Oracle® Hospitality Simphony

Security Guide
Release 2.8.2
E72743-02

May 2017

ORACLE

Contents

Tables

Figures

Preface

This document provides security reference and guidance for Simphony.

Audience

This document is intended for:

- System administrators installing Simphony
- End users of Simphony

Customer Support

To contact Oracle Customer Support, access My Oracle Support at the following URL:
https://support.oracle.com

When contacting Customer Support, please provide the following:

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

Documentation

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

Revision History

Date	Description of Change
March 2016	• Initial publication
May 2016	• Minor Crypt utility edit
May 2017	• Diagram and text updates

1 Simphony Security Overview

This chapter provides an overview of Oracle Hospitality Simphony 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 1.2 (and higher), SSL, and secure passwords. See Performing a Secure Simphony Installation for more information about secure application software installation.
- **Learn about and use the Simphony security features**
  See Implementing Simphony 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 Simphony along with the latest Oracle and Microsoft software patches.

Overview of Simphony 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 Server-Oriented Architecture also controls the way that workstations interface with other applications or devices. Interfaces become services that can run centrally or locally.

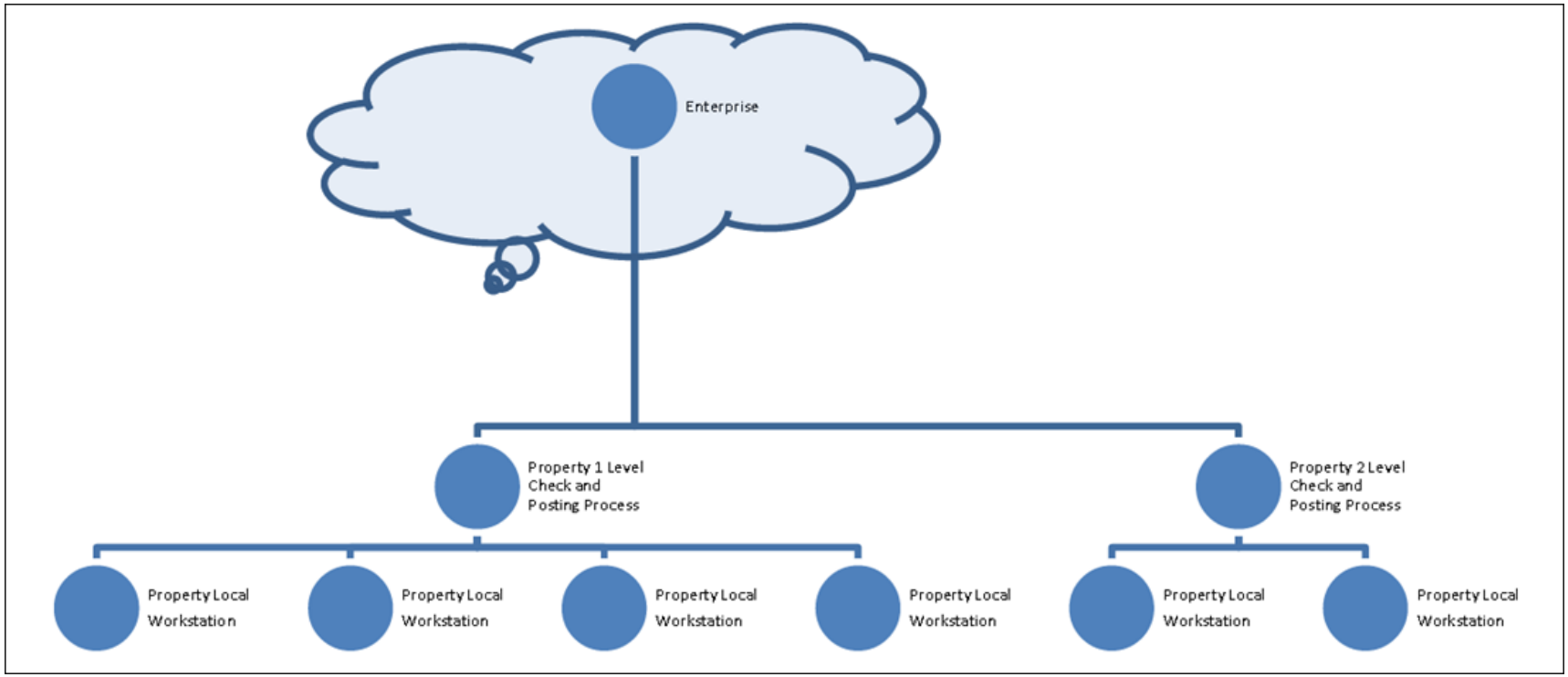


Figure 1 - Basic Enterprise Topology for a Simphony Deployment

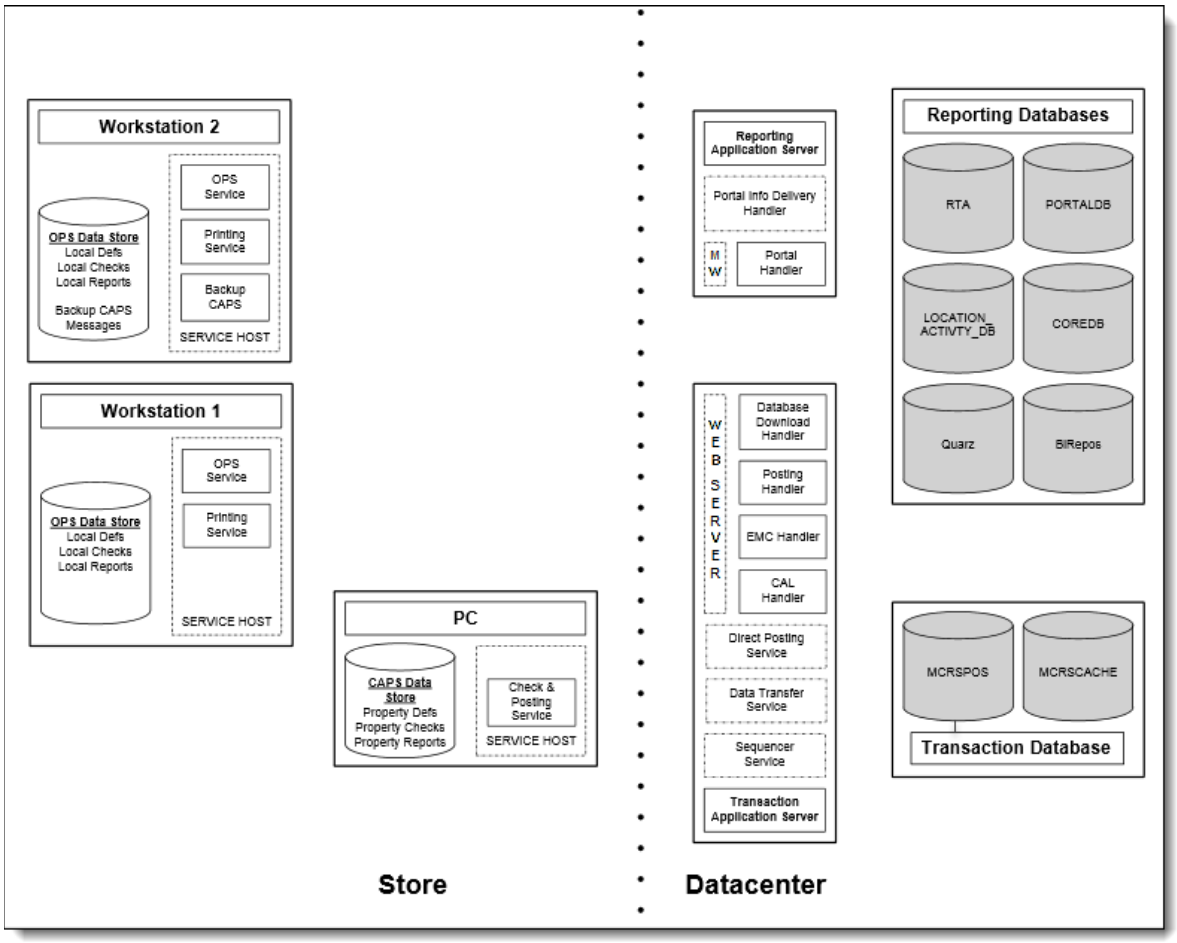


Figure 2 - Details of the Simphony architecture

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

Workstation Authentication

Simphony architecture supports both the server side and client side of authentication. Server authentication is 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 on the Simphony network.

Note: Simphony security does *not* use the Windows Login.

In order for the Simphony workstation to be able to communicate to a Simphony application server, it has to be authenticated first. The process of authentication is accomplished during initial workstation installation, 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 network, a user must authenticate themselves through the workstation by signing in using a unique employee ID number or an employee magnetic card.

Database User Management

The Simphony sample database is installed with only one pre-defined username and password, the Simphony user (micros, micros), which allows access to Simphony's configurator, the Enterprise Management Console (EMC). Oracle Hospitality mandates that users create a different, strong password for the pre-defined Simphony user within the EMC's Enterprise Level, Personnel, and Employees module. The password must follow Payment Card Industry (PCI) Data Security Standard (DSS) guidelines described in the *Simphony PA DSS Implementation Guide*. The password must be at least 8 characters long and include letters and numbers. Simphony'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's installation wizard also prompts for the creation of a System Database User. Simphony'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 Hospitality 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 application server, protected by Microsoft Windows Server file permissions. No applications, except for application server, need access to the database directly. After the initial authentication, the application server performs a check of the authorization for the given user to perform the requested action.

Understanding the Simphony Environment

When planning your Simphony implementation, consider the following:

- **Which resources need to be protected?**
  - You need to protect customer data, such as credit-card numbers
  - You need to protect internal data, such as proprietary source code
  - You need to protect system components from being disabled by external attacks or intentional system overloads

- **Who are you protecting data from?** For example, you need to protect your subscribers' data from other subscribers, but someone in your organization might need to access that data to manage it. You can analyze your workflows to determine who needs access to the data; for example, it is possible that a system administrator can manage your system components without needing to access the system data.
- **What happens if protections of strategic resources fail?** In some cases, a fault in your security scheme is nothing more than an inconvenience. In other cases, a fault might cause great damage to you or your customers. Understanding the security ramifications of each resource helps you protect it properly.

Recommended Deployment Configurations

This section describes recommended deployment configurations for Simphony.

The Simphony product can be deployed on a single server or in a cluster of servers. The simplest deployment architecture is the one shown in **Figure 1 - Basic Enterprise Topology for a Simphony Deployment**.

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.

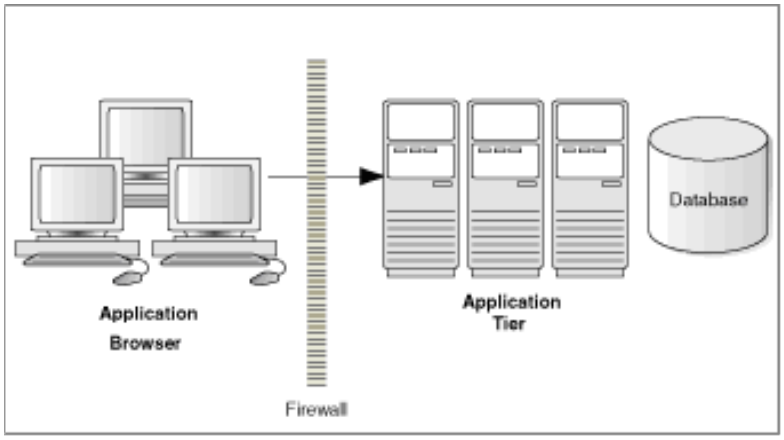


Figure 3 - Single-Computer Deployment Architecture

The general architectural recommendation is to use the well-known and generally accepted Internet-Firewall-DMZ-Firewall-Intranet architecture shown in **Figure 4 - Traditional DMZ View.**

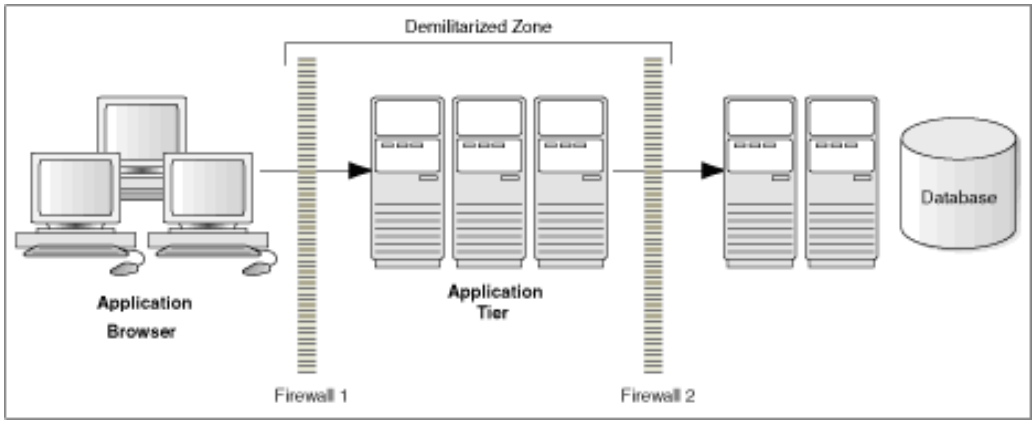


Figure 4 - Traditional DMZ View

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

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

See **Simphony Port Numbers in Appendix B** for more information about Simphony network Port usage.

Simphony Security

Operating System Security

Prior to installation of Simphony, 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:

- Windows Server 2012 Security
- Windows Server 2008 R2 Security

Database Security

Oracle Database

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

Microsoft SQL Server

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

2 Performing a Secure Simphony Installation

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

Pre-Installation Configuration

Prior to installation of Simphony, perform the following tasks:

- Apply critical security patches to the operating system
- Apply critical security patches to the database server application
- Review the Oracle Hospitality Enterprise Back Office Security Guide
- Review the Oracle Hospitality MICROS Hardware Wireless Networking Best Practices Guide
- Create Oracle Database Tablespaces per the instructions in the *Simphony Installation Guide* located at `http://docs.oracle.com/en/industries/hospitality/`

Simphony Installation

You can perform a custom installation or a typical installation. Perform a custom installation to avoid installing options and products you do not need. If you perform a typical installation, remove or disable features that you do not need after the installation.
The installation requires the user running the installation to have administrator privileges. No other users have the required access to successfully complete the installation.
When creating a new database, enter a complex password that adheres to the database hardening guides for all users.
The following Simphony2 web sites and services are required for proper operation of the system:

- EGateway
- WCC
- WS
- API
- ImportExportAPP
- ImportExportAPI
- HMC

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

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

Post-Installation Configuration

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

Application

Software Patches

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

Security Certificates

To use the Simphony Import/ Export Service or the Simphony Engagement Cloud Service, it is required that Transport Layer Security (TLS) 1.2 (and higher) must be configured either on the load balancer or a web server for communication to Simphony Enterprise servers. The TLS 1.2 configuration process requires the use of a certificate generated by a trusted certificate authority. Refer to the *Simphony Installation Guid*e for information about the installation of secure certificates.

Database Platform

Ensure Database Access is Tracked

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

Passwords Overview

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

Maintaining Strong Passwords

Ensure that passwords adhere to the following strength requirements:

1. The password must be at least 8 characters long and maximum 20 characters.
2. The password must contain letters, numbers, and special characters:
   ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~
3. Must not choose a password equal to the last 4 passwords used.

Configuring Passwords for Simphony

The following password policy options are configured as shown below.
In the EMC, Enterprise Parameters, Login tab, Enhanced Password Security tab, ensure these options (highlighted below) are configured as follows:
In the EMC, Enterprise Parameters, Login Tab, Enhanced Password Security Tab, ensure these available options are configured as follows:

1. Ensure the Minimum Password Length is at least 8 characters.
2. Ensure the Password Repeat Interval is at least 4.
3. Ensure the Days Until Expiration is not greater than 90.
4. Ensure the Maximum Allowed Failed Logins is not greater than 6.
5. Ensure the Maximum Idle Time in Minutes is not greater than 15.

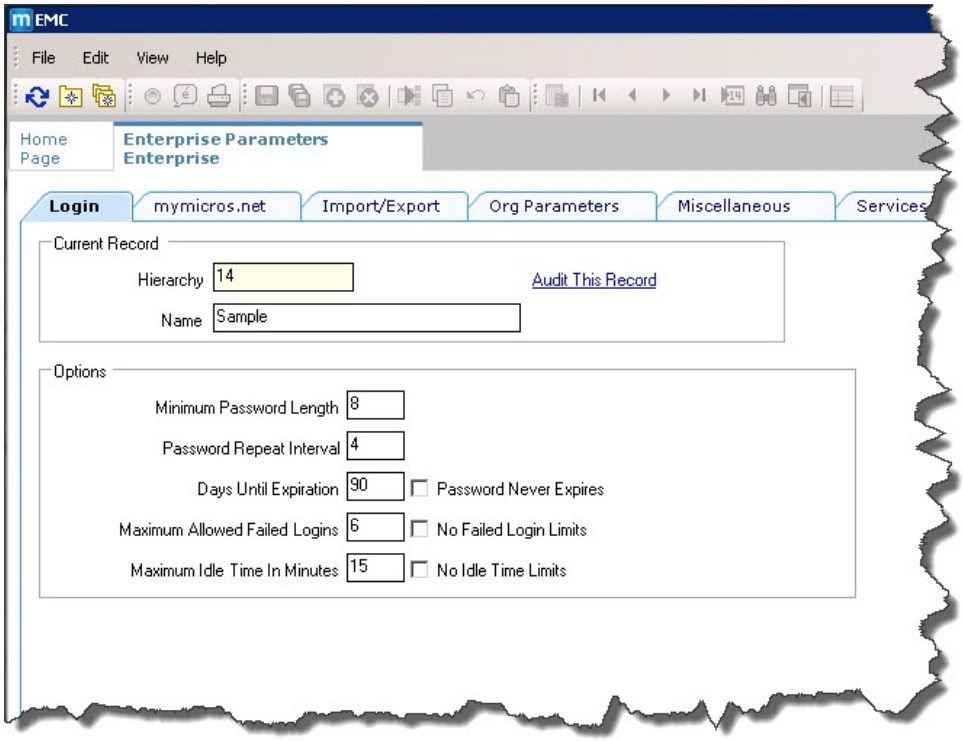


Figure 5 - Enhanced Password Security Tab

Change Default Passwords

Simphony is installed with a default master EMC user and password. Oracle Hospitality mandates changing your master username password in the EMC, following the above guidelines, after logging in for the first time.

Configure User Accounts and Privileges

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

Encryption Keys

Simphony installs an encryption key using a default passphrase. Administrators need to rotate the encryption key on a regular interval. It is suggested to follow the PCI guidelines for encryption key rotation. Refer to the *Simphony Key Manager Manual* in *Appendix D* for further details.

Change Database Passwords

Application Server

Crypt is a database credential management tool for the Simphony 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

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

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

To access the Crypt utility:

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

Figure 6 - Crypt Database Password Encryption Tool

To use the Crypt utility, perform the following steps:

Table 1 - Using the Crypt Database Password Encryption Tool

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

Refer to the *Simphony PA-DSS Implementation Guide* for more information about setting secure database and application passwords.

Workstation

Another required post installation step is geared toward ensuring workstation security. To maintain workstation database access control, you must assign unique user names and complex passwords in the Simphony EMC in the Property Parameters Security tab. Enter strong logon credentials in the following sections of the Security tab:

- User Security Credentials
- User Admin Credentials
- User Database Credentials

Refer to the *Simphony PA-DSS Implementation Guide* for more information about setting workstation passwords.

Data Purging

Review the database purging configuration settings to ensure that and sensitive data is only stored for the minimum required time period. Refer to the *Simphony PA-DSS Implementation Guide* for more information about data purging.

3 Implementing Simphony Security

This chapter reviews Simphony 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.

Roles

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

EMC Configuration

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

General Tab

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

EMC Modules Tab

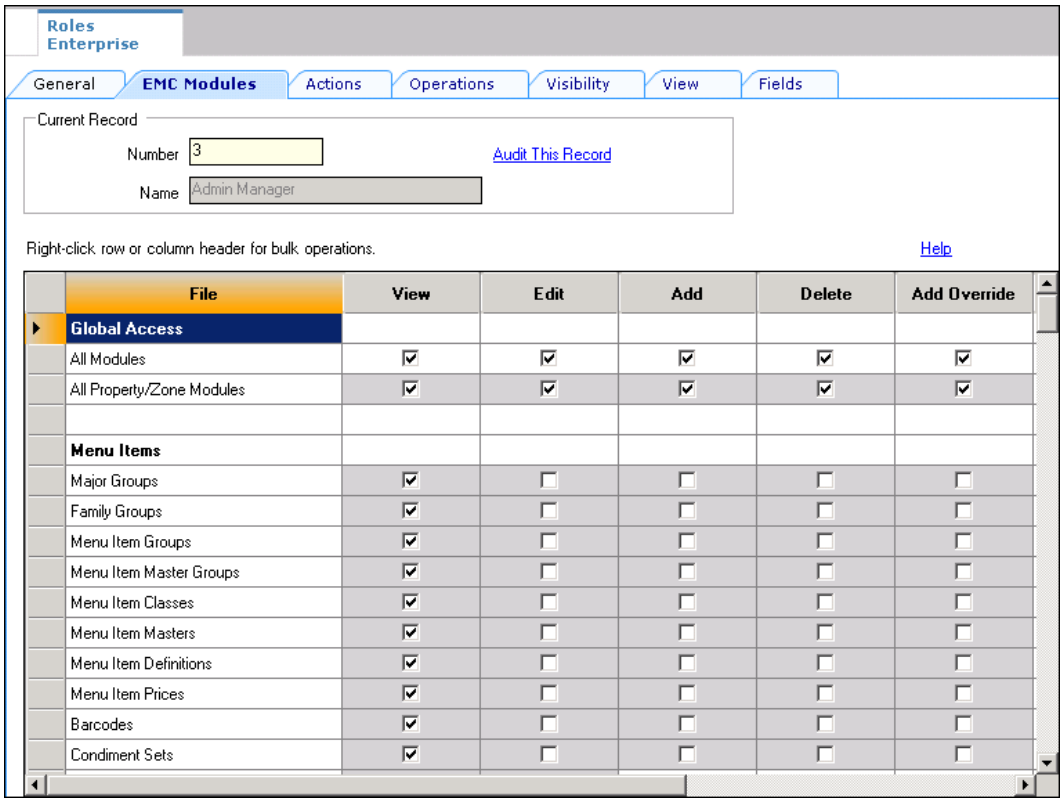


Figure 7 - Roles EMC Modules

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

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

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

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

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

Global Access

The **All Modules and All Property/ Zone Modules** checkboxes are available so that a role may be easily configured to View, Edit, Add, or Delete every module without

having to individually check each box. Further, this checkbox allows access to new modules that will be created in the future. For instance, if a new module "voice ordering" is created and released in a new version, an employee with "Global Access" for "View" will be able to access this module without having a specific checkbox for the "voice ordering" module. Oracle Hospitality recommends that administrator-type roles have the "All Modules" option checked, so that administrators will always be able to access every module in the system.

Actions tab

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

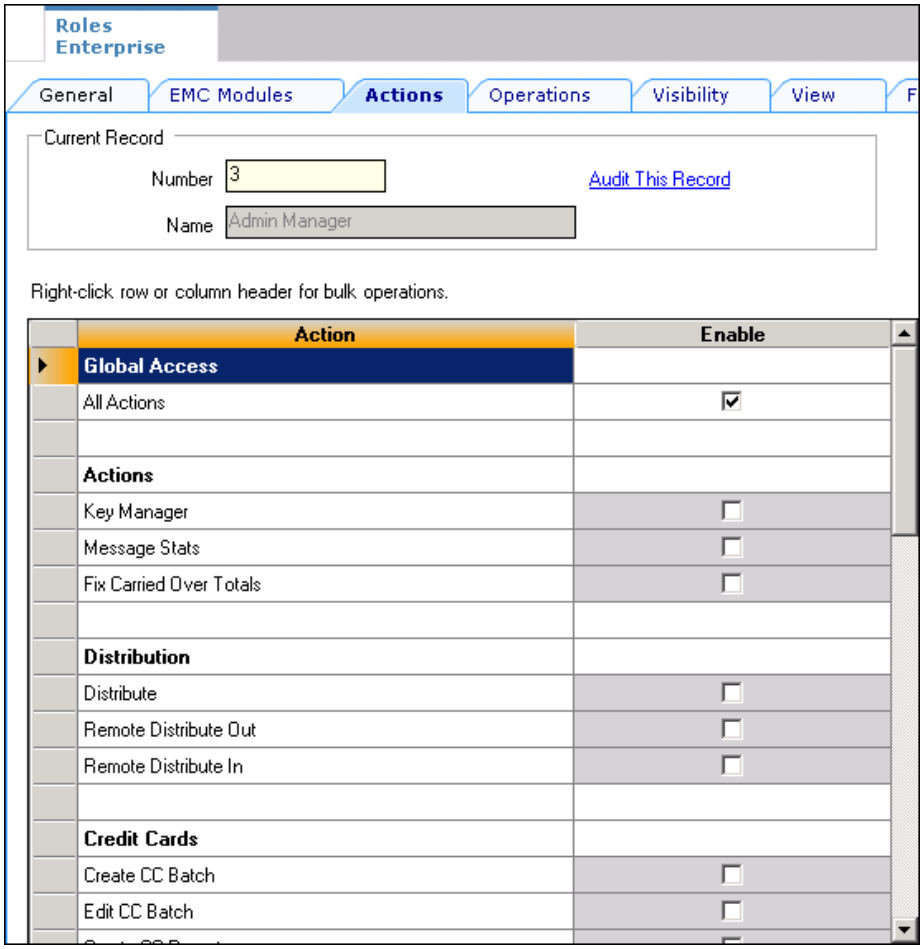


Figure 8 - Roles Actions

Global Access

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

Security

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

Operations Tab

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

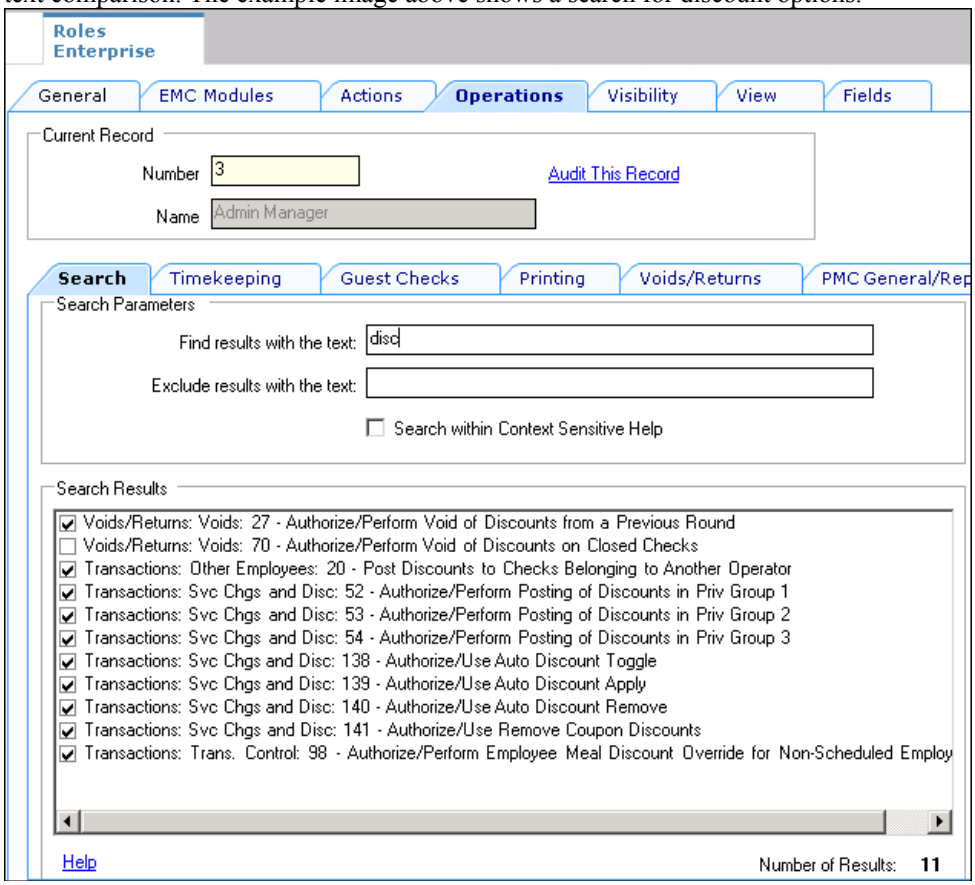


Figure 9 - Roles Operations

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 PMC. See UWS Procedures in Appendix A: Access Control.

Visibility Tab

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

The checkbox allows a Role to be visible in the selected Zones/Locations and all its children; if it is unchecked, the Role will be visible in the selected Zone/Location only, but not its children.

View Tab

The View tab contains one option that controls the Revenue Centers that users can view:

Enable Revenue Center-Level Security: This option relates to workstation behavior only. Employees associated with a Role that have this option checked are only able to view revenue centers in which they are an operator.

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

Fields Tab

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

1. Editable – You are able to view and edit the field.
2. View Only – You are only able to see the field (no editing allowed).
3. Exclude – You cannot view or access the field at all.

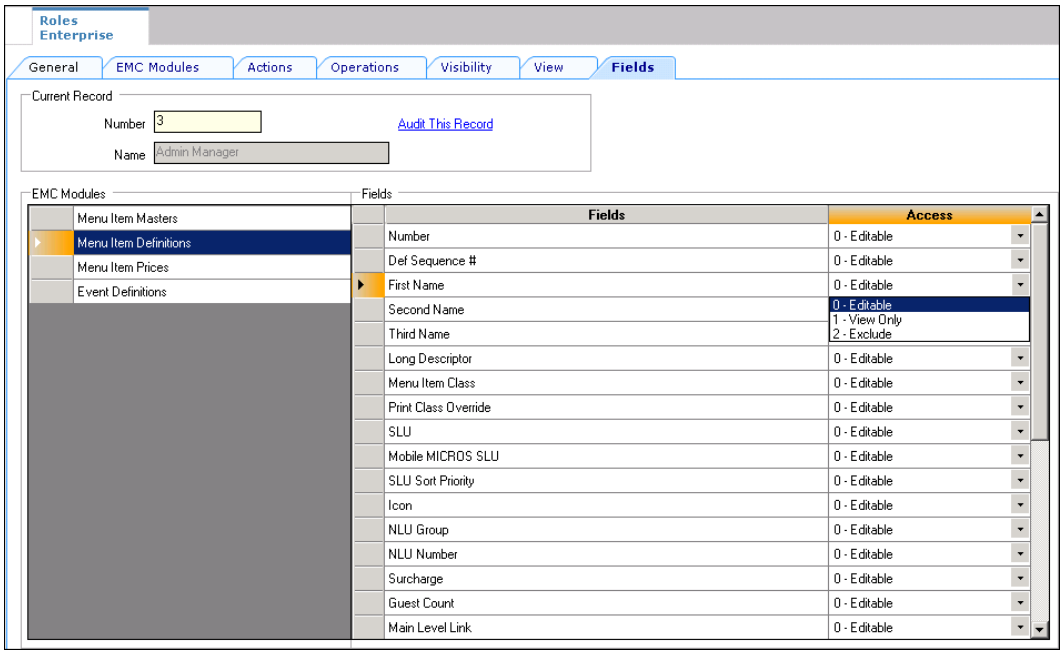


Figure 10 - Roles Fields

Employee IDs

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

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

EMC Viewing

In the EMC, Employee IDs are editable in the Employee Maintenance module. A user can see the ID number of other employees only when the user is associated with a Role 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 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 2 - Employee Level Example Settings

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

Employee Groups

Each employee in a Simphony system is associated with an Employee Group, 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 - Employee Group Example Settings

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

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

Job Code Overrides

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

- The Role field is set to 0-None, the operator will have privileges based on the role(s) assigned in the EMC.
- The Role field is not 0-None, the operator's privileges from EMC do not apply. Only the privileges associated with the role from this field will be active for the duration of the Clock-In Cycle.

Programming Job Code Overrides

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

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

Audit Trail

Overview

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

Accessing Audit Trail

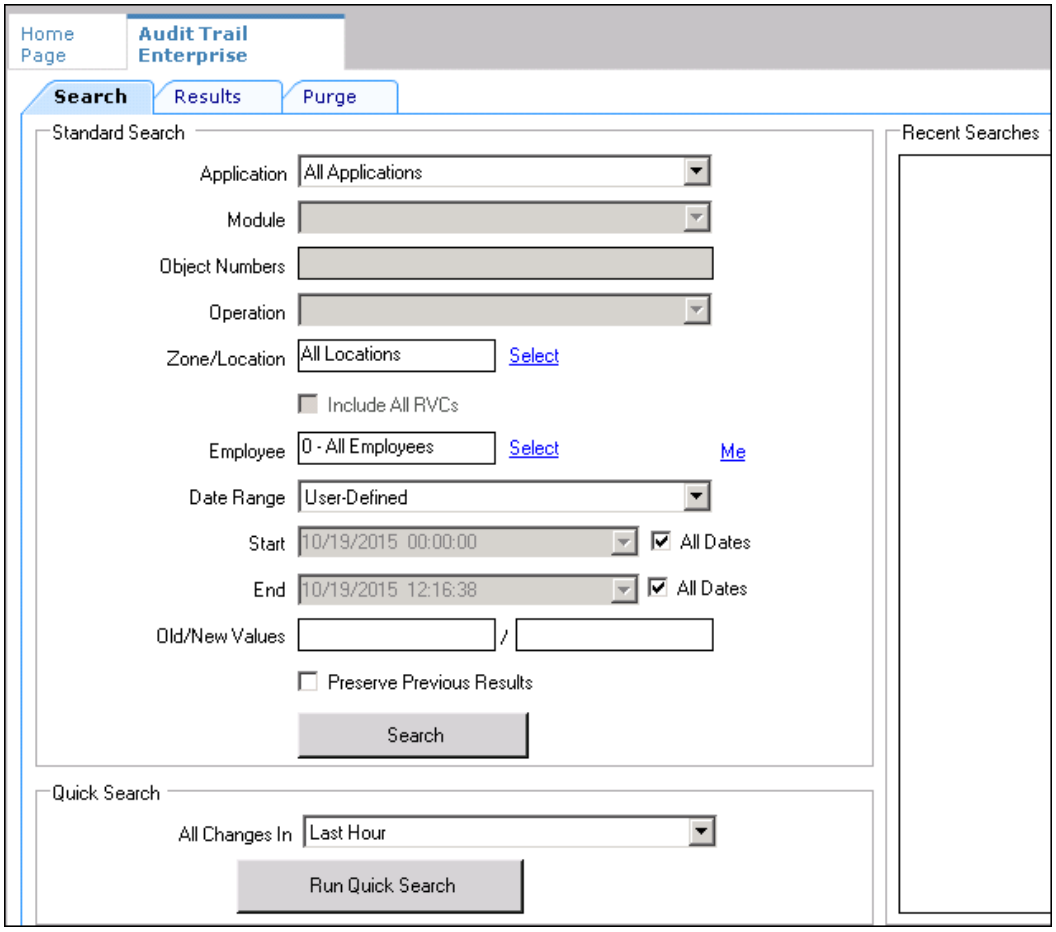


Figure 11 - Audit Trail Search Tab

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

Audit Trail Search Parameters

Standard Search

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

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

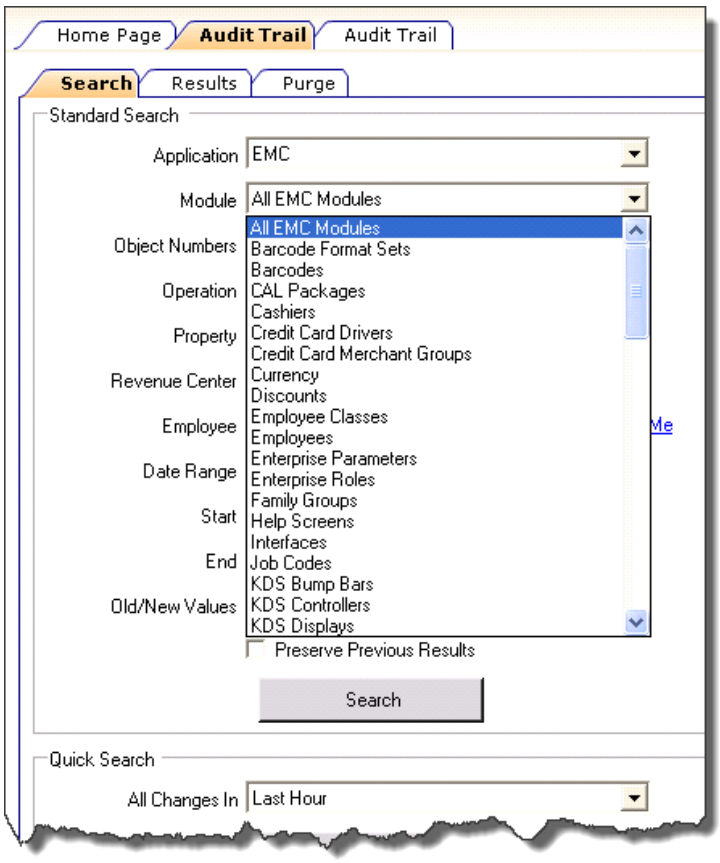


Figure 12 - Audit Trail Standard Search

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

- **Operation**: Select an Operation or choose **All Operations**. This field is enabled based on a combination of the Application and Module drop-downs. This drop-down displays All Operations followed by an alphabetized list of the valid operations.
- **Property**: Select a Property or choose **All Properties**. This field is enabled only when Audit Trail is opened from the Enterprise Level.
- **Revenue Center**: Select a Revenue Center or choose **All RVCs**. This field is enabled only when a specific Property is selected.
- **Employee**: Select an Employee or choose **All Employees**. When a specific employee is selected, only changes made by that employee are included in the list. If **me** is selected, this field changes to the logged-in employee.
- **Date Range**: Select a predefined Date Range that is used to query the Audit Trail, or select "User-Defined" to enable the start/end fields. The predefined date ranges are:
  - Last Hour
  - Last Two Hours
  - Today
  - Last 24 Hours
  - Last 48 Hours
  - Last Week
  - Last Two Weeks
- **Start**: Select a Start date/time or choose **All Dates**. This field lets a user narrow a query to a specific date or date range.
- **End**: Select an End date/time or choose **All Dates**. This field lets a user narrow a query to a specific date or date range.
  - Microsoft SQL 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 that is used to query the **OldValue** and/or **NewValue** columns of the Audit Trail table. These text boxes can be useful to find a specific change to a record, such as, "When did the item Hamburger get renamed to Cheeseburger?"
- **Preserve Previous Results**: If this box is checked, the search results are merged with the previous search results, instead of overwriting them. If this box is not checked, the search results include only the data of the most recent search.

Recent Searches

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

Quick Search

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

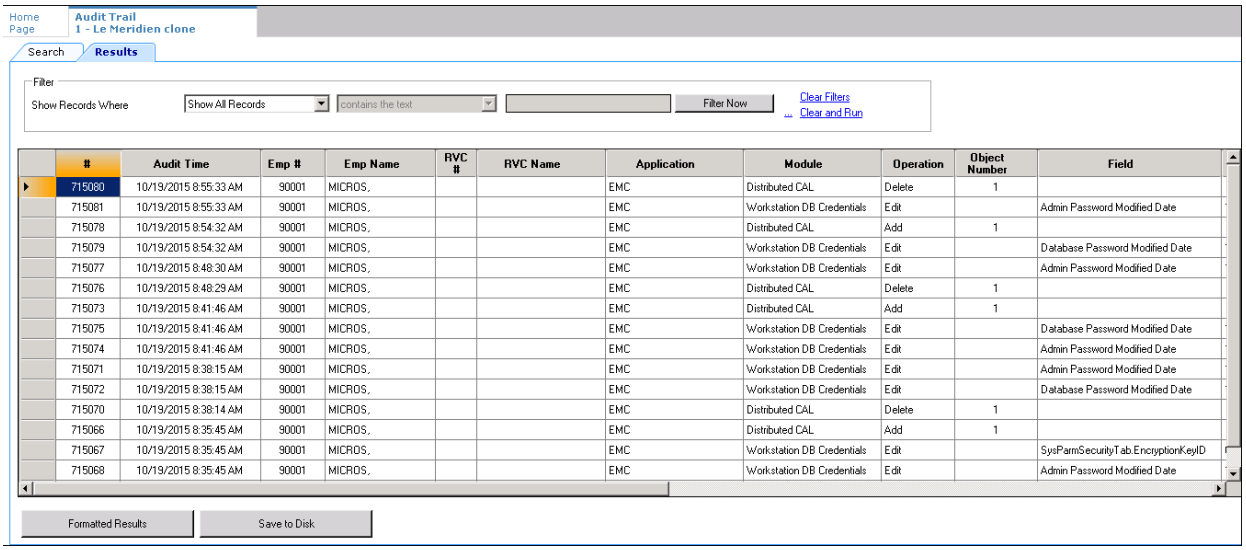
Running a Search

When **Search** or **Run Quick Search** is clicked, the Audit Trail first checks the database to get an estimate on the number of records that are returned. (It is an estimate because changes may be in progress at the time of the query.)

If the number of results that are returned exceeds the pre-configured thresholds for Audit Trail results, the user is prompted to confirm the action. The prompts occur when more than 10,000, 50,000, 100,000, 500,000, and 1,000,000 records are returned. These prompts are meant to confirm that the search criterion being used is desired. With these prompts, the user is prompted

three times (10,000, 50,000, and 100,000) to confirm that the Audit Trail runs a query that returns the expected results of more than 101,000 records.

Audit Trail Search Results



#	Audit Time	Emp #	Emp Name	RVC #	RVC Name	Application	Module	Operation	Object Number	Field
715080	10/19/2015 8:55:33 AM	90001	MICROS,			EMC	Distributed CAL	Delete	1	
715081	10/19/2015 8:55:33 AM	90001	MICROS,			EMC	Workstation DB Credentials	Edit		Admin Password Modified Date
715078	10/19/2015 8:54:32 AM	90001	MICROS,			EMC	Distributed CAL	Add	1	
715079	10/19/2015 8:54:32 AM	90001	MICROS,			EMC	Workstation DB Credentials	Edit		Database Password Modified Date
715077	10/19/2015 8:48:30 AM	90001	MICROS,			EMC	Workstation DB Credentials	Edit		Admin Password Modified Date
715076	10/19/2015 8:48:29 AM	90001	MICROS,			EMC	Distributed CAL	Delete	1	
715073	10/19/2015 8:41:46 AM	90001	MICROS,			EMC	Distributed CAL	Add	1	
715075	10/19/2015 8:41:46 AM	90001	MICROS,			EMC	Workstation DB Credentials	Edit		Database Password Modified Date
715074	10/19/2015 8:41:46 AM	90001	MICROS,			EMC	Workstation DB Credentials	Edit		Admin Password Modified Date
715071	10/19/2015 8:38:15 AM	90001	MICROS,			EMC	Workstation DB Credentials	Edit		Admin Password Modified Date
715072	10/19/2015 8:38:15 AM	90001	MICROS,			EMC	Workstation DB Credentials	Edit		Database Password Modified Date
715070	10/19/2015 8:38:14 AM	90001	MICROS,			EMC	Distributed CAL	Delete	1	
715066	10/19/2015 8:35:45 AM	90001	MICROS,			EMC	Distributed CAL	Add	1	
715067	10/19/2015 8:35:45 AM	90001	MICROS,			EMC	Workstation DB Credentials	Edit		SysParmSecurityTab.EncryptionKeyID
715068	10/19/2015 8:35:45 AM	90001	MICROS,			EMC	Workstation DB Credentials	Edit		Admin Password Modified Date

Figure 13 - Audit Trail Search Results

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

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

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

Audit This Record

In almost every module, 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 selecting Audit This Record, a new tab opens. This tab displays a grid that is similar to Audit Trail Search Results grid, but the Audit This Record grid omits Property/RVC columns and the Module column because this information is the same for every record. Also, the Comments column is always hidden in this view.

In addition, the Object Number column is sometimes omitted (when auditing modules without object numbers, like RVC Parameters) and the Application column displays only when the current record can be edited outside EMC. For example, it is possible to redirect Order Devices from PMC Procedures; when a user chooses Audit This Record for an Order Device, the application column displays. Conversely, it is only possible to edit KDS Displays in EMC, so the Application column does not display.

Advanced Options

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

Module-Specific Notes

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

Selecting All Records

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

1. Click in the upper-left cell of the Table View grid.
2. From the Edit menu, select **Audit This Record**.
3. EMC prompts: `No records are currently selected. Would you like to get Audit Trail information for all activity in this module?`
4. Select **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 display the Old/New value, followed by the value in quotes to show where the extra space characters exist. For example, the new value for “Hot Dog” changing to “Hot Dog” appears like this: Hot Dog (“Hot Dog”).
- Changes made in the Property Merchant Groups module are treated like a single-record module (similar to RVC Parameters or Property Descriptors); all records for this module are logged without an Object Number.
- Other than the name, changes in the Selection Hierarchies module are not currently logged to Audit Trail.
- When a macro record is created, its 16 steps are not created. The first time a macro record is saved after its creation, Audit Trail shows each step being added.
- The configurable data for Credit Card Drivers and Credit Card Merchant Groups are displayed in EMC using standard controls that are found throughout EMC. However, this data is actually stored in the database in a single data column as an XML string. Because of this, changes in these modules show the **Field** as **Configuration**, and the Old/New values display the entire XML string.
- When an Audit Trail report is taken, this activity is logged to Audit Trail. All generated Audit Trail Reports are logged as an Enterprise-Level activity.

Internationalization

Text is stored in the AUDIT_TRAIL database table so that an EMC user views the text in his/her own language. For example, if a user from England changes Menu Item Class option bit #1 from ON to OFF, the data is stored in the table so that 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 4 - Audit Trail Translation Capabilities

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

Audit Trail Purging

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

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

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

Sub-record Formatting

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

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

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

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 displays:

- **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 displays:
- **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 database is encrypted using industry standard AES256 encryption. Each encrypted piece of data has a link to an entry in the encryption key table, which is also encrypted using AES256 encryption.

Simphony provides an EMC Key Manager module to create, rotate, and delete encryption keys. All data that needs to be stored in the database in encrypted format is automatically encrypted using the latest encryption key.

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

Client Data Store Encryption

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

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

Encrypting Data 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 Manager

The EMC Key Manager module 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.

Key Rotation Considerations

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

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

Enabling

For detailed instructions about enabling the Key Manager module and secure key practices, refer to the *Simphony Key Manager Manual in Appendix D*.

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.

EMC Configuration

Timekeeping Tab

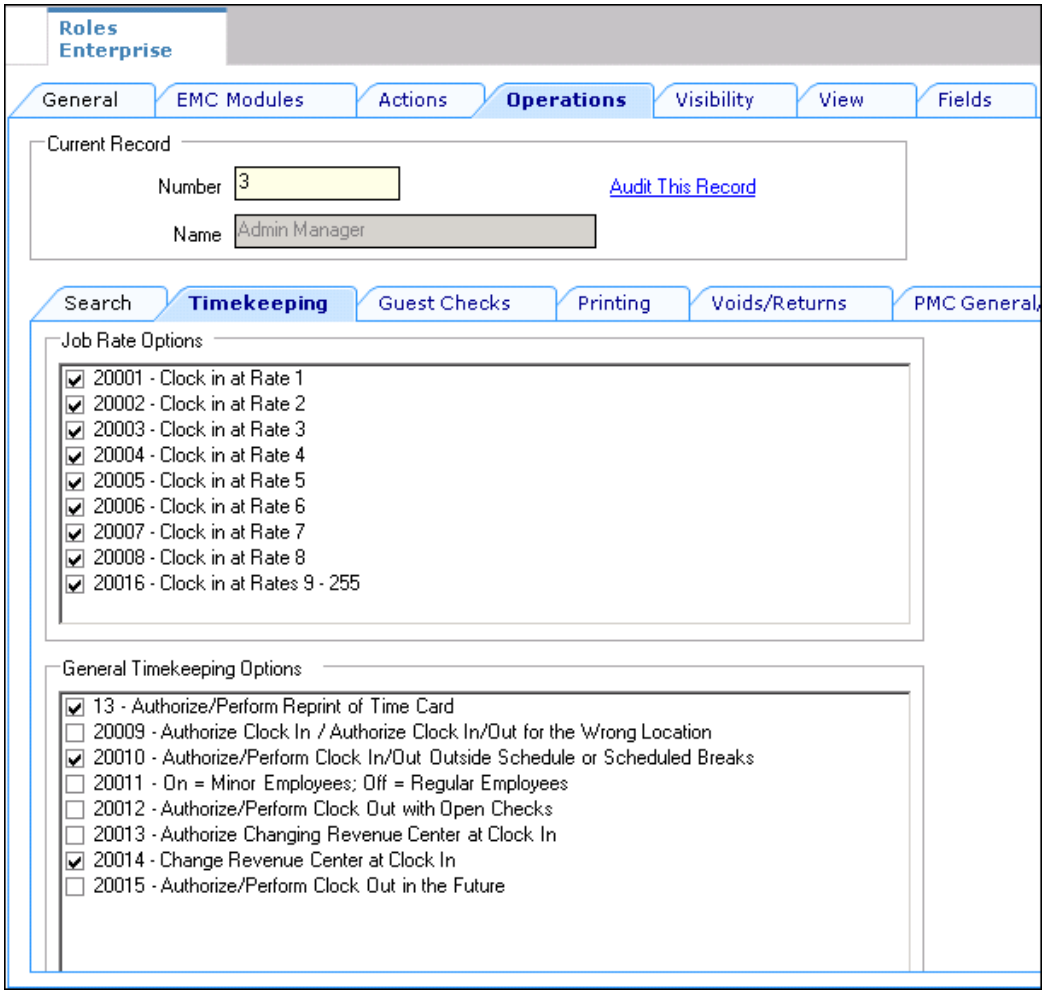


Figure 14 - Roles Timekeeping

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.

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.

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/ 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.

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.

Change 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/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.

Guest Checks Tab

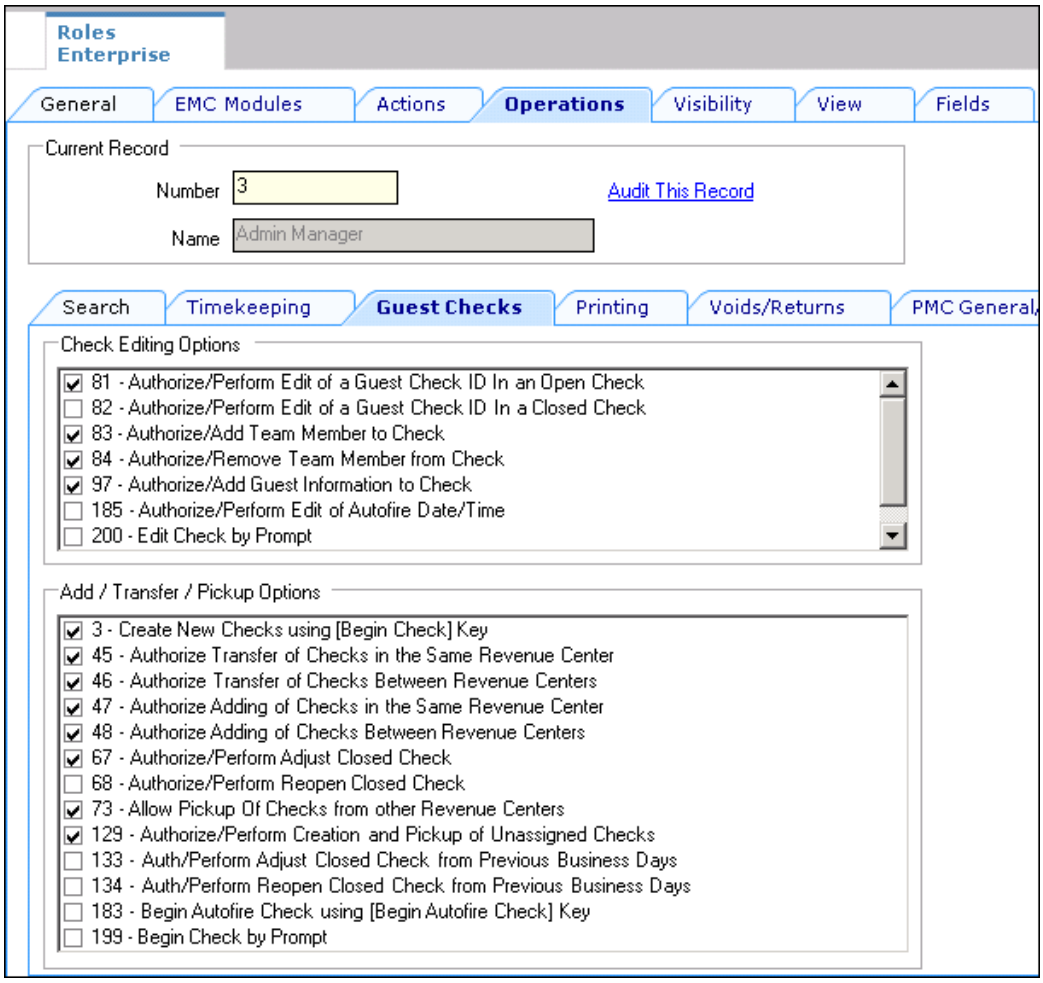


Figure 15 - Roles Guest Checks

Check Editing Options

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.

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/ 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/ Perform Edit of Autofire Date/Time

If enabled, employees associated with this Role can edit the Autofire Date/Time of an existing Autofire check. If not enabled, employees associated with this Role can only view the Autofire Date/Time of an existing Check.

Edit Check by Prompt

Select this option to allow employees associated with this Role to begin check by prompt. This option bit is a part of Banquet Check Printing Process.

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 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 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/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.

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.

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/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 Hospitality 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.

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.

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.

Begin Autofire Check using [Begin Autofire Check] Key

Select this option to allow Employees associated with this Role to begin an Autofire Check. If not set, Employees associated with this Role will not be able to begin an Autofire Check.

Begin Check by Prompt

Select this option to allow employees associated with this Role to begin check by prompt. This option bit is a part of Banquet Check Printing Process.

Guest Check Control Options

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/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/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 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/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 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 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.

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.

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/Perform Find Check

Select this option to allow employees associated with this Role to find a check when Check and Posting is unavailable and to authorize non-privileged employees to do so as well.

Authorize/Perform Pickup of Autofire Check Belonging to Another Operator

Select this option to allow Employees associated with this Role to pick up another Operator's Autofire checks.

Authorize/Perform Pickup From Peer Workstation

Select this option to allow employees associated with this Role to pick up a check from a workstation when Check and Posting is unavailable and to authorize non-privileged employees to do so as well.

Authorize/Perform Pickup From Inaccessible Workstation

Select this option to allow employees associated with this Role to pick up an open check that is inaccessible (e.g., in a locked office) and to authorize non-privileged employees to do so as well.

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

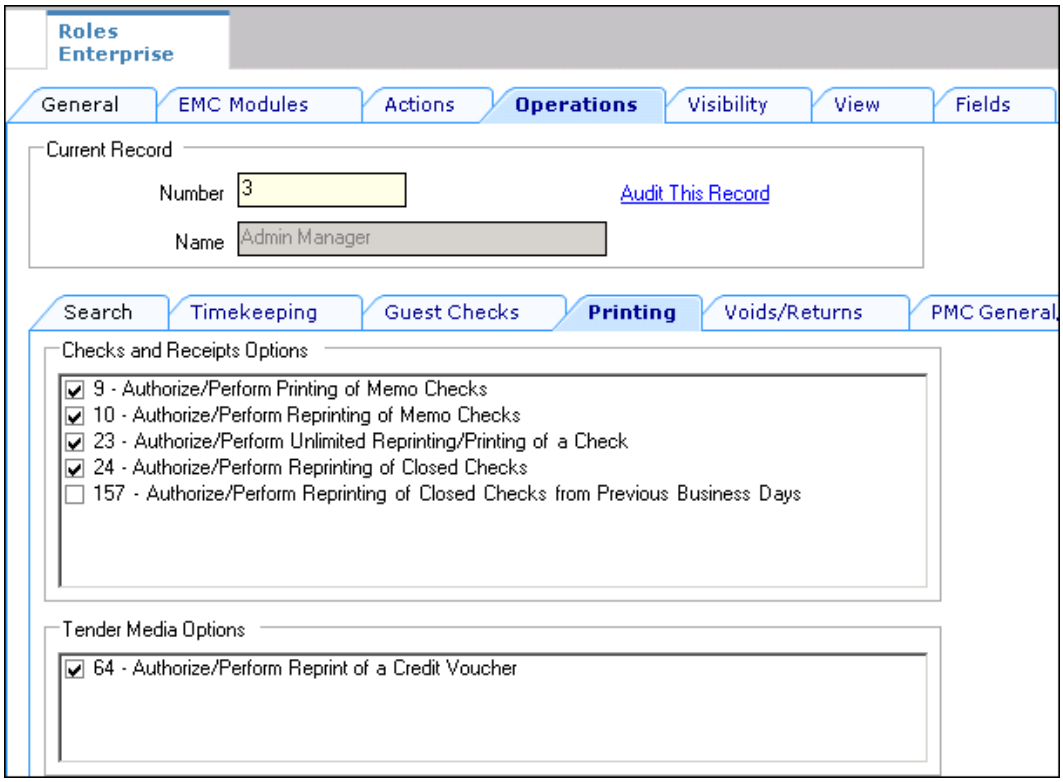


Figure 16 - Roles Printing

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 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 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 Reprinting of Closed Checks from Previous Business Days Workstation

Select this option to allow employees associated with this Role to reprint a guest check from previous business days, and to authorize non-privileged employees to do so as well.

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

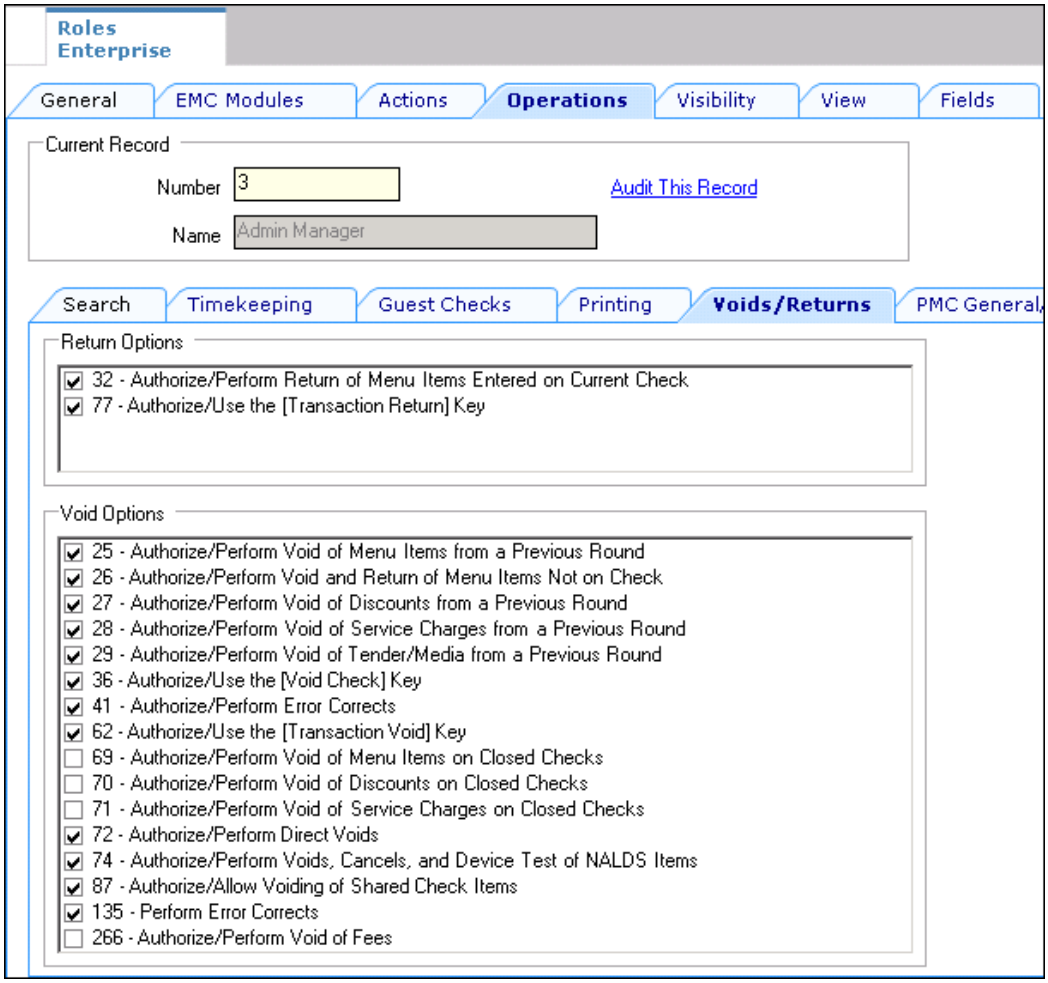


Figure 17 - Roles Voids/ Returns

Return Options

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.

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.

Void Options

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 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 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 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 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/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/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).

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 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 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 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 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 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.

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.

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 Void of Fees

Select this option to allow employees associated with this Role to void Fees (Service Charges), and to authorize non-privileged employees to do so as well.

PMC General/Reports Tab

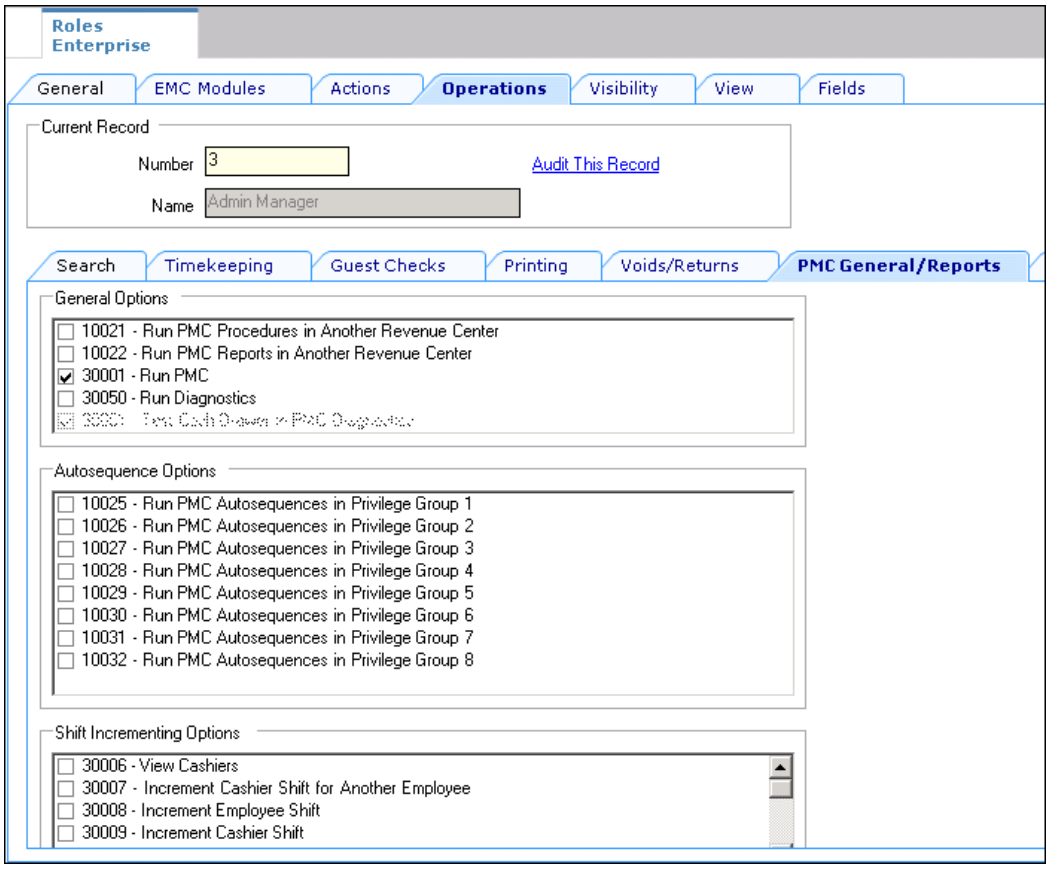


Figure 18 - Roles PMC General/ Reports

General Options

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.

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.

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 Shift for Another Employee

Enable this option for Employees associated with this Role to Increment the Cashier Shifts for another Cashiers using the Increment Cashier Shift for Another Employee. If not set, Employees associated with this Role cannot increment Shifts for another Cashier. This Right requires that Shift Tracking is enabled in Control Parameters.

Increment Employee Shift

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 Cashier Shift

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 Employee Shift when Clocking Out

If set, the Shift for the Employee will increment when Clocking Out. This does not apply if the Employee is Clocking Out on Break. If not set, the Shift for the Employee will remain the same. This option has no effect if Shift Tracking is not enabled in Control Parameters.

Increment Employee Shift when Clocking In

If set, the Shift for the Employee will increment when Clocking In. This does not apply if the Employee is returning from Break. If not set, the Shift for the Employee will remain the same. This option has no effect if Shift Tracking is not enabled in Control Parameters.

Increment Employee Shift when Changing Job

If set, the Shift for the Employee will increment when they Clock In with a different Job. This Clock In occurs automatically if the Employee Signs In to a UWS with a different Revenue Center than the Job in which they are currently Clocked In. If not set, the Shift for the Employee will not increment during this Clock In cycle. This option has no effect if Shift Tracking is not enabled in Control Parameters.

Increment Employee Shift when Changing Revenue Center

If set, the Shift for the Employee will increment when they Sign In to a different Revenue Center. If not set, the Shift for the Employee will not increment when Signing In to a different Revenue Center. This option has no effect if Shift Tracking is not enabled in Control Parameters.

Prompt before incrementing Employee Shift

If set, the Employee will be prompted whether or not to increment the Shift for the Employee when the Shift is set to increment when Clocking In or Out, changing Jobs or changing Revenue Centers. If not set, no prompting will occur when the Employee Shift is set to increment through one of those methods. This option has no effect if Shift Tracking is not enabled in Control Parameters.

Prompt to Increment Employee Shift after Shift Report

If set, when an Employee Shift report is generated, with a Shift scope, the Operator will be prompted whether the Employee Shift should be incremented. If not set, no prompting will occur and the Employee Shift will not increment. This option has no effect if Shift Tracking is not enabled in Control Parameters.

Increment Employee Shift for Another Employee

Enable this option for employees associated with this Role to Increment Employee Shifts (for another Employee) using the Increment Employee Shift for Another Employee Key. If not set, Employees associated with this Role cannot increment Shifts for another Employee. This Right requires that Shift Tracking is enabled in Control Parameters.

Increment Cashier Shift when Clocking Out

If set, the Shift for the Cashier associated with the Clock Out Employee will increment. This does not apply if the Employee is Clocking Out on Break. If not set, the Shift for the Cashier associated with the Employee will remain the same. This option has no effect if Shift Tracking is not enabled in Control Parameters.

Increment Cashier Shift when Clocking In

If set, the Shift for the Cashier associated with the Employee Clocking In will increment. This does not apply if the Employee is returning from Break. If not set, the Shift for the Cashier associated with the Employee will remain the same. This option has no effect if Shift Tracking is not enabled in Control Parameters.

Increment Cashier Shift when Changing Job

If set, the Shift for the Cashier associated with the Employee, will increment when they Clock In with a different Job. This Clock In occurs automatically if the Employee Signs In to a UWS with a different Revenue Center than the Job in which they are currently

Clocked In. If not set, the Shift for the Cashier associated with the Employee will not increment during this Clock In cycle. This option has no effect if Shift Tracking is not enabled in Control Parameters.

Increment Cashier Shift when Changing Revenue Center

If set, the Shift for the Cashier associated with the Employee, will increment when they Sign In to a different Revenue Center. If not set, the Shift for the Cashier associated with the Employee will not increment when Signing In to a different Revenue Center. This option has no effect if Shift Tracking is not enabled in Control Parameters.

Prompt to Increment Cashier Shift after Shift Report

If set, when a Cashier Shift report is generated with a Shift scope, the Operator will be prompted whether the Cashier Shift should be incremented. If not set, no prompting will occur and the Cashier Shift will not increment. This option has no effect if Shift Tracking is not enabled in Control Parameters.

Prompt before incrementing Cashier Shift

If set, the Employee will be prompted whether or not to increment the Shift for the Cashier associated with the Employee when the Shift is set to increment when Clocking In or Out, changing Jobs or changing Revenue Centers. If not set, no prompting will occur when the Cashier Shift is set to increment through one of those methods. This option has no effect if Shift Tracking is not enabled in Control Parameters.

Ad Hoc Reports Tab

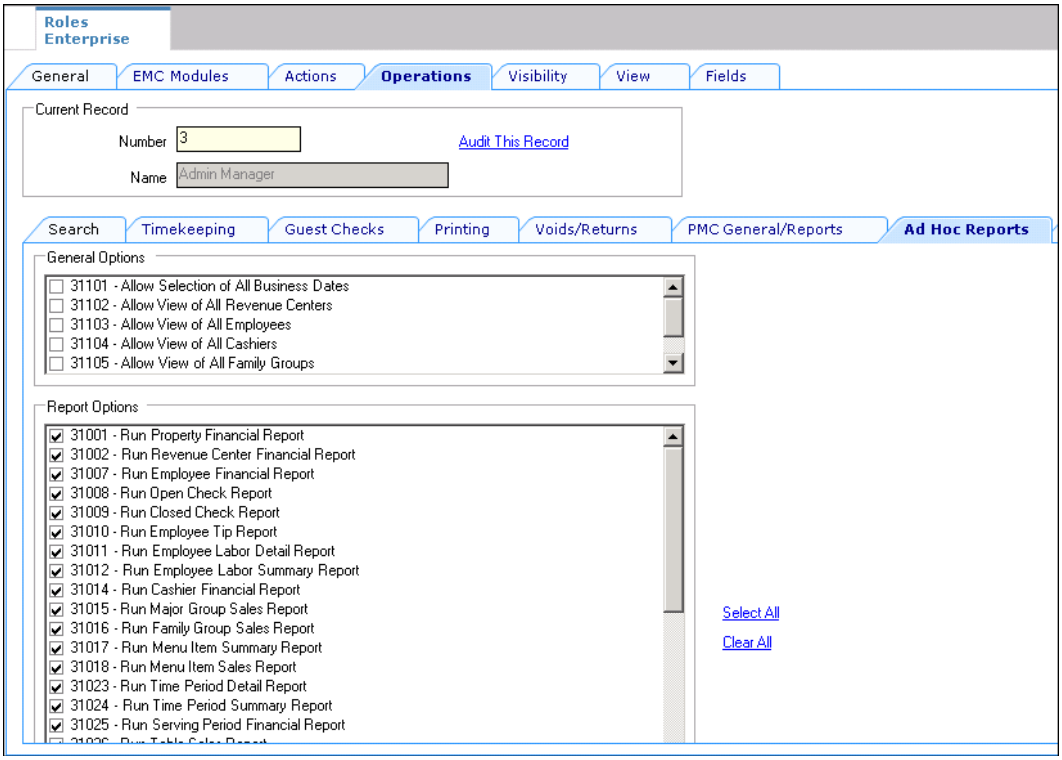


Figure 19 - Roles Ad Hoc Reports

General Options

Allow Selection of All Business Dates

Select this option to allow employees associated with this Role to select Today, Yesterday, etc. from the report business date selection list.

Allow View of All Revenue Centers

Select this option to allow employees associated with this Role to view all revenue centers from the report revenue center selection list.

Allow View of All Employees

Select this option to allow employees associated with this Role to view all employees from the report employee selection list.

Allow View of All Cashiers

Select this option to allow employees associated with this Role to view all cashier from the report cashier selection list.

Allow View of All Family Groups

Select this option to allow employees associated with this Role to view all family groups from the report family group selection list.

Do Not allow to run with Open Checks for Any Report

Select this option to prevent employees associated with this Role from running any report when there are open checks in this property. Only the Employee Open Check report can run in order to view open checks.

Do Not Show Blind Drop Tenders Group

Select this option to not allow employees associated with this Role to see detailed tender media. This option works with Report group Option 4 - Do Not Display for Blind Drop Reports.

Reporting Options

Run Property Financial Report

Select this option to allow employees associated with this Role to run the Property Financial Report.

Run Revenue Center Financial Report

Select this option to allow employees associated with this Role to run the Revenue Center Financial Report.

Run Employee Financial Report

Select this option to allow employees associated with this Role to run the Employee Financial Report.

Run Open Check Report

Select this option to allow employees associated with this Role to run the Open Check Report.

Run Closed Check Report

Select this option to allow employees associated with this Role to run the Closed Check Report.

Run Employee Tip Report

Select this option to allow employees associated with this Role to run the Employee Tip Report.

Run Employee Labor Detail Report

Select this option to allow employees associated with this Role to run the Employee Labor Detail Report.

Run Employee Labor Summary Report

Select this option to allow employees associated with this Role to run the Employee Labor Summary Report.

Run Cashier Financial Report

Select this option to allow employees associated with this Role to run the Cashier Financial Report.

Run Major Group Sales Report

Select this option to allow employees associated with this Role to run the Major Group Sales Report.

Run Family Group Sales Report

Select this option to allow employees associated with this Role to run the Family Group Sales Report.

Run Menu Item Summary Report

Select this option to allow employees associated with this Role to run the Menu Item Summary Report.

Run Menu Item Sales Report

Select this option to allow employees associated with this Role to run the Menu Item Sales Report.

Run Time Period Detail Report

Select this option to allow employees associated with this Role to run the Time Period Detail Report.

Run Time Period Summary Report

Select this option to allow employees associated with this Role to run the Time Period Summary Report.

Run Serving Period Financial Report

Select this option to allow employees associated with this Role to run the Serving Period Financial Report

Run Table Sales Report

Select this option to allow employees associated with this Role to run the Table Sales Report.

Run Clock In Status Report

Select this option to allow employees associated with this Role to run the Clock In Status Report.

Run Labor Availability Report

Select this option to allow employees associated with this Role to run the Labor Availability Report.

Run Job Code Report

Select this option to allow employees associated with this Role to run the Job Code Report.

Run Autofire Open Check Report

Select this option to allow employees associated with this Role to run the Autofire Open Check Report.

Run Offline Revenue Center Financial Report

Select this option to allow employees associated with this Role to run the Offline Revenue Center Financial Report.

Run Offline Employee Financial Report

Select this option to allow employees associated with this Role to run the Offline Employee Financial Report.

Run Offline Cashier Financial Report

Select this option to allow employees associated with this Role to run the Offline Cashier Financial Report.

Run Offline Open Check Report

Select this option to allow employees associated with this Role to run the Offline Open Check Report.

Run Employee Journal

Select this option to allow employees associated with this Role to run the Employee Journal Report.

Run Check Journal Report

Select this option to allow employees associated with this Role to run the Check Journal Report.

Run Employee Financial Report V2

Select this option to allow employees associated with this Role to run the Employee Financial Report.

Run Property Financial - VAT Report

Select this option to allow employees associated with this Role to run the Property Financial - VAT Report.

Run Revenue Center Financial - VAT Report

Select this option to allow employees associated with this Role to run the Revenue Center Financial - VAT Report.

Run Employee Financial - VAT Report

Select this option to allow employees associated with this Role to run the employee Financial - VAT Report.

Run Tax Summary Report

Select this option to allow employees associated with this Role to run the Tax Summary Report.

Run Employee Section Assignment Report

Select this option to allow employees associated with this Role to the Employee Section Assignment Report.

Run Employee Tip Track Report

Select this option to allow employees associated with this Role to run the Employee Tip Report.

Run Till Report

Select this option to allow employees associated with this Role to run the Till Report.

Run Cash Pull Report

Select this option to allow employees associated with this Role to run the Cash Pull Report.

Run Till Banking Report

Select this option to allow employees associated with this Role to run the Till Banking Report.

Run Safes Report

Select this option to allow employees associated with this Role to run the Safes Report.

Run Paid-In/Paid-Out Report

Select this option to allow employees associated with this Role to run the Paid-In/Paid-Out Report.

Run Over/Short Detail Report

Select this option to allow employees associated with this Role to run the Over/Short Detail Report.

Run Bank Deposits Report

Select this option to allow employees associated with this Role to run the Bank Deposits Report.

Run Server Bank Report

Select this option to allow employees associated with this Role to run the Server Bank Report.

Run Petty Cash Report

Select this option to allow employees associated with this Role to run the Petty Cash Report.

Run Server Banking Report

Select this option to allow employees associated with this Role to run the Server Banking Report.

Run Held Item Summary Report

Select this option to allow employees associated with this Role to run the Held Item Summary Report.

Run Employee Waste Report

Select this option to allow employees associated with this Role to run the Employee Waste Report.

Run Menu Item Waste Report

Select this option to allow employees associated with this Role to run the Menu Item Waste Report.

Run Waste Summary Report

Select this option to allow employees associated with this Role to run the Waste Summary Report.

Run Waste Detail Report

Select this option to allow employees associated with this Role to run the Waste Detail Report.

Run Revenue Center Lock Report

Select this option to allow employees associated with this Role to run the Revenue Center Lock Report.

PMC Procedures Tab

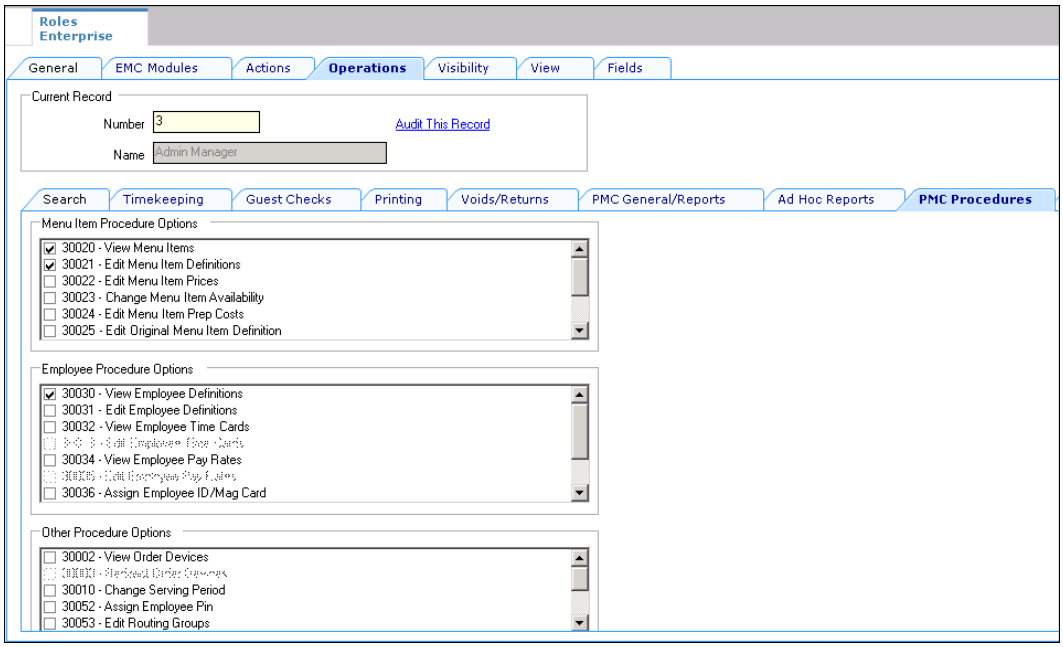


Figure 20 - Roles PMC Procedures

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 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.

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.

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.

Edit Original Menu Item Definition

Enable this option for employees associated with this Role to change the original menu item definition/price where it is defined. In cases where it is defined at the property/zone/enterprise level, when the user has this privilege assigned, the original definition will be changed. Otherwise, an override record at the RVC level will be created. This option is only available when the options "View Menu Items" and "Run PMC" are 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.

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.

Employee Procedure Option

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.

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 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.

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.

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.

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.

Assign Employee Fingerprint Scan

Enable this option for employees associated with this Role to assign Fingerprint Scan to Employees as an ops command or within the PMC Employee Procedure. This option is only available when the option "View Employee Definitions" is enabled.

Other Procedure Options

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.

Assign Employee Pin

Enable this option for employees associated with this Role to assign Employee Pin as an ops command or a PMC Procedure.

Edit Routing Groups

Enable this option for employees associated with this Role to edit Routing Groups as an ops command or a PMC Procedure.

Set Active Kitchen Themes

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

Change Default Revenue Center

Enable this option for employees associated with this Role to change the default Revenue Center of a Workstation.

Backup/Restore KDS Controller

Enable this option for employees associated with this Role to Activate Backup KDS Controller or Restore Primary KDS Controller.

Run Start of Day from OPS

Enable this option for employees associated with this Role to perform Start of Day from OPS. Property Option ‘Run Start of Day from OPS’ should also be enabled.

Prevent Running SOD from OPS with Open Checks

Select this option to prevent Employees associated with this Role from running Start of Day from OPS while there are open checks at the property.

Transactions Tab

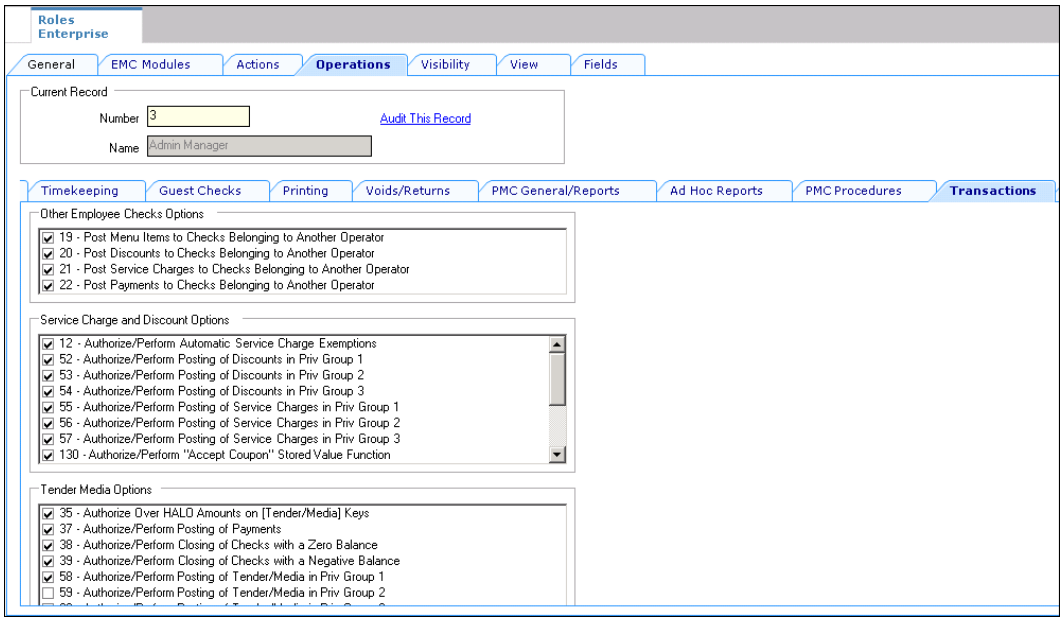


Figure 21 - Roles Transactions

Other Employees Checks Options

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.

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 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 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.

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 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 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 "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.

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/Use Remove Coupon Discounts

Select this option to allow employees associated with this Role to use the Remove Coupon Discounts Function Key (658), and to authorize non-privileged employees to do so as well.

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.

Tender Media Options

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 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 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 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/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/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 [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/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/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/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/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/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/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/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/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/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.

Authorize/Perform Cancel Order

Select this option to allow employees associated with this Role to cancel an entire order, and to authorize other employees to do so as well. This option controls different behavior than the "Authorize/Use the [Transaction Cancel] Key" option; the setting of this option is used to control a user's access to the [Cancel Order] function key (576), which deletes all detail from a check and cancels the order. That function key and this option are often used in quick service environments in conjunction with KDS DOM behavior.

Allow Incomplete Item

When this bit is set and a parent item is being ordered with its 'Allow Incomplete Item Based on Role' bit set, and then the required condiment restrictions will be lifted for that item.

Authorize/Perform Service Total/Payment with Placeholder item

Enable this option to allow employees to perform/authorize tendering a transaction with a Placeholder item, if Tender Media option bit 85 is enabled.

Authorize/Perform SVC Tender of SVC Transactions

Enable this option to allow employees to perform/authorize tendering a Stored Value Card (SVC) Tender for SVC transactions.

Perform Menu Item Refills

Select this option to allow employees associated with this Role to refill Menu Items on a Guest Check.

Miscellaneous Tab

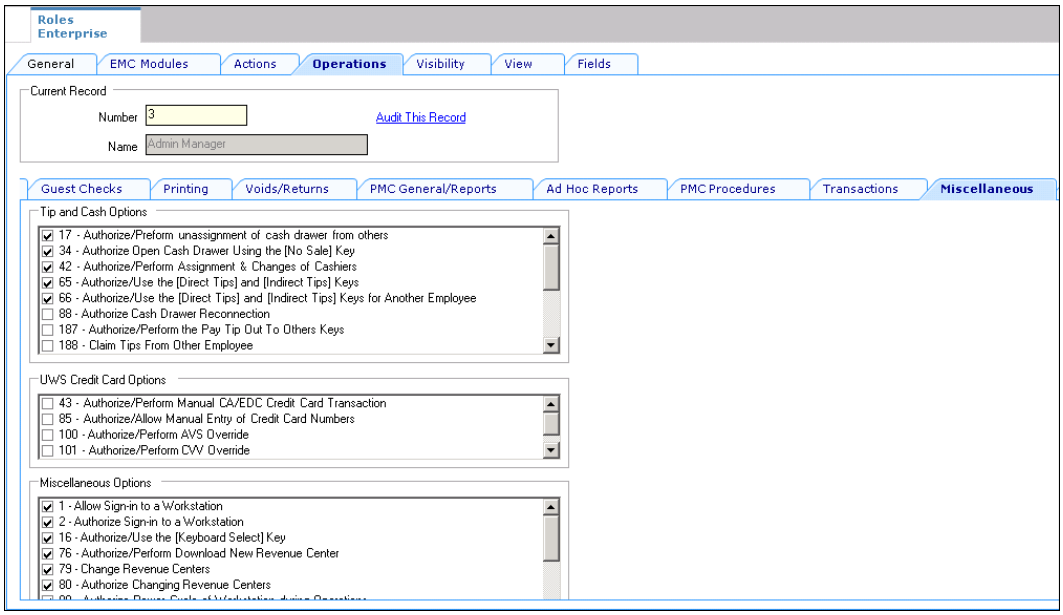


Figure 22 - Roles Miscellaneous

Tip and Cash Options

Authorize/ Perform unassignment of Cash Drawer from Others

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 Class privilege—any employee with access to the [Assign Cash Drawer] button can use it.

This option includes two different functions. #1: Select this option 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 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 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/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/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.

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.

Authorize/Perform the Pay Tip Out To Others Keys

Select this option to allow employees associated with this Role to use these keys to declare cash tips given to others, and to authorize non-privileged employees to do so as well.

Claim Tips From Other Employee

Select this option to allow employees associated with this Role to be included in tip tracking for the purposes of receiving a tip from another employee.

Authorize/Perform Edit Of Any Tip Outs

Select this option to allow employees associated with this Role to use these keys to edit cash tips given to others, and to authorize non-privileged employees to do so as well.

Authorize/Create Team

Select this option to allow employees associated with this Role to use these keys to create a Team and add initial Team Members to it, and to authorize non-privileged employees to do so as well.

Authorize/Add or Delete Team Member to a Team

Select this option to allow employees associated with this Role to add or delete Members to an existing Team, and to authorize non-privileged employees to do so as well.

Authorize/Delete any Team

Select this option to allow employees associated with this Role to delete an existing Team, and to authorize non-privileged employees to do so as well.

Print a list of Teams

Select this option to allow employees associated with this Role to print a Team List showing the name of the Team and all its assigned Members.

Authorize/Assign a Stay Down Team to a Table

Select this option to allow employees associated with this Role to assign a stay down Team to a Table, and to authorize non-privileged employees to do so as well.

Allow Edit of My Tip Out

Select this option to allow employees associated with this Role to Tip Out.

Available as Team Service Team Member

Select this option to allow employees associated with this Role to appear in selection lists when assigning Team Member.

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 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 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 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

Allow Sign-in to a Workstation

Select this option to allow employees associated with this Role to sign into a workstation or a Mobile handheld 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 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 handheld unit.

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 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.

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 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.

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, the client will display a prompt to retry the operation or work offline. If the 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.

Authorize/Use Quebec SRM Control Functions

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 Quebec SRM Control function key.

Turn On Single Sign In

This option prevents an employee from being able to sign into more than workstation at a time. If enabled, the employee will receive a message indicating that the "Employee ID is already in use”.

Clock In Required to Perform Authorizations

If set, Employees associated with this Role are not able to authorize any actions at a UWS unless they are Clocked In. This prevents an off shift employee from performing illegitimate authorizations. If not set, Employees associated with this Role may authorize actions at a UWS without being Clocked In. This option is only used when Property Parameters Option Enable Clock In Requirement for Authorization is enabled. This option does not apply if myLabor is not enabled or Employee is not required to Clock In.

Unlock UWS or Revenue Center

Select this option to allow employees associated with this Role to Unlock a UWS or Revenue Center from the Locked dialog.

Use Workstation Control

Select this option to allow employees associated with this Role to use the [Workstation Control] key, which allows access to various functions such as Lock/Unlock UWS’s and Revenue Centers, trigger Database Updates, etc. If this option is enabled, it also provides the ability to unlock a UWS or Revenue Center from the locked state.

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.

Run Support Diagnostics

Select this option to allow employees associated with this Role to view support diagnostics on a workstation.

Upload Support Diagnostics Data to Enterprise

Select this option to allow employees associated with this Role to upload support diagnostics data from a workstation to the enterprise database.

Can Access CAL Admin Application

Select this option to allow employees to access CAL Android admin mode.

Stored Value Cards Tab

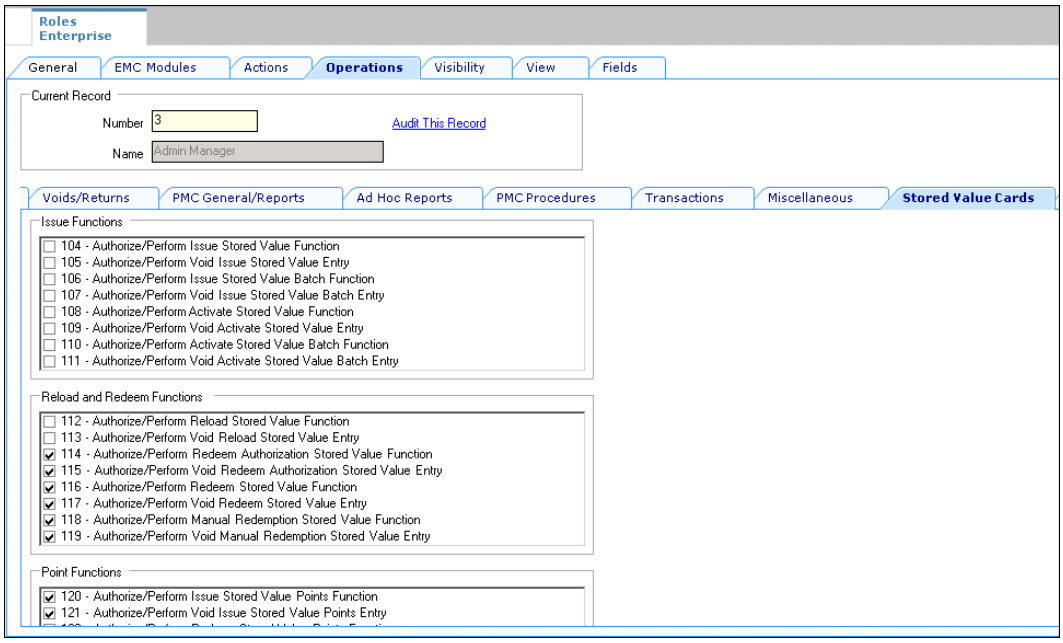


Figure 23 - Roles Stored Value Cards

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 Void Stored Value Cash Out Function

Select this option to allow employees associated with this Role to void the redemption 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.

Loyalty Options

Authorize/Perform Loyalty Coupon Inquiry

Select this option to allow employees associated with this Role to authorize/perform Loyalty Coupon Inquiry.

Authorize Perform Accept Loyalty Coupon Function

Select this option to allow employees associated with this Role to authorize/perform an Accept Loyalty Coupon Inquiry.

Authorize Perform Void Accept Loyalty Coupon Entry

Select this option to allow employees associated with this Role to authorize/perform a Void of an Accept Loyalty Coupon Inquiry.

Authorize Perform Issue Loyalty Coupon Function

Select this option to allow employees associated with this Role to authorize/perform an Issue Loyalty Coupon Inquiry.

Authorize Perform Issue Loyalty Points Function

Select this option to allow employees associated with this Role to authorize/perform an Issue Loyalty Points function.

Authorize Perform Void Issue Loyalty Points Entry

Select this option to allow employees associated with this Role to authorize/perform a Void of an Issue Loyalty Points entry.

Authorize Perform Redeem Loyalty Points Function

Select this option to allow employees associated with this Role to authorize/perform a Redeem Loyalty Points function.

Authorize Perform Void Redeem Loyalty Points Entry

Select this option to allow employees associated with this Role to authorize/perform a Void of a Redeem Loyalty Points entry.

Authorize Perform Redeem And Issue Loyalty Points Entry

Select this option to allow employees associated with this Role to authorize/perform a Redeem and Issue Loyalty Points entry.

Authorize Perform Void Redeem And Issue Loyalty Points Entry

Select this option to allow employees associated with this Role to authorize/perform a a Void of a Redeem and Issue Loyalty Points entry.

Authorize Perform Loyalty Balance Inquiry Function

Select this option to allow employees associated with this Role to authorize/perform a Loyalty Balance Inquiry function.

Authorize Perform Loyalty Unique Item Inquiry Function

Select this option to allow employees associated with this Role to authorize/perform a Loyalty Unique Item Inquiry function.

Authorize Perform Loyalty Balance Transfer Function

Select this option to allow employees associated with this Role to authorize/perform a Loyalty Balance Transfer function.

Authorize Perform Apply Loyalty Card to Check

Select this option to allow employees associated with this Role to authorize/perform the application of a Loyalty Card to a check.

Guest Management Tab

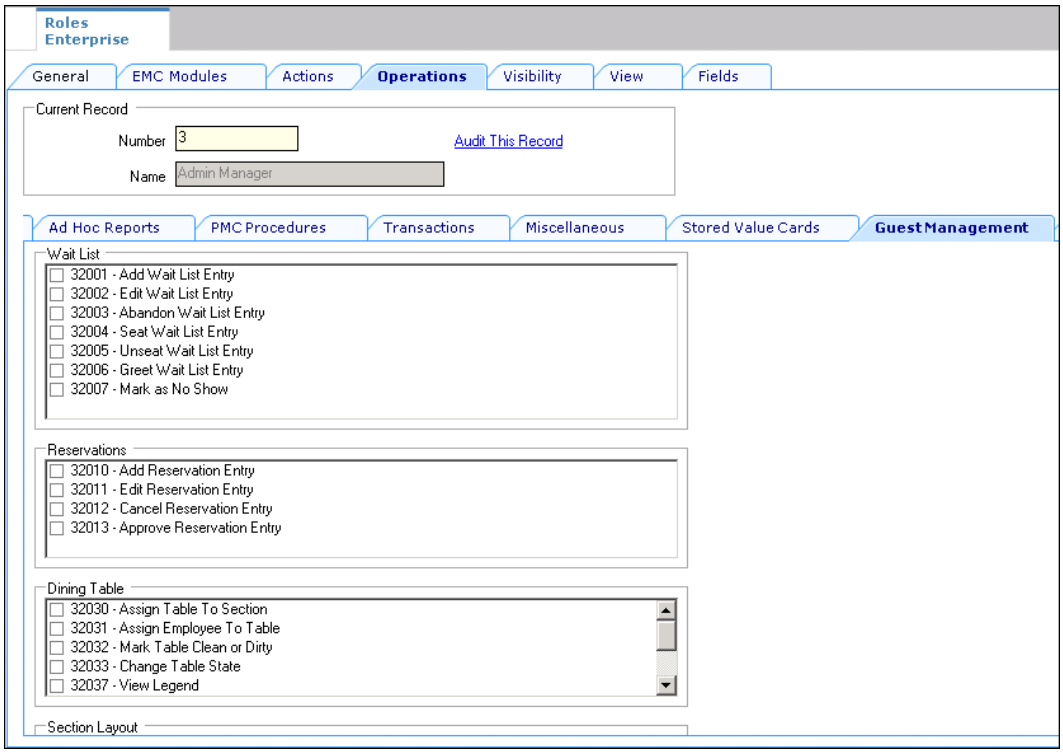


Figure 24 - Roles Guest Management

Wait List

Add Wait List Entry

Enable this option for employees that need to Add Wait List entries.

Edit Wait List Entry

Enable this option for employees that need to Edit Wait List entries.

Abandon Wait List Entry

Enable this option for employees that need to Abandon Wait List entries.

Seat Wait List Entry

Enable this option for employees that need to Seat Wait List entries.

Unseat Wait List Entry

Enable this option for employees that need to Unseat dining tables back to Wait List entries.

Greet Wait List Entry

Enable this option for employees that need to Great Wait List entries.

Mark as No Show

Enable this option for employees that need to mark entries as being a No Show.

Reservations

Add Reservation Entry

Enable this option for employees that need to Add Reservation entries.

Edit Reservation Entry

Enable this option for employees that need to Edit Reservation entries.

Cancel Reservation Entry

Enable this option for employees that need to Cancel Reservation List entries.

Approve Reservation Entry

Enable this option for employees that need to Approve Reservation List entries.

Dining Table

Assign Table To Section

Enable this option for employees that need to Assign Dining Tables to Sections.

Assign Employee To Table

Enable this option for employees that need to Assign Employees to Dining Tables.

Mark Table Clean or Dirty

Enable this option for employees that need to Mark Tables as being either Clean or Dirty.

Change Table State

Enable this option for employees that need to Mark Tables as being Available, Closed, Reserved, or Merged.

View Legend

Allows user to view the legend

Section Layout

Edit Section Layout

Enable this option for employees that need to Add or Edit Section Layouts.

Activate Section Layout

Enable this option for employees that need to Activate Section Layouts.

Delete Section Layout

Enable this option for employees that need to Delete Section Layouts.

Cash Management Tab

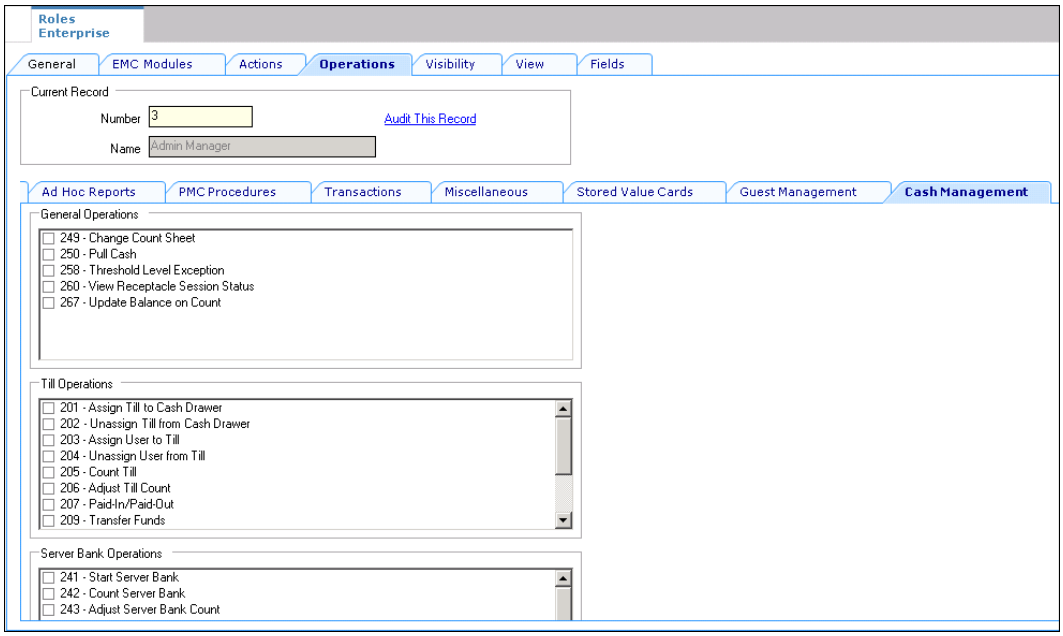


Figure 25 - Cash Management

General Options

Change Count Sheet

Select this option to allow employees with this Role to perform or authorize changing the Count Sheet to be utilized for any Counts

Pull Cash

Select this option to allow employees with this Role to perform or authorize a Cash Pull from a Till or Server Bank.

Threshold Level Exception

Select this option to allow employees with this Role to authorize a Cash Pull Threshold Exception when prompted and permitted.

View Receptacle Session Status

Select this option to allow employees with this Role to perform or authorize the viewing the Receptacle Session Status dialog.

Till Operations

Assign Till to Cash Drawer

Use this operation to create a new Till session. User will be prompted to choose the Till and Cash Drawer that will be utilized for the tracking of cash management transactions. This function may only be utilized on workstations that have a defined and available cash drawer.

Unassign Till from Cash Drawer

Select this option to allow employees with this Role to perform or authorize the unassignment of a cash drawer from an active Till.

Assign User to Til

Select this option to allow employees with this Role to perform or authorize the assignment of employees to an active Till

Unassign User from Till

Select this option to allow employees with this Role to perform or authorize the unassignment of employees from an active Till.

Count Till

Select this option to allow employees with this Role to perform or authorize the counting of a Till.

Adjust Till Count

Select this option to allow employees with this Role to perform or authorize the adjustment of a Till Count.

Paid-In/Paid-Out

Select this option to allow employees with this Role to perform or authorize the execution of a Paid-In or Paid-Out on a Till.

Transfer Funds

Select this option to allow employees with this Role to perform or authorize transferring funds from a Till to another Cash Receptacle.

Deposit Funds

Select this option to allow employees with this Role to perform or authorize depositing cash from a Till to a Bank Deposit.

Close Till

Select this option to allow employees with this Role to perform or authorize the closing of a Till.

Reopen Till

Select this option to allow employees with this Role to perform or authorize the reopening of a Closed Till.

Quick Start Till

Select this option to allow employees with this Role to perform or authorize a Quick start of a Till.

Adjust Till Starting Amount

Select this option to allow employees with this Role to authorize the adjusting of a Till starting amount when prompted and permitted.

Server Bank Operations

Start Server Bank

Select this option to allow employees with this Role to perform or authorize the opening of a Server Bank

Count Server Bank

Select this option to allow employees with this Role to perform or authorize the counting of a Server Bank.

Adjust Server Bank Count

Select this option to allow employees with this Role to perform or authorize the adjustment of a Server Bank Count.

Paid-In/Paid-Out

Select this option to allow employees with this Role to perform or authorize the execution of a Paid-In or Paid-Out on a Server Bank.

Transfer Funds

Select this option to allow employees with this Role to perform or authorize the transfer of funds from a Server Bank to another Cash Receptacle.

Deposit Funds

Select this option to allow employees with this Role to perform or authorize depositing cash from a Server Bank to a Bank Deposit.

Close Server Bank

Select this option to allow employees with this Role to perform or authorize the closing of a Server Bank.

Reopen Server Bank

Select this option to allow employees with this Role to perform or authorize the reopening of a Closed Server Bank.

Adjust Server Bank Starting Amount

Select this option to allow employees with this Role to authorize the adjusting of a Server Bank starting amount when prompted and permitted.

Consolidate Server Banks

Select this option to allow employees with this Role to perform or authorize the consolidation of two server bank sessions.

Safe Operations

Open Safe

Select this option to allow employees with this Role to perform or authorize the opening of a new Safe.

Count Safe

Select this option to allow employees with this Role to perform or authorize the counting of a Safe.

Adjust Safe Count

Select this option to allow employees with this Role to perform or authorize adjusting a count for the Safe.

Paid-In/Paid-Out

Select this option to allow employees with this Role to perform or authorize the execution of a Paid-In or Paid-Out on a Safe.

Transfer Funds

Select this option to allow employees with this Role to perform or authorize the transferring of funds from a Safe to another Cash Receptacle.

Deposit Funds

Select this option to allow employees with this Role to perform or authorize depositing cash from a Safe to a Bank Deposit.

Close Safe

Select this option to allow employees with this Role to perform or authorize the closing of a Safe.

Add Funds to Safe

Select this option to allow employees with this Role to perform or authorize the execution of a adding funds to a Safe.

Remove Funds from Safe

Select this option to allow employees with this Role to perform or authorize the execution of a removing funds from a Safe.

Petty Cash Operations

Open Petty Cash

Select this option to allow employees with this Role to perform or authorize the opening of a new Petty Cash receptacle.

Count Petty Cash

Select this option to allow employees with this Role to perform or authorize the counting of Petty Cash.

Adjust Petty Cash Count

Select this option to allow employees with this Role to perform or authorize adjusting a count for Petty Cash.

Paid-In/Paid-Out

Select this option to allow employees with this Role to perform or authorize the execution of a Paid-In or Paid-Out on Petty Cash.

Transfer Funds

Select this option to allow employees with this Role to perform or authorize the transferring of funds from Petty Cash to another Cash Receptacle.

Deposit Funds

Select this option to allow employees with this Role to perform or authorize depositing cash from Petty Cash to a Bank Deposit.

Close Petty Cash

Select this option to allow employees with this Role to perform or authorize the closing of Petty Cash.

Bank Deposit Operations

Create a Bank Deposit

Select this option to allow employees with this Role to perform or authorize the creation of a new Bank Deposit.

Transfer Funds

Select this option to allow employees with this Role to perform or authorize transferring funds from a Bank Deposit to another Cash Receptacle.

Adjust Cash Deposit

Select this option to allow employees with this Role to perform or authorize adjusting a cash amount deposited into the Bank Deposit.

Reconcile Bank Deposit

Select this option to allow employees with this Role to perform or authorize the reconciliation of a Bank Deposit.

Adjust Bank Deposit

Select this option to allow employees with this Role to perform or authorize adjusting a Bank Deposit.

Change Order Operations

Create Change Order

Select this option to allow employees with this Role to perform or authorize the creation of a new Change Order request.

Workstation Privileges

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

EMC Configuration

Display/Security Tab

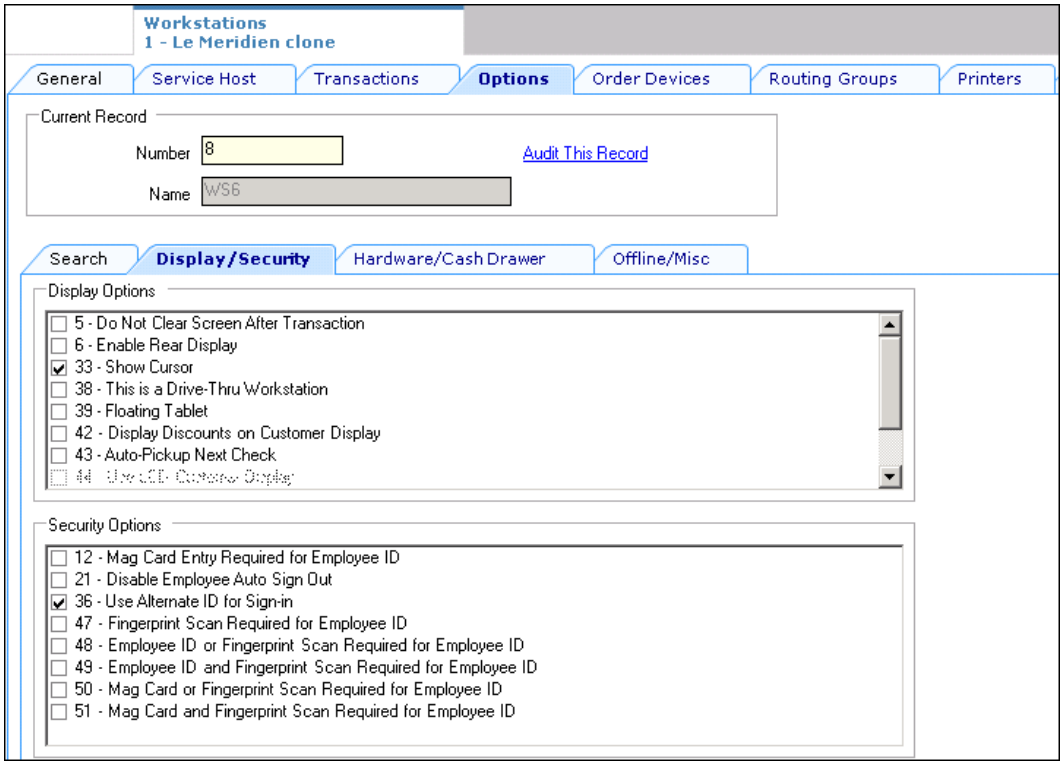


Figure 26 - Workstations Display/ Security

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.

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.

This is a Drive-Thru Workstation

When this option is enabled, this workstation's Pickup Check SLU will only display the checks that match the default Order Type of this workstation. This option is intended for use in a multi-

workstation drive-thru where the Drive Thru orders are viewed on the paying workstation, but Dine In and Take Out orders are not.

Floating Tablet

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 traditional workstations support.

Display Discounts on Customer Display

When this option is enabled, the discount totals and amount due on the second line of the customer display. When this is disabled, only the amount due is displayed.

Auto-Pickup Next Check

This option is intended for Drive-Thru environments where there is an Ordering Window and a Payment Window; this option would be enabled for the Payment Window workstation. When this option is enabled, the workstation will automatically pick up the oldest open check (that has this Workstation's Order Type) as soon as the current check has been paid. When this option is not enabled, checks are not automatically picked up by this workstation. Note that when no more checks are open and this option is enabled, the user will be shown a dialog that prompts to check again or to exit the Auto-Pickup functionality.

Use LCD Customer Display

This option is enabled if another option called **Enable Rear Display** is enabled. This will be grayed out if Enable Rear Display is not set. If **Use LCD Customer Display** is enabled the LCD Customer Display will be used; if it is not enabled then the old pole display will be used

Display non-rounded amounts on rear/customer display

When enabled this option will display non-rounded value for the total due amount in a customer display. This option is only valid when the **Round Currency** option in Currency Parameters is enabled.

Display Change to dispense in Bills in the Change due dialog

When enabled this option will display the change to dispense in Bills in the Change Due dialog. This will help the user to easily determine the change due in Bills while the coin dispenser dispenses the rest of the amount.

Security Options

Mag Card Entry Required for Employee ID

Select this option to require that all employee ID entries at this workstation be 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.

Finger Print Scan Required for Employee ID

Select this option to require that all employee ID entries at this workstation be made using a Fingerprint Scan. This applies to signing in, authorizing privileged operations, etc. If this option is selected, the workstation will not accept an employee ID number entered through the keyboard or touchscreen and only accept a Fingerprint Scan.

Employee ID or Fingerprint Scan Required for Employee ID

Employee ID or Fingerprint Scan Required for Employee ID </string><help>Select this option to require that all employee ID entries at this workstation are made using a Fingerprint Scan or an employee ID number entered through the keyboard or touchscreen. This applies to signing in, authorizing privileged operations, etc. If this option is selected, the workstation will only accept either an employee ID number entered through the keyboard or touchscreen or a Fingerprint Scan.

Employee and Fingerprint Scan Required for Employee ID

Select this option to require that all employee ID entries at this workstation are made using a Fingerprint Scan and an employee ID number entered through the keyboard or touchscreen. This applies to signing in, authorizing privileged operations, etc. If this option is selected, the workstation will only accept an employee ID number entered through the keyboard or touchscreen and a Fingerprint Scan.

Mag Card or Fingerprint Scan Required for Employee ID

Select this option to require that all employee ID entries at this workstation are made using a Fingerprint Scan or a Mag Card swiped. This applies to signing in, authorizing privileged operations, etc. If this option is selected, the workstation will only accept either a Mag Card swiped or a Fingerprint Scan.

Mag Card and Fingerprint Scan Required for Employee ID

Select this option to require that all employee ID entries at this workstation are made using a Fingerprint Scan and a Mag Card swiped. This applies to signing in, authorizing privileged operations, etc. If this option is selected, the workstation will only accept a Mag Card swiped and a Fingerprint Scan.

Hardware/Cash Drawer Tab

Hardware/Interface Options

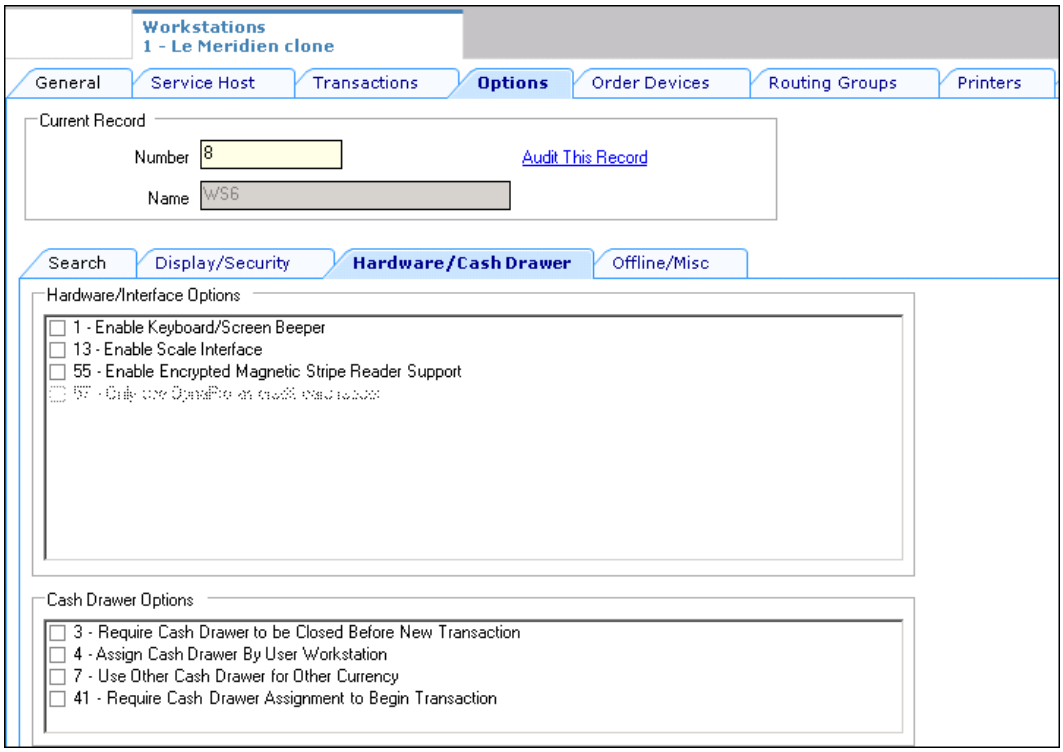


Figure 27 - Workstations Options

Enable Keyboard/Screen Beeper

When this option is enabled, a beep will sound each time a user presses a key on this workstation. If this option is disabled, no beep occurs.

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 Encrypted Magnetic Stripe Reader Support

Enable this option to use an encrypted MSR. During an upgrade, the DynaPro device will be added to this workstation's device list if Option 55 was checked prior to the upgrade. If this device is an Oracle MICROS workstation, the magnetic card reader in the workstation will have its encryption capabilities turned on when checked. Refer to the individual workstation model documentation to ensure your internal reader is capable of encryption. The credit card entry field which is displayed in OPS will be secured and no longer allow numeric entry to ensure data encryption.

Note: Once this option is enabled, it cannot be turned off. Before enabling this option, ensure that the credit card processor/gateway is capable of supporting the encryption functionality.

Only user DynaPro as credit card reader

Enabling this option bit will cause the workstation to only allow credit card swipes to occur on a DynaPro reader and the internal reader will no longer be usable for credit card swipes. Any card data processed through the internal reader which appears to be credit card data will not be accepted. NOTE: If this option bit is enabled and there is either no reader configured in the workstation's device table or the reader is not attached to the workstation, it will not be possible to process credit cards through this workstation.

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 Other Cash Drawer 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.

Require Cash Drawer Assignment to Begin Transaction

Select this option to require an employee to have a cash drawer assigned prior to beginning a transaction at this workstation. Do not select this option to allow any operator to begin a transaction at this workstation.

Offline/ Misc Tab

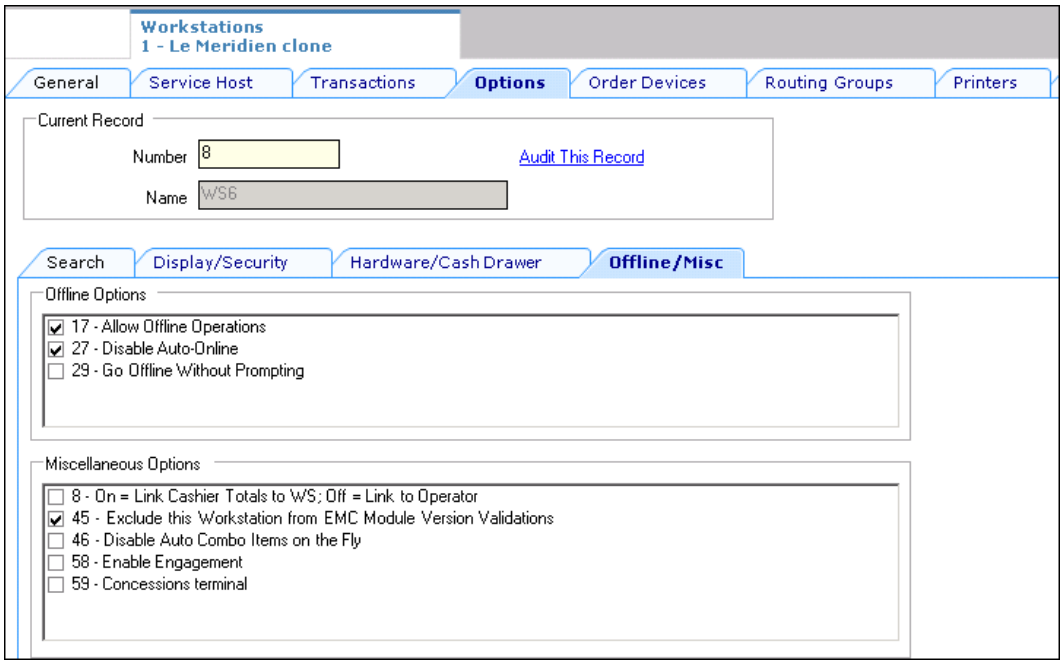


Figure 28 - Workstations Offline/ Misc Options

Offline Options

Allow Offline Operations

Enable this option to allow this workstation to operate in **Offline Mod**e. 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.

Miscellaneous Options

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 Port Numbers

Port Numbers

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

Enterprise Ports

Table 5 - Enterprise Ports

Service	Port Number	Configurable?
Simphony/EGateway (Oracle Database)	1521	Yes
Simphony/EGateway (Microsoft SQL Server)	1433	Yes
Simphony/EGateway (Simphony FE legacy ports after fresh install of 2.6)	8010	Yes
Simphony/EGateway (Pre-Simphony version 2.6)	8050	Yes
Simphony/EGateway (Simphony FE legacy ports after upgrade to 2.6)	8010 & 8050	Yes
Simphony v2/EGateway (After upgrade/install of Simphony version 2.6)	8080	Yes
EMC/Remote EMC	8080	Yes
Simphony/Reporting and Analytics Advanced	0 - Browser, 81 - myLabor service	Yes

Property Ports

Table 6 - Property Ports

Service	Port Number	Configurable?
ServiceHost version 2	8080	Yes
ServiceHost as a Service (no Ops)	8071	Yes
Print Controller	8080	Yes
IP Printer Listening	9100	No
Banquet Printing	9100	No
KDS Client (Display)	8080	Yes

Service	Port Number	Configurable?
KDS Controller Service	8080	Yes
Client Application Loader (server selection screen)	TCP 7300, UDP 7301	No
Client Application Loader (property selection screen)	8080	Yes
Credit Card Batching	8080	Yes
Cash Management Lite	5100	No
NetTCPRelayBinding (TMS/Azure)	TCP: 9350, 9351, 9352	No
NetTCPRelayBinding (TMS/Azure)	HTTP: 80	No

Traffic Note

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

Other ports: Please make sure to check the wrapper.conf file for environment-specific mymicros ports. <Drive>, MICROS, mymicros, myPortal, server, default, **wrapper.conf**.

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

Table 7 - Interface Ports

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 8 - iCare\ Loyalty Ports

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 9 - Oracle Component Ports

Component	Port	Range
Enterprise Manager Agent Enterprise Manager Database Control	HTTP	1830 - 1849
Enterprise Manager Agent Enterprise Manager Database Control	HTTP	5500 - 5519
Enterprise Manager Agent Enterprise Manager Database Control	RMI	5520 - 5539
Enterprise Manager Agent 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 EMC Module Accessibility

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

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

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

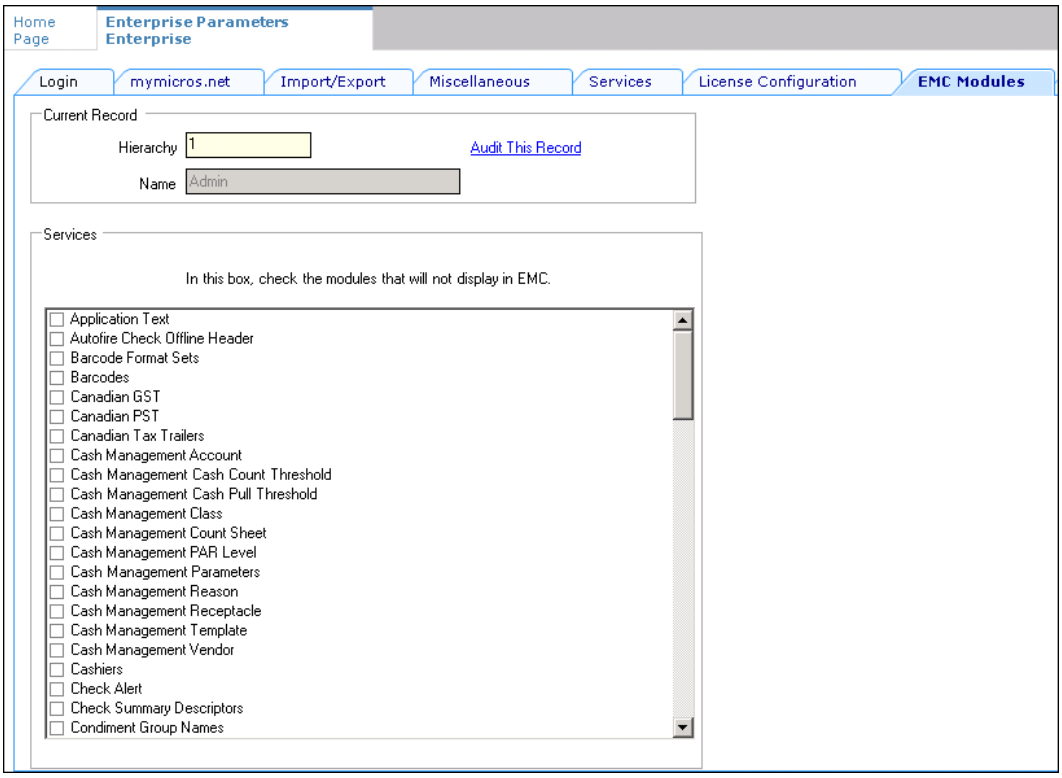


Figure 29 - EMC Modules

Appendix D Key Manager Manual

General Information

About the Simphony 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. In accordance with the PCI Data Security Standard, Oracle Hospitality mandates each site protect encryption keys against both disclosure and misuse.

Secure Key Practices

To ensure secure distribution, Oracle Hospitality 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. The Key Custodian sign off form is located in the *Simphony PA-DSS Implementation Guide.*

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.

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

The Encryption Scheme

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

Operational Considerations

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

Simphony - Fresh Installation

The following should be noted when conducting a fresh Simphony v2.x installation:
To ensure PCI compliance, MICROS Systems Inc. mandates that the site run the initial key rotation after the Simphony software installation is complete.

1. After a fresh install, Encryption key tables need to be created in the security database table before it can be rotated from the EMC.
2. From the Simphony application server, using Windows Explorer, navigate to the <Drive Letter>:\Micros\Simphony2\Tools\KeyManager and launch the **KeyManager.exe**.
3. Browse to the DbSettings.xml file in the Simphony2 folder structure and click **OK**.

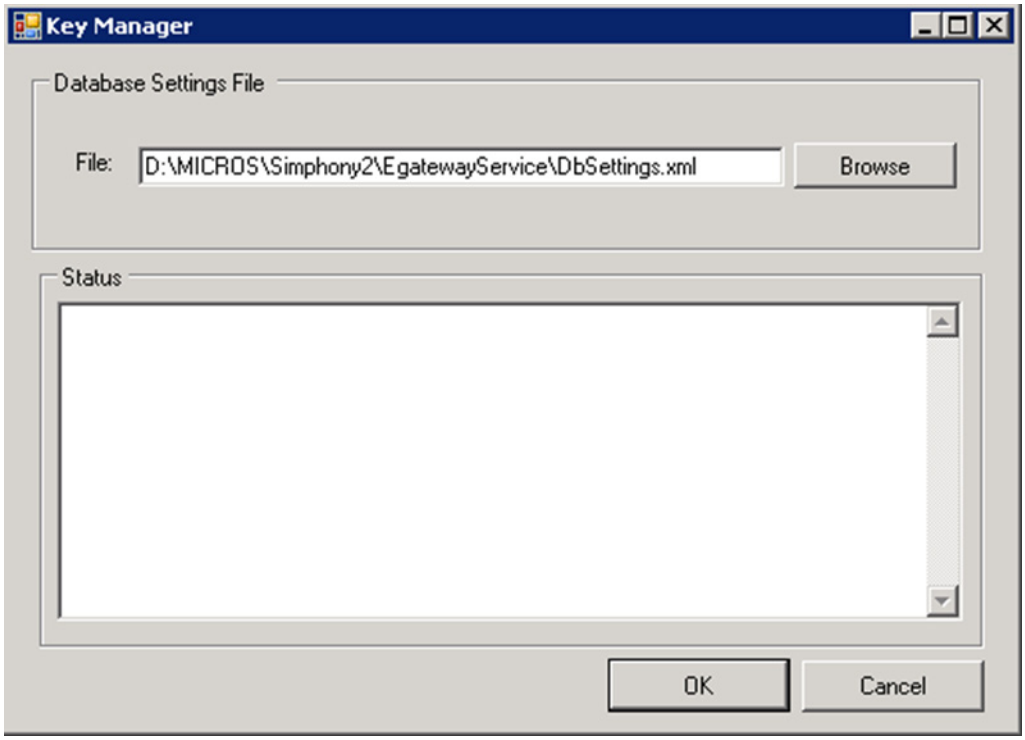


Figure 30 - Key Manager Utility

4. Ensure that all Credit Card transactions have been batched and settled, and all databases have been backed up and click **Yes**.

5. The status of the operation appears. Click **OK**.

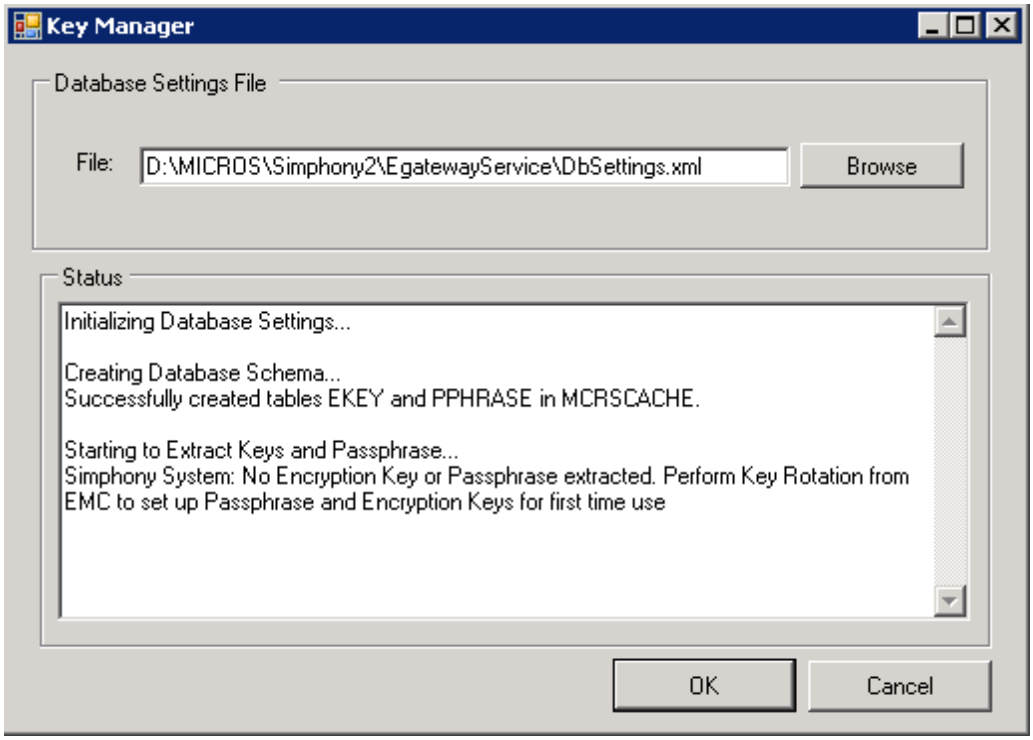


Figure 31 - Key Rotation Results

If an attempt is made to use the Key Manager Module in the EMC prior to executing the KeyManager.exe utility as outlined in the previous steps, users will receive the message shown below. Click **OK** to close the message.

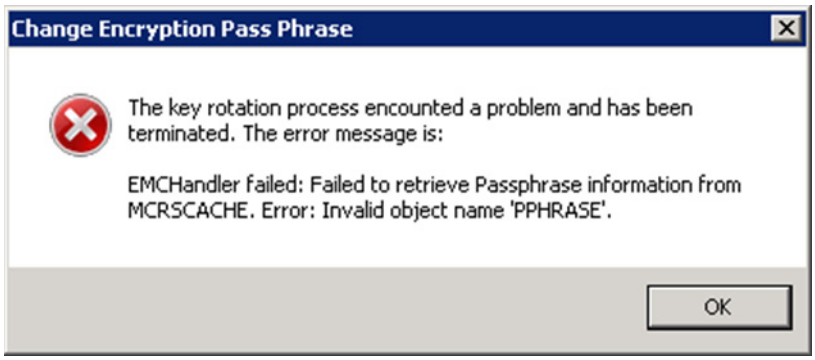


Figure 32 - Pass Phrase Message

Periodic Key Rotation

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

Key Manager Module

Operating Conditions

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

- The Simphony EGateway service must be up and running—with a web server installed and running.
- The 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.

Key Manager Module

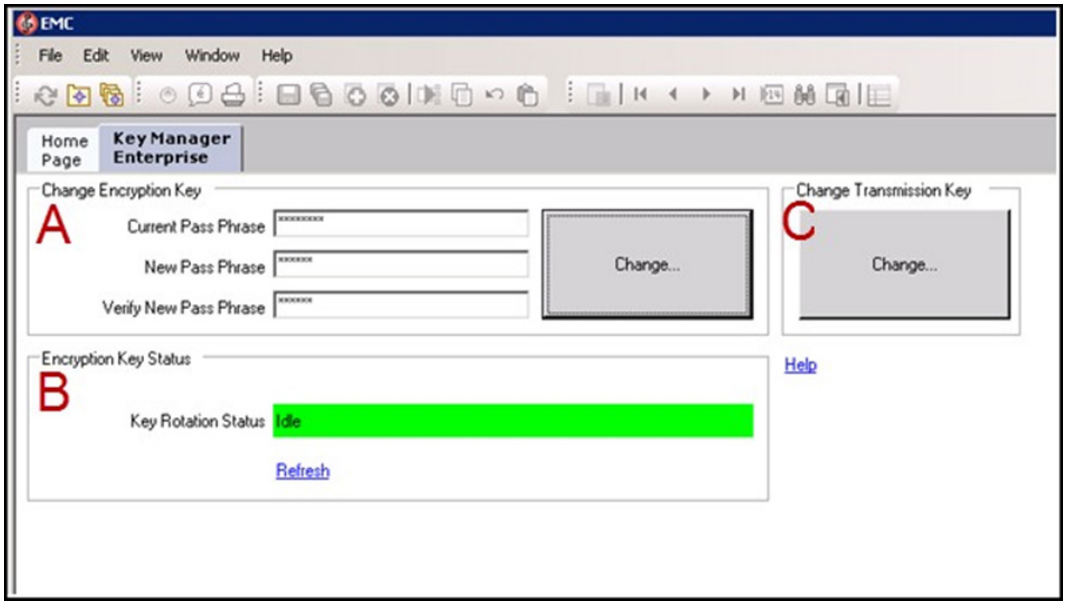


Table 10 - EMC - Key Manager Module

The areas of the module are:

A: Change Encryption Key area.

B: Encryption Key Status area.

C: Change Transmission Key area.

Area C, the Change Transmission Key area, 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.

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 the following:
  ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` | ~ {}
- 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

Caution: If the pass phrase 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.
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, circled below.

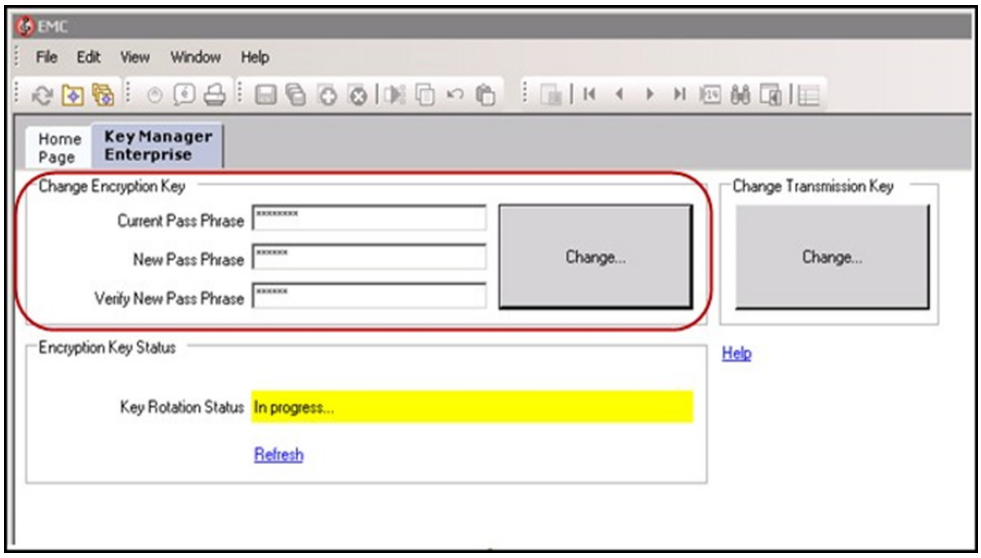


Figure 33 - Key Manager Module - In Progress

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 displays. 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.

   Click **No** if a database backup is currently in progress and begin the key rotation process again after the backup is finished.
   The Key Rotation Status section indicates that the task is **In progress...**.
7. Once the pass phrase has successfully changed, click **OK**.