleted, this column shows “- 1.” If the change was an Enterprise-level change, this column is blank. If the change was made in a RVC, this column displays the Property to which the RVC belongs.

- **Prop Name**: This column displays the name of the property, if any, where the change was made. If the property was deleted, this column shows “??? 1234” (where 1234 is the database HierStrucID of the deleted item). If the change was made on the Enterprise, this column shows “(Enterprise).” If the change was made in a RVC, this column shows the name of the Property to which the RVC belongs.
- **RVC #**: This column displays the RVC number, if any, where the change was made. If the RVC of the change was deleted, this column shows “-1.” If the change was an Enterprise-level or Property-level change, this column is blank.
- **RVC Name**: This column displays the name of the RVC, if any, where the change was made. If the RVC was deleted, this column shows “??? 1234” (where 1234 is the database HierStrucID of the deleted item). If the change was made on the Enterprise or Property level, this column is blank.
- **Application**: This column displays the application where the change was made. The list includes different applications within Simphony such as EMC, PMC Procedures, PMC Reports, and others.
- **Module**: This column displays the module, if any, within the application where the change was made. This column typically displays an EMC Module name. When the audit record displays a PMC Report, this column displays the name of the report that was taken.
- **Operation**: This column displays the type of operation that occurred.
- **Obj Num**: This column displays the object number of the record that was changed. If the audit record is a PMC Report, this column displays the Autosequence Number that was run.
- **Field**: This column generally applies only to changed records. This column shows the field that was changed. For example, if a Discount's Option #1 is changed from ON to OFF, this column shows **Option 1, ON = Open; OFF = Preset**.
- **Old Value**: This column generally applies only to changed records. When a field is changed, this shows the value of that field before the change.
- **New Value**: This column generally applies only to changed records. When a field is changed, this shows the value of that field after the change.
- **Dist Source**: When a user performs distribution, this column shows the Property or Source RVC from which the original record was distributed.
- **Comments**: This column displays comments added to the Audit Trail record. Some applications may record comments to help clarify the change or activity being audited.

Audit This Record

In almost every module, you can select **Audit This Record** from the Edit menu of the EMC menu bar to see changes to the current record or selection of records. This functionality can also be accessed from the common panel used in Form View and the Table View Right-Click Menu. After selecting Audit This Record, a new tab opens. This tab shows a grid that is similar to Audit Trail Search Results grid, but the Audit This Record grid omits Property/RVC columns and the Module column because this information is the same for every record. Also, the **Comments** column is always hidden in this view.

In addition, the Object Number column is sometimes omitted (when auditing modules without object numbers, like RVC Parameters) and the Application column displays only when the current record can be edited outside EMC. For example, it is possible to redirect Order Devices from PMC Procedures; when a user chooses Audit This

Record for an Order Device, the application column displays. Conversely, it is only possible to edit KDS Displays in EMC, so the Application column does not display.

Advanced Options

When a user clicks the **Show Advanced Options** link, the Advanced Search panel is displayed. This panel lets the user run specific queries on the selected record(s), using the same Search Parameters that are available in the Audit Trail module. Note that the **Run Search** button retrieves records from the database; there is no "filtering" of table view records from this form.

Module-Specific Notes

Employee Maintenance and Menu Item Maintenance allow **Audit This Record** functionality only from the Table View Right-Click Menu.

Selecting All Records

When in a Table View/Form View module, a user can audit all records in the module by using the following steps:

1. Click in the upper-left cell of the Table View grid.
2. From the Edit menu, select **Audit This Record**.
3. EMC prompts: `No records are currently selected. Would you like to get Audit Trail information for all activity in this module?`
4. Click **Yes**.

This EMC prompt also occurs if there are no records in the module, or if all the records have been filtered out of view.

Other Audit Trail Considerations

Oddities and Exceptions

- Trailing white space changes can be difficult to determine when looking at the Old Value and New Value columns of the grid. For example, if a user changes the text "Hot Dog" to "Hot Dog ", the user would not be able to tell that something changed, because the Old/ New values would appear to look the same. Because of this, changes of this type display the Old/New value, followed by the value in quotes to show where the extra space characters exist. For example, the new value for "Hot Dog" changing to "Hot Dog" appears like this: Hot Dog ("Hot Dog").
- Changes made in the Property Merchant Groups module are treated like a single-record module (similar to RVC Parameters or Property Descriptors); all records for this module are logged without an Object Number.
- Other than the name, changes in the Selection Hierarchies module are not currently logged to Audit Trail.
- When a macro record is created, its 16 steps are not created. The first time a macro record is saved after its creation, Audit Trail shows each step being added.
- The configurable data for Credit Card Drivers and Credit Card Merchant Groups are displayed in EMC using standard controls that are found throughout EMC. However, this data is actually stored in the database in a single data column as an XML string. Because of this, changes in these modules show the **Field** as **Configuration**, and the Old/New values display the entire XML string.

- When an Audit Trail report is taken, this activity is logged to Audit Trail. All generated Audit Trail Reports are logged as an Enterprise-Level activity.

Internationalization

Text is stored in the AUDIT_TRAIL database table so that an EMC user views the text in his/her own language. For example, if a user from England changes Menu Item Class option bit 1 from ON to OFF, the data is stored in the table so that the Audit Trail report shows the name of the option in Japanese for an EMC user from Japan. (The Audit Trail report translates the text key that is stored in the database at the time the Audit Trail report is generated, using the logged-in user's EmcText file.)

The following table summarizes the methods for Audit Trail internationalization:

Table 3-3 Audit Trail Translation Capabilities

Audit Trail Column(s)	Description	Translatable?
Employee Application Module Operation	These fields are all stored as numbers in the database. When taking the report, the number is converted into the appropriate text.	Yes
Field	The name of the field or option bit that was changed.	Yes
Sub-record Name	The name of the sub-record. A “sub-record” is something that has its own database table but is used by other records. Examples include Macro Steps, Workstation Devices, and Touchscreen Keys, etc.	Yes
Sub-record Field	The name of the field for the sub-record. For example, a Touchscreen Key legend or a KDS Bump Bar Scan code Value.	Yes
Old Value New Value	Displays the old/new values of a changed record.	Sometimes. In most cases, these fields are not translatable. For example, if a user changes a Menu Item Definition's SLU or name, Audit Trail determines the old/new value appropriately; there is no need for translation. Sometimes this field is translated when the change is made as an example, if a Discount's Menu Level #1 is changed from ON to OFF, the text “ON” and “OFF” comes from the EmcText file of the EMC handler.

Table 3-3 (Cont.) Audit Trail Translation Capabilities

Audit Trail Column(s)	Description	Translatable?
Comments	The data in this field is typically not used by EMC end-users. It is simply a mechanism for providing more information about the audit trail record.	No

Audit Trail Purging

For privileged users, the Purge tab is visible in the Audit Trail module. This tab is visible when the Audit Trail is opened from the Enterprise and the logged-in employee is associated with an Enterprise Role with the option, Purge Audit Trail, enabled. From this tab, the logged-in user can remove old records from the Audit Trail table in the database.

In the date field, users can select a date whereby records that are dated prior to that date are purged. For example, when this field is set to October 30, 2015, all records dated from October 30 and earlier are deleted. Note that records are deleted based on the UTC date of the Audit Trail record.

In addition to this manually initiated purge, the Data Transfer Service (DTS) purges Audit Trail records automatically.

Sub-record Formatting

A sub-record is any record that is added/removed to primary records. Some sub-record examples include Touchscreen Keys, Menu Item Group detail rows, and workstation devices. All sub-record modifications are considered edits. For example, if a touchscreen key is added to screen #10, this logs as an Edit to screen #10.

> **Note:**
>
> For most records, the index included in the brackets for a sub-record is a useful number. For instance, “Key [30]” shown in these examples refers to the 30th key added to the screen. For some records, there is no useful indexing field. For example, Menu Item Groups and CAL Package deployment rows do not have any type of object number that defines the order of the sub-records. When these records log to Audit Trail, additions are logged as index [0]. Deletions and edits to these records are listed with the index of the database primary key for the sub-record.

When a sub-record is added, the Audit Trail shows:

- **Field**: Name and number of the sub-record, followed by the field that changed (for example, **Key [30]: Legend**).
- **Old/New Value Fields**: The old and new values of the field. When a sub-record is deleted, Audit Trail shows:
  - **Field**: Name and number of the sub-record (for example, **Key [30]**).

  - **Old Value**: A description of the sub-record. For touchscreen keys, this is **Function: 7-1, Legend: Cash**. This text gives a user enough information to know what was removed. In this example, a key that used Tender #1 with the legend **Cash** was removed.
  - **New Value**: (removed)

Long Text in the Old/New Value Fields

- The Old Value and New Value fields can hold only up to 2000 characters. If the Old/New value exceeds this length, the text is logged as the first 1980 characters plus the text "**....**".
- If a value is too long to read in the Audit Trail results grid, it can be easily viewed if the user expands the row height.

Encryption

Overview

Encryption is the reversible transformation of data from the original (plain text) to a difficult-to-interpret format (cipher text).

Permanent Data Store Encryption

Sensitive data in the Simphony database is encrypted using industry standard AES256 encryption. Each encrypted piece of data has a link to an entry in the encryption key table, which is also encrypted using AES256 encryption. Simphony provides an EMC Key Manager module to create, rotate, and delete encryption keys. All data that needs to be stored in the database in encrypted format is automatically encrypted using the latest encryption key.

> **Note:**
>
> **Caution**: If the encryption key is lost, the encrypted data in the database is unrecoverable. There are no backdoors!

Client Data Store Encryption

Workstation operations need to store a local copy of the data that contains sensitive information that needs to be encrypted. Since employees usually have full access to the workstation, the decryption key is not stored on the workstation to prevent a potential security risk.

Using asymmetric encryption, the public key contained within the authentication token encrypts the data, but only the database containing a corresponding private key is able to decrypt data during playback.

Encrypting Data Transmission

Simphony supports HTTPS protocol for secure data communication. The TLS 1.2 configuration process requires the use of a certificate generated by a trusted certificate authority. Refer to the Simphony Installation Guide for information about the installation of secure certificates.

Key Manager

The EMC Key Manager module allows the database encryption pass phrase, the transmission key and the integrity keys to be changed. The database encryption pass phrase is used to encrypt secure data (credit card numbers, etc.) in the database; its value can be defined based on site security needs. The transmission key is the encryption scheme for network traffic; this key is not user-defined. The integrity keys are used to ensure that certain sensitive files that are transmitted to workstations have not been tampered with in transit or at rest.

Key Rotation Considerations

In order to achieve maximum security, Oracle Food and Beverage mandates the system administrator regularly rotate the site's keys, at least annually, and delete any old or comprised encryption keys. Simphony's entire design of data encryption, key generation, and storage is built to facilitate such practice. For more information, refer to the About the Simphony Encryption Key Manager Module.

A privileged employee may conduct key rotation in the EMC within the Enterprise level, Tasks tab, and Key Manager Tab. To authorize an employee to access the Key Manager module, the Key Manager action must be enabled within the EMC Roles module Actions tab. Only grant this authorization to the site's system administrator who is familiar with the site's management procedures and encryption key custodian duties.

Enabling

For detailed instructions about enabling the Key Manager Module and secure key practices, see Appendix C: Key Manager Manual.

4

Appendix A: Simphony Port Numbers

Access the link provided below in reference to Simphony Port Management.

- Port Numbers

Port Numbers

Access the topic links that include listings of port numbers that can be used in Simphony. Many port numbers are configurable in the EMC. Open only the minimum required ports based upon the installation type and deployment configuration.

- Enterprise Ports
- Property Ports
- Traffic Note
- Interface Ports
- iCare/Loyalty Ports
- Oracle Component Ports

Enterprise Ports

Table 4-1 Enterprise Ports

Service	Port Number	Configurable?
Simphony/EGateway (Oracle Database)	1521	Yes
Simphony/EGateway (Pre-Simphony version 2.6)	8050	Yes
Simphony2/EGateway (After upgrade/install of Simphony)	8080\443	Yes
EMC /Remote EMC	443	Yes
Simphony/Reporting and Analytics Advanced	80 – Browser 81–myLabor Service	Yes
SMTP Service for Email	25	Yes

Property Ports

Table 4-2 Property Ports

Service	Port Number	Configurable?
ServiceHost version 2	8080	Yes

Table 4-2 (Cont.) Property Ports

Service	Port Number	Configurable?
ServiceHost as a Service (no Ops)	8071	Yes
Print Controller	8080	Yes
IP Printer Listening	9100	No
Banquet Printing	9100	No
KDS Client (Display)	8080	Yes
KDS Controller Service	8080	Yes
Client Application Loader (server selection screen)	TCP 7300	No
Client Application Loader (property selection screen)	8080	Yes
NetTCPRelayBinding (TMS/ Azure)	TCP: 9350, 9351, 9352	No
NetTCPRelayBinding (TMS/ Azure)	HTTP: 80	No

Note that workstations running Linux for Micros are preconfigured with firewall rules, and available ports are limited.

Traffic Note

In general, all traffic is initiated by the workstation and requires only outbound TCP connections to the outside of the property. Check the site configuration as there are likely be exceptions to this rule.

Other ports: Check the wrapper.conf file for environment-specific Reporting and Analytics (formerly myMicros ports). The file's location is: `[Drive letter]:\MICROS\mymicros\myPortal\server\default\`**wrapper.conf**.

Note that for workstations running on Linux for MICROS, SSH is used for support. Therefore, SSH inbound might be needed for these connections (normally Port 22). If this port is intended for a local connection only, take measures to restrict wider access (that is, on WAN Firewall).

Interface Ports

All TCP ports used for Simphony interfaces are configurable from within the interface configuration of EMC. The following are the default TCP ports for common interfaces:

Table 4-3 Default Interface Port Numbers

Interface	Port Number	Configurable?
Table Management System	5006	Yes
Property Management System	5007	Yes
Credit Authorization	5008	Yes

Table 4-3 (Cont.) Default Interface Port Numbers

Interface	Port Number	Configurable?
System Interface Module (SIM)	5009	Yes

iCare/Loyalty Ports

The following table lists the default port numbers for the iCare/Loyalty interface.

Table 4-4 Loyalty Default Ports

Service	Port Number or Any Other Secure HTTPS Port	Configurable?
Access to Websites	9443	Yes
Secure Sockets Layer (SSL) Connectivity	9443	Yes

Oracle Component Ports

Here are links to Oracle Database documentation outlining the port ranges used by components that are configured during the installation. By default, the first port in the range is assigned to the component if it is available.

- Managing Oracle Database Port Numbers for Oracle Database 18c Release 1
- Managing Oracle Database Port Numbers for Oracle Database 12c Release 1

See the Oracle Database 18c Installation Guide for more information about default component port ranges.

5

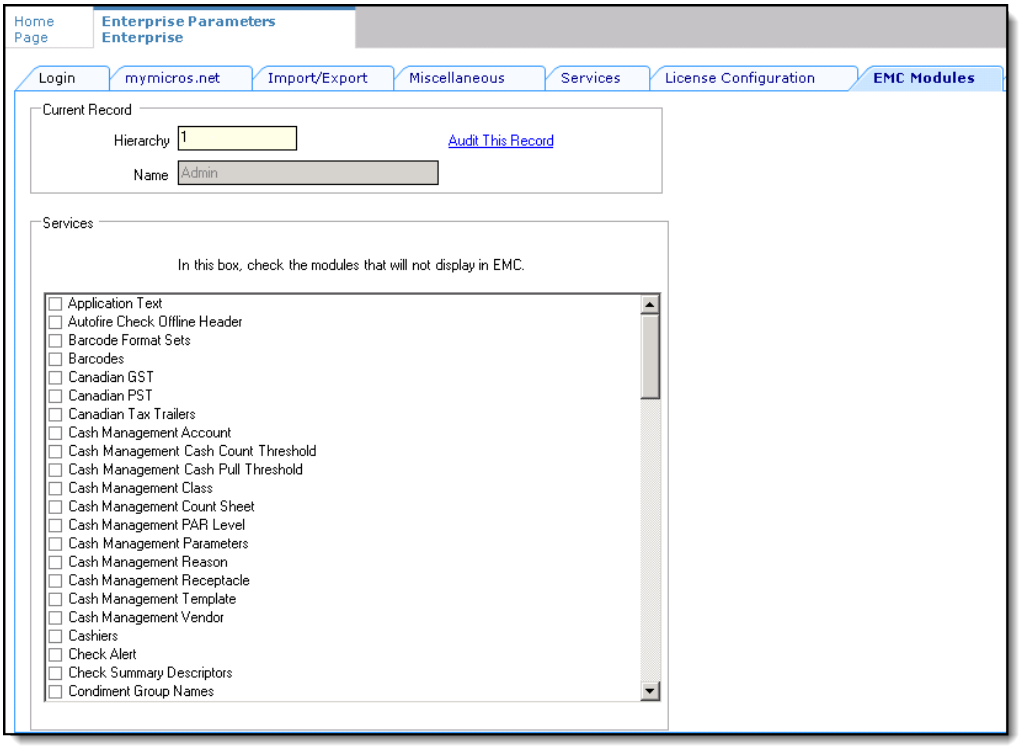
Appendix B: Module Accessibility

EMC Modules may be hidden from view by configuring the **EMC Modules** tab in the Enterprise Parameters module.

Any module that is selected in the following figure will not be displayed in the EMC. The purpose of this box is to allow customers to customize the modules that can be viewed. For example, if Kitchen Display Systems (KDS) are not in use, all of the KDS modules can be removed from view. Similarly, a site may want to exclude modules after they have been configured (for example, Major Groups), so that no one else is able to change the configuration.

Once a check box is selected here, the module or text is hidden from view for all Enterprise EMC users until the check box is deselected and the changes are saved.

Figure 5-1 Enterprise Parameters EMC Modules Tab



6

Appendix C: Key Manager Manual

This chapter reviews securing your system with Key Management and proper key rotation.

- General Information

General Information

Access the following links in reference to Key Management.

- About the Simphony Encryption Key Manager Module
- D-Secure Key Practices
- Key Manager Security Enhancements
- The Encryption Scheme
- Operational Considerations
- Periodic Key Rotation

About the Simphony Encryption Key Manager Module

The purpose of the Simphony Key Manager module within the EMC is to allow the user to set the encryption pass phrase for Simphony, and to rotate encryption and integrity keys when needed. Oracle Food and Beverage mandates that each site protect encryption keys against both disclosure and misuse.

D-Secure Key Practices

To ensure secure distribution, Oracle Food and Beverage mandates that users divide knowledge of a specific encryption key among two or three people. Users should establish dual control of keys so that it requires two to three people, each knowing only his or her part of the key, to reconstruct the entire key.

A site's management procedures must require the prevention of unauthorized substitution of keys. Furthermore, a site's management procedures must require the replacement of known or suspected compromised keys.

Key Manager Security Enhancements

Simphony stores the encryption keys used to encrypt and decrypt secure data, such as credit card numbers, in the database. The encryption keys themselves are encrypted using a master key that was generated on the fly based upon on an encrypted pass phrase stored in a separate database.

Simphony uses a new encryption scheme that allows for the secure deletion of encryption keys.

The Encryption Scheme

The secure deletion of existing encryption key data is accomplished through the deletion of the row of data containing the current passphrase and ID from the security database. After the row is deleted, a new row is inserted into the table along with the new passphrase data and an incremental ID. The process of key rotation runs in the background so that it does not require the system to be down during the key rotation process.

Operational Considerations

> **Note:**
>
> **Caution**: After a key rotation is performed by the Key Manager, the key database and transaction database become synchronized with new encryption key data. Because of this, users should not swap databases (restoring/replacing the existing database with a different one) until they are absolutely sure that the new databases are also in sync together (between the transaction database and the key database).

Periodic Key Rotation

In order to achieve maximum security, Oracle Food and Beverage mandates that the system administrator regularly rotate the site's encryption keys. Encryption key rotations are necessary and must occur periodically, at least annually. For maximum security, key rotations must occur on a regular basis.

7

Appendix D: Key Manager Module

This chapter reviews the steps for securing your system with proper Key Management and encryption key pass phrase rotation.

- Operating Conditions

Operating Conditions

The following conditions must be true for the Key Manager to run:

- The Simphony EGateway service must be up and running — IIS installed and running.
- The database must be accessible.

- Authorizations
- Key Manager Module
- Changing the Pass Phrase

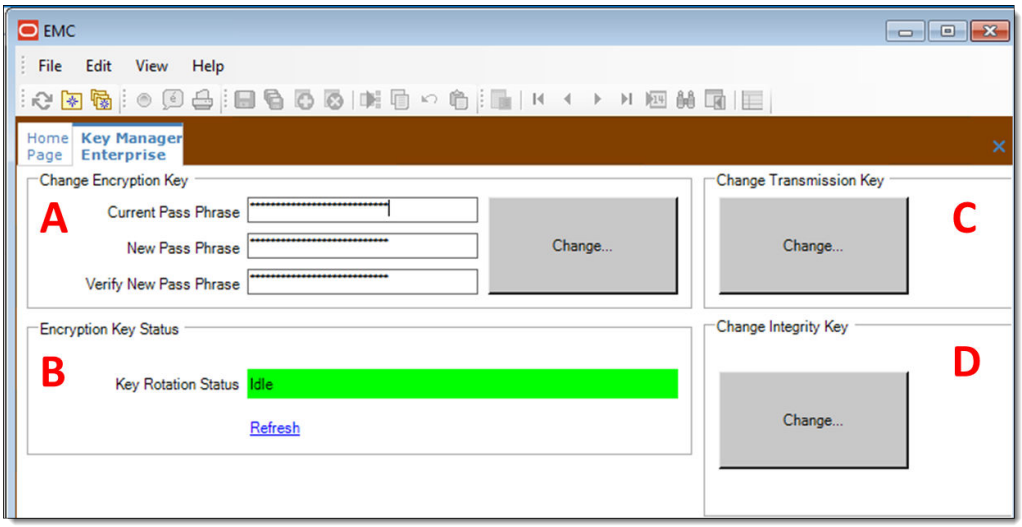
Authorizations

To access and use the Key Manager module, EMC users must be associated with an Enterprise Role with the Key Manager action enabled.

Only grant this authorization to the site's system administrator who is familiar with the site's management procedures and encryption key custodian duties. Restrict key access to the fewest number of custodians necessary

Key Manager Module

Figure 7-1 EMC Enterprise Key Manager Module



The areas of the module are:

- **A**: Change Encryption Key area.
- **B**: Encryption Key Status area.
- **C**: Change Transmission Key area.
- **D**: Change Integrity Key area.

Areas C and D, the Change Transmission Key and Change Integrity Key areas respectively, are unrelated to the database encryption pass phrase used to encrypt secure data. The transmission key is the encryption scheme for network traffic and the integrity keys are not user-defined.

Changing the Pass Phrase

The new pass phrase should adhere to the following rules:

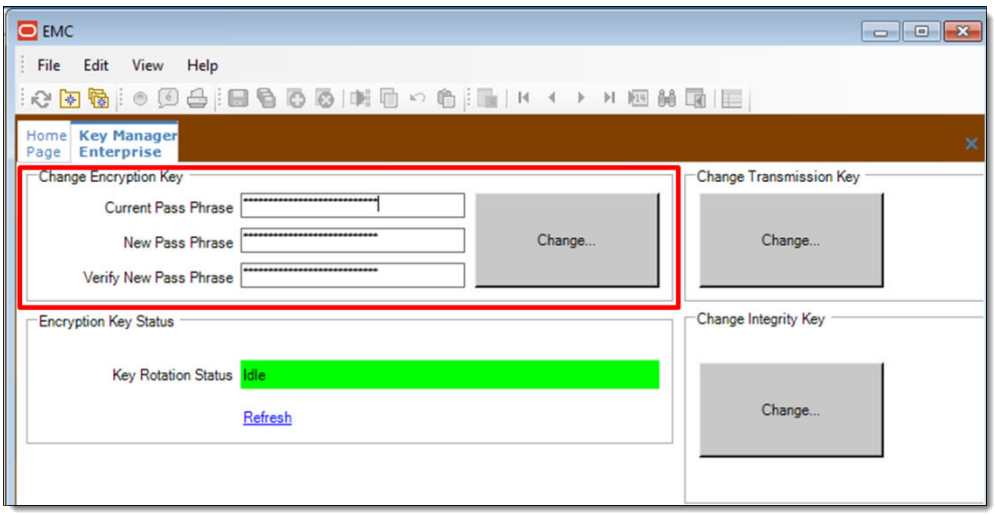
- Contain at least one uppercase alphabetic character
- Contain at least one numeric character
- Contain at least one special character from the following:

  ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` | ~ {}
- Must use a minimum of twenty characters (maximum of thirty characters)
- Must use a series of words for the pass phrase
  - Must use a minimum of three words
  - Each word must be separated using a space
- Must not use consecutive spaces

- Must be different from the last three previous pass phrases
- The pass phrase and confirmed pass phrases must match
- The transaction database must be accessible
- Must not contain any restricted expressions, company, or product names

> **Note:**
>
> **Caution**: If the pass phrase is lost, the encrypted data in the database is unrecoverable. There are no back doors!

Figure 7-2 Key Manager Module - In Progress



To change the pass phrase:

1. In the EMC, select the Enterprise level, and then select **Key Manager**.
2. In the Change Encryption Key section, enter the **Current Pass Phrase**, the **New Pass Phrase**, and re-enter the new pass phrase in the **Verify New Pass Phrase** field.
3. Click the **Change...** button.
4. A confirmation prompt appears. Click **Yes** to start the key rotation process.

   Another confirmation prompt displays.
5. Click **Yes** if there are no database backups currently in progress.

   Backing up the database during the key rotation process can potentially cause the data in the backup database to become out of sync with Simphony.
6. Click **No** if a database backup is currently in progress, and begin the key rotation process again after the backup is finished. The Key Rotation Status section indicates that the task is in progress.
7. After the pass phrase has successfully changed, click **OK**.

8

Appendix E: Simphony Payment Interface

The Simphony Payment Interface (SPI) is a standard set of messages that are exchanged between the Simphony Transaction System and Payment Service Providers (PSP). The purpose of the interface is to collect electronic payments in a way that keeps the transaction system free of Payment Card Industry (PCI) data. The messages themselves also do not contain PCI data, so wire transmission does not expose PCI data.

Oracle Food and Beverage recommends that configurations use a secure channel to communicate with PSPs. The level of security varies depending on the provider, so this should be a consideration when choosing a provider.

- Configuration Requirements for PSP using Transport Layer Security (TLS) in EMC

Configuration Requirements for PSP using Transport Layer Security (TLS) in EMC

This section contains information about TLS in relation to securing communications with Payment Service Providers (PSP).

- No TLS Support
- TLS Server Certificate Support

No TLS Support

In this case, Simphony is communicating with the PSP using a standard HTTP connection, without encryption. Customers using this configuration may use other compensating controls, such as Microsoft NT LAN Manager (NTLM), among others, to secure the network channel.

TLS Server Certificate Support

This configuration has two options:

- **No Certificate**: In this use case, the PSP wishes to use TLS, but does not provide a certificate (.cer file) to the client. The communication is secure, but the client has no way to validate the server private key.
- **Certificates**: Certificates are used to validate that the Server Public Key, which is presented to the client, is all right to use.
  - PSPs can use certificates from a known Certificate Authority, in which case the client can use the local pre-installed certificate to validate the Server Certificate.
  - PSPs can also use a self-signed certificate.
  - The PSP provides a .cer file so the client has the ability to validate the x509 certificate presented by the server.

TLS Client Certificate Support

Client Certificates can be used in a similar fashion to Server Certificates to validate that the client is a trusted client.

Certificate Handling by PSPs is outside the scope of our configuration and code.

Client Certificate Files are typically .pfx files and contain both private and public keys, along with a password to access the file. This .pfx file is sensitive and should be handled carefully.