Oracle® Simphony Essentials
Security Guide

F44999-08
February 2025

Oracle Simphony Essentials Security Guide,

F44999-08

Contents

Preface

The Oracle MICROS Simphony Cloud Service, Essentials Edition, is the point-of-sale solution for small- and medium-sized restaurants.

Purpose

This document provides security reference and guidance for Simphony Essentials.

Audience

This document is intended for:

- Implementation Teams
- System Owners
- End Users

Customer Support

To contact Oracle Customer Support, access the Customer Support Portal at:

https://iccp.custhelp.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
September 2021	Initial publication for Release 19.3
September 2022	Initial publication for Release 19.4.
March 2023	Initial publication for Release 19.5.
January 2024	Initial publication for Release 19.6.
September 2024	Initial publication for Release 19.7.
February 2025	Initial publication for Release 19.8.

1

Simphony Essentials Edition Security Overview

This chapter provides an overview of Oracle MICROS Simphony Essentials 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 Essentials 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.

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 Essentials Client Authentication

The Simphony Essentials 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 for each POS and KDS device. Clients use their unique RSA keys to create an authentication header for each message sent to the cloud service. The cloud service uses the corresponding key to validate message authenticity, for example 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.

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.

Simphony Transaction Services Gen 2 Authentication

Simphony 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, see 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, see the *Oracle Cloud Applications* documentation.
- **STSG2 Location-Level API Authentication**: The local STSG2 API uses X.509 certificates at the transport level (that is, TLS v1.2) for server-side authentication. For more information on how to configure these certificates, see the *Oracle MICROS Simphony Essentials Configuration Guide*.

Authorization

Authorization is the setting of user privileges to determine what users are able to do after accessing a system.

Simphony Essentials handles authorization using a role-based access control (RBAC) mechanism. RBAC defines a set of privileges and actions that can be performed for each role.

Administrators assign one or more roles to each user depending on their specific access requirements to the different features and functions within Simphony Essentials. Follow the principle of “least privilege” when assigning roles to users; in other words, only assign the required roles for their duties.

User privileges are configured in EMC. Refer to the *Oracle MICROS Simphony Essentials Configuration Guide* for more information about creating and assigning roles to Simphony Essentials users.

Logging and Auditing

Simphony Essentials keeps a chronological record of system changes and other events, such as successful and failed logins to the EMC, in the Audit Trail module within the EMC. This logging behavior is enabled by default and does not require additional configuration.

Use the Audit Trail module to view and search log records at any time.

Refer to the *Oracle MICROS Simphony Essentials Configuration Guide* for more information about logging and auditing.

Encryption

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

Point of Sale clients provide end-to-end encryption of sensitive information by using a combination of asymmetric (that is, RSA-2048) and symmetric (that is, AES-256) encryption schemes. Only the Simphony Cloud Service, Essentials Edition, can decrypt the data after it arrives securely in the data center.

Simphony Essentials encrypts all cloud communications using HTTPS and TLS 1.2.

Client Operating System and Database Security Updates

Oracle Linux for MICROS hardware receives operating system updates directly from the Oracle MICROS Simphony Cloud Service. After each cloud update, update the on-premise hardware as soon as possible to ensure the updates are applied.

2

Configure Workstation Database Passwords

To maintain workstation database access control, you must assign unique usernames and complex passwords in the Simphony EMC.

See Configure Workstation Database Passwords in the *Oracle MICROS Simphony Essentials Configuration Guide* for more information about configuring workstation database passwords.

3
Simphony Port Numbers

Many port numbers are configurable in the EMC. Open only the minimum required ports based upon the installation type and deployment configuration. Refer to the following tables:

Table 3-1 Enterprise Ports

Service	Port Number
Simphony Cloud (EMC/POS)	443
Reporting and Analytics	443
Labor Management	443

Table 3-2 Property Ports

Service	Port Number
Point of Sale Client	8080
IP Printer Listening	9100
KDS Client (Display)	8080
KDS Controller Service	8080
Client Application Loader (Server Selection Screen)	TCP 7300
Client Application Loader (Property Selection Screen)	8080

4 Disabling USB Ports

Locking down the USB ports on the Oracle MICROS Hardware provides additional protection from unwanted intrusions.

Follow these directions to disable unnecessary USB ports:

Workstation 600 Series

1. Press the **F2** key while the workstation is starting up to enter the BIOS/Setup screen.
2. Navigate to and select the **Advanced** tab.
3. Select **Special Configuration**.
4. Select the desired **USB port**.
5. Press **Enter**, scroll up to **Disabled**, and then press **Enter** again to select it.
6. Press the **F10** key to save and exit.

Workstation 310

1. Press the **F2** key while the workstation is starting up to enter the BIOS/Setup screen.
2. Select **Special Configuration**.
3. Select the desired **USB port** from the drop-down list, and then select **Disabled**.
4. Click **Save**.
5. Confirm the save by clicking **Yes** from the Setup Confirmation prompt.

5

Secure Communications for Simphony Payment Interface

The Simphony Payment Interface (SPI) is a set of messages exchanged between the Simphony Transaction System and Payment Service Providers (PSPs). The purpose of the interface is to securely collect electronic payments, keeping the transaction system free of Payment Card Industry (PCI) data.

Simphony configurations must use a secure channel to communicate with PSPs. The level of security varies depending on the provider. The following list contains more information about secure communications with PSPs:

- **Without TLS Support**: Simphony communicates with the PSP by using a standard HTTP connection without encryption. In addition to using this configuration, other compensating controls (such as Microsoft NT LAN Manager) can be used to secure the network channel.
- **With TLS Support**: This configuration type has two options:
  - **Without Certificates**: The communication is secure, but the PSP does not provide a certificate and the client cannot validate the server private key.
  - **With Certificates**: Certificates are used to validate the server public key. The following certificate types are used by PSPs:
    - Certificates from a known Certificate Authority
    - Self-signed certificates
    - A provided .cer file

TLS Client Certificate Support

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

Certificate Handling by PSPs outside the scope of Client Certificates are known as .pfx files. They contain both private and public keys, along with a password to access the file. This file is sensitive and must be handled securely.