Oracle® MICROS Enterprise Back Office

Security Guide

Release 20.1
F17863-04
April 2024

Oracle MICROS Enterprise Back Office Security Guide, Release 20.1

F17863-04

Contents

Preface

This document provides security reference and guidance for the following Oracle MICROS Enterprise Back Office products:

- Reporting and Analytics
- Gift and Loyalty
- Labor Management
- Forecasting and Budget
- InMotion Mobile (server-side security)
- Oracle Payments Cloud Service

This document does not include information specific to Inventory Management.

Audience

This document is intended for the following audience:

- Datacenter administrators
- Database administrators
- Professional services

Customer Support

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

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
- Screenshots of each step you take

Documentation

Oracle MICROS product documentation is available on the Oracle Help Center at http://docs.oracle.com/en/industries/food-beverage/.

Revision History

Date	Description of Change
October 2020	Initial publication.
September 2023	Updated Preface.
April 2024	Added Secure Protocols.

1

Security Considerations

This section lists security considerations for Enterprise Back Office user types.

Considerations for Administrators and Application Users

Keep the following in mind when administering and using applications:

- 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.
- When done using an application, log off before closing the browser session.
- Reporting and Analytics uses cookies to improve the application experience by remembering visits and activity. If you disable cookies, you will have to enter your user name and enterprise name each time you login, you will not be redirected to the last page you were working on when you login, you may have to sign in more often, and in some cases you may not be able to login.
- Keep up to date with GDPR information at https://support.oracle.com/epmos/faces/DocumentDisplay?id=114.2.

Considerations for Developers

For clients that call web services hosted by Oracle, use Transport Layer Security (TLS) 1.1 or above to avoid man-in-the-middle attacks. Web client developers should enforce encrypted data transport when the application transports sensitive data and should validate that all certificates are legitimate and signed by public authorities.

Restrict ciphers to modern implementations.

Secure Protocols

SSH Protocol

Secure Shell (SSH) protocol allows secure connections between (remote) devices using public key cryptography (PKC).

Oracle Security Technology Standards-approved SSH cipher suites (key exchange, symmetric encryption, MAC, host key algorithms) are used by Enterprise Back Office products when negotiating connections to customer or third-party SFTP services.

Supported Cipher Suite

The ciphers in the table are supported in the following Enterprise Back Office product suite releases:

- Reporting and Analytics starting from 20.1.15 release.

- Inventory Management starting from 9.1.37 release.

New cipher additions in these releases are noted with an asterisk (*).

Category	Cipher/Algorithm (Alternate) Names
Key Exchange (KEX)	• curve25519-sha256 (curve25519-sha256@libssh.org)* • curve448-sha512* • diffie-hellman-group14-sha256* • diffie-hellman-group15-sha512* • diffie-hellman-group16-sha512* • diffie-hellman-group17-sha512* • diffie-hellman-group18-sha512* • ecdh-sha2-nistp256 • ecdh-sha2-nistp384 • ecdh-sha2-nistp521 • diffie-hellman-group-exchange-sha256
Server Host Key Algorithms	• ssh-ed25519 (ssh-ed25519-cert-v01@openssh.com)* • ecdsa-sha2-nistp384 (ecdsa-sha2-nistp384-cert-v01@openssh.com) • rsa-sha2-512 (rsa-sha2-512-cert-v01@openssh.com)* • rsa-sha2-256 (rsa-sha2-256-cert-v01@openssh.com)* • ecdsa-sha2-nistp256 (ecdsa-sha2-nistp256-cert-v01@openssh.com) • ecdsa-sha2-nistp521 (ecdsa-sha2-nistp521-cert-v01@openssh.com)
Symmetric Encryption	• chacha20-poly1305@openssh.com* • aes256-gcm (aes256-gcm@openssh.com)* • aes128-gcm (aes128-gcm@openssh.com)* • aes256ctr • aes192ctr • aes128ctr
Message Authentication Code (MAC)	• hmac-sha2-512-etm@openssh.com* • hmac-sha2-256-etm@openssh.com* • hmac-sha2-512* • hmac-sha2-256*

Weak, Deprecated Cipher Suites

The table includes weak or deprecated ciphers that were supported in the following Enterprise Back Office product suite releases:

- Reporting and Analytics releases from 20.1 to 20.1.14
- Inventory Management releases from 9.1 to 9.1.36

These ciphers will not be supported in future releases.

Category	Cipher/Algorithm (Alternate) Names
Key Exchange (KEX)	• diffie-hellman-group1-sha1 • diffie-hellman-group14-sha1 • diffie-hellman-group-exchange-sha1
Server Host Key Algorithms	• ssh-rsa (ssh-rsa-cert-v01@openssh.com) • ssh-dss
Symmetric Encryption	• aes128-cbc • aes192-cbc • aes256-cbc • blowfish-cbc • 3des-cbc • 3des-ctr • arcfour • arcfour128 • arcfour256
Message Authentication Code (MAC)	• hmac-md5 • hmac-sha1-etm@openssh.com • hmac-sha1 • hmac-md5-96 • hmac-sha1-96