

Oracle[®] MICROS Symphony

Security Guide



Release 19.6

F85295-04

April 2024

The Oracle logo, consisting of the word "ORACLE" in white, uppercase, sans-serif font, centered within a solid red square.

ORACLE[®]

Copyright © 2010, 2024, Oracle and/or its affiliates.

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

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

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

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

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

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

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

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

Contents

Preface

1 Symphony Security Overview

Basic Security Considerations	1-1
Service-Oriented Architecture (SOA)	1-1
Authentication	1-2
Enterprise Management Console Authentication	1-2
Simphony Client Authentication	1-2
Point of Sale User Authentication	1-3
Running a Workstation Securely with Windows Standard Users	1-3
Database User Management	1-3
Oracle MICROS Hardware Support Account	1-4
Simphony Transaction Services Gen 2 Authentication	1-4
Understanding the Simphony Environment	1-4
Recommended Deployment Configurations	1-5
Operating System Security	1-5
Database Security	1-6
Oracle Database	1-6
Database Engine Not Present on Workstations (Windows-based Workstations only)	1-6
Database Engine Exists on Workstations (Windows-based Workstations only)	1-6
Database on Linux for MICROS Workstations	1-7

2 Performing a Secure Simphony Installation

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

Post-Installation Configuration	2-6
Operating System	2-6
Application	2-7
Database Platform	2-7
Passwords Overview	2-7
Changing Default Passwords	2-9
Encryption Keys	2-9
Integrity Keys	2-9
Changing Database Passwords	2-9

3 Implementing Symphony Security

Encryption	3-1
------------	-----

4 Appendix A: Symphony Port Numbers

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

5 Appendix B: Key Manager

General Information	5-1
About the Symphony Encryption Key Manager Module	5-1
D-Secure Key Practices	5-1
Key Manager Security Enhancements	5-1
The Encryption Scheme	5-1
Operational Considerations	5-2
Periodic Key Rotation	5-2
Operating Conditions	5-2
Authorizations	5-2
Key Manager Module	5-3
Changing the Pass Phrase	5-3

Custom Legal Notice

Preface

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

Purpose

This document provides security reference and guidance for Oracle MICROS Symphony.

Audience

This document is intended for:

- System administrators installing Symphony
- End users of Symphony

Customer Support

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

<https://support.oracle.com>

When contacting Customer Support, please provide the following:

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

Documentation

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

Revision History

Date	Description of Change
January 2024	Initial publication.
January 2024	Updated Property Ports in the Appendix A: Symphony Port Numbers chapter.
February 2024	Updated Running a Workstation Securely with Windows Standard Users in the Authentication topic.

Date	Description of Change
April 2024	Reorganized, updated, and removed several chapters, topics, and appendices.

1

Simphony Security Overview

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

Basic Security Considerations

The following principles are fundamental to using any application securely:

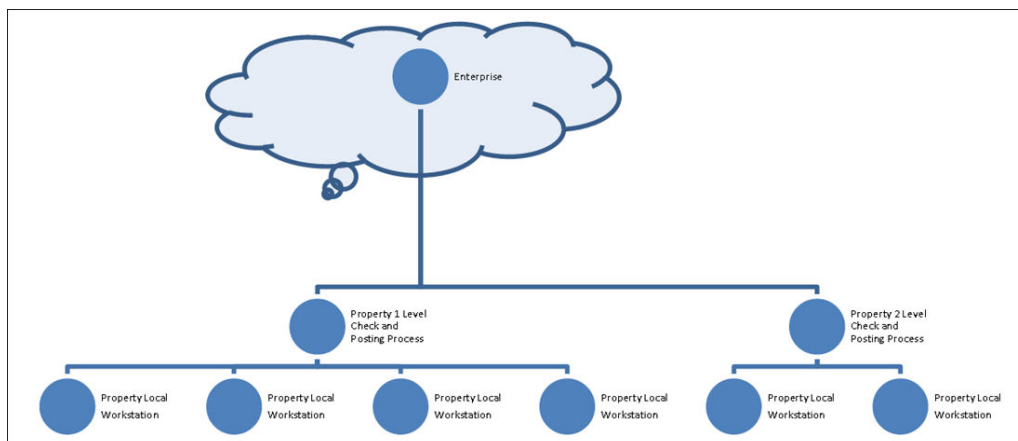
- Install the software securely. For example, use firewalls, secure protocols using TLS (SSL), and secure passwords.
- Learn about and use the Simphony security features. Keep up to date on security information.
- Keep the software up to date by installing the latest product releases and patches as soon as possible. See the Critical Patch Updates and Security Alerts website, located at <http://www.oracle.com/technetwork/topics/security/alerts-086861.html> to access this information.
- Limit user access to necessary job functions. Review user privileges 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.

Service-Oriented Architecture (SOA)

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

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

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

Figure 1-1 Symphony Server-Oriented Architecture

See the [Oracle MICROS Symphony Installation Guide](#), specifically the **Implementation Deployment Scenarios** section for more information.

Authentication

Authentication is the process of ensuring that people on both ends of the connection are legitimate. Authentication is applicable to entities trying to access a service, and entities providing the service.

Enterprise Management Console Authentication

Each user has a unique username and must enter it along with their valid password to access the Enterprise Management Console (EMC). Passwords must adhere to the system's complexity requirements, as follows:

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

Simphony Client Authentication

The Simphony Point of Sale (POS) and Kitchen Display System (KDS) clients connect to the cloud using HTTPS and TLS 1.2.

The software installation process, performed by the Oracle MICROS Client Application Loader application, includes an initial authentication step. This step requires the user to enter their EMC credentials, and if the user has the required privilege to connect a device to the system, the installation process proceeds.

After successful authentication, the cloud service creates a pair of RSA 2048-bit keys and sends the public key to the client. The client uses the public key to create an authentication header used for each message sent to the cloud service. The cloud service uses the corresponding private key to validate message authenticity (i.e.

whether the message was generated by a legitimate client) before processing its contents.

Point of Sale User Authentication

The POS client authenticates users by way of using a numeric value assigned to each user, via one of the following methods:

- Swiping a Magnetic Card
- Tapping a RFID card
- Entering the numbers by using the touchscreen buttons

The POS client also supports fingerprint authentication as either an additional or as the only authentication method. Fingerprint authentication is used either in conjunction with or in place of the numeric value.

Running a Workstation Securely with Windows Standard Users

On workstations running Microsoft Windows, workstations should operate with a Microsoft Windows standard user for daily Symphony client operations, and a separate account used only for the Symphony installations and upgrades with only the minimum required administrative permissions to install software components and Symphony services.

Simphony Installation and Upgrade - Uses the operating system account with only the minimum required administrative permissions to install software components and Symphony services:

In order to successfully install or upgrade Simphony Workstations via CAL client, users need to change the Microsoft Windows user to an administrative Microsoft Windows user prior to any new installation or upgrade of Simphony client via CAL on any Microsoft Windows client devices. This account is a limited administrative account in scope, with only privileges to installing software components which require administrative permissions and registering services.

Daily Operations - Running the Simphony Ops Client using the standard limited operating system user:

After a successful installation and configuration of a service host (Ops), workstations can be run with a Microsoft Windows standard user. Using a standard user minimizes the risk of remote code execution and other exploits.

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

Database User Management

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

Security Note

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

Oracle MICROS Hardware Support Account

A support user account is created during the Oracle MICROS workstation hardware installation process. Securely store the password for this account to prevent unauthorized system access. Only provide this information when necessary to diagnose system issues.

Symphony Transaction Services Gen 2 Authentication

Symphony Transaction Services Gen 2 (STSG2) utilizes the following authentication mechanisms for the following components:

- **STSG2 Human Integrator Authentication** – human integrators authenticate using OpenID Connect (OIDC). For more information on how to create and configure OIDC accounts for human integrators, refer to the *Oracle Cloud Applications* documentation.
- **STSG2 Third-Party Components** – third-party integrator components authenticate through human integrators during installation, after authentication via the OpenID Connect Authorization Code Flow. For more information on how to create and configure OIDC accounts for third-party components, refer to the *Oracle Cloud Applications* documentation.
- **STSG2 Location-Level API Authentication** – the local STSG2 API uses X.509 certificates at the transport level (i.e. TLS v1.2) for server-side authentication. For more information on how to configure these certificates, refer to the *Oracle MICROS Symphony Configuration Guide*.

Understanding the Symphony Environment

When planning your Symphony 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.

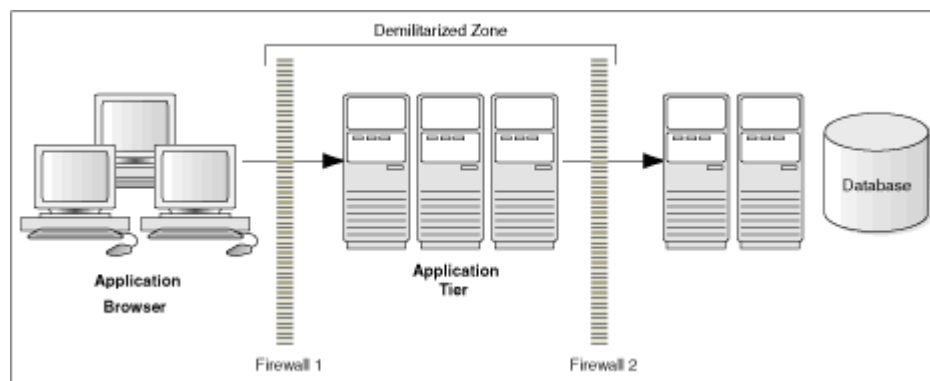
Recommended Deployment Configurations

This section describes recommended deployment configurations for Symphony.

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

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

Figure 1-2 Traditional DMZ



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

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

See [Port Numbers](#) in Appendix A for more information about Symphony network port usage.

Operating System Security

Prior to installing Symphony, it is essential that the operating system be updated with the latest security updates. See the [Oracle Food and Beverage Compatibility Matrix](#) for more information about supported operating systems.

Microsoft Windows-based Symphony point of sale (POS) devices require Certificate Authorities (CAs) certificates from well-known industry vendors to be present in the operating system's **Trusted Root Certification Authorities** certificate store.

These certificates are distributed when the Microsoft Windows Update process is periodically run however, there may be instances where a manual update is needed.

Before upgrading your Microsoft Windows-based POS devices to Symphony 19.6 or later, ensure the Microsoft Windows operating system is up to date and consult your IT support

team to add the **DigiCert Trusted Root G4** certificate in case it is not present in the **Trusted Root Certification Authorities** certificate store.

The **DigiCert Trusted Root G4** certificate can be manually downloaded from: <https://cacerts.digicert.com/DigiCertTrustedRootG4.crt>

Follow your IT team's guidance and the operating system's vendor manual, which covers tasks such as: *Adding Certificates to the Certificates Store on the Client*.

See the following Microsoft TechNet site for more information about operating system security: [Microsoft Windows Server Security](#).

Database Security

Oracle Database

Transparent Data Encryption

The Oracle Database versions supported by Symphony 19.1.x, include Oracle Database 19c, Oracle Database 18c, Oracle Database 12c Release 2, and Oracle Database 12c Release 1. Each version provides Transparent Data Encryption (TDE) capabilities. TDE protects data at rest by way of automatically encrypting/decrypting sensitive data that is stored in tables and tablespaces used by Symphony. Oracle MICROS strongly recommends enabling TDE at the Oracle Database. More information about TDE can be found at:

[Introduction to Transparent Data Encryption for 12c](#)

[Oracle Database Advanced Security Guide for 18c](#)

See the [Oracle Database Security Guide](#) for more information about Oracle Database security.

See [Oracle Database Documentation](#) for detailed information about various releases of Oracle Database.

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

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

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

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

Best Practices

On an installed instance of Microsoft SQL Server Express on the workstation, Oracle Food and Beverage recommends that you apply the latest security updates and critical

updates including general distribution releases (GDRs), service packs (SPs), and cumulative updates (CUs).

Applying Updates

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

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

Source

See [Install SQL Server Servicing Updates](#) for Microsoft recommendations.

Additional Microsoft SQL Server Information

Table 1-1 Microsoft SQL Server 2008 R2

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

Table 1-2 Microsoft SQL Server 2012

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

Database on Linux for MICROS Workstations

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

2

Performing a Secure Symphony Installation

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

Pre-Installation Configuration

Prior to installation of Symphony, perform the following tasks:

- Apply critical security patches and other updates to the operating system.
- Apply critical security patches to the database server application.
- Follow the Microsoft TechNet guidelines to harden the TLS configuration, especially to disable weak TLS 1.2 cipher Suites.
- Review the [Oracle Hospitality Enterprise Back Office Security Guide](#).
- Review the [Oracle MICROS Hardware Wireless Networking Best Practices Guide](#).
- If you are installing Symphony version 19.1 (or earlier), create Oracle Database Tablespaces per the instructions in the [Oracle MICROS Symphony Installation Guide](#). Tablespace requirements may vary based on the customer's specifications.

 **Note:**

Beginning with Symphony version 19.2.1, the installation application automatically creates all necessary Oracle Database Tablespaces.

- Acquire TLS 1.2 compliant security certificate from a valid Certification Authority (CA).

Symphony Installation

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

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

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

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

Required Websites and Services for Simphony

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

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

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

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

Multi-Factor Authentication

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

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

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

Simphony MFA Configuration Prerequisite Requirement

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

Simphony MFA Configuration During the Installation of Simphony

Beginning with the Simphony 18.2 release's installation application, you are prompted to configure MFA. Your choices are:

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

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

Figure 2-1 Symphony Install MFA Configuration

Accessing the Symphony EMC Using MFA for the First Time

To configure MFA on your Symphony system:

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

Your registered email address is written to your EMC employee record. This email address is used to send you the one-time-password (OTP) each time you attempt to log on to the EMC.

3. Access the email account you registered in step 1 and open the email containing the OTP.
4. Enter the temporary password in the **One-Time Password** field and then click **Enter**.

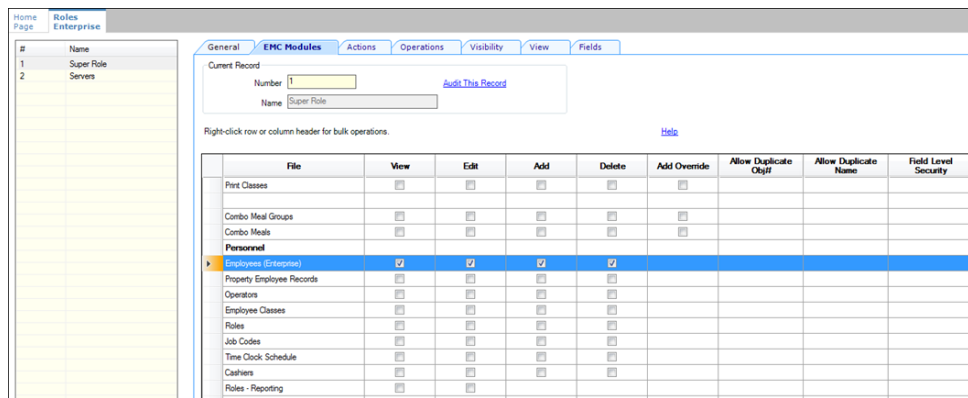
Newly generated OTP passwords expire and become invalid after five minutes. If the OTP's five minute threshold is exceeded, you are required to log in again to the EMC to generate another OTP. After entering a valid OTP, the EMC opens.

Assigning MFA EMC Access Privileges

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

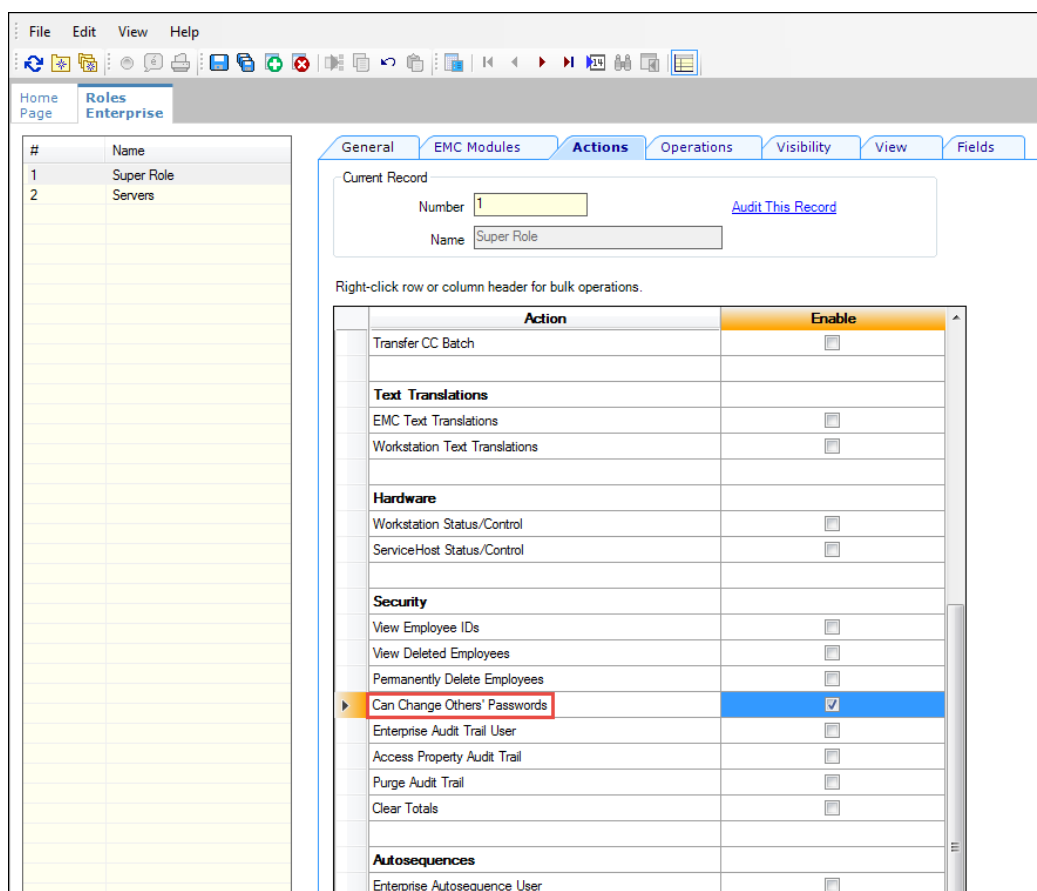
1. Select the **Enterprise** level, click **Configuration**, and then click **Roles**.
2. Click the **EMC Modules** tab and scroll to the Personnel section.
3. Select the check boxes for the **Employees (Enterprise)** access privileges for each of the following columns:
 - View
 - Edit
 - Add
 - Delete

Figure 2-2 Roles Options for Assigning MFA Privileges



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

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



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

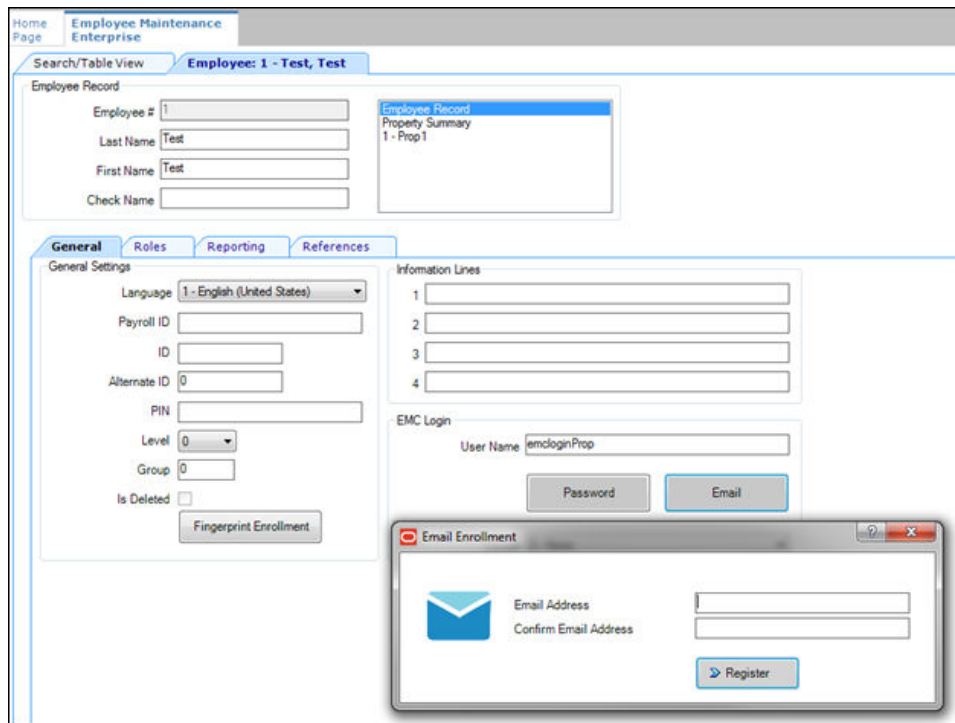
Enrolling Users MFA Email Addresses and Passwords

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

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

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

Figure 2-4 Email Enrollment



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

Post-Installation Configuration

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

Turning Off Remote Assistance

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

Browser Security

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

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

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

Application

Software Patches

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

Security Certificates

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

Database Platform

Ensure that database login auditing is enabled.

Passwords Overview

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

Maintaining Strong Passwords

Ensure that passwords adhere to the following strength requirements:

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

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

 **Note:**

When creating new passwords, they cannot begin with a number, contain an existing username, or include the following special characters:

' \ " (apostrophe, back-slash, and quotation marks)

When entering new usernames or passwords, the EMC validates and returns a message if the potential usernames or passwords are not compatible with the system.

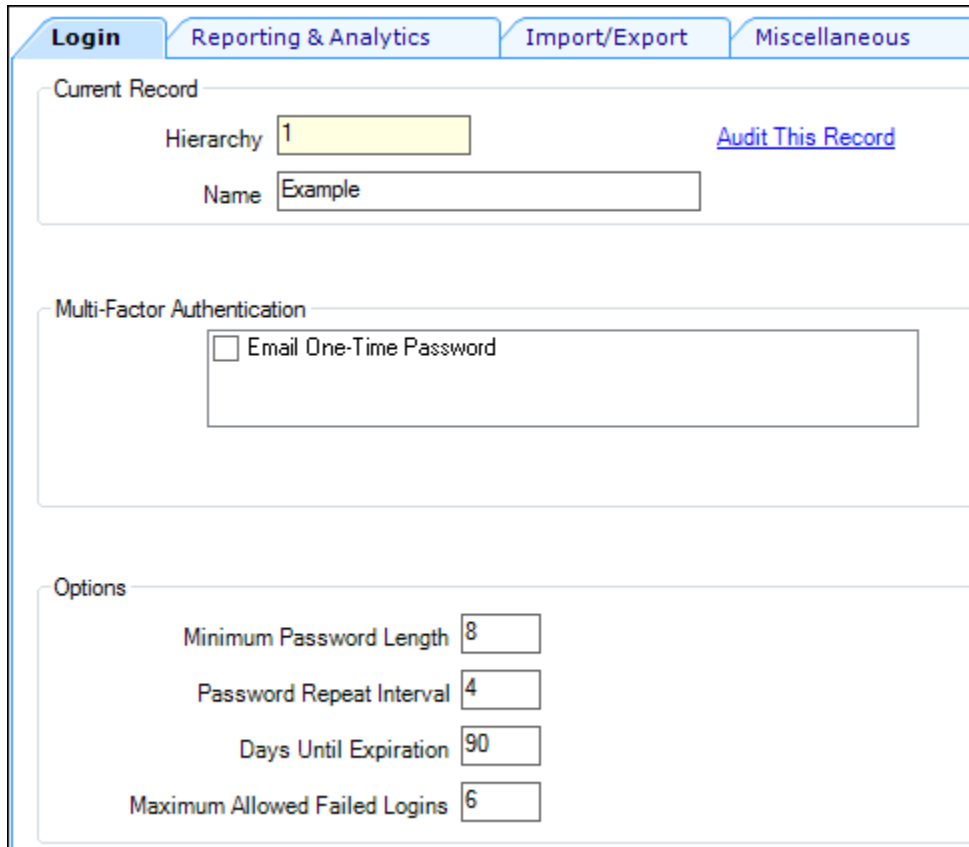
3. The user must not choose a password equal to the last 4 passwords used.

Configuring Passwords for Symphony

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

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

Figure 2-5 Enhanced Password Security



Section	Field	Value
Current Record	Hierarchy	1
	Name	Example
Multi-Factor Authentication	Email One-Time Password	<input type="checkbox"/>
Options	Minimum Password Length	8
	Password Repeat Interval	4
	Days Until Expiration	90
	Maximum Allowed Failed Logins	6

Changing Default Passwords

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

Encryption Keys

Simphony installs an encryption key using a default passphrase. Administrators need to rotate the encryption key on a regular interval. See [Appendix B: Key Manager](#) for more information.

Integrity Keys

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

Changing Database Passwords

Application Server

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

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

Note:

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

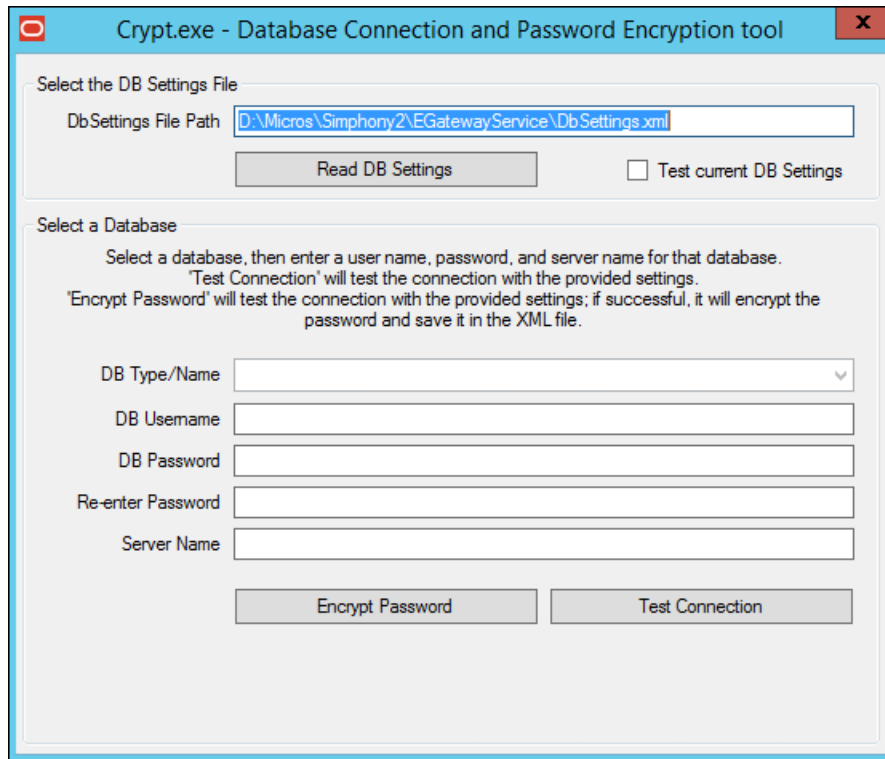
To ensure strict access control of the Simphony application, always assign unique usernames and complex passwords to each account (even if they won't be used), and then disable or do not use the accounts. Oracle Food and Beverage mandates applying these guidelines to not only Simphony passwords but to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

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

To access the Crypt utility:

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

Figure 2-6 Crypt Database Password Encryption Tool



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

- b. To test other database connections, select the database from the **DB Type/Name** drop-down list and then click the **Text Connection** button.

Workstation

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

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

3

Implementing Symphony Security

This chapter reviews Oracle MICROS Symphony security features.

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



Note:

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

Client Data Store Encryption

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

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

Encrypting Data Transmission

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

Key Manager

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

Key Rotation Considerations

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

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

Enabling

For detailed instructions about enabling the Key Manager Module and secure key practices, see [Appendix B: Key Manager](#).

4

Appendix A: Symphony Port Numbers

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

Port Numbers

Access the topic links that include listings of port numbers that can be used in Symphony. 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 4-1 Enterprise Ports

Service	Port Number	Configurable?
Simphony/EGateway (Oracle Database)	1521	Yes
Simphony/EGateway (Pre-Simphony version 2.6)	8050	Yes
Simphony2/EGateway (After upgrade/install of Simphony)	8080\443	Yes
EMC /Remote EMC	443	Yes
Simphony/Reporting and Analytics Advanced	80 – Browser 81–MyLabor Service	Yes
SMTP Service for Email	25	Yes
SMTP Transport Layer Security (TLS)	587	Yes

Property Ports

Starting with Symphony 19.6, a **Secure Port** column is now available from the Symphony EMC modules listed below. ServiceHosts now listen on separate HTTP and HTTPS ports for peer communications.

Access the EMC and then navigate to each module by selecting the following:

- Location, Setup, **Property Parameters**, **Workstations** tab
- Location, Setup, **Workstations**, **Service Host** tab
- Location, Setup, **KDS Controllers**, **Service Host** tab
- Location, Setup, **KDS Controllers**, **Backup Service Host** tab
- Enterprise, Setup, **Service Hosts** module
- Enterprise, Setup, **Interfaces** module

The Secure Port number column is non-configurable by design. You should expect (and allow) increased network traffic from any ServiceHosts assigned to these secure ports.

Table 4-2 Property Ports

Service	Port Number	Configurable?
ServiceHost version 2	HTTP: 8080 HTTPS: 8087	Only HTTP is configurable
ServiceHost as a Service (no Ops)	HTTP: 8071 HTTPS: 8087	Only HTTP is configurable
Print Controller	HTTP: 8080 HTTPS: 8087	Only HTTP is configurable
IP Printer Listening	HTTP: 9100	Yes
Banquet Printing	HTTP: 9100	Yes
KDS Client (Display)	HTTP: 5022	Yes
KDS Controller Service	HTTP: 5023	Yes
KDS Backup Controller Service	HTTP: 5031	Yes
Client Application Loader (server selection screen)	TCP 7300	No
Client Application Loader (property selection screen)	HTTP: 8080	Yes
NetTCPRelayBinding (TMS/Azure)	TCP: 9350, 9351, 9352	No
NetTCPRelayBinding (TMS/Azure)	HTTP: 80	No

 **Note:**

Workstations running Oracle Linux for MICROS are preconfigured with firewall rules, and available ports are limited. If this feature is needed, then the firewall rules must be manually adjusted.

Traffic Note

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

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

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

Interface Ports

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

Table 4-3 Default Interface Port Numbers

Interface	Port Number	Configurable?
Table Management System	5006	Yes
Property Management System	5007	Yes
Credit Authorization	5008	Yes
System Interface Module (SIM)	5009	Yes

iCare/Loyalty Ports

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

Table 4-4 Loyalty Default Ports

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

Oracle Component Ports

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

- [Managing Oracle Database Port Numbers for Oracle Database 18c Release 1](#)
- [Managing Oracle Database Port Numbers for Oracle Database 12c Release 1](#)

See the [Oracle Database 18c Installation Guide](#) for more information about default component port ranges.

5

Appendix B: Key Manager

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

General Information

Access the following links in reference to Key Management.

About the Symphony Encryption Key Manager Module

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

D-Secure Key Practices

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

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

Key Manager Security Enhancements

Symphony 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 an encrypted pass phrase stored in a separate database.

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

The Encryption Scheme

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

Operational Considerations

 **Note:**

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

Periodic Key Rotation

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

Operating Conditions

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

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

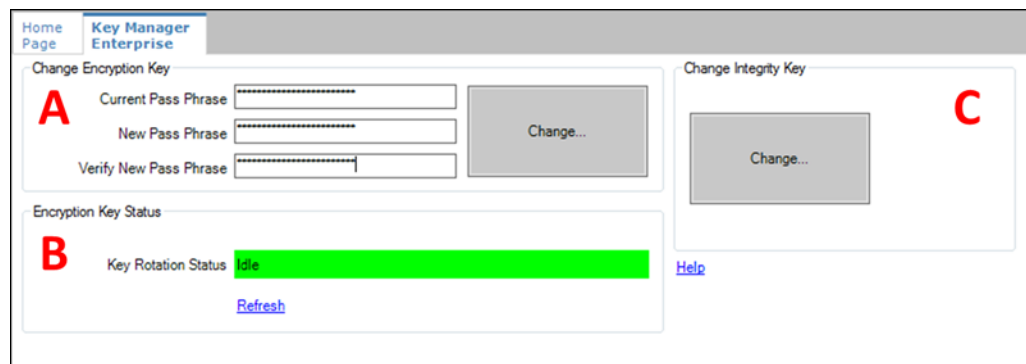
Authorizations

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

Figure 5-1 EMC Enterprise Key Manager Module



The areas of the module are:

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

Area C, the **Change Integrity Key** area, is unrelated to the database encryption pass phrase used to encrypt secure data. The integrity keys are not user-defined.

Changing the Pass Phrase

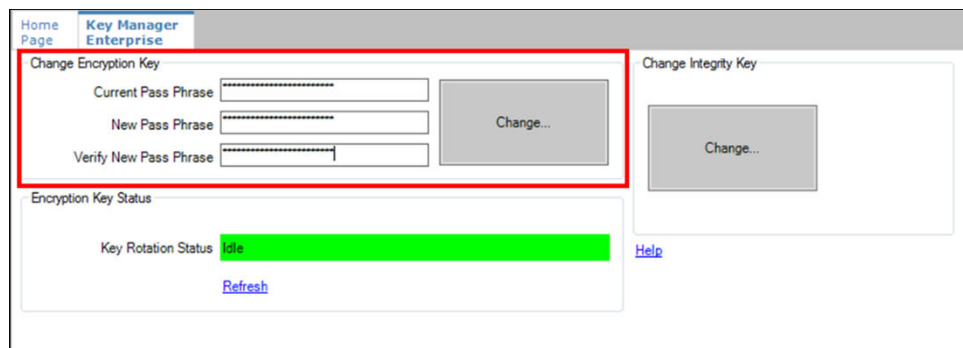
The new pass phrase should adhere to the following rules:

- Contain at least one uppercase alphabetic character
- Contain at least one numeric character
- Contain at least one special character from the following:
!"#\$%&'()*+,-./:;<=>?@[\\]^_`{|~}
- Must use a minimum of twenty characters (maximum of thirty characters)
- Must use a series of words for the pass phrase
 - Must use a minimum of three words
 - Each word must be separated using a space
- Must not use consecutive spaces
- Must be different from the last three previous pass phrases
- The pass phrase and confirmed pass phrases must match
- The transaction database must be accessible
- Must not contain any restricted expressions, company, or product names

 **Note:**

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

Figure 5-2 Key Manager Module - In Progress



The screenshot shows the Key Manager Enterprise interface. The 'Change Encryption Key' section is highlighted with a red box. It contains three input fields: 'Current Pass Phrase', 'New Pass Phrase', and 'Verify New Pass Phrase', each with a masked password field. A 'Change...' button is located to the right of these fields. Below this section is the 'Encryption Key Status' section, which shows 'Key Rotation Status' as 'Idle' in a green bar, with a 'Refresh' button below it. To the right of the 'Change Encryption Key' section is the 'Change Integrity Key' section, which has a 'Change...' button. A 'Home Page' link is visible in the top left corner, and a 'Help' link is visible in the bottom right corner of the 'Encryption Key Status' section.

To change the pass phrase:

1. In the EMC, select the Enterprise level, and then select **Key Manager**.
2. In the Change Encryption Key section, enter the **Current Pass Phrase**, the **New Pass Phrase**, and re-enter the new pass phrase in the **Verify New Pass Phrase** field.
3. Click the **Change...** button.
4. A confirmation prompt appears. Click **Yes** to start the key rotation process.
Another confirmation prompt displays.
5. Click **Yes** if there are no database backups currently in progress.
Backing up the database during the key rotation process can potentially cause the data in the backup database to become out of sync with Symphony.
6. Click **No** if a database backup is currently in progress and begin the key rotation process again after the backup is finished. The **Key Rotation Status** section indicates the task's progress or current status.
7. After the pass phrase has successfully changed, click **OK**.