# Oracle MICROS Simphony First Edition

## Security Guide

Release 1.8
F22933-03
August 2023

Oracle MICROS Simphony First Edition Security Guide, Release 1.8

F22933-03

# Contents

# Preface

This document provides security reference and guidance for Oracle MICROS Simphony First Edition.

### Audience

This document is intended for:

- Implementation consultants installing Oracle MICROS Simphony First Edition
- System administrators
- End users of Oracle MICROS Simphony First Edition

### Customer Support

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

https://support.oracle.com

When contacting Customer Support, please provide the following:

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

### Documentation

Oracle MICROS Food & Beverage product documentation is available on the Oracle Help Center at https://docs.oracle.com/en/industries/food-beverage/pos.html

### Revision History

| Date | Description |
|---|---|
| January 2020 | • Initial Publication. |
| February 2020 | • Added the “Reporting and Analytics Authentication” topic to the Chapter 1 – Simphony First Edition Security Overview Users Authentication section. |
| August 2023 | • Updated the Passwords Overview section in the Performing a Secure Simphony Installation chapter. |

# 1 Simphony First Edition Security Overview

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

## Basic Security Considerations

The following principles are fundamental to using any application securely:

- **Keep software up to date**

  This includes the latest product release and any patches that apply to it.
- **Limit privileges as much as possible**

  Users should be given only the access necessary to perform their work. User privileges should be reviewed periodically to determine relevance to current work requirements.
- **Monitor system activity**

  Establish who should access which system components, and how often, and monitor those components.
- **Install software securely**

  For example, use firewalls, secure protocols using TLS, and secure passwords. See Performing a Secure Simphony First Edition Installation for more information about secure application software installation.
- **Learn about and use the Oracle MICROS Simphony First Edition security features**

  See Implementing Oracle MICROS Simphony First Edition Security for more information about application security features.
- **Use secure development practices**

  Take advantage of existing database platform 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* at: `http://www.oracle.com/technetwork/topics/security/alerts-086861.html`
- **Testing**

  Testing is performed regularly with Oracle MICROS Simphony First Edition along with the latest Oracle and Microsoft software patches.

# Overview of Oracle MICROS Simphony First Edition Security

## Simphony Architecture Overview

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.

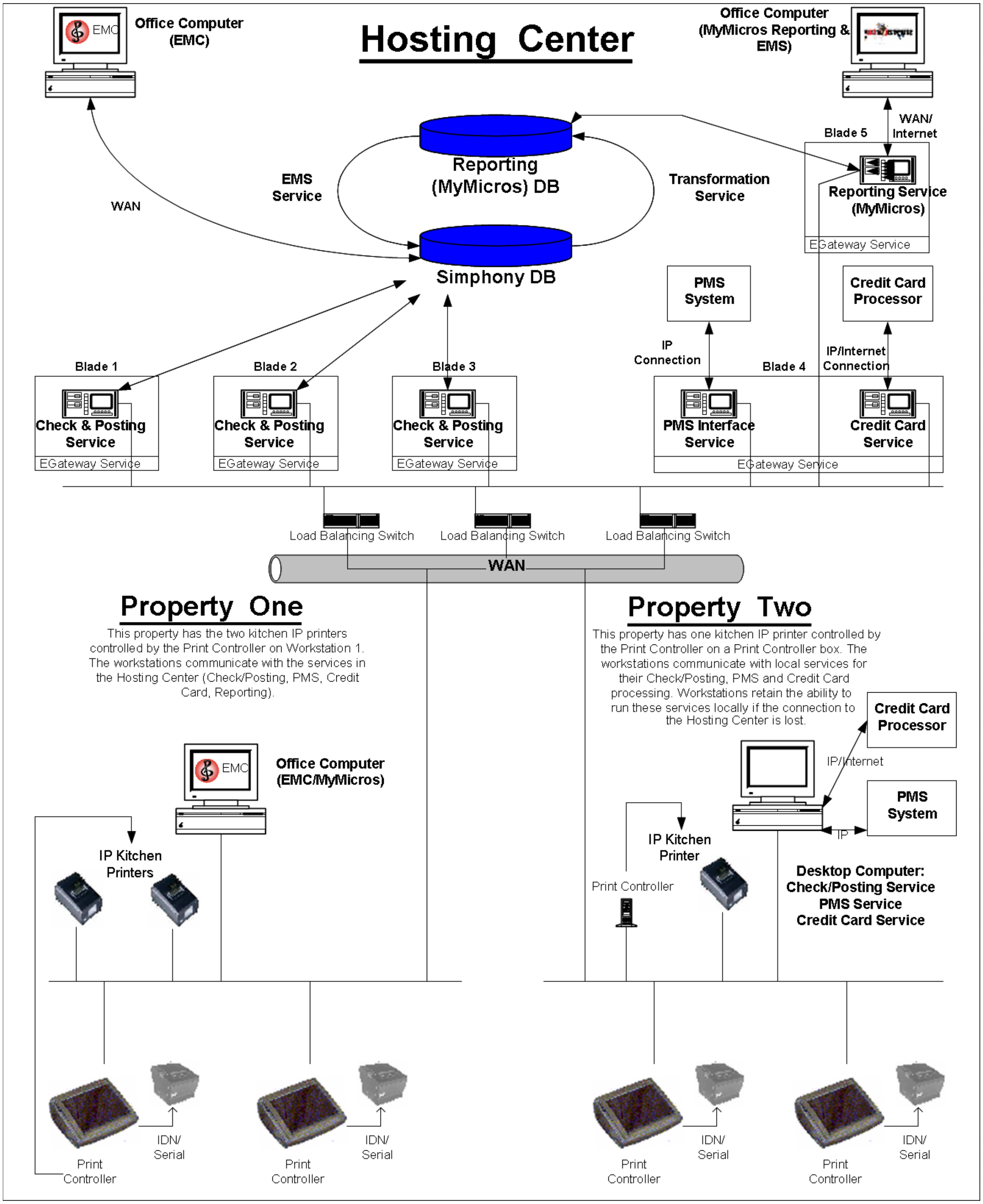
## Simphony Architecture vs. Single Server Systems

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.

## Technology

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

**Figure 1-1 - Basic Enterprise Topology for a Hosted Simphony Deployment**



This property has the two kitchen IP printers controlled by the Print Controller on Workstation 1. The workstations communicate with the services in the Hosting Center (Check/Posting, PMS, Credit Card, Reporting).

This property has one kitchen IP printer controlled by the Print Controller on a Print Controller box. The workstations communicate with local services for their Check/Posting, PMS and Credit Card processing. Workstations retain the ability to run these services locally if the connection to the Hosting Center is lost.

# Users Authentication

## Overview

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

## EMC Authentication

All users' logon credentials for Simphony First Edition are stored in the central database. If using biometrics, all fingerprint data is also stored in the central database. Anyone who has access to the Enterprise Management Console (EMC) must provide a login of a valid username/password or their fingerprint data. No two MICROS 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 First Edition application, always assign unique usernames and complex passwords to each account. Passwords are encrypted using the latest secure hashing as per Oracle's security standards. Refer to the *Simphony First Edition PA-DSS Implementation Guide* for more information about creating complex passwords.

## Workstation Authentication

Simphony architecture supports both the server side and the workstation client side of authentication. Server authentication is optional and is accomplished via configuring the HTTPS connection and installing a signed certificate on the server. Client side authentication is required for Simphony operations and cannot be disabled. Setup during initial workstation installation, Simphony requires a workstation to authenticate itself before workstation services are able to communicate over the Simphony First Edition network.

> **NOTE:**
>
> Simphony First Edition security does not use the Windows Login.

In order for the Simphony First Edition workstation to be able to post transactions to a Simphony application server, it has to be authenticated first. The process of authentication is accomplished during initial workstation installation, when an installer is prompted to enter a set of credentials—User Name/Password—that are transmitted over an encrypted channel to the application server. After the application server validates the credentials, it issues an authentication token 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 signed with the private key contained within the authentication token. The server stores a public key for each authenticated client in the database and can verify authenticity of an incoming request.

## User Authentication

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

## Reporting and Analytics Authentication

To generate a PMC Report in Simphony First Edition, the workstation sends an authenticated HTTPS request to the enterprise server.

The enterprise server securely connects to the R&A server using HTTPS. After a session is established, the report request sends with the R&A credentials previously configured using the EMC, and is then stored securely in the Simphony database. The R&A server authenticates the request using the provided credentials and checks the authorization level. If successful, the report generates and returns to the Simphony Server, which in turn processes and returns a formatted report for the workstation.

## Database User Management

The Simphony First Edition sample database is installed with only one pre-defined username and password, the Simphony First Edition user (micros, micros), which allows access to Simphony First Edition's configurator, the Enterprise Management Console (EMC). Oracle MICROS Food & Beverage mandates that users create a different, strong password for the pre-defined Simphony First Edition user within the EMC's Enterprise level, Personnel, and Employees module. The password must follow Payment Card Industry (PCI) Data Security Standard (DSS) guidelines described in the *Simphony First Edition PA-DSS Implementation Guide*. The password must be at least 8 characters long and include letters and numbers. Simphony First Edition's installation wizard prompts for the creation of a System Administrator username and password. The System Administrator is used to log into the Oracle Database (or Microsoft SQL Server database, depending on the Enterprise's setup). Simphony First Edition's installation wizard also prompts for the creation of a System Database User. Simphony First Edition's code uses the System Database User to access the database during communication with services. Before any code can make database statements to the Oracle Database (or Microsoft SQL Server database), the Microsoft SQL Server database requires a username and password in the SQL string. Oracle MICROS Food & Beverage mandates using a unique username and a complex password consisting of more than eight characters including alphanumeric and special characters.

## Security Note

Authentication Database credentials are stored in the configuration file on the Simphony First Edition application server, protected by Microsoft Windows Server file permissions. No applications, except for the Simphony First Edition application server, requires direct access to the transaction database. 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 First Edition Environment

When planning your Simphony First Edition implementation, consider the following:

1. **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

2. **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.

3. **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.

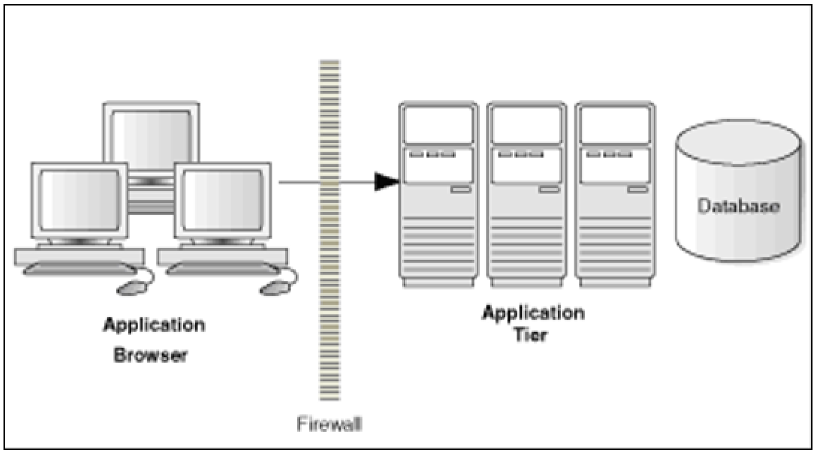
# Recommended Deployment Configurations

This section describes recommended deployment configurations for Simphony First Edition.

The Simphony First Edition product can be deployed on a single server or in a cluster of servers. The simplest deployment architecture is the one shown in Figure 1-2 below.

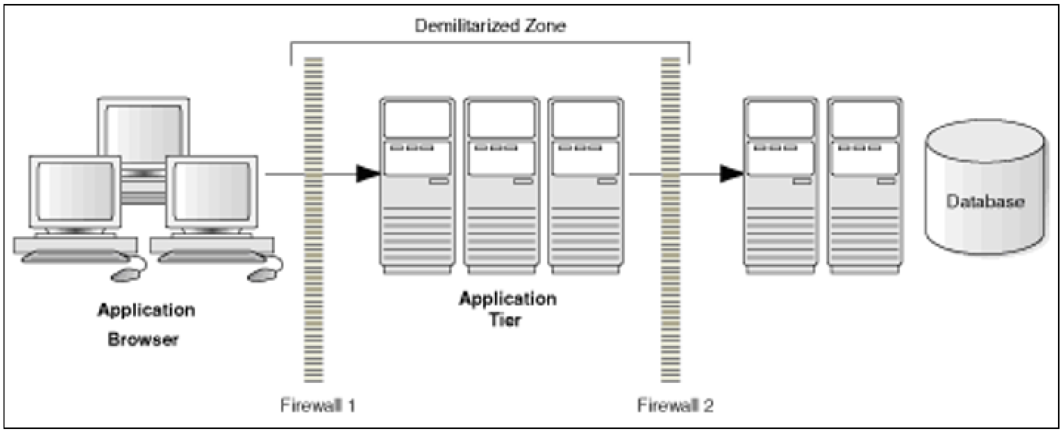
This single-computer deployment may be cost effective for small organizations; however, it cannot provide high availability because all components are stored on the same computer. In a single server environment such as the typical installation, the server should be protected behind a firewall.

**Figure 1-2 - Single-Computer Deployment Architecture**



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

**Figure 1-3 - Traditional DMZ View**



The term demilitarized zone (DMZ) refers to a server that is isolated by firewalls from both the Internet and 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 Simphony First Edition Port Numbers in Appendix B for more information about Simphony First Edition network Port usage.

# Simphony First Edition Security

## Operating System Security

Prior to installation of Simphony First Edition, it is essential that the operating system be updated with the latest security updates

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

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

## Database Platform Security

Ensure that database login auditing is enabled regardless of the database platform that is being utilized.

## Oracle Database

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

## Microsoft SQL Server

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

2

# Performing a Secure Simphony First Edition Installation

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

## Pre-Installation Configuration

Prior to installation of Simphony First Edition, perform the following tasks:

- Apply critical security patches to the operating system
- Apply critical security patches to the database server application
- Ensure that connections to the database are restricted to a few trusted nodes using firewall rules or the Oracle listener invited nodes feature
- Review the Oracle MICROS Enterprise Back Office Security Guide based on the version of Reporting and Analytics (R&A) that you are using. R&A versions 8.5.1, 9.0, or 9.1 are supported.
- Review the Oracle MICROS Hardware Wireless Networking Best Practices Guide

## Oracle MICROS Simphony First Edition 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.

During the installation of Simphony First Edition version 1.8, the installation application disables all administrative shares on the Simphony First Edition application server.

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 guidelines for all users.

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

- Simphony EGateway
- Simphony SimFEWebSvc

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

- Data Posting Service (DPS)
- Data Transfer Service (New DTS)
- Labor Posting Service (LPS)
- Enterprise Maintenance Service (EMS) Batch Service
- Sequencer Service

Simphony First Edition requires the **SimFEWebPortal** web application to download the CAL and Remote EMC setup files from the Simphony First Edition Web Portal (SFEWP).

# Post-Installation Configuration

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

## Operating System

### Turn On Data Execution Prevention (DEP)

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

### Turning Off Auto Play

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

### Browser Security

The Simphony First Edition 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.

Below is a list of some of the more commonly used browsers along with a link to documentation that describes the security settings of each browser.

Internet Explorer

`http://windows.microsoft.com/en-us/internet-explorer/ie-security-privacy-settings`

Mozilla Fire Fox

`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 First Edition patches available on My Oracle Support. Follow the deployment instructions included with the patch.

# Passwords Overview

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

### Maintaining Strong Passwords

Ensure that passwords adhere to the following strength requirements:

1. The password must be at least 12 characters long with a maximum of 20 characters.
2. The password must contain letter(s), number(s), and punctuation character(s): ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [ \ ] ^ _ ` { | } ~
3. Users may not choose a password equal to any of the last 4 passwords used.
4. Passwords cannot be the same as a user name.

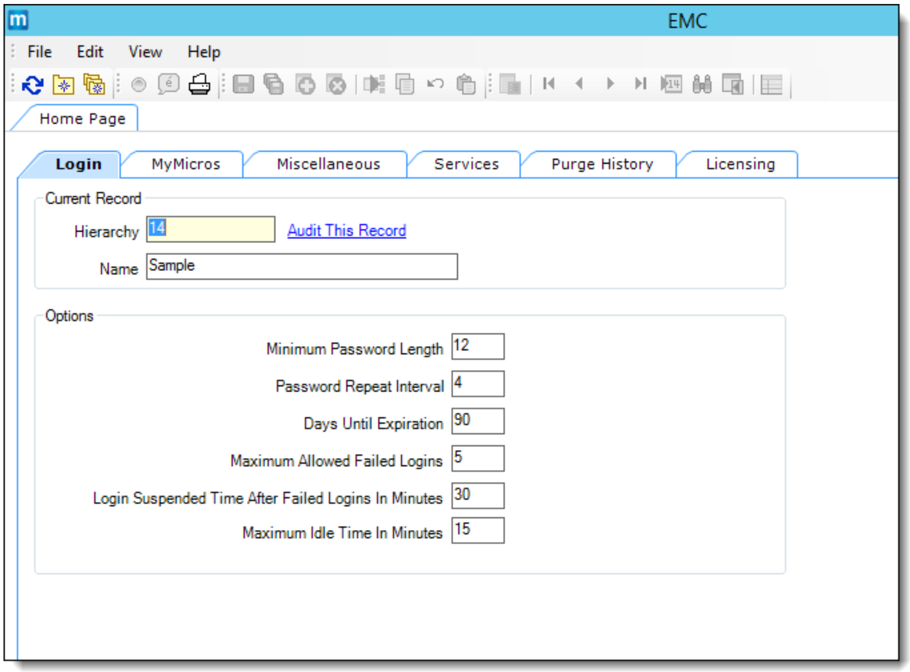
### Configuring Passwords

The following password policy options are configured as shown below.

In the EMC, Enterprise Parameters, Login tab, Enhanced Password Security tab, ensure that the corresponding options are configured as follows:

- Minimum Password Length contains at least 12 characters with a maximum of 20
- Password Repeat Interval must be set between numbers 4 and 10 and cannot be set to 0
- Days Until Expiration must not be greater than 90 days and cannot be set to 0
- Maximum Allowed Failed Logins has a maximum of 5 attempts and cannot be set to 0
- Maximum Idle Time In Minutes has a maximum of 15 minutes and cannot be set to 0
- After 5 failed EMC login attempts, logins are suspended for a configurable time between 5 and 30 minutes

**Figure 2-1 - Enterprise Parameters Login Tab – Password Configuration**



Current Record

Hierarchy: 14

Name: Sample

Options

Minimum Password Length: 12

Password Repeat Interval: 4

Days Until Expiration: 90

Maximum Allowed Failed Logins: 5

Login Suspended Time After Failed Logins In Minutes: 30

Maximum Idle Time In Minutes: 15

## Change Default Passwords

The Simphony First Edition Sample/Demo databases are installed with default master EMC users and passwords. Oracle MICROS Food & Beverage mandates changing your master username password after logging in for the first time in the EMC, while adhering to the above guidelines. When logging into EMC, if the password that is entered does not meet the requirements, the user is prompted to change the password.

## Configure User Accounts and Privileges

When configuring users of the Simphony First Edition application, ensure that they are assigned the minimum privilege level required to perform their job function. User privileges are described in the Access Control section.

## Encryption Keys

Simphony First Edition installs an encryption key using a default passphrase. System administrators need to rotate the encryption key on a regular basis. It is suggested to follow the PCI guidelines for encryption key rotation. Refer to the Key Manager Manual for more information about encryption key rotation.

## Configure Workstation USB Ports

To prohibit unauthorized use of standard USB ports for malicious purposes on client workstations while SAROPS is up and running, all the standard USB ports on the client workstations are disabled by default upon starting SAROPS. In order to enable the USB ports, you need to configure the port numbers to be enabled/disabled either in the EMC or the SAROPS PMC module. In the EMC, ports enabled/disabled can be configured in the workstations and printers configuration module at the property level. To enable or disable USB ports using the PMC, the appropriate privilege for configuring USB ports should be granted for the associated employee role.

## Change Database Passwords

**Crypt** is a database credential management tool for the Simphony First Edition application. Crypt allows you to manage existing 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:

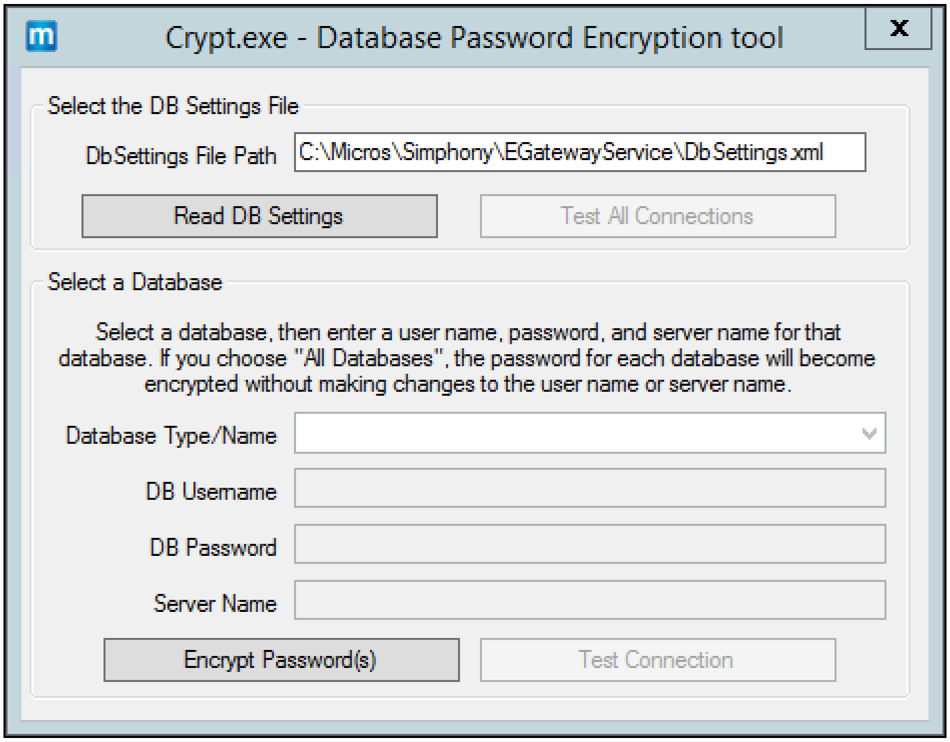
- Test database connections
- Change database passwords
- Encrypt database passwords

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

To access the Crypt utility:

1. Sign onto the Simphony FE application server.
2. Access the <*Drive letter*>:\Micros\Simphony\Tools\ and double-click the **Crypt** executable. The utility edits the Simphony FE DbSettings.xml file.

**Figure 2-2 - Crypt Database Password Encryption Tool**



DbSettings File Path: C:\Micros\Simphony\EGatewayService\DbSettings.xml

Select a database, then enter a user name, password, and server name for that database. If you choose "All Databases", the password for each database will become encrypted without making changes to the user name or server name.

To use the Crypt utility, perform the following steps:

**Table 2-1 - Using the Crypt Database Password Encryption Tool**

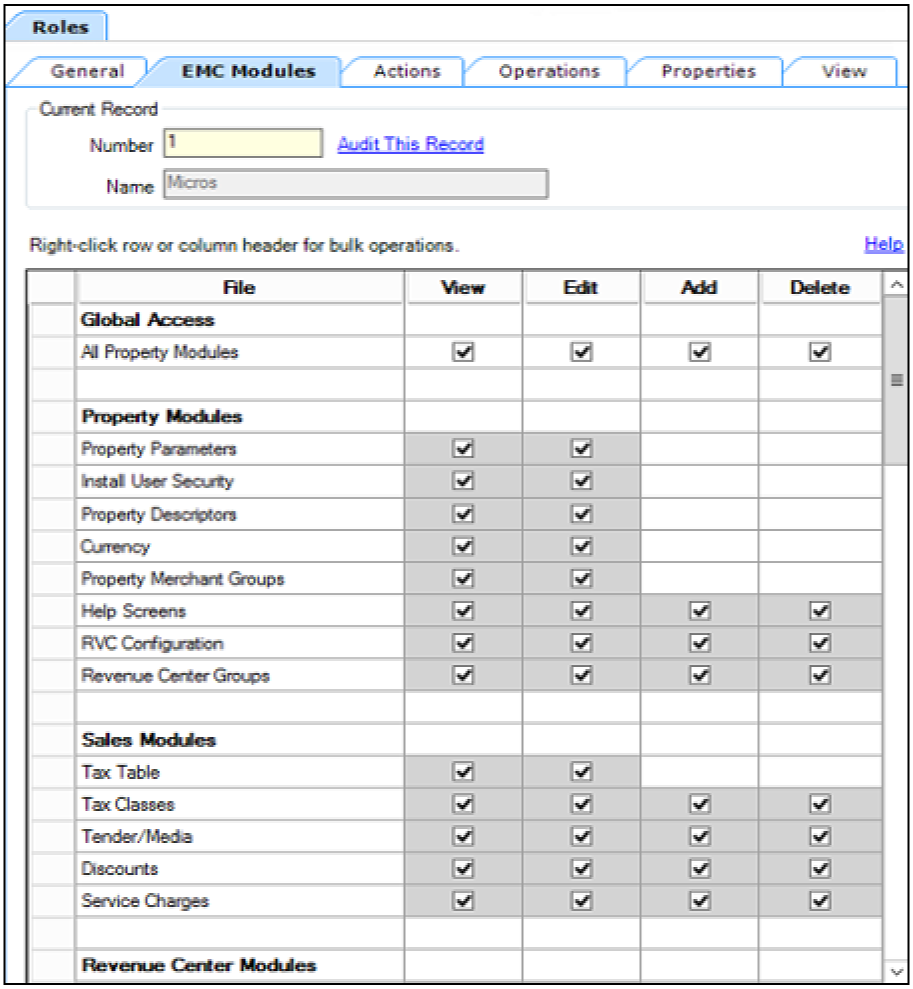
| To: | Perform the following steps: |
|---|---|
| Change Database Passwords | 1. Select your database of choice or **ALL Databases**.<br>2. Enter the username in the **DB Username** field.<br>3. Enter a new password in the **DB Password** field.<br>4. Enter the Simphony FE application server name in the **Server Name** field.<br>5. Click the **Encrypt Password(s)** button.<br>6. Click the **Test Connection** button to verify that the Simphony FE application DB Passwords match the database passwords. |
| Encrypt Database Passwords | 1. Select your database of choice or **ALL Databases**.<br>2. Click the **Encrypt Passwords(s)** button.<br>3. Click the **Test Connection** button. |
| Test Database Connections | 1. Select your database of choice or **ALL Databases**.<br>2. Click the **Test Connection** button. |

# Property Password Maintenance

Change your Simphony First Edition Property's **Install Username** and **Database Password**.

1. Navigate to EMC, Roles, and the EMC Modules tab.
2. Ensure the employee’s assigned Role has **Install User Security** View and Edit access enabled for the user(s) making the change and click **Save**.

**Figure 2-3 - Enterprise Roles EMC Modules Tab - Access Control**



Current Record

Number 1

Name Micros

Right-click row or column header for bulk operations.

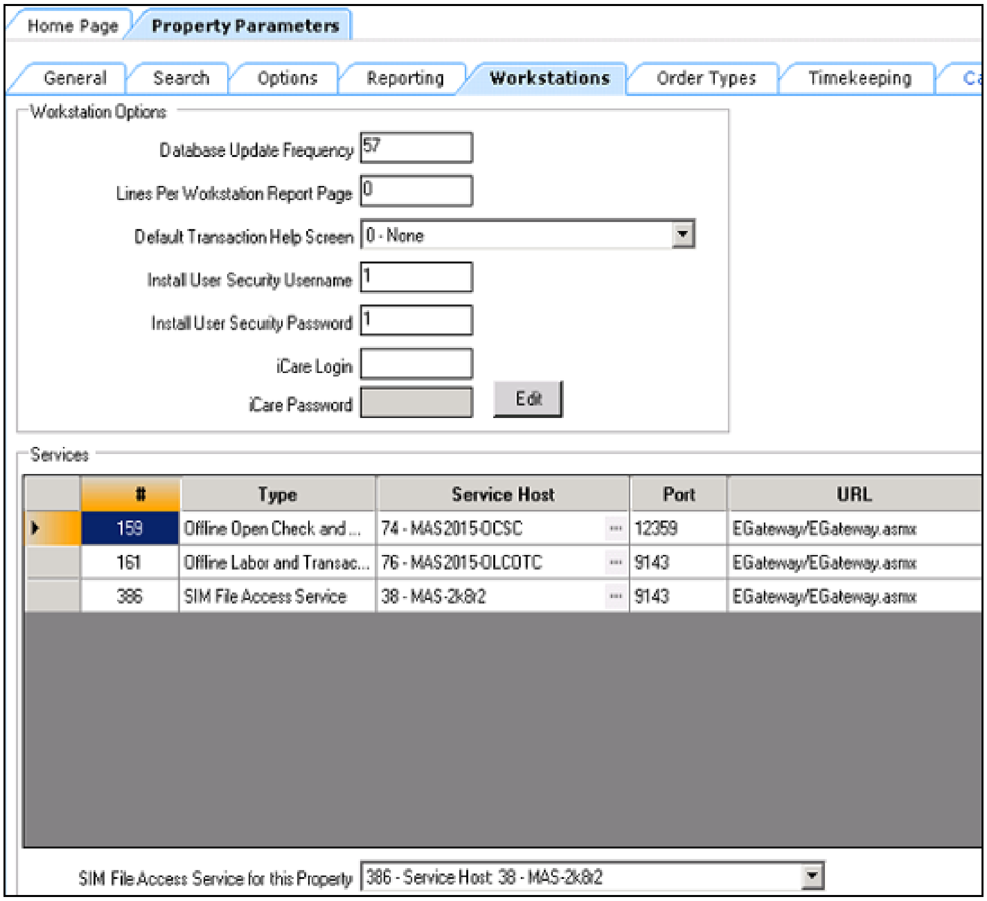
| File | View | Edit | Add | Delete |
|---|---|---|---|---|
| **Global Access** | | | | |
| All Property Modules | ☑ | ☑ | ☑ | ☑ |
| | | | | |
| **Property Modules** | | | | |
| Property Parameters | ☑ | ☑ | | |
| Install User Security | ☑ | ☑ | | |
| Property Descriptors | ☑ | ☑ | | |
| Currency | ☑ | ☑ | | |
| Property Merchant Groups | ☑ | ☑ | | |
| Help Screens | ☑ | ☑ | ☑ | ☑ |
| RVC Configuration | ☑ | ☑ | ☑ | ☑ |
| Revenue Center Groups | ☑ | ☑ | ☑ | ☑ |
| | | | | |
| **Sales Modules** | | | | |
| Tax Table | ☑ | ☑ | | |
| Tax Classes | ☑ | ☑ | ☑ | ☑ |
| Tender/Media | ☑ | ☑ | ☑ | ☑ |
| Discounts | ☑ | ☑ | ☑ | ☑ |
| Service Charges | ☑ | ☑ | ☑ | ☑ |
| | | | | |
| **Revenue Center Modules** | | | | |

# Configure Workstation Installer Passwords

1. Navigate to EMC, Property Parameters, and select the **Workstations** tab.
2. Enter the **Install User Security Username** and **Install User Security Password** which is used to install all workstations that Simphony uses to access the enterprise for the specified property.
3. After entering the user name and password, click **Save**.

Repeat these steps for all of the properties in the Enterprise.

**Figure 2-4 - Property Parameters Workstations Tab**



Workstation Options

Database Update Frequency: 57
Lines Per Workstation Report Page: 0
Default Transaction Help Screen: 0 - None
Install User Security Username: 1
Install User Security Password: 1
iCare Login:
iCare Password:

Services

| # | Type | Service Host | Port | URL |
|---|---|---|---|---|
| 159 | Offline Open Check and ... | 74 - MAS2015-OCSC | 12359 | EGateway/EGateway.asmx |
| 161 | Offline Labor and Transac... | 76 - MAS2015-OLCOTC | 9143 | EGateway/EGateway.asmx |
| 386 | SIM File Access Service | 38 - MAS-2k8r2 | 9143 | EGateway/EGateway.asmx |

SIM File Access Service for this Property: 386 - Service Host: 38 - MAS-2k8r2

# Data Purging

Review the database purging configuration settings to ensure that any sensitive data is only stored for the minimum required time period. Data purging is configured in EMC under Enterprise Parameters in the **Miscellaneous** tab.

Refer to the *Simphony First Edition PA-DSS Implementation Guide* for more information about data purging.

# 3 Implementing Oracle MICROS Simphony First Edition Security

This chapter explains the Simphony First Edition security features.

## Authorization Privileges

### Overview

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

User authorization privileges are configured in the EMC within the Enterprise level, Personnel, Enterprise Roles, Roles module. Workstation services also have their own EMC privileges within the Property level, Property Hardware, and Workstations module.

### Enterprise Roles

An Enterprise Role is a group of privilege options defining which enterprise-level EMC modules a user can access, and which Enterprise level actions the user can perform. Enterprise Roles function the same as Employee Roles with regard to determining an employee's access to a module; multiple Enterprise Roles may be assigned to a single employee, making the configuration of an Enterprise Roles a task-based procedure. For example, a role may include permissions that only allow a user to edit employees.

### EMC Configuration

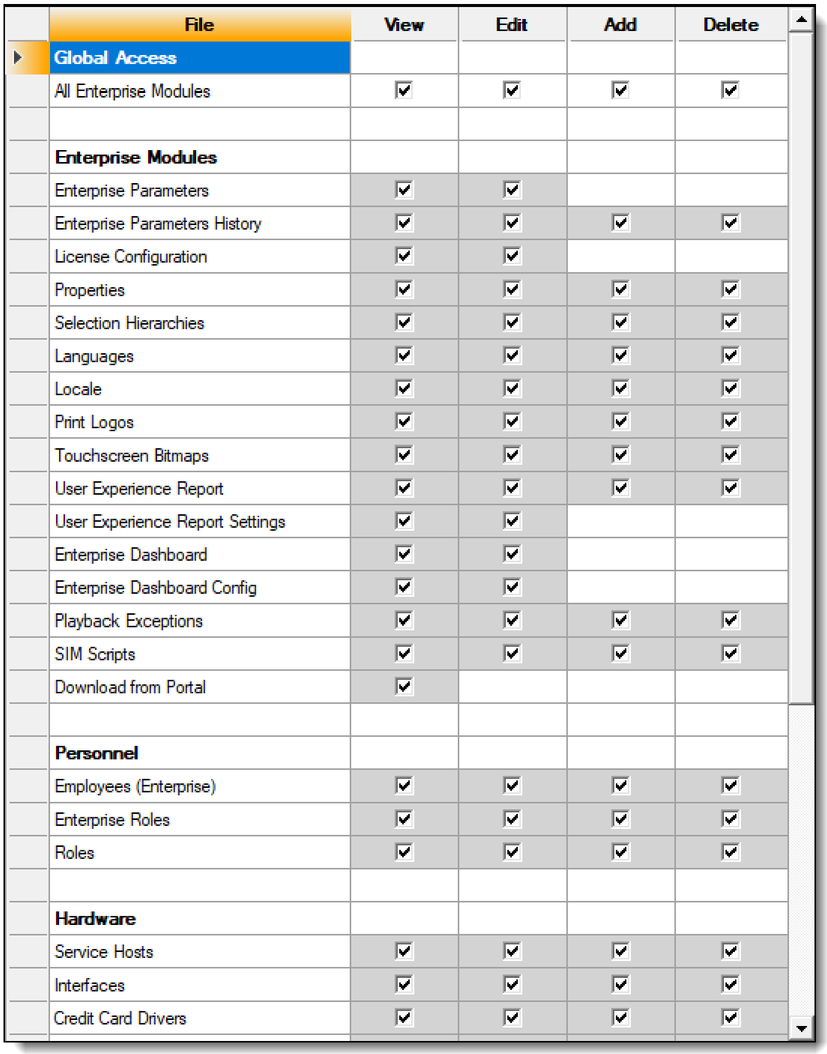
The Enterprise Roles module is opened from the Enterprise level of EMC. Do not confuse with the Employee Roles module, which is also located on the Enterprise level.

**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 - Enterprise Roles EMC Modules Tab**



| File | View | Edit | Add | Delete |
|---|---|---|---|---|
| Global Access | | | | |
| All Enterprise Modules | ☑ | ☑ | ☑ | ☑ |
| | | | | |
| **Enterprise Modules** | | | | |
| Enterprise Parameters | ☑ | ☑ | | |
| Enterprise Parameters History | ☑ | ☑ | ☑ | ☑ |
| License Configuration | ☑ | ☑ | | |
| Properties | ☑ | ☑ | ☑ | ☑ |
| Selection Hierarchies | ☑ | ☑ | ☑ | ☑ |
| Languages | ☑ | ☑ | ☑ | ☑ |
| Locale | ☑ | ☑ | ☑ | ☑ |
| Print Logos | ☑ | ☑ | ☑ | ☑ |
| Touchscreen Bitmaps | ☑ | ☑ | ☑ | ☑ |
| User Experience Report | ☑ | ☑ | ☑ | ☑ |
| User Experience Report Settings | ☑ | ☑ | | |
| Enterprise Dashboard | ☑ | ☑ | | |
| Enterprise Dashboard Config | ☑ | ☑ | | |
| Playback Exceptions | ☑ | ☑ | ☑ | ☑ |
| SIM Scripts | ☑ | ☑ | ☑ | ☑ |
| Download from Portal | ☑ | | | |
| | | | | |
| **Personnel** | | | | |
| Employees (Enterprise) | ☑ | ☑ | ☑ | ☑ |
| Enterprise Roles | ☑ | ☑ | ☑ | ☑ |
| Roles | ☑ | ☑ | ☑ | ☑ |
| | | | | |
| **Hardware** | | | | |
| Service Hosts | ☑ | ☑ | ☑ | ☑ |
| Interfaces | ☑ | ☑ | ☑ | ☑ |
| Credit Card Drivers | ☑ | ☑ | ☑ | ☑ |

From the EMC Modules tab, Enterprise 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
- **Delete** records

> **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.

The Enterprise Parameters module does not offer Add or Delete options because individual records cannot be added or deleted.

### All Enterprise Modules

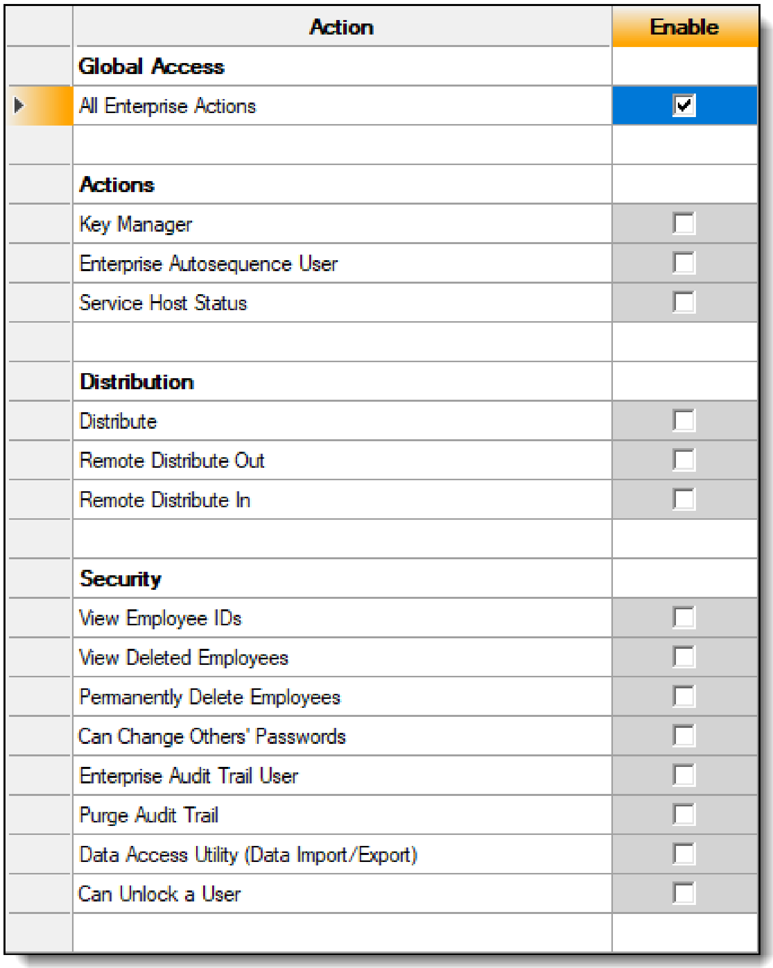
The **Global Access** check boxes are available so that a role may be easily configured to allow users to View, Edit, Add, or Delete within modules without having to individually select each box. Furthermore, enabling these check boxes allows access to new modules that are created in the future. For instance, if a new Enterprise level module is created and released in a new version, an employee with the **All Enterprise Modules** check box enabled is able to access this module without having to have a specific check box for that new module enabled.

Oracle MICROS Food & Beverage recommends that Enterprise administrator-type roles have the **All Enterprise Modules** checkboxes selected, so that administrators are always be able to access every module in the system.

### Actions tab (Enterprise level)

From the Actions tab, Enterprise Roles are provided access to specific actions that can be performed in the EMC.

**Figure 3-2 - Enterprise Roles Actions Tab**



| | Action | Enable |
|---|---|---|
| | **Global Access** | |
| ▶ | All Enterprise Actions | ☑ |
| | | |
| | **Actions** | |
| | Key Manager | □ |
| | Enterprise Autosequence User | □ |
| | Service Host Status | □ |
| | | |
| | **Distribution** | |
| | Distribute | □ |
| | Remote Distribute Out | □ |
| | Remote Distribute In | □ |
| | | |
| | **Security** | |
| | View Employee IDs | □ |
| | View Deleted Employees | □ |
| | Permanently Delete Employees | □ |
| | Can Change Others' Passwords | □ |
| | Enterprise Audit Trail User | □ |
| | Purge Audit Trail | □ |
| | Data Access Utility (Data Import/Export) | □ |
| | Can Unlock a User | □ |
| | | |

### All Enterprise Actions

Similar to the Global Access options on the **EMC Modules** tab, selecting the **Enable** check box gives users associated with this role permission to perform all actions. Oracle MICROS Food & 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 an Enterprise Role assigned is not able to access any Enterprise level modules. If a site upgrades a 9700 HMS system to Simphony First Edition, no users have an Enterprise Role assigned; the DbProcs utility must be run to create an Enterprise Role and associate it with a user.

## Employee Roles

Security privileges are established within the EMC, Enterprise level, Personnel, and Roles module.

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 Employee Role may be configured for all properties in the Simphony FE system or a role may be active in only one or a few properties. In addition, multiple Employee 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). 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.

> **NOTE:**
>
> Employee Roles are assigned to an employee in the EMC within the Enterprise level, Personnel, Employees, and Roles tab.

## EMC Configuration

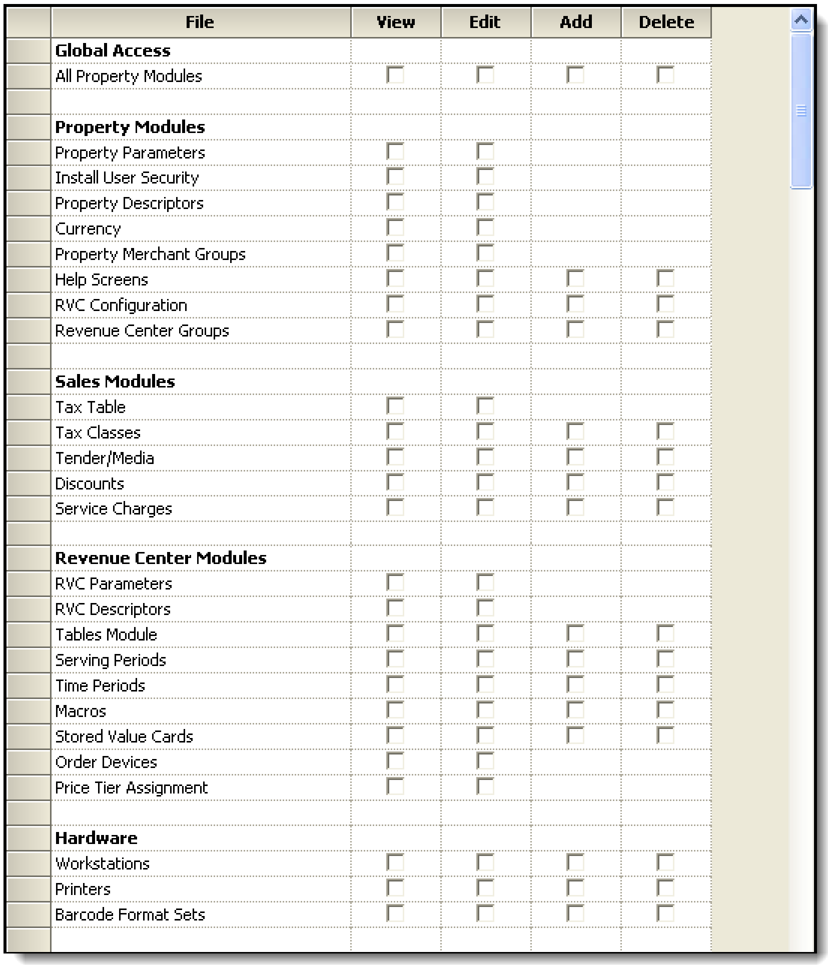
### General Tab

Only three configurable fields exist on the General tab. They are:

- **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 (Property level)

Figure 3-3 - Property level Roles EMC Modules Tab



| File | View | Edit | Add | Delete |
|---|---|---|---|---|
| **Global Access** | | | | |
| All Property Modules | □ | □ | □ | □ |
| | | | | |
| **Property Modules** | | | | |
| Property Parameters | □ | □ | | |
| Install User Security | □ | □ | | |
| Property Descriptors | □ | □ | | |
| Currency | □ | □ | | |
| Property Merchant Groups | □ | □ | | |
| Help Screens | □ | □ | □ | □ |
| RVC Configuration | □ | □ | □ | □ |
| Revenue Center Groups | □ | □ | □ | □ |
| | | | | |
| **Sales Modules** | | | | |
| Tax Table | □ | □ | | |
| Tax Classes | □ | □ | □ | □ |
| Tender/Media | □ | □ | □ | □ |
| Discounts | □ | □ | □ | □ |
| Service Charges | □ | □ | □ | □ |
| | | | | |
| **Revenue Center Modules** | | | | |
| RVC Parameters | □ | □ | | |
| RVC Descriptors | □ | □ | | |
| Tables Module | □ | □ | □ | □ |
| Serving Periods | □ | □ | □ | □ |
| Time Periods | □ | □ | □ | □ |
| Macros | □ | □ | □ | □ |
| Stored Value Cards | □ | □ | □ | □ |
| Order Devices | □ | □ | | |
| Price Tier Assignment | □ | □ | | |
| | | | | |
| **Hardware** | | | | |
| Workstations | □ | □ | □ | □ |
| Printers | □ | □ | □ | □ |
| Barcode Format Sets | □ | □ | □ | □ |

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
- **Delete** records

**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 RVC Parameters or Order Devices, there is not an Add or Delete option because individual records cannot be inserted or deleted.

# All Property Modules

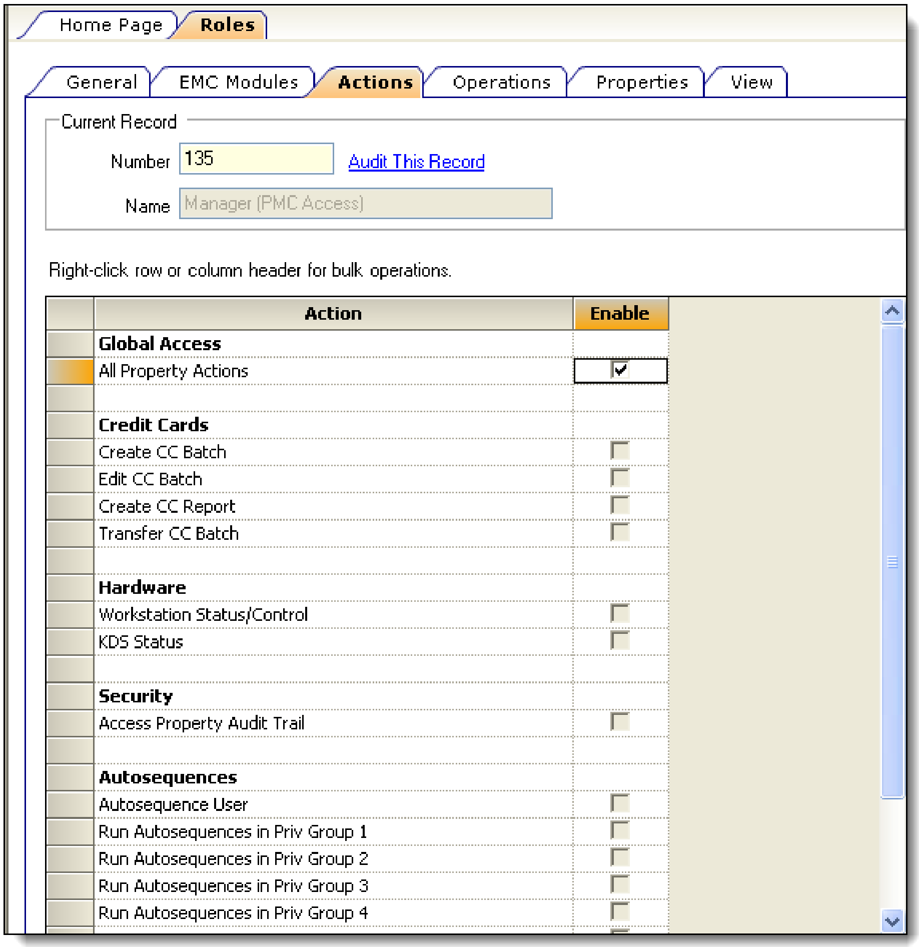
The **Global Access** check boxes are available so that a role may be easily configured to View, Edit, Add, or Delete every module without having to individually check each box. Furthermore, these check boxes allow access to new modules that may be created in the future.

For instance, if a new module is created and released in a new version, an employee with the Global Access check box enabled for View is able to access this module without having a specific checkbox selected. Oracle MICROS Food & Beverage recommends that administrator-type roles have the **All Property Actions** checkbox selected, so that administrators are always able to access every module in the system.

### Actions Tab (Property level)

From the Actions tab, Roles are assigned access to specific actions that can be performed in the EMC. Note that all of the **Run PC Autosequences in Privilege Group *X*** checkboxes are disabled unless the **Autosequence User field** checkbox is selected first.

**Figure 3-4 - Property level Roles Actions Tab**



Current Record

Number 135

Name Manager (PMC Access)

Right-click row or column header for bulk operations.

| Action | Enable |
|---|---|
| **Global Access** | |
| All Property Actions | ☑ |
| | |
| **Credit Cards** | |
| Create CC Batch | □ |
| Edit CC Batch | □ |
| Create CC Report | □ |
| Transfer CC Batch | □ |
| | |
| **Hardware** | |
| Workstation Status/Control | □ |
| KDS Status | □ |
| | |
| **Security** | |
| Access Property Audit Trail | □ |
| | |
| **Autosequences** | |
| Autosequence User | □ |
| Run Autosequences in Priv Group 1 | □ |
| Run Autosequences in Priv Group 2 | □ |
| Run Autosequences in Priv Group 3 | □ |
| Run Autosequences in Priv Group 4 | □ |

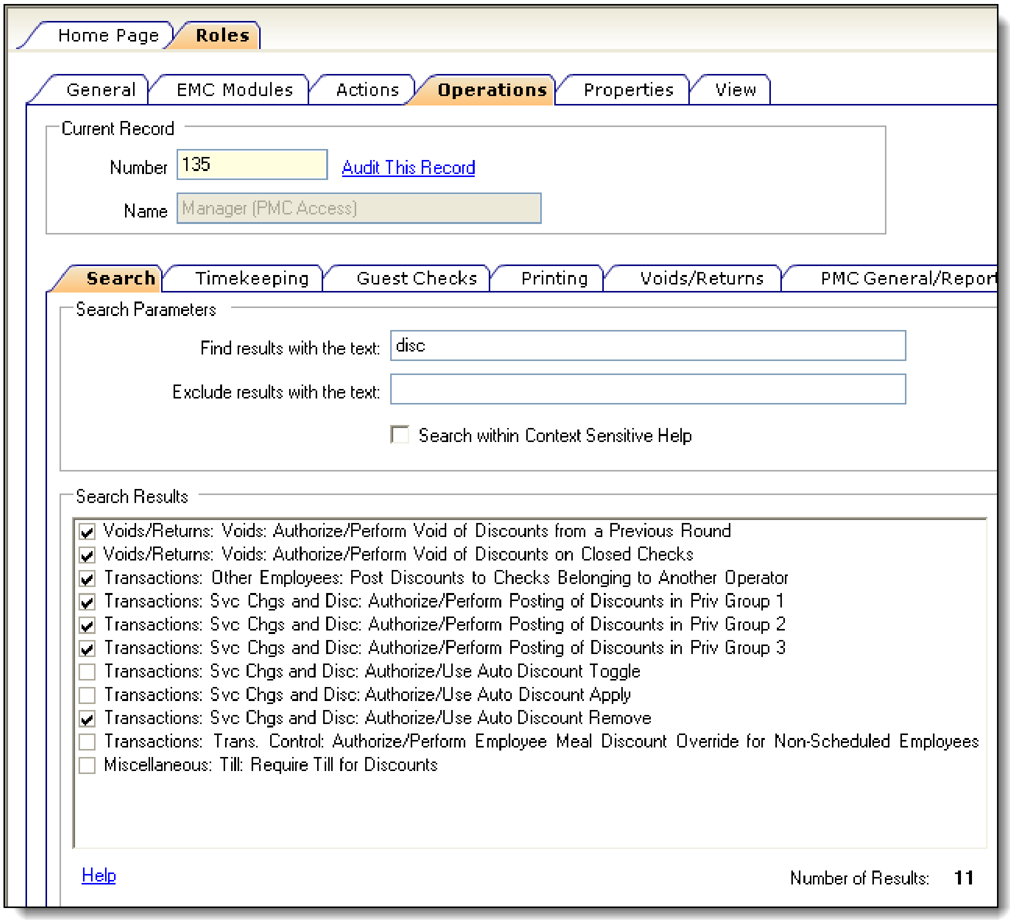
### All Property Actions

Similar to the All Property Modules checkboxes available on the EMC Modules tab, the **All Properties Actions** check box gives users associated with this role, permission to perform all actions. Oracle MICROS Food & Beverage recommends that administrator-type roles have this option enabled so that administrators are always able to perform all types of actions, including future actions that are not currently in the system.

### 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 image here shows a search for discount options.

**Figure 3-5 - Property level Roles Operations Tab**



Current Record

Number 135

Name Manager (PMC Access)

Search Parameters

Find results with the text: disc

Exclude results with the text:

□ Search within Context Sensitive Help

Search Results

☑ Voids/Returns: Voids: Authorize/Perform Void of Discounts from a Previous Round
☑ Voids/Returns: Voids: Authorize/Perform Void of Discounts on Closed Checks
☑ Transactions: Other Employees: Post Discounts to Checks Belonging to Another Operator
☑ Transactions: Svc Chgs and Disc: Authorize/Perform Posting of Discounts in Priv Group 1
☑ Transactions: Svc Chgs and Disc: Authorize/Perform Posting of Discounts in Priv Group 2
☑ Transactions: Svc Chgs and Disc: Authorize/Perform Posting of Discounts in Priv Group 3
□ Transactions: Svc Chgs and Disc: Authorize/Use Auto Discount Toggle
□ Transactions: Svc Chgs and Disc: Authorize/Use Auto Discount Apply
☑ Transactions: Svc Chgs and Disc: Authorize/Use Auto Discount Remove
□ Transactions: Trans. Control: Authorize/Perform Employee Meal Discount Override for Non-Scheduled Employees
□ Miscellaneous: Till: Require Till for Discounts

Number of Results: **11**

The Operations tab contains all of the options related to workstation functionality. The Operations tab itself is broken down into sub-tabs based on similar functionality: Timekeeping, Voids, and the property management console (PMC). Refer to UWS Procedures in Appendix A: Access Control for more information about setting access privileges for users.

### Properties Tab

Within the Properties tab, a Role is assigned to individual properties or assigned to the Enterprise. In many situations, if a Role is assigned to the Enterprise—it is likely that a Server or Bartender role is the same for all properties.

### View Tab

The View tab contains two options that control the Properties and Revenue Center’s that users can view:

- **Enable Property-Level Security**: Employees associated with a Role that has this option checked is only able to view properties to which they are assigned. This functionality affects EMC users only. Employees are assigned to properties in the Enterprise Employee Module. Note that when an employee is associated with a role with this enabled, the employee is not able to add new properties, even if the user is associated with an Enterprise Role with the **Add Properties** option enabled.
- **Enable Revenue Center-Level Security**: Employees associated with a Role that have this option checked is only able to view Revenue Center’s in which they are an operator. Employees can be set as an operator in a Revenue Center in the Employee Edit Form. Note that when an employee is associated with a Role with this 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.

## 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 an Enterprise Role with 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 First Edition 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-programmed database. Notice that levels for Roles are configured with some gaps that allow flexibility for assigning levels in the future for different types of users.

**Table 3-1 - Employee Level Example**

| 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 - Employee Maintenance, Menu Item Maintenance, and possibly Order Devices. |
| 5 | |

| Level Number | Type of User/Role |
|---|---|
| 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, programmed in the EMC's **Employee Maintenance** module. This field is a layer of security; it controls how employees interact with other employees by preventing some employees from accessing other employee records. While useful, this field is quite restrictive; it is more typical that the Employee Level field is used.

## 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

### OPS Behavior

During workstation operations, the **Employee Group** field controls which employees may perform authorizations (such as voids) for other employees. Consider the following chart; 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 Example**

| 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` message appears on the workstation.

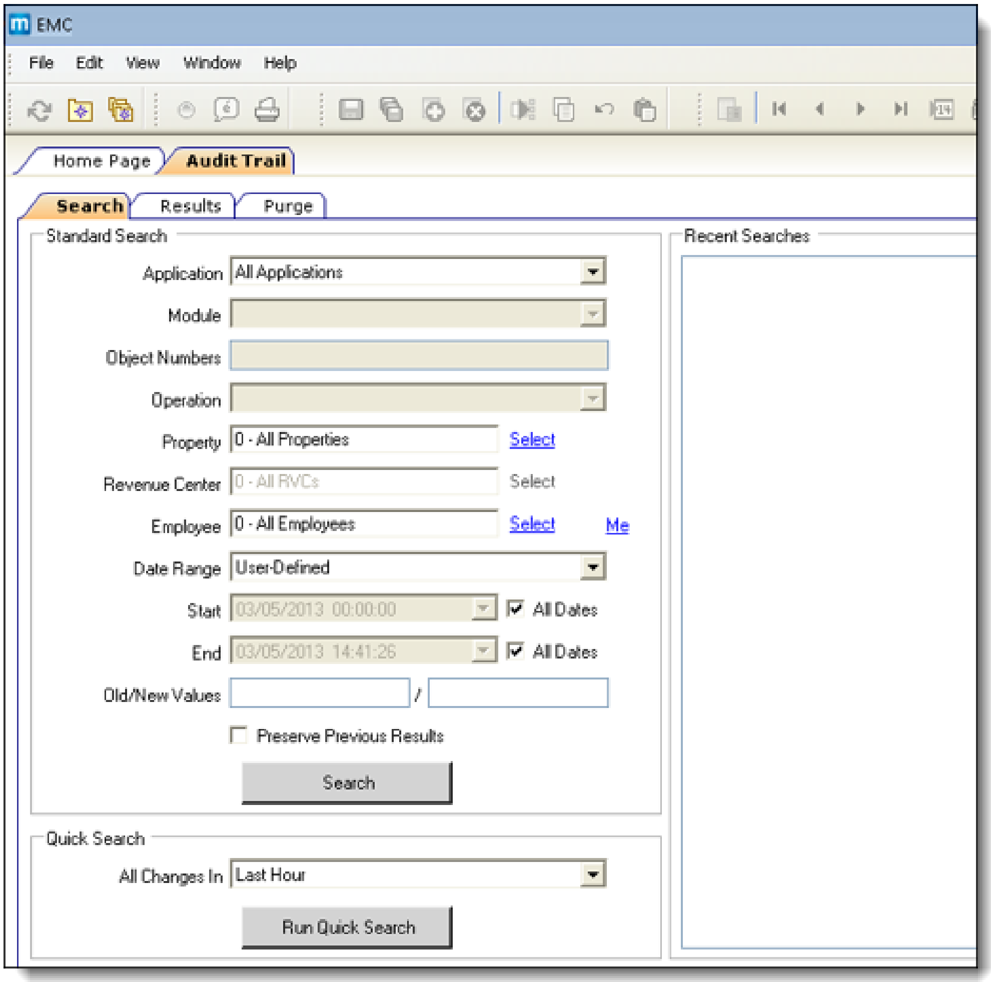
# Audit Trail

## Overview

Audit Trail is the EMC module that shows 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.

### Accessing Audit Trail

**Figure 3-6 - Audit Trail Module**



Application: All Applications
Module:
Object Numbers:
Operation:
Property: 0 - All Properties
Revenue Center: 0 - All RVCs
Employee: 0 - All Employees
Date Range: User-Defined
Start: 03/05/2013 00:00:00 ☑ All Dates
End: 03/05/2013 14:41:26 ☑ All Dates
Old/New Values: /
□ Preserve Previous Results
All Changes In: Last Hour

The Audit Trail module is located on the Enterprise level and the Property level of the EMC. There are two privileges that determine a user's ability to enter the module:

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

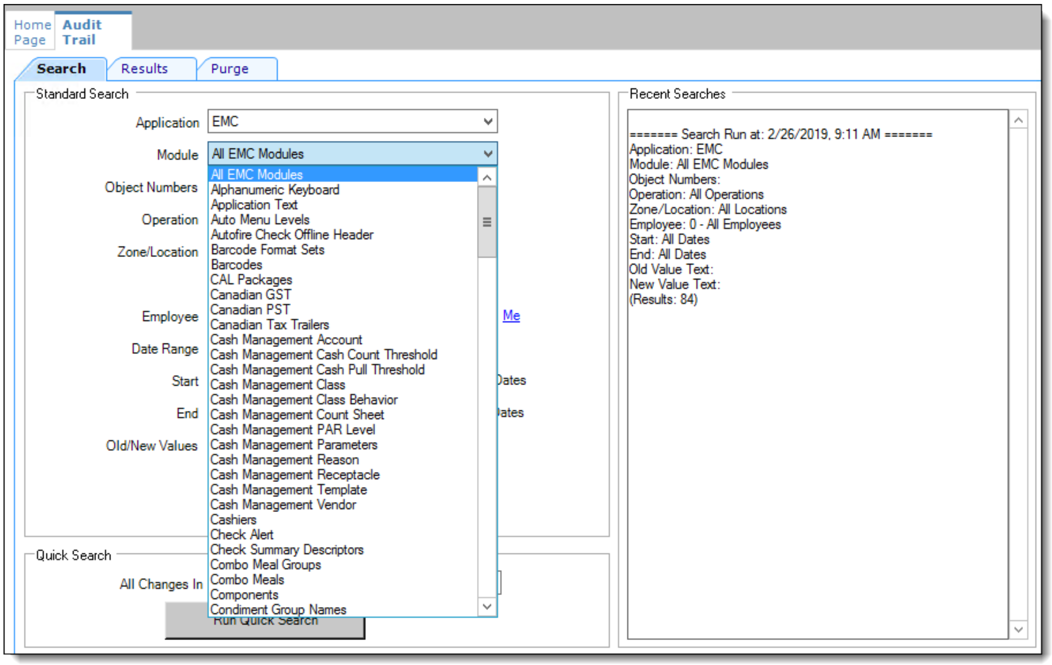
# Audit Trail Search Parameters

## Standard Search

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

- **Application**: Select an application or choose **All Applications**. When the drop-down menu shows 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**. The drop-down menu shows **All EMC Modules** followed by an alphabetized list of available modules. The drop-down menu 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 3-7 - Using the Audit Trail Module**



Application: EMC

Module: All EMC Modules

```
======= Search Run at: 2/26/2019, 9:11 AM =======
Application: EMC
Module: All EMC Modules
Object Numbers:
Operation: All Operations
Zone/Location: All Locations
Employee: 0 - All Employees
Start: All Dates
End: All Dates
Old Value Text:
New Value Text:
(Results: 84)
```

- **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-down menus. If the drop-down menu shows **All Operations**, it is followed by an alphabetized list of the valid operations.
- **Zone/Location**: Select a Zone, Location, or All Locations. When Audit Trail is opened from the Enterprise level, you can select any Property, Zone, or RVC. When opened from the Property level, you can select RVCs in the property.

- **Employee**: Select an Employee or All Employees. When a specific employee is selected, only changes made by that employee are included in the list. Select **Me** to set this field to your own employee record.
- **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 to search. Audit Trail data is automatically purged for data one month prior to the current month. The Audit Trail is typically reset nightly (by FileMaintenance.exe). It is possible that only today's Business Date shows Audit Trail information.
- **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.
- Microsoft SQL Server text comparisons often take longer than comparisons that do not search text. While a search using these text fields may return the specific Audit Record you want, a search for the module of the item returns results more quickly.
- **Old/New Values**: Enter text to query the Old Value and/or New Value columns of the Audit Trail table. This is good for finding a specific change to a record, such as, "When did Hamburger get renamed to Cheeseburger?"
- **Preserve Previous Results**: If this checkbox is selected, the search results are merged with previous search results, instead of overwriting them. If not selected, search results only include the information generated from 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

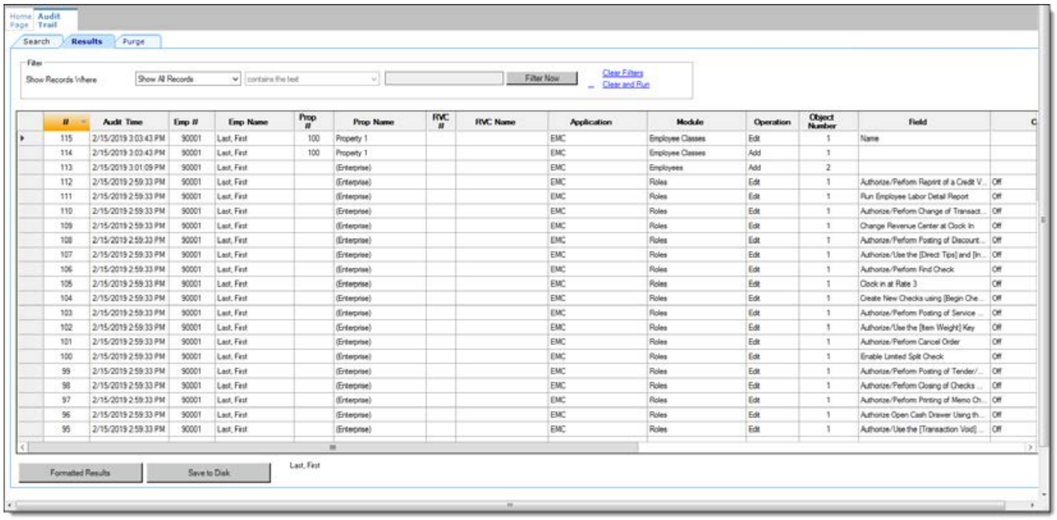
In this box, select a predefined date range and run a search. When this is used, the **Standard Search** criterion is ignored; only the date range selected is used.

### Running a Search

When **Search** or **Run Quick Search** button is clicked, the Audit Trail first checks the database to get an estimate on the number of records that are returned (it is only 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.

**Figure 3-8 - Audit Trail Search Results**



Show Records Where: Show All Records | contains the text

| # | Audit Time | Emp # | Emp Name | Prop # | Prop Name | RVC # | RVC Name | Application | Module | Operation | Object Number | Field | C |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 115 | 2/15/2019 3:03:43 PM | 90001 | Last, First | 100 | Property 1 | | | EMC | Employee Classes | Edit | 1 | Name | |
| 114 | 2/15/2019 3:03:43 PM | 90001 | Last, First | 100 | Property 1 | | | EMC | Employee Classes | Add | 1 | | |
| 113 | 2/15/2019 3:01:09 PM | 90001 | Last, First | | (Enterprise) | | | EMC | Employees | Add | 2 | | |
| 112 | 2/15/2019 2:59:33 PM | 90001 | Last, First | | (Enterprise) | | | EMC | Roles | Edit | 1 | Authorize/Perform Reprint of a Credit V... | Off |
| 111 | 2/15/2019 2:59:33 PM | 90001 | Last, First | | (Enterprise) | | | EMC | Roles | Edit | 1 | Run Employee Labor Detail Report | Off |
| 110 | 2/15/2019 2:59:33 PM | 90001 | Last, First | | (Enterprise) | | | EMC | Roles | Edit | 1 | Authorize/Perform Change of Transact... | Off |
| 109 | 2/15/2019 2:59:33 PM | 90001 | Last, First | | (Enterprise) | | | EMC | Roles | Edit | 1 | Change Revenue Center at Clock In | Off |
| 108 | 2/15/2019 2:59:33 PM | 90001 | Last, First | | (Enterprise) | | | EMC | Roles | Edit | 1 | Authorize/Perform Posting of Discount... | Off |
| 107 | 2/15/2019 2:59:33 PM | 90001 | Last, First | | (Enterprise) | | | EMC | Roles | Edit | 1 | Authorize/Use the [Direct Tips] and [In... | Off |
| 106 | 2/15/2019 2:59:33 PM | 90001 | Last, First | | (Enterprise) | | | EMC | Roles | Edit | 1 | Authorize/Perform Find Check | Off |
| 105 | 2/15/2019 2:59:33 PM | 90001 | Last, First | | (Enterprise) | | | EMC | Roles | Edit | 1 | Clock in at Rate 3 | Off |
| 104 | 2/15/2019 2:59:33 PM | 90001 | Last, First | | (Enterprise) | | | EMC | Roles | Edit | 1 | Create New Checks using [Begin Che... | Off |
| 103 | 2/15/2019 2:59:33 PM | 90001 | Last, First | | (Enterprise) | | | EMC | Roles | Edit | 1 | Authorize/Perform Posting of Service ... | Off |
| 102 | 2/15/2019 2:59:33 PM | 90001 | Last, First | | (Enterprise) | | | EMC | Roles | Edit | 1 | Authorize/Use the [Item Weight] Key | Off |
| 101 | 2/15/2019 2:59:33 PM | 90001 | Last, First | | (Enterprise) | | | EMC | Roles | Edit | 1 | Authorize/Perform Cancel Order | Off |
| 100 | 2/15/2019 2:59:33 PM | 90001 | Last, First | | (Enterprise) | | | EMC | Roles | Edit | 1 | Enable Limited Split Check | Off |
| 99 | 2/15/2019 2:59:33 PM | 90001 | Last, First | | (Enterprise) | | | EMC | Roles | Edit | 1 | Authorize/Perform Posting of Tender/... | Off |
| 98 | 2/15/2019 2:59:33 PM | 90001 | Last, First | | (Enterprise) | | | EMC | Roles | Edit | 1 | Authorize/Perform Closing of Checks ... | Off |
| 97 | 2/15/2019 2:59:33 PM | 90001 | Last, First | | (Enterprise) | | | EMC | Roles | Edit | 1 | Authorize/Perform Printing of Memo Ch... | Off |
| 96 | 2/15/2019 2:59:33 PM | 90001 | Last, First | | (Enterprise) | | | EMC | Roles | Edit | 1 | Authorize Open Cash Drawer Using th... | Off |
| 95 | 2/15/2019 2:59:33 PM | 90001 | Last, First | | (Enterprise) | | | EMC | Roles | Edit | 1 | Authorize/Use the [Transaction Void] ... | Off |

Last, First

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

The following columns are displayed:

- #: This column shows the Audit Trail Record ID of each Audit Trail Entry
- **Audit Time**: This column shows the time of the change or activity
- **Emp #**: This column shows the employee number of the employee who made the change. If the change was made by an employee who is now deleted, a zero is assigned to that record.
- **Emp Name**: This column shows 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 shows the Property number, if any, where the change was made. If the Property of the change is deleted, this column shows **-1**. If a change is made on the Enterprise level, this column remains blank. If a change is made to a RVC, this column shows the Property to which the RVC belongs.
- **Prop Name**: This column shows the name of the property where a change is made. If the property is deleted, this column shows **??? 1234** (where 1234 is the database HierStrucID of the deleted item). If a change is made on the Enterprise level, this column shows **Enterprise**. If a change is made to a RVC, this column shows the name of the property to which the RVC belongs.
- **RVC #**: This column shows the RVC number where a change is made. If the same RVC (with the change) is deleted, this column shows **-1**. If a change is made on the Enterprise or Property level, this column remains blank.
- **RVC Name**: This column shows the name of the RVC where the change is made. If the RVC is deleted, this column shows **??? 1234** (where 1234 is the database

HierStrucID of the deleted item). If a change is made on the Enterprise or Property level, this column remains blank.

- **Application**: This column shows the application where a change is made. The list includes different applications within Simphony such as EMC, PMC Procedures, PMC Reports, and others.
- **Module**: This column shows the module within the application where a change is made. This column typically shows an EMC Module name. When the audited record shows a PMC Report, this column shows the name of the report that was generated.
- **Operation**: This column shows the type of operation that occurred.
- **Obj Num**: This column shows the object number of the record that was changed. If the audit record is a PMC Report, this column shows 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 shows comments added to the Audit Trail record. Some applications may record comments to help clarify the change or activity being

### Audit This Record

In almost every module, a user 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 choosing 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 appears 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 appears. 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, click **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 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 show the Old/New value, followed by the value in quotes to indicate where the extra space character exists. 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, these data are 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 show the entire XML string.
- When an Audit Trail report is taken, this activity is logged to Audit Trail. All Audit Trail Reports taken 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 an 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 Internationalization 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 Scancode 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. |
| 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 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 |

## 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 3, 2018, all records dated from October 3rd 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. For example, Key [30].

Old Value: (added)

New 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 added. In this example, a key that uses Tender #1 with the legend “Cash” was added.

When a sub-record is edited, 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 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 First Edition database is encrypted using industry standard AES-256 encryption. Each encrypted piece of data has a link to an entry in the encryption key table, which is also encrypted using AES-256 encryption.

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

### Encrypting Data in the Temporary Data Cache

In offline mode, workstation operations need to store a local copy of the data cache 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 During Transmission

While Simphony supports the HTTPS protocol for secure data communication, it is not required because Simphony uses a built-in protocol that adheres to Web Services standards.

### Key Rotation Considerations

In order to achieve maximum security, Oracle MICROS Food & Beverage mandates the system administrator regularly rotate the site’s keys, at least annually, and delete any old or comprised encryption keys. Simphony First Edition’s entire design of data encryption, key generation, and storage is built to facilitate such practice. For more information, refer to the Key Manager Manual. A privileged employee may conduct key rotation in the EMC within the Enterprise level, Enterprise, and Key Manager Module. To authorize an employee to access the Key Manager module, the action **Key Manager** must be enabled within the EMC **Enterprise Roles** module (Enterprise level, Personnel, Enterprise Roles, and **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 on the Key Manager Module and secure key practices, refer to the Key Manager Manual.

### Key Manager

Key Manager is an EMC module that allows the database encryption Pass phrase and the transmission key 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.

# Appendix A
# Access Control

## UWS Procedures

User Workstation (UWS) Procedures may be restricted to a specific Employee Role in the EMC within the Enterprise level, Personnel, Roles, and Operations tabs. Access to each UWS Procedure is controlled by a separate privilege. Here is a listing of the UWS Procedures privilege options.

### POS Operations Privileges

Each Employee Role may be prevented from performing certain functions during Point of Sales (POS) Operations.

**Time Clock Privileges**

Access to specific functions of the employee time clock can be restricted by the Time Clock Privileges that are set for each Employee Role. Time Clock Privileges may include those for clocking in or out, overriding the time clock schedule, or clocking into a different Revenue Center.

**Transaction Detail Item Privileges**

Menu Item, Discount, Service Charge, and Tender/Media keys may be assigned to one of three Privilege Groups to restrict employee access to a specific item.

**Transaction Privileges**

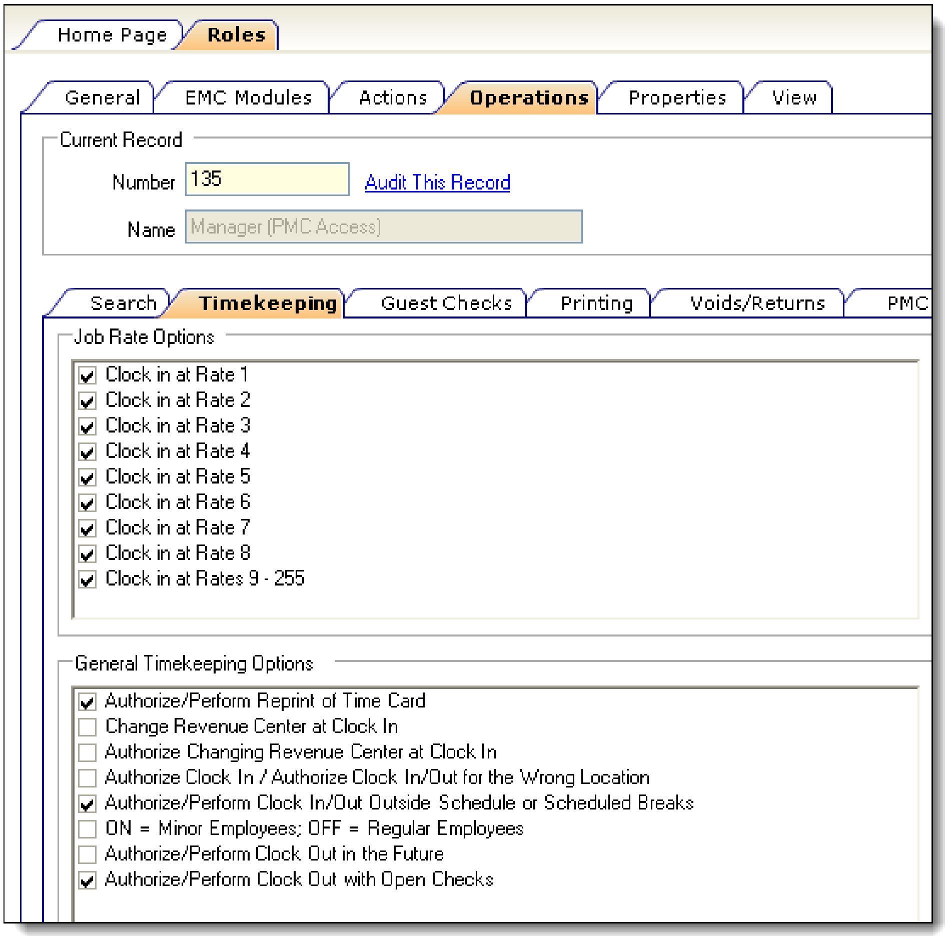
Access to certain actions in POS Operations can be restricted by the Transaction Privileges that are set for each Employee Role. Transaction Privileges may include those that control signing in to a UWS, beginning a transaction, and voiding or returning items.

**Enabling**

POS Operations Privileges are enabled in the EMC within the Enterprise level, Personnel, Roles, and Operations tab.

# EMC Configuration

**Figure 3-9 - Timekeeping Tab**



Current Record

Number: 135

Name: Manager (PMC Access)

Job Rate Options

☑ Clock in at Rate 1
☑ Clock in at Rate 2
☑ Clock in at Rate 3
☑ Clock in at Rate 4
☑ Clock in at Rate 5
☑ Clock in at Rate 6
☑ Clock in at Rate 7
☑ Clock in at Rate 8
☑ Clock in at Rates 9 - 255

General Timekeeping Options

☑ Authorize/Perform Reprint of Time Card
□ Change Revenue Center at Clock In
□ Authorize Changing Revenue Center at Clock In
□ Authorize Clock In / Authorize Clock In/Out for the Wrong Location
☑ Authorize/Perform Clock In/Out Outside Schedule or Scheduled Breaks
□ ON = Minor Employees; OFF = Regular Employees
□ Authorize/Perform Clock Out in the Future
☑ Authorize/Perform Clock Out with Open Checks

## Job Rate Options

### Clock in at Rate (1-255)

Select this option to allow employees associated with this Role to Clock in at Job Rate *X*.

## General Timekeeping Options

### Authorize/Perform Reprint of Time Card

Select this option to allow employees associated with this Role to reprint a timecard using the [Reprint Timecard] key and to authorize non- privileged employees to do so as well.

### Change Revenue Center at Clock-In

Select this option to allow employees associated with this Role to authorize changes in the Revenue Center assignment of other employees who are clocking in.

### Authorize Changing Revenue Center at Clock In

Select this option to allow employees associated with this Role to change their Revenue Center assignment when clocking in.

### Authorize Clock In / Authorize Clock In/Out for the Wrong Location

Select this option to allow employees associated with this Role to authorize other employees to clock in. Also, this option controls the ability to allow users to clock in or out for the “Wrong Location”; this situation occurs when a Property Employee Record has the option “Limit Clock-In to Workstations in the Clock-In RVC” or “Limit Clock-Out to Workstations in the Clock-Out RVC” enabled.

### Authorize/Perform Clock In/Out Outside Schedule or Scheduled Breaks

Select this option to allow employees associated with this Role to clock in or out at times that conflict with their assignment in the ‘Time Clock Schedules’ module.

### ON = Minor Employees; OFF = Regular Employees

Some jurisdictions have labor laws that apply specifically to minors (16 and under). This option is used in conjunction with the Time Clock Parameters, in the System Parameters module. The option allows you to create separate definitions of paid and unpaid breaks for minors and regular employees. Select this option to designate employees associated with this Role as minors. Do not select this option to designate employees associated with this Role as regular (adult) employees.

### Authorize/Perform Clock Out in the Future

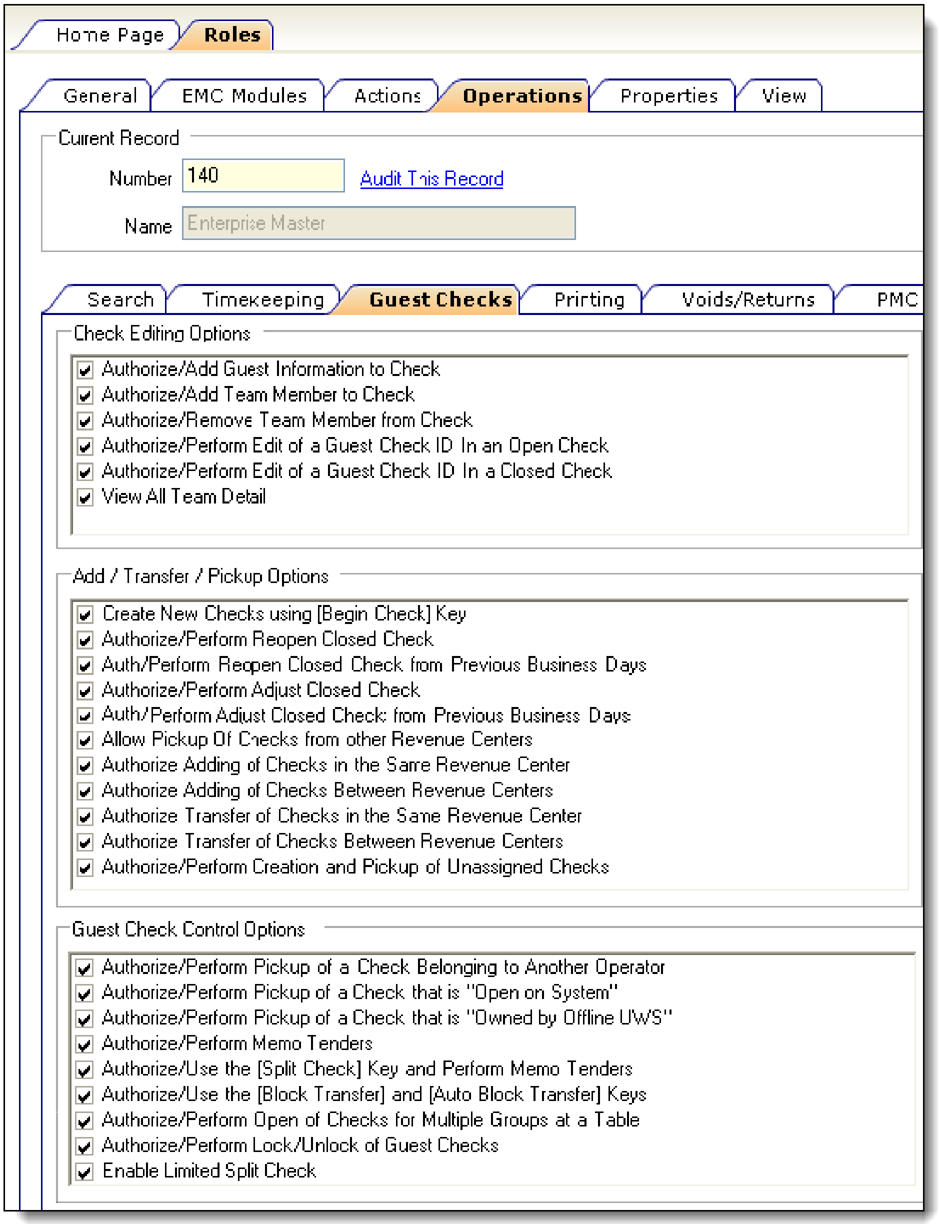
Select this option to allow employees associated with this Role to clock themselves out at a time ahead of the system time or to authorize an employee without this privilege to clock out at a time ahead of the system time.

### Authorize/Perform Clock Out with Open Checks

Select this option to allow employees associated with this Role to clock out at the end of a shift even if they still have open Guest Checks and to authorize other employees to do so as well. If this option is enabled, it overrides the setting of the [Cannot Clock Out with Open Checks] option in the Job Codes module.

## Guest Checks Tab

### Figure 3-10 - Roles Guest Check Privileges



Current Record

Number 140

Name Enterprise Master

Check Editing Options

- ☑ Authorize/Add Guest Information to Check
- ☑ Authorize/Add Team Member to Check
- ☑ Authorize/Remove Team Member from Check
- ☑ Authorize/Perform Edit of a Guest Check ID In an Open Check
- ☑ Authorize/Perform Edit of a Guest Check ID In a Closed Check
- ☑ View All Team Detail

Add / Transfer / Pickup Options

- ☑ Create New Checks using [Begin Check] Key
- ☑ Authorize/Perform Reopen Closed Check
- ☑ Auth/Perform Reopen Closed Check from Previous Business Days
- ☑ Authorize/Perform Adjust Closed Check
- ☑ Auth/Perform Adjust Closed Check from Previous Business Days
- ☑ Allow Pickup Of Checks from other Revenue Centers
- ☑ Authorize Adding of Checks in the Same Revenue Center
- ☑ Authorize Adding of Checks Between Revenue Centers
- ☑ Authorize Transfer of Checks in the Same Revenue Center
- ☑ Authorize Transfer of Checks Between Revenue Centers
- ☑ Authorize/Perform Creation and Pickup of Unassigned Checks

Guest Check Control Options

- ☑ Authorize/Perform Pickup of a Check Belonging to Another Operator
- ☑ Authorize/Perform Pickup of a Check that is "Open on System"
- ☑ Authorize/Perform Pickup of a Check that is "Owned by Offline UWS"
- ☑ Authorize/Perform Memo Tenders
- ☑ Authorize/Use the [Split Check] Key and Perform Memo Tenders
- ☑ Authorize/Use the [Block Transfer] and [Auto Block Transfer] Keys
- ☑ Authorize/Perform Open of Checks for Multiple Groups at a Table
- ☑ Authorize/Perform Lock/Unlock of Guest Checks
- ☑ Enable Limited Split Check

## Check Editing Options

### Authorize/Add Guest Information to Check

Enable this option to allow employees associated with this Role to use the [Enter Guest Info] key to enter guest information when creating a special event check on the workstation and to authorize non-privileged employees to do so as well.

### Authorize/Add Team Member to Check

Select this option to allow employees associated with this Role to use the [Add Team Member] key to add additional servers to a check.

#### Authorize/Remove Team Member from Check

Select this option to allow employees associated with this Role to use the [Remove Team Member] key to remove servers from a check.

#### Authorize/Perform Edit of a Guest Check ID In an Open Check

Select this option to allow employees associated with this Role to edit a Guest Check ID of an open check using the [Guest Check ID] key and to authorize non-privileged employees to do so as well.

#### Authorize/Perform Edit of a Guest Check ID In a Closed Check

Select this option to allow employees associated with this Role to edit a Guest Check ID of a closed check using the [Guest Check ID] key and to authorize non-privileged employees to do so as well.

#### View All Team Detail

A Guest Check must be started with the [Begin Party Check] key (key code 399) to use this Employee Role option. Enable this option to allow employees associated with this Role to view the detail posted by all team members on a special event check and to authorize non-privileged employees to do so as well. If this option is disabled, employees associated with this Role can only view the detail that they have posted to the Guest Check.

### Add / Transfer / Pickup Options

#### Create New Checks using [Begin Check] Key

Select this option to allow employees associated with this Role to begin a Guest Check.

#### Authorize/Perform Reopen Closed Check

Select this option to allow employees associated with this Role to use the [Reopen Closed Check] key and to authorize non-privileged employees to do so as well.

#### Auth/Perform Reopen Closed Check from Previous Business Days

Select this option to allow employees associated with this Role to Reopen Closed Checks from business days other than the current business day. If this option is enabled, an operator in this Role will have access to the [Reopen Closed Check from Previous Business Day] function key.

#### Authorize/Perform Adjust Closed Check

Select this option to allow employees associated with this Role to use the [Adjust Closed Check] key and to authorize non-privileged employees to do so as well. A closed check adjustment allows the user (if privileged to void Tender/Media from a previous round) to adjust the Tender/Media or Service Charge on a closed check.

#### Auth/Perform Adjust Closed Check from Previous Business Days

Select this option to allow employees associated with this Role to Adjust Closed Checks from business days other than the current business day. If this option is enabled, an operator in this class will have access to the [Adjust Closed Check from Previous Business Day] function key.

### Allow Pickup Of Checks from other Revenue Centers

Select this option to allow employees associated with this Role to pick up checks in other Revenue Centers using the [Pickup Check, RVC] keys. Disable this option to prevent employees from picking up checks in other Revenue Centers.

### Authorize Adding of Checks in the Same Revenue Center

Select this option to allow employees associated with this Role to add checks (to be in a check and add another check to it) within a Revenue Center and to authorize non-privileged employees to do so as well.

### Authorize Adding of Checks Between Revenue Centers

Select this option to allow employees associated with this Role to add checks (to be in a check and add another check to it) from another Revenue Center and to authorize non-privileged employees to do so as well.

### Authorize Transfer of Checks in the Same Revenue Center

Select this option to allow employees associated with this Role to transfer checks from another operator within the same Revenue Center and to authorize non-privileged employees to do so as well.

### Authorize Transfer of Checks Between Revenue Centers

Select this option to allow employees associated with this Role to transfer checks from another Revenue Center and to authorize non-privileged employees to do so as well.

### Authorize/Perform Creation and Pickup of Unassigned Checks

Select this option to allow employees associated with this Role to begin and pickup “Unassigned Checks” and to allow non-privileged employees to do so as well.

An Unassigned Check is a check that is begun in the system (usually by a Professional Services application or other Oracle MICROS Food & Beverage peripheral product such as Suites Management) without an owner. When an Open Check SLU is used, Privileged Operators will see their own checks, as well as any “Unassigned Checks” in the Revenue Center, but they will not see other operators’ open checks.

## Guest Check Control Options

### Authorize/Perform Pickup of a Check Belonging to Another Operator

Select this option to allow employees associated with this Role to pick up another operator's checks and to authorize non-privileged employees to do so as well.

### Authorize/Perform Pickup of a Check that is “Open on System”

Select this option to allow employees associated with this Role to pick up checks that already have an “open” status and to authorize non-privileged employees to do so as well. Checks with an “open” status are checks that are considered in use at another workstation or by another process.

### Authorize/Perform Pickup of a Check that is “Owned by Offline UWS”

If a check is rung on a workstation that proceeds to go offline, the check is considered Owned by an Offline Workstation. Select this option to allow employees associated with this Role to pick up these checks from another workstation and to authorize non-privileged employees to do so as well.

### Authorize/Perform Memo Tenders

Enable this option to allow privileged employees associated with this Role to perform memo tenders and to authorize non-privileged employees to do so as well.

### Authorize/Use the [Split Check] Key and Perform Memo Tenders

Select this option to allow employees associated with this Role to split Guest Checks and to perform memo tenders and to authorize non- privileged employees to do so as well.

### Authorize/Use the [Block Transfer] and [Auto Block Transfer] Keys

Select this option to allow employees associated with this Role to transfer an entire block of checks from another operator and to authorize non- privileged employees to do so as well. This function is useful with a shift change, when an entire group of checks must be turned over from the operator who is leaving to the operator who is just signing in.

### Authorize/Perform Open of Checks for Multiple Groups at a Table

Select this option to allow employees associated with this Role to open multiple checks at the same table. Each succeeding check is assigned a successive check number. An employee who is authorized to split checks (option “Authorize/Use the [Split Check] key and Perform Memo Tenders”) is also authorized to open checks for multiple groups at a table.

### Authorize/Perform Lock/Unlock of Guest Checks

Enable this option to allow employees associated with this Role to use the [Lock Guest Check] and [Unlock Guest Check] keys and to authorize non-privileged employees to do so as well.

### Enable Limited Split Check

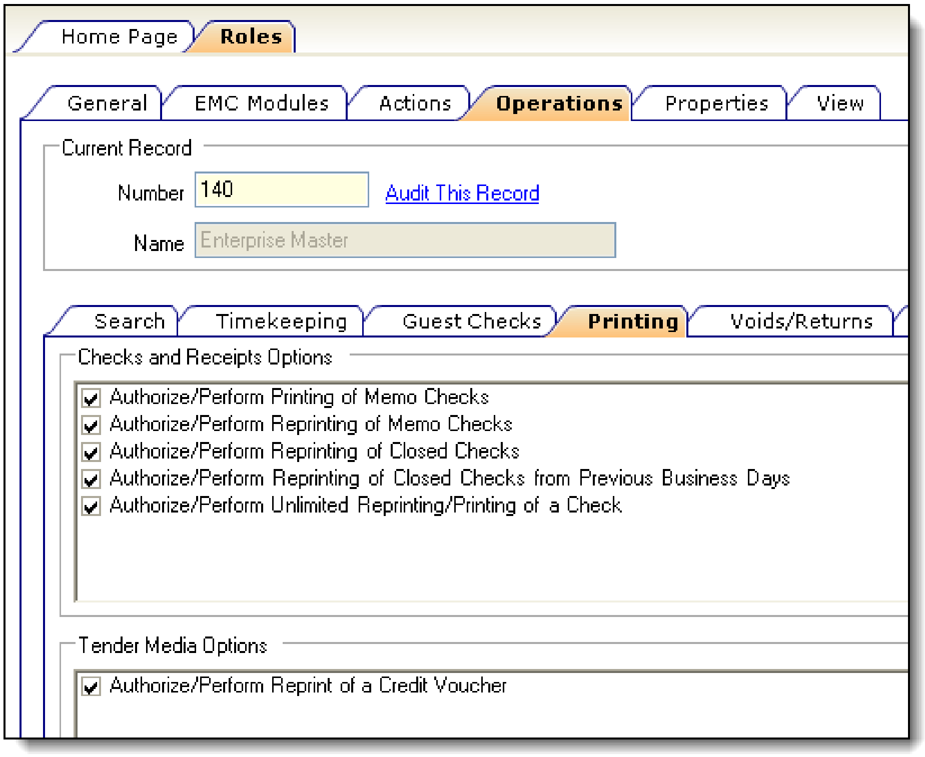
Enable this option to prevent an employee from performing the Split Check function more than once on a check. If this option is enabled, the Authorize/Use Split Check option must be disabled. Note: This option was created to safeguard against the “floating soda” technique.

### Authorize/Begin Menu Item Waste Check

Enable this option to allow an employee to begin a menu item waste check or authorize another employee to do the same.

## Printing Tab

### Figure 3-11 - Roles Printing Privileges



Current Record

Number 140

Name Enterprise Master

Checks and Receipts Options

- ☑ Authorize/Perform Printing of Memo Checks
- ☑ Authorize/Perform Reprinting of Memo Checks
- ☑ Authorize/Perform Reprinting of Closed Checks
- ☑ Authorize/Perform Reprinting of Closed Checks from Previous Business Days
- ☑ Authorize/Perform Unlimited Reprinting/Printing of a Check

Tender Media Options

- ☑ Authorize/Perform Reprint of a Credit Voucher

#### Authorize/Perform Printing of Memo Checks

Select this option to allow employees associated with this Role to print Memo checks and to authorize non-privileged employees to do so as well.

#### Authorize/Perform Reprinting of Memo Checks

Select this option to allow employees associated with this Role to reprint Memo checks and to authorize non-privileged employees to do so as well.

#### Authorize/Perform Reprinting of Closed Checks

Select this option to allow employees associated with this Role to reprint a Guest Check after it has been closed and to authorize non-privileged employees to do so as well.

#### Authorize/Perform Unlimited Reprinting/Printing of a Check

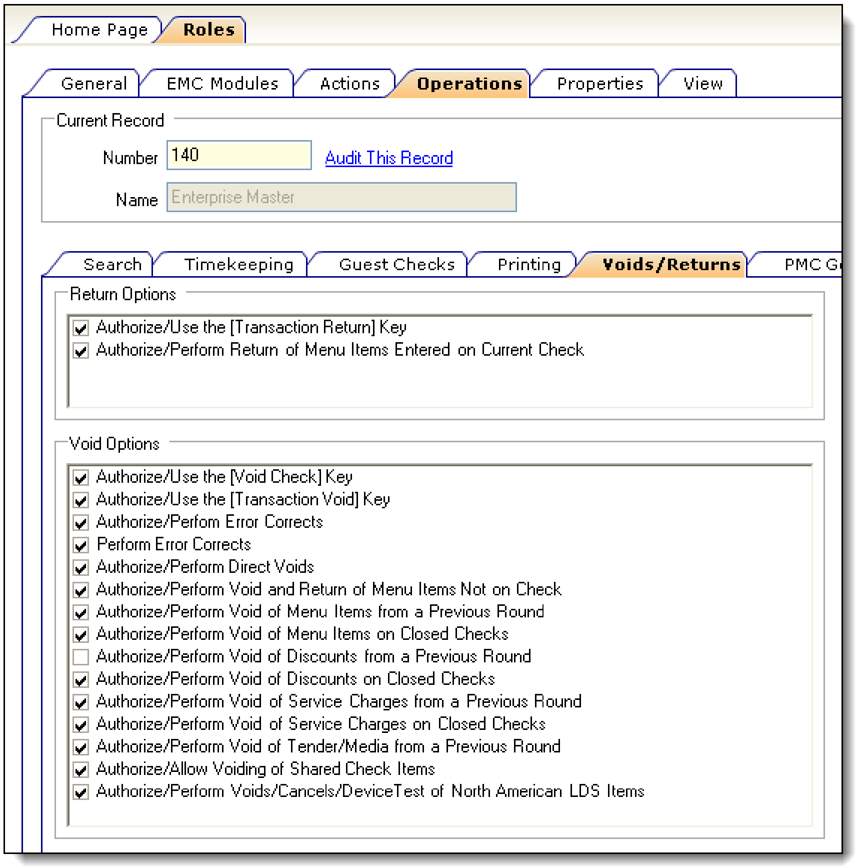
Select this option to allow employees associated with this Role to perform two functions. #1: Allow On-Demand operators to print Guest Checks more than the maximum number allowed in the Revenue Center Parameters Module. #2: Allow By-round operators to use the [Reprint Check] key. This privilege also allows employees associated with this Role to give authorization to non-privileged employees for these functions.

#### Authorize/Perform Reprint of a Credit Voucher

Select this option to allow employees associated with this Role to reprint a credit card voucher slip and to authorize non-privileged employees to do so as well.

## Voids/Returns Tab

### Figure 3-12 - Roles Voids/ Returns Privileges



Current Record

Number 140

Name Enterprise Master

Return Options

- ☑ Authorize/Use the [Transaction Return] Key
- ☑ Authorize/Perform Return of Menu Items Entered on Current Check

Void Options

- ☑ Authorize/Use the [Void Check] Key
- ☑ Authorize/Use the [Transaction Void] Key
- ☑ Authorize/Perfom Error Corrects
- ☑ Perform Error Corrects
- ☑ Authorize/Perform Direct Voids
- ☑ Authorize/Perform Void and Return of Menu Items Not on Check
- ☑ Authorize/Perform Void of Menu Items from a Previous Round
- ☑ Authorize/Perform Void of Menu Items on Closed Checks
- □ Authorize/Perform Void of Discounts from a Previous Round
- ☑ Authorize/Perform Void of Discounts on Closed Checks
- ☑ Authorize/Perform Void of Service Charges from a Previous Round
- ☑ Authorize/Perform Void of Service Charges on Closed Checks
- ☑ Authorize/Perform Void of Tender/Media from a Previous Round
- ☑ Authorize/Allow Voiding of Shared Check Items
- ☑ Authorize/Perform Voids/Cancels/DeviceTest of North American LDS Items

## Return Options

### Authorize/Use the [Transaction Return] Key

Select this option to allow employees associated with this Role to use the [Transaction Return] key and to authorize non-privileged employees to do so as well. The [Transaction Return] key is used when performing several returns in a transaction--every menu item rung after pressing [Transaction Return] will be a returned menu item.

### Authorize/Perform Return of Menu Items Entered on Current Check

Select this option to allow employees associated with this Role to return menu items posted in the current round (using the [Return] key) and to authorize non-privileged employees to do so as well. To perform voids in the current round, the employee class option Authorize/Perform Error Corrects] must be enabled.

## Void Options

### Authorize/Use the [Void Check] Key

Select this option to allow employees associated with this Role to use the [Void Check] key, which will void all the items on the check and to authorize non-privileged employees to do so as well.

### Authorize/Use the [Transaction Void] Key

Select this option to allow employees associated with this Role to use the [Transaction Void] key and to authorize non-privileged employees to do so as well. The [Transaction Void] key is used when performing several voids in a transaction—every menu item rung after pressing [Transaction Void] will become a voided menu item.

### Authorize/Perform Error Corrects

Select this option to allow employees associated with this Role to authorize and perform voids in the current round (i.e., last-item voids, direct voids, line-number voids, and touch-voids).

### Perform Error Corrects

Select this option to allow employees associated with this Role to perform voids in the current round (i.e., last-item voids, direct voids, line-number voids, and touch-voids).

### Authorize/Perform Direct Voids

Select this option to allow employees associated with this Role to void transaction items by pressing the [Void] key and then the key for the item (e.g., a Menu Item key). Also, select this option to authorize non- privileged employees to do so as well.

### Authorize/Perform Void and Return of Menu Items Not on Check

Select this option to allow employees associated with this Role to void and return menu items that were never posted to the Guest Check and to authorize non-privileged employees to do so as well.

### Authorize/Perform Void of Menu Items from a Previous Round

Select this option to allow employees associated with this Role to void menu items that were posted in a previous transaction round and to authorize non-privileged employees to do so as well.

### Authorize/Perform Void of Menu Items on Closed Checks

Select this option to allow employees associated with this Role to void menu items from closed checks after they have been reopened and to authorize non-privileged employees to do so as well. (In addition, the “Authorize/Perform Void of a Menu Item from a Previous Round” option must be selected.)

### Authorize/Perform Void of Discounts from a Previous Round

Select this option to allow employees associated with this Role to void discounts that were posted in a previous transaction round and to authorize non-privileged employees to do so as well.

### Authorize/Perform Void of Discounts on Closed Checks

Select this option to allow employees associated with this Role to void discounts from closed checks after they have been reopened and to authorize non-privileged employees to do so as well. (In addition, the “Authorize/Perform Void of a Discount from a Previous Round” option must be selected.)

### Authorize/Perform Void of Service Charges from a Previous Round

Select this option to allow employees associated with this Role to void service charges that were posted in a previous transaction round and to authorize non-privileged employees to do so as well.

### Authorize/Perform Void of Service Charges on Closed Checks

Select this option to allow employees associated with this Role to void service charges from closed checks after they have been reopened and to authorize non-privileged employees to do so as well. In addition, the “Authorize/Perform Void of a Service Charge from a Previous Round” option must be selected.

### Authorize/Perform Void of Tender/Media from a Previous Round

Select this option to allow employees associated with this Role to void tender/media entries that were posted in a previous transaction round and to authorize non-privileged employees to do so as well.

### Authorize/Allow Voiding of Shared Check Items

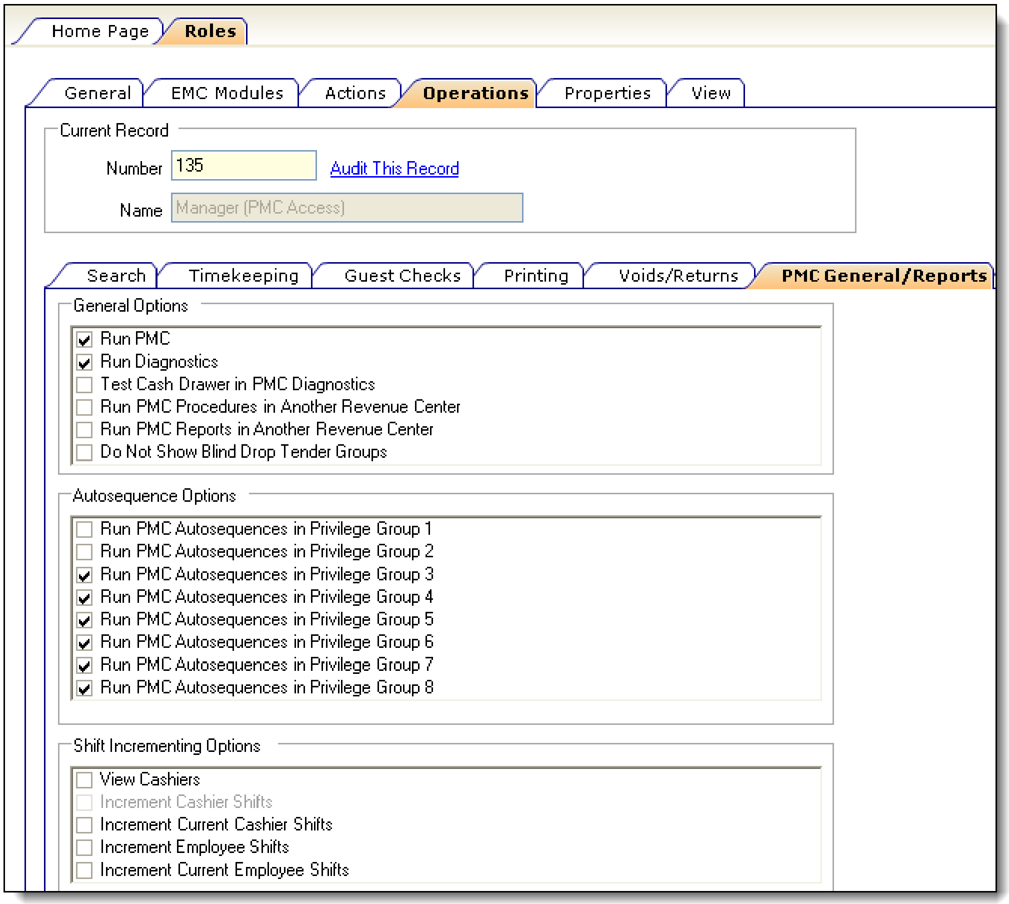
Select this option to allow employees associated with this Role to void items which are shared between seats or checks, and to authorize non- privileged employees to do so as well.

### Authorize/Perform Voids/Cancels of North American LDS Items

Select this option to allow employees associated with this Role to perform voids or cancels of menu items ordered through a North American Liquor Dispensing System (NA LDS) and to authorize non-privileged employees to do so as well.

## PMC General/Reports Tab

**Figure 3-13 - Roles PMC General/ Reports**



Current Record

Number 135

Name Manager (PMC Access)

General Options

☑ Run PMC
☑ Run Diagnostics
□ Test Cash Drawer in PMC Diagnostics
□ Run PMC Procedures in Another Revenue Center
□ Run PMC Reports in Another Revenue Center
□ Do Not Show Blind Drop Tender Groups

Autosequence Options

□ Run PMC Autosequences in Privilege Group 1
□ Run PMC Autosequences in Privilege Group 2
☑ Run PMC Autosequences in Privilege Group 3
☑ Run PMC Autosequences in Privilege Group 4
☑ Run PMC Autosequences in Privilege Group 5
☑ Run PMC Autosequences in Privilege Group 6
☑ Run PMC Autosequences in Privilege Group 7
☑ Run PMC Autosequences in Privilege Group 8

Shift Incrementing Options

□ View Cashiers
□ Increment Cashier Shifts
□ Increment Current Cashier Shifts
□ Increment Employee Shifts
□ Increment Current Employee Shifts

## General Options

### Run PMC

Enable this option for employees associated with this Role to have access to launch the PMC application via the function key [300 - Launch PMC]. This option must be enabled to set other options on this page.

### Run Diagnostics

Enable this option for employees who can run diagnostics from PMC. In the diagnostics module, a user can test peripheral hardware, including printers, barcode scanners, and other devices. This option is only available when the “Run PMC” option is enabled.

### Test Cash Drawer in PMC Diagnostics

Enable this option to allow employees associated with this Role to open the cash drawers while in PMC Diagnostics. This option is only available when the “Run Diagnostics” option is enabled.

### Run PMC Procedures in Another Revenue Center

Select this option to allow employees associated with this Role to perform PMC Procedures for a Revenue Center to which they are not currently assigned. For instance, if this option is selected, a manager eating lunch in Revenue Center 1 could change the Serving Period (if so privileged) in Revenue Center 2, saving the manager from having to walk to Revenue Center 2 to change the Serving Period, because the manager can simply change the Serving Period from a workstation in Revenue Center 1 while enjoying his/her lunch.

### Run PMC Reports in Another Revenue Center

Select this option to allow employees associated with this Role to run PMC Autosequences (Reports) for Revenue Centers other than the current Revenue Center to which they are currently assigned.

### Do Not Show Blind Drop Tender Groups

This option prevents tenders from showing in reports. This option enables the Report Groups, Tender Media type; Options tab [4 - Do Not Display for Blind Drop Reports]. An employee cannot see Blind Drop Tenders if both of these options are enabled.

## Autosequence Options

### Run PMC Autosequences in Privilege Group (1-8)

Select these option(s) to allow employees associated with this Role to run PMC Autosequences belonging to the Privilege Group of choice (1-8).

Note that all employees can run PMC Autosequences belonging to Privilege Group ‘0’. This option is only available when the “Run PMC” option is enabled.

## Shift Incrementing Options

### View Cashiers

Enable this option for employees associated with this Role to access the Cashier Procedure within the PMC. This option is only available when the “Run PMC” option is enabled.

### Increment Cashier Shifts

Enable this option for employees associated with this Role to Increment Cashier Shifts for other Cashiers within the PMC Cashier Procedure. This option is only available when the options “View Cashiers” and “Run PMC” are enabled.

### Increment Current Cashier Shifts

Enable this option for employees associated with this Role to Increment their own Cashier Financial Shift. This option is only available when the “Run PMC” option is enabled.

### Increment Employee Shifts

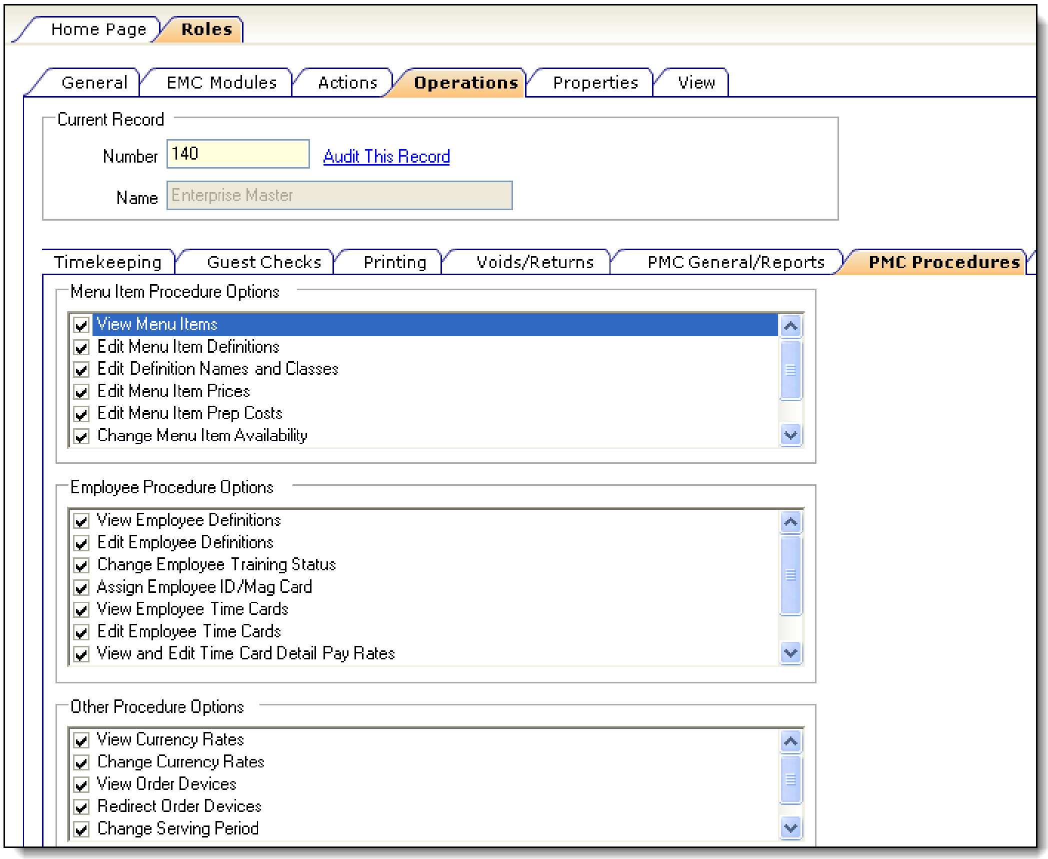
Enable this option for employees associated with this Role to Increment Employee Shifts of other employees within the PMC Employee Procedure. This option is only available when the options “View Employee Definitions” and “Run PMC” are enabled.

### Increment Current Employee Shifts

Enable this option for employees associated with this Role to Increment their own Employee Financial Shift. This option is only available when the “Run PMC” option is enabled.

## PMC Procedures Tab

### Figure 3-14 - Roles PMC Procedures



Number 140

Name Enterprise Master

Menu Item Procedure Options

☑ View Menu Items
☑ Edit Menu Item Definitions
☑ Edit Definition Names and Classes
☑ Edit Menu Item Prices
☑ Edit Menu Item Prep Costs
☑ Change Menu Item Availability

Employee Procedure Options

☑ View Employee Definitions
☑ Edit Employee Definitions
☑ Change Employee Training Status
☑ Assign Employee ID/Mag Card
☑ View Employee Time Cards
☑ Edit Employee Time Cards
☑ View and Edit Time Card Detail Pay Rates

Other Procedure Options

☑ View Currency Rates
☑ Change Currency Rates
☑ View Order Devices
☑ Redirect Order Devices
☑ Change Serving Period

## Menu Item Procedure Options

### View Menu Items

Enable this option for employees associated with this Role to access the Menu Item Procedure within the PMC. This option is only available when the “Run PMC” option is enabled.

### Edit Menu Item Definitions

Enable this option for employees associated with this Role to edit Menu Item Definitions within the PMC Menu Item Procedure. This option is only available when the “Run PMC” option is enabled.

### Edit Definition Names and Classes

Enable this option bit to allow employees associated with the Role to edit a menu item definition’s Name 1, Name 2 and class. This option is only available when the “Edit Menu Item Definitions”, “View Menu Items” and “Run PMC” options are enabled.

### Edit Menu Item Prices

Enable this option for employees associated with this Role to edit Menu Item Prices within the PMC Menu Item Procedure. This option is only available when the options “View Menu Items” and “Run PMC” are enabled.

### Edit Menu Item Prep Costs

Enable this option for employees associated with this Role to edit Menu Item Prep Costs within the PMC Menu Item Procedure. This option is only available when the “View Menu Items and “Run PMC” options are enabled.

### Change Menu Item Availability

Enable this option for employees associated with this Role to change the availability of Menu Items within the PMC Menu Item Procedure. This option is only available when the options “View Menu Items” and “Run PMC” are enabled.

### View Barcodes

Enable this option for employees associated with this Role to access the Barcode Procedure within the PMC. This option is only available when the “Run PMC” option is enabled.

### Edit Barcodes

Enable this option for employees associated with this Role to change Edit Barcodes within the PMC Barcode Procedure. This option is only available when the options “View Barcodes” and “Run PMC” are enabled.

### View Employee Definitions

Enable this option for employees associated with this Role to access the Employee Procedure within the PMC. This option is only available when the “Run PMC” option is enabled.

### Edit Employee Definitions

Enable this option for employees associated with this Role to edit Employee Records within the PMC Employee Procedure. This option is only available when the options “View Employee Definitions” and “Run PMC” are enabled.

### Change Employee Training Status

Enable this option for employees associated with this Role to edit Employee Training Status within the PMC Employee Training Mode Procedure. This option is only available when the “Run PMC” option is enabled.

### Assign Employee ID/Mag Card

Enable this option for employees associated with this Role to assign IDs or Mag Cards to Employees within the PMC Employee Procedure. This option is only available when the options “View Employee Definition” and “Run PMC” are enabled.

### View Employee Time Cards

Enable this option for employees associated with this Role to access the Time Card Procedure within the PMC. This option is only available when the “Run PMC” option is enabled.

### Edit Employee Time Cards

Enable this option for employees associated with this Role to edit Employee Time Cards within the PMC Time Card Procedure. This option is only available when the options “View Employee Timecards” and “Run PMC” are enabled.

### View and Edit Time Card Detail Pay Rates

Enable this option for employees associated with this Role to view and edit Time Card Entry Pay Rates. In Simphony, an individual time card detail record may have its pay rate adjusted, allowing mid-pay period raises or specific shift-rate work. This option is only available when the “Edit Employee Time Cards” and “Run PMC” options are enabled.

### View Employee Pay Rates

Enable this option for employees associated with this Role to access the Pay Rates Procedure within the PMC. This option is only available when the “Run PMC” option is enabled.

### Edit Employee Pay Rates

Enable this option for employees associated with this Role to edit Employee Pay Rates within the PMC Pay Rates Procedure. This option is only available when the options “View Employee Pay Rates” and “Run PMC” are enabled.

## Other Procedure Options

### View Currency Rates

Enable this option for employees associated with this Role to access the Currency Procedure within the PMC. This option is only available when the “Run PMC” option is enabled.

### Change Currency Rates

Enable this option for employees associated with this Role to change Currency Rates within the PMC Currency Procedure. This option is only available when the options “View Currency Rates” and “Run PMC” are enabled.

### View Order Devices

Enable this option for employees associated with this Role to access the Order Devices Procedure within the PMC. This option is only available when the “Run PMC” option is enabled.

### Redirect Order Devices

Enable this option for employees associated with this Role to redirect Order Devices within the PMC Order Devices Procedure. This option is only available when the options “View Order Devices” and “Run PMC” are enabled.

### Change Serving Period

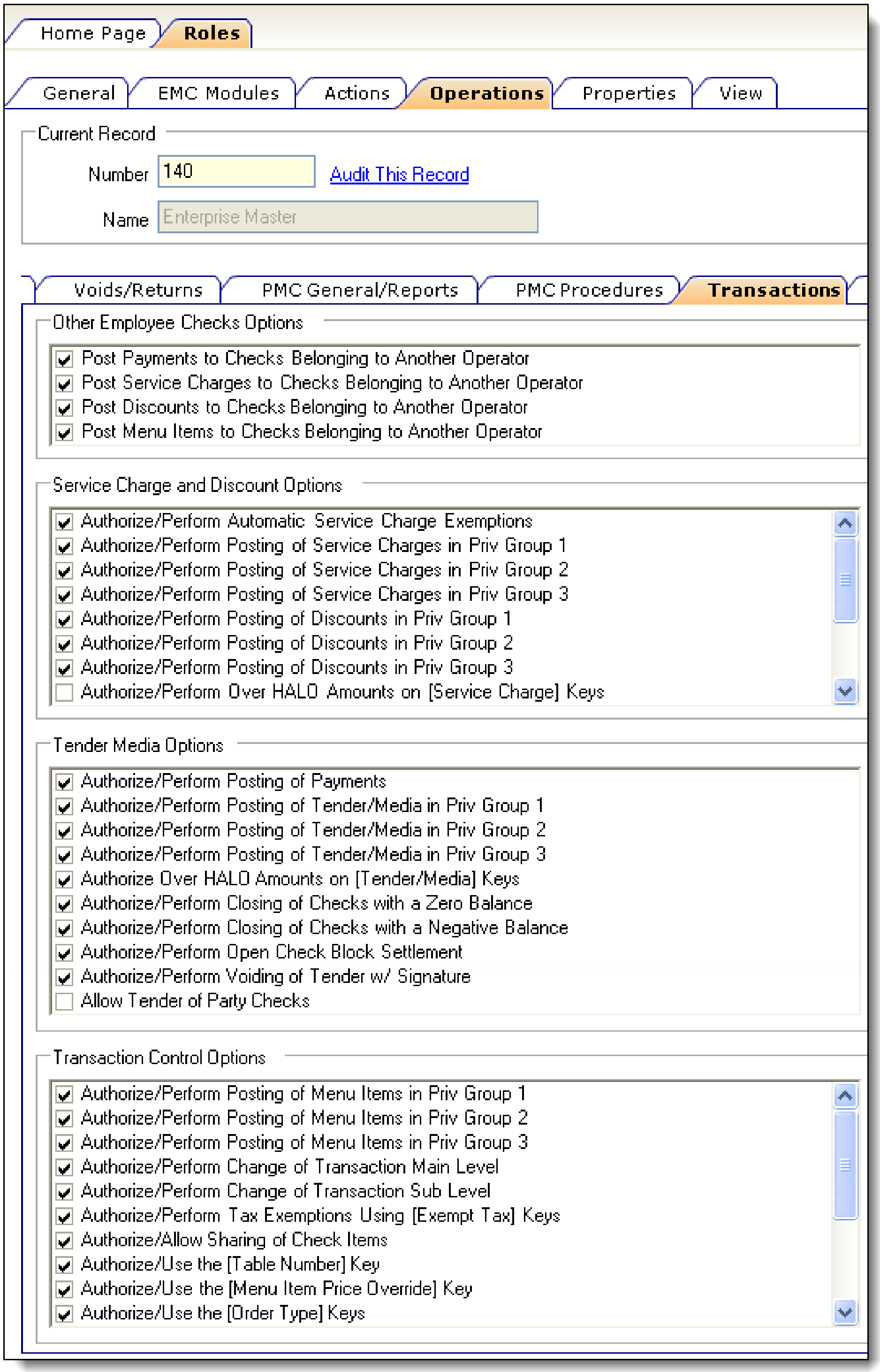
Enable this option for employees associated with this Role to change the serving period within the PMC Serving Period Procedure. This option is only available when the “Run PMC” option is enabled.

### Set Active Kitchen Themes

Enable this option for employees associated with this Role to set the active kitchen theme.

### Transactions Tab

**Figure 3-15 - Roles Transaction Privileges**



Current Record

Number 140

Name Enterprise Master

Other Employee Checks Options

☑ Post Payments to Checks Belonging to Another Operator
☑ Post Service Charges to Checks Belonging to Another Operator
☑ Post Discounts to Checks Belonging to Another Operator
☑ Post Menu Items to Checks Belonging to Another Operator

Service Charge and Discount Options

☑ Authorize/Perform Automatic Service Charge Exemptions
☑ Authorize/Perform Posting of Service Charges in Priv Group 1
☑ Authorize/Perform Posting of Service Charges in Priv Group 2
☑ Authorize/Perform Posting of Service Charges in Priv Group 3
☑ Authorize/Perform Posting of Discounts in Priv Group 1
☑ Authorize/Perform Posting of Discounts in Priv Group 2
☑ Authorize/Perform Posting of Discounts in Priv Group 3
□ Authorize/Perform Over HALO Amounts on [Service Charge] Keys

Tender Media Options

☑ Authorize/Perform Posting of Payments
☑ Authorize/Perform Posting of Tender/Media in Priv Group 1
☑ Authorize/Perform Posting of Tender/Media in Priv Group 2
☑ Authorize/Perform Posting of Tender/Media in Priv Group 3
☑ Authorize Over HALO Amounts on [Tender/Media] Keys
☑ Authorize/Perform Closing of Checks with a Zero Balance
☑ Authorize/Perform Closing of Checks with a Negative Balance
☑ Authorize/Perform Open Check Block Settlement
☑ Authorize/Perform Voiding of Tender w/ Signature
□ Allow Tender of Party Checks

Transaction Control Options

☑ Authorize/Perform Posting of Menu Items in Priv Group 1
☑ Authorize/Perform Posting of Menu Items in Priv Group 2
☑ Authorize/Perform Posting of Menu Items in Priv Group 3
☑ Authorize/Perform Change of Transaction Main Level
☑ Authorize/Perform Change of Transaction Sub Level
☑ Authorize/Perform Tax Exemptions Using [Exempt Tax] Keys
☑ Authorize/Allow Sharing of Check Items
☑ Authorize/Use the [Table Number] Key
☑ Authorize/Use the [Menu Item Price Override] Key
☑ Authorize/Use the [Order Type] Keys

## Other Employees Checks Options

### Post Payments to Checks Belonging to Another Operator

Select this option to allow employees associated with this Role to post tender/media entries to checks belonging to another operator.

### Post Service Charges to Checks Belonging to Another Operator

Select this option to allow employees associated with this Role to add service charges to checks belonging to another operator.

### Post Discounts to Checks Belonging to Another Operator

Select this option to allow employees associated with this Role to add discounts to checks belonging to another operator.

### Post Menu Items to Checks Belonging to Another Operator

Select this option to allow employees associated with this Role to add menu items to checks belonging to another operator.

## Service Charge and Discount Options

### Authorize/Perform Automatic Service Charge Exemptions

Select this option to allow employees associated with this Role to forgive automatic service charges using the [Exempt Auto Service Charge] key and to authorize non-privileged employees to do so as well.

### Authorize/Perform Posting of Service Charges in Priv Group (1-3)

Select this option to allow employees associated with this Role to post Service Charges belonging to Privilege Group X and to authorize non- privileged employees to do so as well. (Note that all employees can post Service Charges belonging to Privilege Group ‘0’).

### Authorize/Perform Posting of Discounts in Priv Group (1- 3)

Select this option to allow employees associated with this Role to post Discounts belonging to Privilege Group X and to authorize non- privileged employees to do so as well. (Note that all employees can post Discounts belonging to Privilege Group ‘0’)

### Authorize/Perform Over HALO Amounts on [Service Charge] Keys

Select this option to allow employees associated with this Role to exceed the HALO amount set for Service Charges.

### Authorize/Use Auto Discount Toggle

Select this option to allow employees associated with this Role to use the Auto Discount Toggle Function Key (655) and to authorize non- privileged employees to do so as well.

### Authorize/Use Auto Discount Apply

Select this option to allow employees associated with this Role to use the Auto Discount Apply Function Key (656) and to authorize non-privileged employees to do so as well.

### Authorize/Use Auto Discount Remove

Select this option to allow employees to remove an Auto Discount and to authorize non-privileged employees to do so as well.

#### Authorize/Perform “Accept Coupon” Stored Value Function

Select this option to allow employees to perform the Accept Coupon stored value function and to authorize non-privileged employees to do so as well.

#### Authorize/Perform “Void Accept Coupon” Stored Value Function

Select this option to allow employees to perform the Void Accept Coupon stored value function and to authorize non-privileged employees to do so as well.

### Tender Media Options

#### Authorize/Perform Posting of Payments

Select this option to allow employees associated with this Role to post payments to a transaction and to authorize non-privileged employees to do so as well.

#### Authorize/Perform Posting of Tender/Media in Priv Group (1-3)

Select this option to allow employees associated with this Role to post Tender/Media entries belonging to Privilege Group X and to authorize non-privileged employees to do so as well. (Note that all employees can post Tender/Media entries belonging to Privilege Group ‘0’).

#### Authorize Over HALO Amounts on [Tender/Media] Keys

Select this option to allow employees associated with this Role to exceed the HALO amount set for a Tender/Media key and to authorize non- privileged employees to do so as well.

#### Authorize/Perform Closing of Checks with a Zero Balance

Select this option to allow employees associated with this Role to tender and close transactions that have a balance due of 0.00 and to authorize non-privileged employees to do so as well.

#### Authorize/Perform Closing of Checks with a Negative Balance

Select this option to allow employees associated with this Role to tender and close transactions that have a negative balance due and to authorize non-privileged employees to do so as well.

#### Authorize/Perform Open Check Block Settlement

Select this option to allow employees associated with this Role to close all of their open checks to the Default Cash Tender/Media (specified in Revenue Center Parameters) and to authorize non-privileged employees to do so as well.

#### Authorize/Perform Voiding of Tender w/ Signature

Select this option to allow employees associated with this Role to void a tender from a check with a signature capture and to authorize non- privileged employees to do so as well.

#### Allow Tender of Party Checks

Select this option to allow employees associated with this Role to Tender and close “Party Checks.”

## Transaction Control Options

### Authorize/Perform Posting of Menu Items in Priv Group (1-3)

Select this option to allow employees associated with this Role to post Menu Items belonging to Privilege Group X and to authorize non- privileged employees to do so as well. (Note that all employees can post Menu Items belonging to Privilege Group '0').

### Authorize/Perform Change of Transaction Main Level

Select this option to allow employees associated with this Role to change the Main Level using one of the eight [Main Level] keys and to authorize non-privileged employees to do so as well.

### Authorize/Perform Change of Transaction Sub Level

Select this option to allow employees associated with this Role to change the Sub Menu Level using one of the eight [Sub Level] keys and to authorize non-privileged employees to do so as well.

### Authorize/Perform Tax Exemptions Using [Exempt Tax] Keys

Select this option to allow employees associated with this Role to forgive tax using one of the [Exempt Tax] keys and to authorize non-privileged employees to do so as well.

### Authorize/Allow Sharing of Check Items

Select this option to allow employees associated with this Role to share menu items and to authorize non-privileged employees to do so as well. Sharing menu items is performed when using the [TouchSplit] and [TouchEdit] functions to put part of a menu item on two different checks (e.g., 1/2 Bottle of Wine "shared" between two couples at a table).

### Authorize/Use the [Table Number] Key

Select this option to allow employees associated with this Role to use the [Table Number] key and to authorize non-privileged employees to do so as well.

### Authorize/Use the [Menu Item Price Override] Key

Select this option to allow employees associated with this Role to use the [Menu Item Price Override key] and to authorize non-privileged employees to do so as well. Menu Item Price Overrides are usually used to override a preset price of a barcode menu item.

### Authorize/Use the [Order Type] Key

Select this option to allow employees associated with this Role to select an Order Type and to authorize non-privileged employees to do so as well.

### Authorize/Use the [Item Weight] Key

Select this option to allow employees associated with this Role to post weighed menu items and to authorize non-privileged employees to do so as well.

### Authorize/Use the [Transaction Cancel] Key

Select this option to allow employees associated with this Role to use the [Transaction Cancel] key and to authorize non-privileged employees to do so as well.

### Authorize/Cause a Transaction to have a Negative Balance

Select this option to allow employees associated with this Role to create a check with a negative balance and to authorize non-privileged employees to do so as well.

**Authorize/Perform Change of Number of Guests**

Select this option to allow employees associated with this Role to change the number of guests in a transaction using the [Number of Guests] key and to authorize non-privileged employees to do so as well.

**Authorize/Perform Signature Capture Override**

Select this option to allow employees associated with this Role to use the [Signature Capture Override] key and to authorize non-privileged employees to do so as well. Signature Capture Override is used to bypass the signature capture process, in the event that the customer refuses to sign, or if the customer has left without signing.

**Authorize/Perform Employee Meal Discount Override for Non-Scheduled Employees**

Enable this option to allow employees associated with this Role to permit non-scheduled employees to receive the employee meal discount and to authorize non-privileged employees to do so as well. This option works in conjunction with the “Employee Meal” and “Employee Meal Discount Applies to Scheduled Employees Only” options in the ‘Discounts’ module.

**Authorize/Perform Payment and Service Total of Insufficient Beverage Checks**

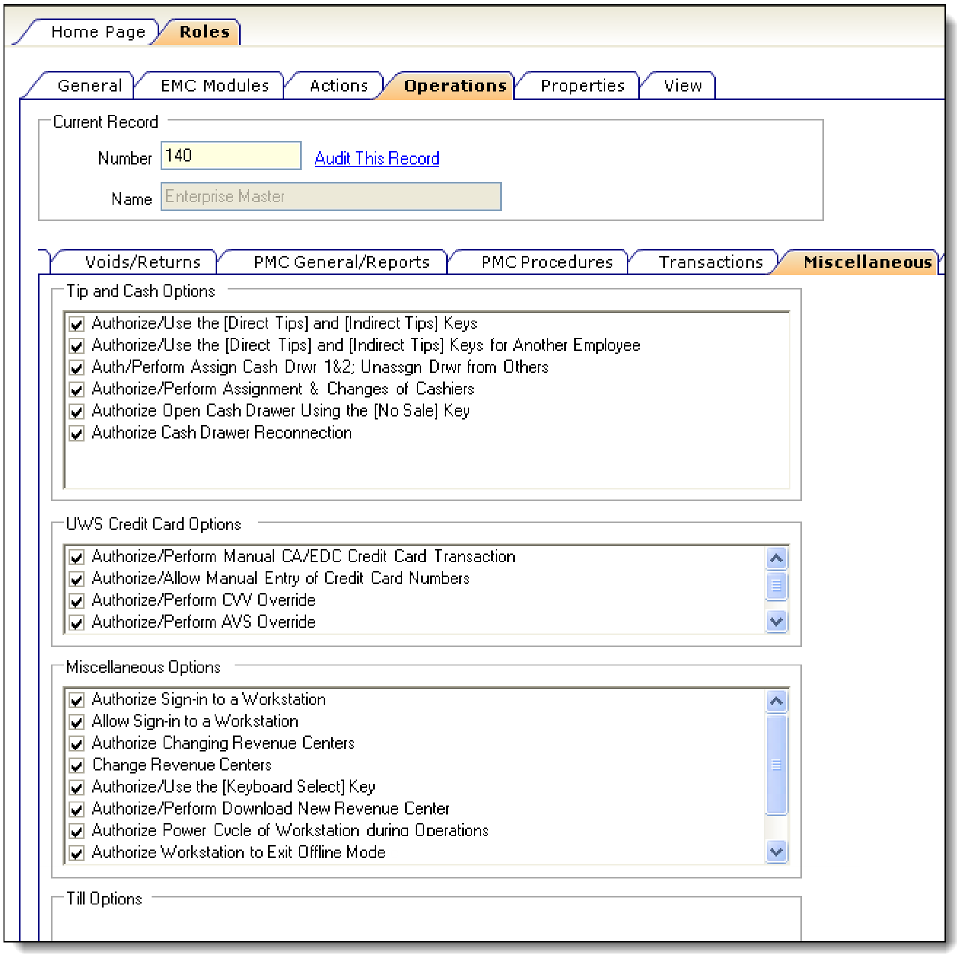
Select this option to allow employees associated with this Role to pay and service total checks that have an Insufficient Beverage Count. When the RVC Parameters | General Option “Disallow Payment or Service Total of Insufficient Beverage Checks” is enabled, workstations will require the Beverage Count to match or exceed the Guest Count before the check can be paid or service totaled. If the workstation user is not associated with a Role that has this option enabled, he/she will not be able to pay or service total the check.

**Authorize/Perform Automatic Combo Meal Recognition on Previous Round Menu Items**

Enable this option to allow employees associated with this Role to include previous round Menu Items when attempting to create a Combo Meal from existing Menu Items, and to authorize non-privileged employees to do so as well.

## Miscellaneous Tab

### Figure 3-16 - Roles - Miscellaneous tab



Current Record

Number 140 Audit This Record

Name Enterprise Master

Tip and Cash Options

- ☑ Authorize/Use the [Direct Tips] and [Indirect Tips] Keys
- ☑ Authorize/Use the [Direct Tips] and [Indirect Tips] Keys for Another Employee
- ☑ Auth/Perform Assign Cash Drwr 1&2; Unassgn Drwr from Others
- ☑ Authorize/Perform Assignment & Changes of Cashiers
- ☑ Authorize Open Cash Drawer Using the [No Sale] Key
- ☑ Authorize Cash Drawer Reconnection

UWS Credit Card Options

- ☑ Authorize/Perform Manual CA/EDC Credit Card Transaction
- ☑ Authorize/Allow Manual Entry of Credit Card Numbers
- ☑ Authorize/Perform CVV Override
- ☑ Authorize/Perform AVS Override

Miscellaneous Options

- ☑ Authorize Sign-in to a Workstation
- ☑ Allow Sign-in to a Workstation
- ☑ Authorize Changing Revenue Centers
- ☑ Change Revenue Centers
- ☑ Authorize/Use the [Keyboard Select] Key
- ☑ Authorize/Perform Download New Revenue Center
- ☑ Authorize Power Cycle of Workstation during Operations
- ☑ Authorize Workstation to Exit Offline Mode

Till Options

## Tip and Cash Options

### Authorize/Use the [Direct Tips] and [Indirect Tips] Keys

Select this option to allow employees associated with this Role to use these keys to declare cash tips received (by themselves) and to authorize non-privileged employees to do so as well.

### Authorize/Use the [Direct Tips] and [Indirect Tips] Keys for Another Employee

Select this option to allow employees associated with this Role to use these keys to declare cash tips received by another employee and to authorize non-privileged employees to do so as well.

### Auth/Perform Assign Cash Drwr 1&2; Unassgn Drwr from Others

This option bit includes two different functions. #1: Select this option bit to allow employees associated with this Role to use the [Assign Cash Drawer 1] and [Assign Cash Drawer 2] keys to assign the cash drawer to themselves, and to authorize non-privileged employees to use the [Assign Cash Drawer 1] or [Assign Cash Drawer 2] keys to become assigned to a drawer. #2 If this option bit is enabled, employees in this employee class can use the [Unassign Cash Drawer] key to unassign cash drawers from other operators. Note that the [Assign Cash Drawer] key does not require an Employee Role privilege--any employee with access to the [Assign Cash Drawer] button can use it.

#### Authorize/Perform Assignment & Changes of Cashiers

Select this option to allow employees associated with this Role to assign themselves a cashier link or change their cashier link with the [Assign Cashier] key and to authorize non-privileged employees to do so as well.

#### Authorize Open Cash Drawer Using the [No Sale] Key

Select this option to allow employees associated with this Role to open the cash drawer outside of a transaction using the [No Sale] key and to authorize non-privileged employees to do so as well.

#### Authorize Cash Drawer Reconnection

Select this option to allow employees associated with this Role to authorize a cash drawer cable reconnection on a workstation. If an operator has the option bit enabled to “Require Authorization for Cash Drawer Reconnection,” the operator will need an authorization before performing another transaction. If this option bit is enabled, employees associated with this Role can perform this authorization.

### UWS Credit Card Options

#### Authorize/Perform Manual CA/EDC Credit Card Transaction

Select this option to allow employees associated with this Role to manually authorize a Credit Authorization transaction using the [Manual Authorize] key and to authorize non-privileged employees to do so as well.

#### Authorize/Allow Manual Entry of Credit Card Numbers

Select this option to allow manual entry of credit card numbers (typing the numbers into the workstation instead of swiping the credit card) and to authorize non-privileged employees to do so as well.

#### Authorize/Perform CVV Override

Enable this option to allow employees associated with this Role to proceed with a credit card process without entering the CVV, CVC, or CID (the Card-Present Number) and to authorize non-privileged employees to do so as well.

#### Authorize/Perform AVS Override

Enable this option to allow employees associated with this Role to proceed with a credit card process without entering the AVS (Address Verification Service) information and to authorize non-privileged employees to do so as well.

#### Authorize/Perform Tender Above Unauthorized Credit Threshold

Select this option to allow employees associated with this Role to pay checks where a credit card authorization has been performed, but subsequent entries on the check have caused the Tender/Media’s “Unauthorized Authorization Threshold” to be exceeded.

This option is generally used when a workstation enters the offline mode. When a workstation is unable to communicate with the database and a second authorization is required, the workstation does not have access to the encrypted credit card number. In this situation, a workstation will consider all credit card authorizations “good” while under the “Unauthorized Authorization Threshold”, if that limit is exceeded, only employees with this option enabled may pay transactions.

## Miscellaneous Options

### Authorize Sign-in to a Workstation

Select this option to allow employees associated with this Role to authorize a non-privileged employee (one for whom the “Allow Sign into a Workstation” option is disabled) to sign in to a workstation or Mobile MICROS unit.

### Allow Sign-in to a Workstation

Select this option to allow employees associated with this Role to sign into a workstation or a Mobile MICROS unit. Do not select this option to prevent employees from performing any operations other than clocking in and out unless they gain authorization from a privileged employee. (Refer to the Authorize Sign-in to a Workstation option.)

### Authorize Changing Revenue Centers

Select this option to allow employees associated with this Role to Change Revenue Centers and to authorize non-privileged employees to do so as well.

### Change Revenue Centers

Select this option to allow employees associated with this Role to change Revenue Centers by signing into a workstation that belongs to a Revenue Center that is different from RVC to which the employee is currently assigned.

### Authorize/Use the [Keyboard Select] Key

Select this option to allow employees associated with this Role to change keyboards using one of the [Keyboard Select] keys and to authorize non- privileged employees to do so as well.

### Authorize/Perform UWS Download New Revenue Center

Select this option to allow employees associated with this Role to download a new Revenue Center to a workstation and to authorize non- privileged employees to do so as well.

### Authorize Power Cycle of Workstation during Operations

Select this option to allow employees associated with this Role to authorize a Power Cycle of a workstation. If an operator has the option bit enabled to “Require Authorization for Power Cycle of UWS during Operations,” the operator will need an authorization before performing another transaction. If this option bit is enabled, employees associated with this Role can perform this authorization.

### Authorize Workstation to Enter Offline Mode

Select this option to allow employees associated with this Role to enter offline mode on a workstation. When an operation is attempted that normally causes the workstation to contact the Simphony database, if contact cannot be established, a message prompt appears for users to retry the operation or to work offline. If a user chooses to work offline, the operator needs to have an authorization, which is represented by this option bit.

### Authorize Workstation to Exit Offline Mode

Select this option to allow employees associated with this Role to enter online mode (while currently in offline mode) on a workstation. While offline, if communication with the Simphony Database is detected, a prompt will be displayed to work in online mode. If the user chooses to work online, the operator needs to have an authorization, which is represented by this option bit.

### Authorize Running of Offline Reports

Select this option to allow employees associated with this Role to generate Offline Reports when the workstation is offline.

### Can Minimize Ops Application

Select this option to allow employees associated with this Role to minimize the Ops application on a workstation.

### Can Close Ops Application

Select this option to allow employees associated with this Role to close the Ops application on a workstation.

### Enable/Disable Sales Recording Module

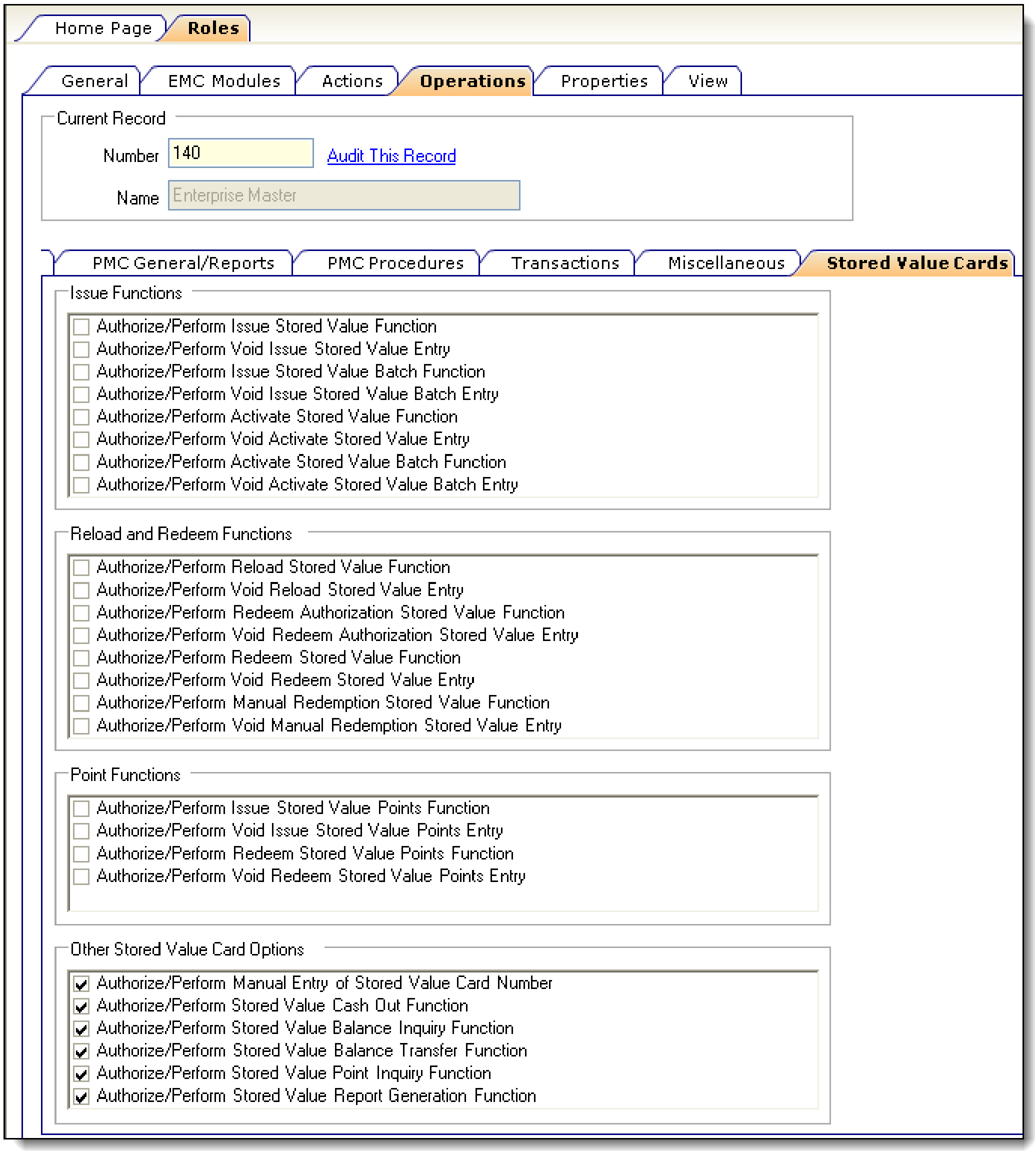
This option allows employees to disable the SRM device and directly connect the printer. When the SRM device is broken and must be bypassed, use the enable/disable SRM function (862).

### Till Options

No Till Options are available at this time.

## Stored Value Cards Tab

### Figure 3-17 - Roles Stored Value Cards Options



Current Record

Number 140

Name Enterprise Master

Issue Functions

- □ Authorize/Perform Issue Stored Value Function
- □ Authorize/Perform Void Issue Stored Value Entry
- □ Authorize/Perform Issue Stored Value Batch Function
- □ Authorize/Perform Void Issue Stored Value Batch Entry
- □ Authorize/Perform Activate Stored Value Function
- □ Authorize/Perform Void Activate Stored Value Entry
- □ Authorize/Perform Activate Stored Value Batch Function
- □ Authorize/Perform Void Activate Stored Value Batch Entry

Reload and Redeem Functions

- □ Authorize/Perform Reload Stored Value Function
- □ Authorize/Perform Void Reload Stored Value Entry
- □ Authorize/Perform Redeem Authorization Stored Value Function
- □ Authorize/Perform Void Redeem Authorization Stored Value Entry
- □ Authorize/Perform Redeem Stored Value Function
- □ Authorize/Perform Void Redeem Stored Value Entry
- □ Authorize/Perform Manual Redemption Stored Value Function
- □ Authorize/Perform Void Manual Redemption Stored Value Entry

Point Functions

- □ Authorize/Perform Issue Stored Value Points Function
- □ Authorize/Perform Void Issue Stored Value Points Entry
- □ Authorize/Perform Redeem Stored Value Points Function
- □ Authorize/Perform Void Redeem Stored Value Points Entry

Other Stored Value Card Options

- ☑ Authorize/Perform Manual Entry of Stored Value Card Number
- ☑ Authorize/Perform Stored Value Cash Out Function
- ☑ Authorize/Perform Stored Value Balance Inquiry Function
- ☑ Authorize/Perform Stored Value Balance Transfer Function
- ☑ Authorize/Perform Stored Value Point Inquiry Function
- ☑ Authorize/Perform Stored Value Report Generation Function

## Issue Functions

### Authorize/Perform Issue Stored Value Function

Select this option to allow employees associated with this Role to issue a stored value card and to authorize non-privileged employees to do so as well.

### Authorize/Perform Void Issue Stored Value Entry

Select this option to allow employees associated with this Role to void an issued card and to authorize non-privileged employees to do so as well. Note: Touch Voids and Direct Voids are allowed; Last Item Voids and Returns are not allowed.

**Authorize/Perform Issue Stored Value Batch Function**

Select this option to allow employees associated with this Role to issue a batch of stored value cards and to authorize non-privileged employees to do so as well.

**Authorize/Perform Void Issue Stored Value Batch Entry**

Select this option to allow employees associated with this Role to void a batch of stored value cards and to authorize non-privileged employees to do so as well. Note: Touch Voids and Direct Voids are allowed; Last Item Voids and Returns are not allowed.

**Authorize/Perform Activate Stored Value Function**

Select this option to allow employees associated with this Role to activate a stored value card and to authorize non-privileged employees to do so as well.

**Authorize/Perform Void Activate Stored Value Entry**

Select this option to allow employees associated with this Role to void the activation of a stored value card and to authorize non-privileged employees to do so as well. Note: Touch Voids and Direct Voids are allowed; Last Item Voids and Returns are not allowed.

**Authorize/Perform Activate Stored Value Batch Function**

Select this option to allow employees associated with this Role to activate a batch of stored value cards and to authorize non-privileged employees to do so as well.

**Authorize/Perform Void Activate Stored Value Batch Entry**

Select this option to allow employees associated with this Role to void the activation of a batch of stored value cards and to authorize non-privileged employees to do so as well.

**Reload and Redeem Functions**

**Authorize/Perform Reload Stored Value Function**

Select this option to allow employees associated with this Role to Reload (add credit) a dollar amount to an existing stored value card and to authorize non-privileged employees to do so as well.

**Authorize/Perform Void Reload Stored Value Entry**

Select this option to allow employees associated with this Role to void a Reload transaction and to authorize non-privileged employees to do so as well. Touch Voids and Direct Voids are allowed; Last Item Voids and Returns are not allowed.

**Authorize/Perform Redeem Authorization Stored Value Function**

Select this option to allow employees associated with this Role to perform a redemption authorization and to authorize non-privileged employees to do so as well.

**Authorize/Perform Void Redeem Authorization Stored Value Entry**

Select this option to allow employees associated with this Role to void a redemption authorization and to authorize non-privileged employees to do so as well.

**Authorize/Perform Redeem Stored Value Function**

Select this option to allow employees associated with this Role to perform a redemption transaction (a stored value card is used to make a purchase and a dollar amount is deducted from the account) and to authorize non- privileged employees to do so as well.

#### Authorize/Perform Void Redeem Stored Value Entry

Select this option to allow employees associated with this Role to void a redemption transaction and to authorize non-privileged employees to do so as well.

#### Authorize/Perform Manual Redemption Stored Value Function

Select this option to allow employees associated with this Role to perform a manual redemption and to authorize non-privileged employees to do so as well.

#### Authorize/Perform Void Manual Redemption Stored Value Entry

Select this option to allow employees associated with this Role to void a manual redemption transaction and to authorize non-privileged employees to do so as well.

### Point Functions

#### Authorize/Perform Issue Stored Value Points Function

Select this option to allow employees associated with this Role to issue points to a stored value card and to authorize non-privileged employees to do so as well.

#### Authorize/Perform Void Issue Stored Value Points Entry

Select this option to allow employees associated with this Role to void issued points on a stored value card and to authorize non-privileged employees to do so as well. Touch Voids and Direct Voids are allowed; Last Item Voids and Returns are not allowed.

#### Authorize/Perform Redeem Stored Value Points Function

Select this option to allow employees associated with this Role to perform a point’s redemption transaction and to authorize non-privileged employees to do so as well.

#### Authorize/Perform Void Redeem Stored Value Points Entry

Select this option to allow employees associated with this Role to void a point’s redemption transaction and to authorize non-privileged employees to do so as well.

### Other Stored Value Card Options

#### Authorize/Perform Manual Entry of Stored Value Card Number

Select this option to allow employees associated with this Role to manually enter the stored value card account number and to authorize non-privileged employees to do so as well.

#### Authorize/Perform Stored Value Cash Out Function

Select this option to allow employees associated with this Role to debit some or all of the remaining balance on a stored value card and to authorize non-privileged employees to do so as well.

#### Authorize/Perform Stored Value Balance Inquiry Function

Select this option to allow employees associated with this Role to check a stored value card balance and to authorize non-privileged employees to do so as well.

#### Authorize/Perform Stored Value Balance Transfer Function

Select this option to allow employees associated with this Role to transfer the balance from one stored value card to another and to authorize non- privileged employees to do so as well.

### Authorize/Perform Stored Value Point Inquiry Function

Select this option to allow employees associated with this Role to check a stored value card point balance and to authorize non-privileged employees to do so as well.

### Authorize/Perform Stored Value Report Generation Function

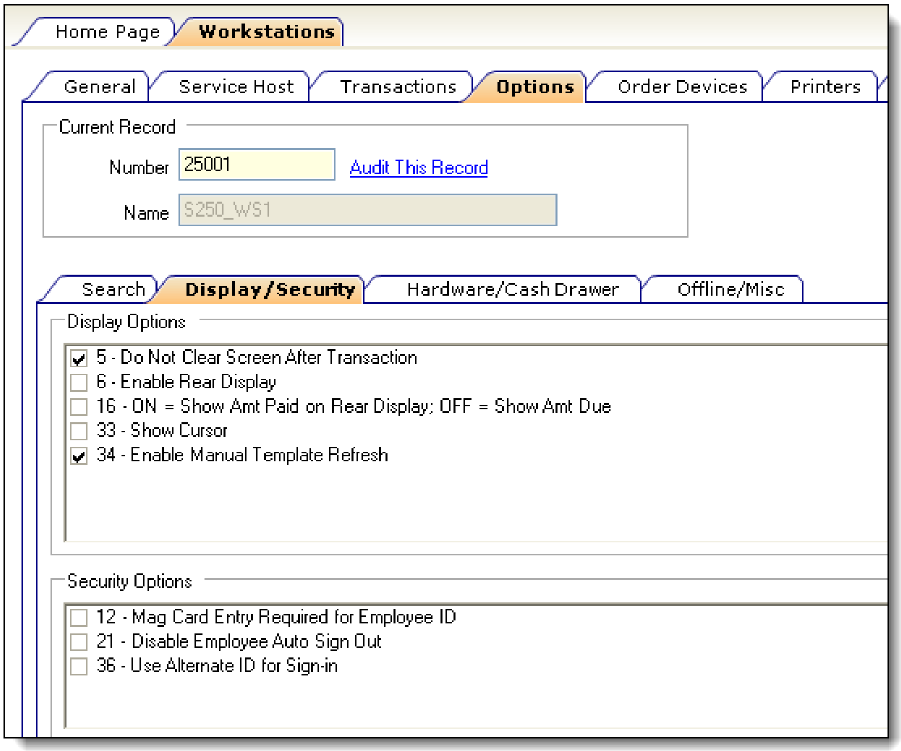
Select this option to allow employees associated with this Role to generate stored value card reports and to authorize non-privileged employees to do so as well.

# Workstation Privileges - EMC Configuration

Workstation Privileges are configured in the EMC within the Property level, Hardware, Workstations, and Options tab.

## Display/Security Tab

### Figure 3-18 - Workstations Display/ Security Options



Current Record

Number 25001

Name S250_WS1

Display Options

☑ 5 - Do Not Clear Screen After Transaction
□ 6 - Enable Rear Display
□ 16 - ON = Show Amt Paid on Rear Display; OFF = Show Amt Due
□ 33 - Show Cursor
☑ 34 - Enable Manual Template Refresh

Security Options

□ 12 - Mag Card Entry Required for Employee ID
□ 21 - Disable Employee Auto Sign Out
□ 36 - Use Alternate ID for Sign-in

## Display Options

### Do Not Clear Screen After Transaction

Select this option to cause the last screen of a transaction to remain on the display after the transaction is complete. This option is enabled for workstations in Revenue Centers who want to use the “Print Customer Receipt” function key to print receipts after the close of a transaction.

### Enable Rear Display

Select this option to enable output to a rear customer display attached to this workstation.

#### ON = Show Amt Paid on Rear Display; OFF = Show Amt Due

Select this option to cause the amount paid by the customer to show on the rear display (customer display). Do not select this option to cause the Amount Due to show on the rear display.

#### Show Cursor

Enable this option to display the mouse cursor for this workstation. This option is typically enabled for workstations that are installed on PCs, such as a hostess desk, and is usually disabled for WS4 and other Oracle MICROS hardware platforms.

#### Enable Manual Template Refresh

Enable this option for the workstation to reread the template configuration file and refresh the display without having to manually exit and enter Ops. If this option is disabled, Templates will only refresh after the Ops application has been exited and restarted.

### Security Options

#### Mag Card Entry Required for Employee ID

Select this option to require that all employee ID entries at this workstation are made using a magnetic employee ID card. This applies to signing in and authorizing privileged operations. If this option is selected, the workstation will not accept an employee ID number entered through the keyboard or touchscreen. Do not select this option to allow the employee ID to be entered by either a magnetic card or by the keyboard or touchscreen.

#### Disable Employee Auto Sign Out

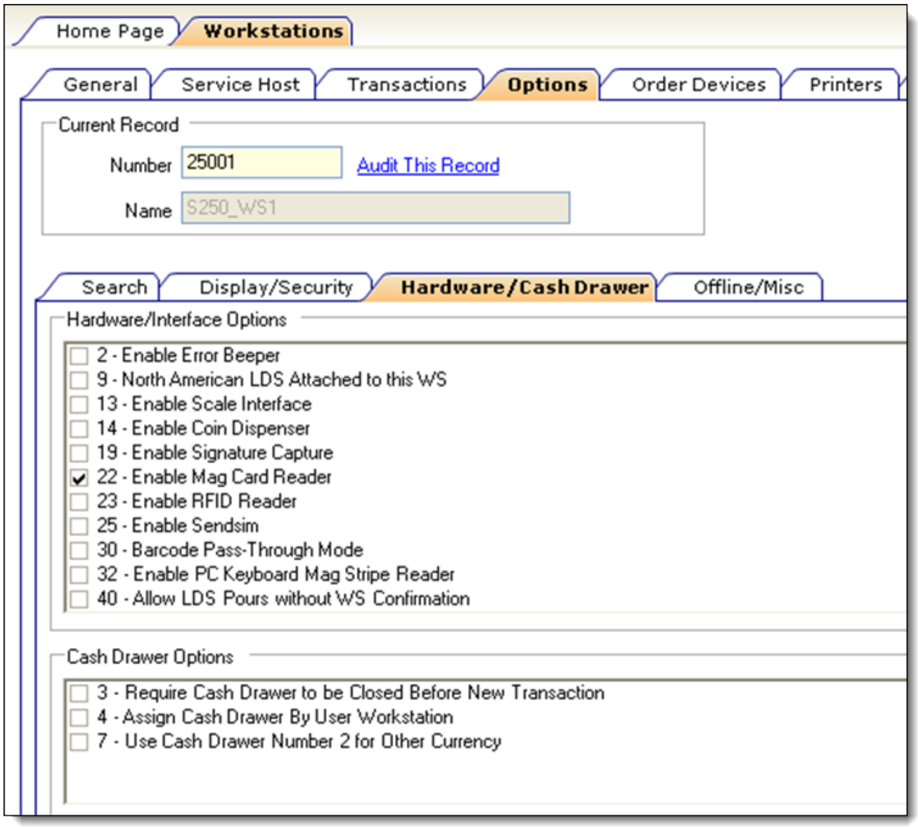
Select this option to disable the Automatic Operator Popup Interval programmed in ‘Revenue Center Parameters’. Do not select this option to cause operators to be signed out of this workstation after the ‘Automatic Operator Popup Interval’ expires.

#### Use Alternate ID for Sign-in

Select this option to allow the operator to sign-in using a four-digit Alternate ID number rather than a ten-digit Employee ID number.

### Hardware/ Cash Drawer Tab

**Figure 3-19 - Workstations Hardware/ Cash Drawer**



Number: 25001

Name: S250_WS1

- □ 2 - Enable Error Beeper
- □ 9 - North American LDS Attached to this WS
- □ 13 - Enable Scale Interface
- □ 14 - Enable Coin Dispenser
- □ 19 - Enable Signature Capture
- ☑ 22 - Enable Mag Card Reader
- □ 23 - Enable RFID Reader
- □ 25 - Enable Sendsim
- □ 30 - Barcode Pass-Through Mode
- □ 32 - Enable PC Keyboard Mag Stripe Reader
- □ 40 - Allow LDS Pours without WS Confirmation

- □ 3 - Require Cash Drawer to be Closed Before New Transaction
- □ 4 - Assign Cash Drawer By User Workstation
- □ 7 - Use Cash Drawer Number 2 for Other Currency

## Hardware/ Interface Options

### Enable Error Beeper

When this option is enabled, a beep will sound each time an error occurs. If this option is disabled, no beep occurs.

### North American LDS Attached to this UWS

This option only applies to workstations using a Liquor Dispensing System. Select this option to indicate to the system that the Liquor Dispensing System (LDS) attached to this UWS is a North American LDS. Do not select this option to indicate that an ILDS (International Liquor Dispensing System) is in use.

### Enable Scale Interface

Select this option to enable communication between this workstation and a scale.

### Enable Coin Dispenser

Select this option to enable communication between this workstation and a coin dispenser.

### Enable Signature Capture

Select this option to enable communication between this workstation and a Signature Capture pad.

#### Enable Mag Card Reader

Select this option to enable the Mag Card on this workstation. Disable this option if the workstation doesn't have a magnetic card reader.

#### Enable RFID Reader

Select this option to enable an RFID reader on this workstation. Disable this option if the workstation doesn’t have an RFID reader.

#### Enable SendSim

If this option is enabled, this workstation will be able to receive SendSim messages. Disable this option to prevent this workstation from receiving SendSim messages.

#### Barcode Pass-Through Mode

This option is used to disable the barcode format transformation performed by Ops. When this option is enabled, the raw barcode text is processed by Ops. This option is often enabled in instances where the system interface module (SIM) accepts barcodes directly, instead of being translated by Ops first.

#### Enable PC Keyboard Mag Stripe Reader

When this option is enabled, Ops will examine key presses to determine if they originate from a keyboard or from a mag stripe reader. When a PC Keyboard Mag Read is attached, this option should be enabled.

#### Allow LDS Pours without WS Confirmation

This option controls NA/LDS behavior; when enabled, the NA/LDS will pour a drink prior to receiving the release acknowledgement from Ops. When this option is not enabled, the NA/LDS will wait for a response from Ops prior to pouring the drink.

### Cash Drawer Options

#### Require Cash Drawer to be Closed Before New Transaction

Select this option to require that cash drawers attached to this workstation be closed before a new transaction may be begun. Do not select this option to allow transactions to begin while a cash drawer is open.

#### Assign Cash Drawer By User Workstation

If this option is enabled, operators must assign themselves to a cash drawer by using the one of the Function Keys 848, 839, or 840 (Assign Cash Drawer, Assign Cash Drawer 1, and Assign Cash Drawer 2). Then, only the operator assigned to the drawer will be able to open it (or a privileged manager, who can unassign a drawer from a user). If this option is disabled, the Operator “Cash Drawer” field determines if an operator can access a cash drawer or not. In this scenario, all operators with the “Cash Drawer” field set to ‘1’ will be able to open Cash Drawer 1.

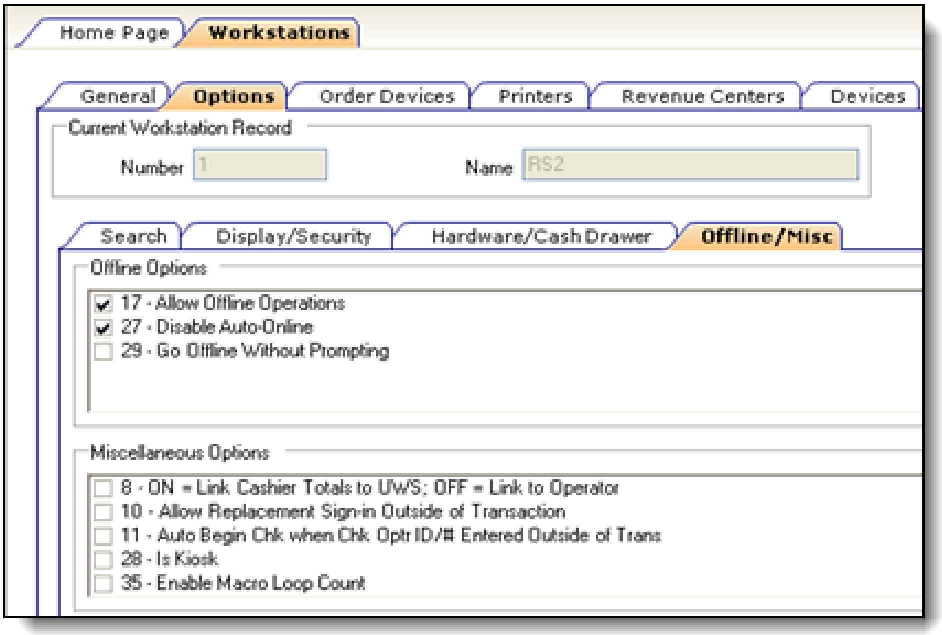
Note: Giving multiple employees access to a single cash drawer is not as secure as requiring employees to be assigned to a Cash Drawer!

### Use Cash Drawer Number 2 for Other Currency

This option is used only if two cash drawers are in use for this workstation and one is dedicated to foreign currency. Select this option to cause the second cash drawer (not the drawer currently assigned) to open, when using a tendering key that opens the cash drawer and that is used with currency conversion. In addition, the foreign currency must allow change to be made in that currency.

## Offline/ Misc Tab

**Figure 3-20 - Workstations Offline/ Misc Options**



Current Workstation Record

Number 1

Name RS2

Offline Options

☑ 17 - Allow Offline Operations
☑ 27 - Disable Auto-Online
□ 29 - Go Offline Without Prompting

Miscellaneous Options

□ 8 - ON = Link Cashier Totals to UWS; OFF = Link to Operator
□ 10 - Allow Replacement Sign-in Outside of Transaction
□ 11 - Auto Begin Chk when Chk Optr ID/# Entered Outside of Trans
□ 28 - Is Kiosk
□ 35 - Enable Macro Loop Count

### Allow Offline Operations

Enable this option to allow this workstation to operate in Offline Mode. “Offline Mode” is a situation where the workstation cannot communicate with the data center and/or the Check and Posting Service.

### Disable Auto-Online

A workstation will automatically return to Online Mode if communications have been reestablished and the number of transactions rung offline is less than the amount specified in the Property Parameters “Automatic Online Transaction Limit” field. By enabling this option, the workstation will prompt the user to return online, instead of continuing online automatically.

### Go Offline Without Prompting

When this option is enabled, a workstation will go offline automatically when communication with the server is lost. When this option is disabled, the user will be prompted to work offline.

### ON = Link Cashier Totals to UWS; OFF = Link to Operator

Select this option to allow this workstation to be linked to a single Cashier Record. This option can only be used with a workstation that is assigned to a single Revenue Center (when this is enabled, Revenue Centers 2-8 become disabled on the Revenue Centers tab). Cashiers are linked to a workstation by using the [Assign Cashier] function key on the workstation. When this option is disabled, totals are posted to the operator's Cashier Record, if one exists.

### Allow Replacement Sign-in Outside of Transaction

Select this option to allow an operator to sign in when another operator is already signed in, causing the system to automatically sign out the first operator. Do not select this option to require that an operator sign out manually before the next operator can sign in.

### Auto Begin Chk when Chk Optr ID/# Entered Outside of Trans

This option is active only if the “Allow Replacement Sign in Outside Transaction” option is disabled. Select this option to allow an operator to begin a Guest Check transaction by entering an operator ID or employee number. The signed-in operator becomes the transaction operator; the employee whose ID or employee number was entered becomes the check operator. If this option is enabled, sales totals and tenders posting are determined by the setting of the Revenue Center Parameters Posting options “Post Totals to Transaction Operator” and “Post Tender to Transaction Operator.” The system will require the use of either the employee ID or the employee number, as determined by the setting of the Operator option “Use Employee Number to Open Check for Another Employee.”

### Is Kiosk

Enable this option if this workstation is a Kiosk. This option prevents certain option bits from applying, such as “Prompt to Confirm Begin Check” and beverage control options. Additionally, “Kiosk” workstations are always allowed to work while offline.

### Enable Macro Loop Count

This option is used primarily for testing purposes and it applies only if the ‘Property Parameters’ option “Do Not Check for Macro Loop Limit” is enabled. If this option is enabled, macros can loop over themselves only for the number of times specified on the Workstation, General tab, in the “Macro Loop Count” field.

### Base Not Required

Set this option if this is an mTablet that will not be docked to an mStation. If this option is set, then the tablet will not be able to configure or use the majority of the hardware devices that the traditional workstations support.

# Appendix B
# Simphony First Edition Port Numbers

## Port Numbers

This is a list of port numbers that are used in Simphony First Edition. Many port numbers are configurable in the EMC. Open only the minimum required ports based upon the installation type and deployment configuration.

### Enterprise Ports

**Table 3-4 - Enterprise Port Numbers**

| Service | Port Number | Configurable? |
|---|---|---|
| Database Default (Oracle) | 1521 | Yes |
| Database Default (Microsoft SQL Server) | 1433 | Yes |
| Simphony/EGateway Application server (Oracle/SQL) | 443 | Yes |
| EMC/Remote EMC | 443 | Yes |
| CAL Client | 7301 (UDP) | Yes |
| CAL Handler | 7301 (UDP) | Yes |
| Classic CAL Service | 7301 (UDP) | Yes |

### Property Ports

**Table 3-5 - Property Port Numbers**

| Service | Port Number | Configurable? |
|---|---|---|
| SarOps | 12359 | No |
| CAL Client | 7300, 7301, 7302 | Yes |
| Offline Labor/Check Cache (running on SarOps) | 12359 | Yes |
| Offline Labor/Check Cache (stand-alone ServiceHost) | 8080 | Yes |
| IP Printing | 9100 | Yes |
| IP Printer Listening | 9100 | No |
| Banquet Printing | 9100 | No |
| KDS Client (Display) | 12359 & 5022 (preferred) | Yes |
| KDS Controller Service | 12359 & 5022 (preferred) | Yes |
| Interface Service | 8080 (Client & external sides) | Yes |

## Port Range for SarOps Clients

Note that SarOps actually uses 12359+ where OLC is running through SarOps for the additional connections, so you might end up seeing port 12360, 12361, etc. in use with multiple WS all talking to the OLC at the same time. The potential Port number range is dynamic based on how many connections are needed.

## Interface Ports

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

**Table 3-6 - Interface Port Numbers**

| Interface | Port Number |
|---|---|
| Table Management System | 5006 |
| Property Management System | 5007 |
| Credit Authorization | 5008 |
| System Interface Module (SIM) | 5009 |
| SIM DB Server | 5021 |

## iCare\ Loyalty Ports

**Table 3-7 - iCare\ Loyalty Port Numbers**

| Service | Port Number |
|---|---|
| Access to websites | 80 |
| SSL Connectivity | 9443 |

## Oracle Component Ports

The following table lists 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. Refer to the Oracle Database Installation Guide for more information about default component port ranges.

**Table 3-8 - Oracle Component Port Numbers**

| Component | Port | Range |
|---|---|---|
| Enterprise Manager Agent<br>Enterprise Manager Database Control | HTTP | 1830 - 1849 |
| Enterprise Manager Agent<br>Enterprise Manager Database Control | HTTP | 5500 - 5519 |
| Enterprise Manager Agent<br>Enterprise Manager Database Control | RMI | 5520 - 5539 |
| Enterprise Manager Agent<br>Enterprise Manager Database Control | JMS | 5540 - 5559 |
| iSQL*Plus | HTTP | 5560 - 5579 |
| iSQL*Plus | RMI | 5580 - 5599 |
| iSQL*Plus | JMS | 5600 - 5619 |
| Ultra Search | HTTP | 5620 - 5639 |
| Ultra Search | RMI | 5640 - 5659 |
| Ultra Search | JMS | 5660 - 5679 |

# Appendix C
# Key Manager Manual

## General Information

### About the Simphony FE Encryption Key Manager Module

The purpose of the Simphony Key Manager module within the Enterprise Management Console (EMC) is to allow the user to set the encryption pass phrase for Simphony FE. In accordance with the PCI Data Security Standard, Oracle MICROS Food & Beverage mandates each site protect encryption keys against both disclosure and misuse.

## Secure Key Practices

To ensure secure distribution, Oracle MICROS Food & 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.

The site also must require each key custodian to sign a form stating that he or she understands and accepts his or her key-custodian responsibilities.

## Key Manager Security Enhancements

Simphony First Edition 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 First Edition uses credit card masking and 3DES encryption to ensure credit card data is stored in a secure manner.

Due to a recent Payment Card Industry Data Security Standard (PCI-DSS) requirement that mandates the secure deletion of unused or invalid encryption keys, Simphony FE uses a new encryption scheme that allows for the secure deletion of encryption keys.

### The New 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

**WARNING:**

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).

## Simphony FE version 1.8 Fresh Installation

The following should be noted when conducting a fresh installation of Simphony FE version 1.8:

- To ensure PCI compliance, Oracle MICROS Food & Beverage mandates that the site run the key rotation after the installation is complete
- For more information on how to rotate keys, refer to the next section

# Performing a Key Rotation

## Operating Conditions

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

- The Simphony EGateway service must be up and running – Internet Information Services (IIS) installed and running
- The Transactional database must be accessible

## 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.

The sections of the module are labelled below:

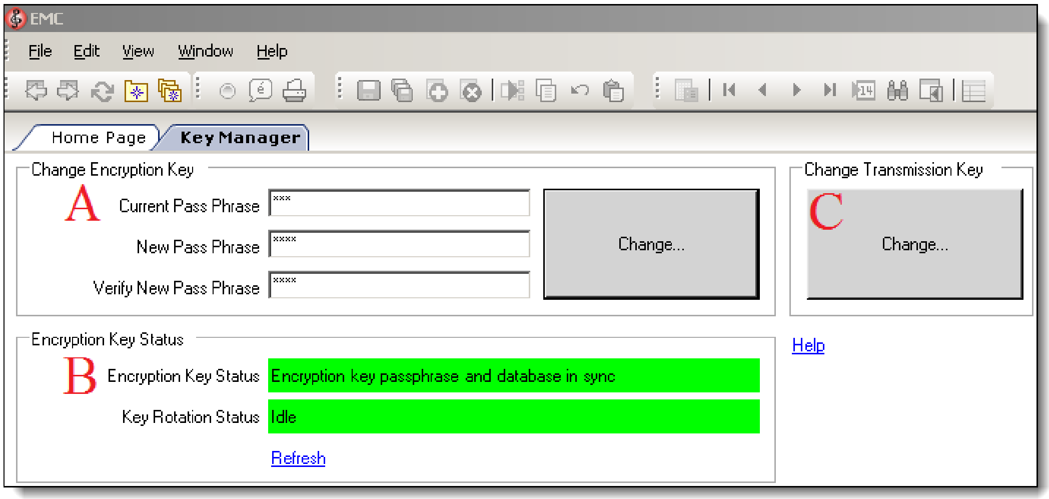
A. Change Encryption Key

B. Encryption Key Status

C. Change Transmission Key

The Change Transmission Key (section **C** below), is unrelated to the database encryption pass phrase used to encrypt secure data. The transmission key is the encryption scheme for network traffic and is not user-defined.

**Figure 3-21 - Key Manager Tab**



Encryption Key Status: Encryption key passphrase and database in sync

Key Rotation Status: Idle

# Changing the Pass Phrase

The new pass phrase must:

- Contain at least 1 alphabetic character
- Contain at least 1 numeric character
- At least 1 special character from: **! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [ \ ] ^ _ ` | ~ { }**
- Must be a minimum of 15 characters long (up to 24)
- Must not contain any dictionary word
- The pass phrase and confirmed pass phrases must match
- The transaction database must be accessible

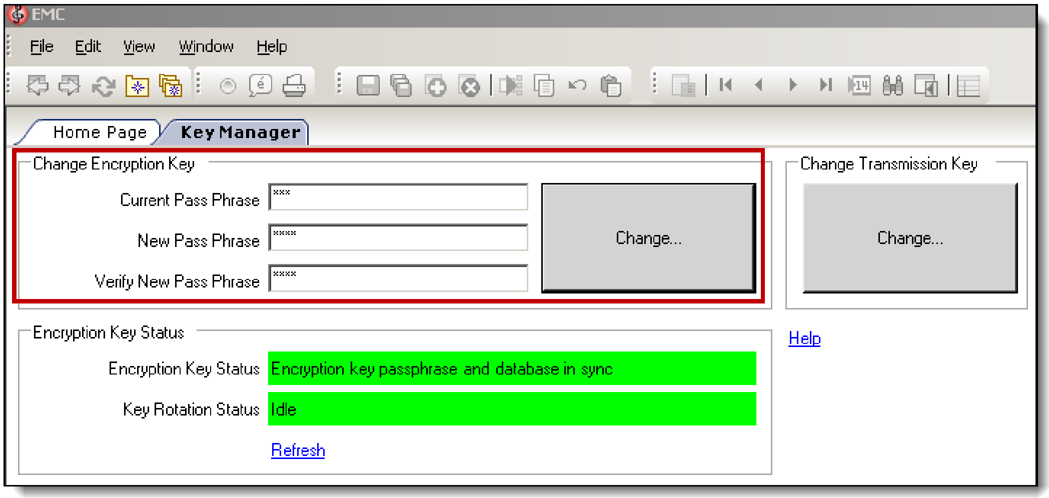
**NOTE:**

If the encryption key is lost, the encrypted data in the database is unrecoverable. There are no backdoors!

To change the pass phrase, follow the directions below.

1. Navigate to the Enterprise Level of the EMC and navigate to under the **Tasks** header.
2. Open the **Key Manager** module.
3. Enter the current pass phrase, the new pass phrase, and confirm the new pass phrase within the **Change Encryption Key** section, outlined below.

**Figure 3-22 - Change Encryption Key Section**

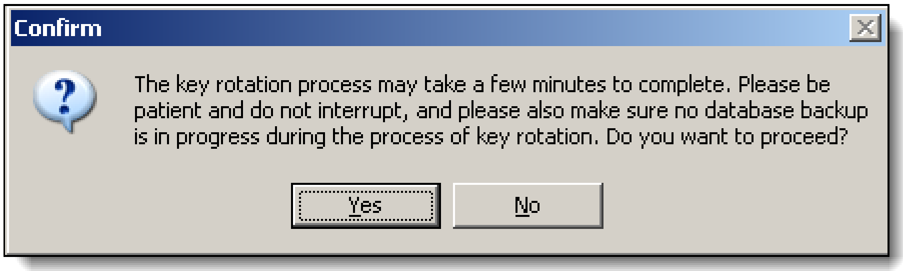


Current Pass Phrase ***
New Pass Phrase ****
Verify New Pass Phrase ****

Encryption Key Status: Encryption key passphrase and database in sync
Key Rotation Status: Idle

4. Click the **Change...** button within the Change Encryption Key section.
5. A confirmation prompt appears. Click **Yes** to start the key rotation process.
6. Another confirmation prompt appears. 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 FE. Click **No** if a database backup is currently in progress and begin the key rotation process again after the backup is finished.

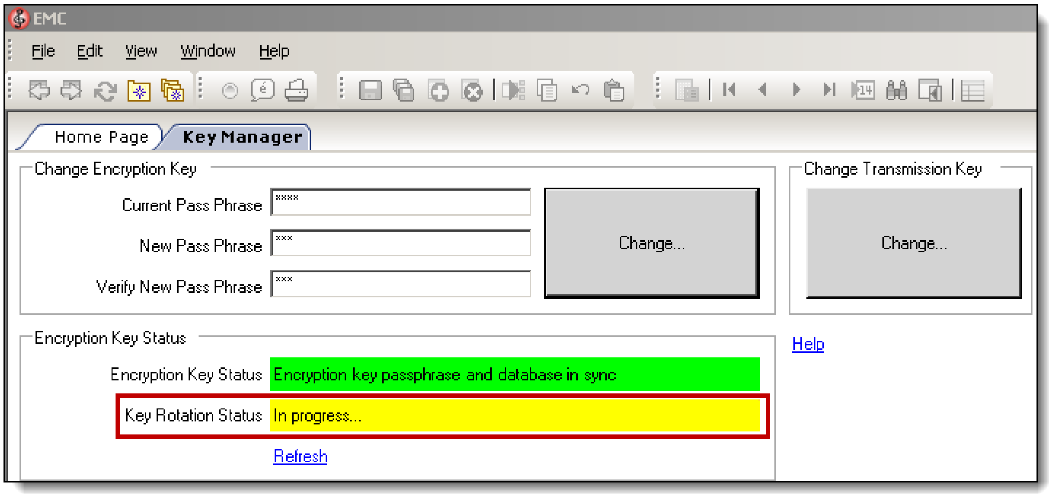
**Figure 3-23 - Key Rotation Confirmation Prompt**



The key rotation process may take a few minutes to complete. Please be patient and do not interrupt, and please also make sure no database backup is in progress during the process of key rotation. Do you want to proceed?

7. The Key Rotation Status field updates to **In progress**.

**Figure 3-24 - Key Rotation Status Field**



Current Pass Phrase ****
New Pass Phrase ***
Verify New Pass Phrase ***

Encryption Key Status: Encryption key passphrase and database in sync
Key Rotation Status: In progress...

8. Once the pass phrase has successfully completed, click **OK** to exit.

# Periodic Key Rotation

In order to achieve maximum security, Oracle MICROS Food & Beverage mandates that the system administrator regularly rotate the site’s encryption keys. Oracle MICROS Food & Beverage recommends that customers, resellers, or integrators rotate the keys every 180 days.