Oracle Warehouse Management Cloud

Technical Requirements Guide

Release 25C

Oracle Warehouse Management Cloud
Technical Requirements Guide

Release 25C

G34760-02

Author: Oracle WMS Cloud Product Team

Contents

Get Help

There are a number of ways to learn more about your product and interact with Oracle and other users.

Get Help in the Applications

Access the online help from the user drop-down menu in the Warehouse Management application.

Get Support

You can get support at *My Oracle Support*. For accessible support, visit *Oracle Accessibility Learning and Support*.

Get Training

Increase your knowledge of Oracle Cloud by taking courses at *Oracle University*.

Join Our Community

Use *Cloud Customer Connect* to get information from industry experts at Oracle and in the partner community. You can join forums to connect with other customers, post questions, and watch events.

Learn About Accessibility

For information about Oracle's commitment to accessibility, visit the *Oracle Accessibility Program*. (if videos) Videos included in this guide are provided as a media alternative for text-based topics also available in this guide.

Share Your Feedback

We welcome your feedback about Oracle Warehouse Managment. If you need clarification, or find an error, you can direct your questions via a service request to *My Oracle Support.*

2 Data Retention and Purging

Data Retention and Purging

WMS transactional data (such as orders, shipments, inventory etc.) are normally retained for at least 12 months. Beyond that time frame, data that has been “processed” may be purged from the WMS database, to better manage system performance.

- “Processed” refers to data in statuses such as “Shipped”, “Completed”, “Canceled” etc. where no further processing is possible
- Unprocessed data (such as open orders or unused inventory) is never purged regardless of the time frame
- Since WMS is an execution system, with transactional data generally created by external systems such as ERPs, and interfaced into WMS, there is no archiving of purged data. Customers wanting to save such data can use the multiple data extraction mechanisms to extract and save the data. Refer to the WMS Data Extraction Guide.
- Note that there are many internal tables in which WMS creates records during normal processing, that are automatically purged on a more frequent basis. Users normally never see this data. These are unrelated to WMS transactional entities like orders, shipments, inventory etc.

3 Network Requirements

Network Requirements

As a cloud SaaS application, Oracle® Fusion Cloud Warehouse Management, formerly LogFire, is accessed over the internet. Adequate bandwidth is required to provide a responsive experience. Bandwidth requirements vary based on the volume at a client site. Bandwidth is not the only determining factor for application responsiveness. Among other factors, network related items such as latency and reliability of the network service may affect the application response.

To calculate the bandwidth required at a site, the determining factors are the number of users at the site, split into number of RF device users and number of Desktop Web interface users. This information will be used by Oracle Warehouse Management (WMS) Cloud to recommend a bandwidth for the site. To provide some rough guidance, we recommend a minimum of 1.5Mbps dedicated and that can support about 60 users (45 RF and 15 Desktop UI). Even if user counts are lower than that, we do not recommend going below this minimum bandwidth at a site.

Dedicated Bandwidth

- Shared non-commercial internet services such as cable internet or DSL are not recommended.
- The bandwidth should be primarily allocated for WMS, and not shared for other purposes, so that, for example a laptop user on the same Wi-Fi network playing streaming music or video does not affect the bandwidth available to the WMS. Ideally, the RF Wi-Fi network should not be used for other purposes.

4 Hardware

Hardware

The following section describes the various hardware devices used by end users to access the Oracle Warehouse Management Cloud application or devices that are accessed by the application.

> **Note:** The customer IT department is responsible for setting up and configuring these. For testing purposes, and with each monthly update, the customer is responsible for keeping their 3rd party hardware and software up-to-date.

Desktop PCs

Oracle Warehouse Management Cloud provides a Desktop Web Interface to access the application. Any recent computer running Windows, Mac OS X, or Linux with a modern browser is supported. A minimum browser resolution of 1440x900 is recommended. The application will work at lower resolutions but screen layout may be sub-optimal. A resolution of 1920x1080 will provide a much better experience.

The following browser versions were used for testing WMS Cloud version 25A:

- Chrome 129
- Firefox 131
- Edge 131
- Safari 18.1

Earlier versions of these browsers, especially within the past 12 months, should mostly work fine. Issues found using these versions will likely not be fixable and the customer may be asked to switch to a supported one.

For more information see *Oracle Fusion Cloud Applications System Requirements*.

RF Devices

> **Note:** This section is for the legacy RF application that will be soon retired. Redwood Mobile is our modern graphical mobile solution that new customers should start with. See the Redwood Mobile WMS section.

Oracle Warehouse Management Cloud supports a handheld RF (Radio Frequency) device interface to access the Mobile RF terminal based application. The basic requirement for these devices are:

- Should have a Secure Shell (SSH) app that can connect via secure encrypted SSH protocol to any configurable port number
- Capable of supporting vt100 terminal emulation

- Ability to display at least 24 characters by 16 lines of text, preferably 29 x 19
- A physical keyboard should have separate alpha and numeric keys with support for Control keys

Typical RF Devices used in warehouses these days run the Android operating system. WaveLink, Termius, Velocity, some SSH applications used by Oracle Cloud WMS customers, and others can be used as well.

We recommend using a device running newer versions of Android, to also be compatible with the new Redwood Mobile appsolution. For new implementations, we recommend using Redwood Mobile WMS over the legacy RF application. Please see the Redwood Mobile WMS section for more details.

SSH Apps

> **Note:** SSH apps may not be included with the RF Device and may need to be bought separately. The RF Device vendor may offer other SSH apps. SSH apps should be compatible with the following mentioned Ciphers, keys, and algorithms.

Ciphers	Key Exchanges	Macs	Host Ke
aes256-gcm	*ecdh-sha2-nistp256*	hmac-sha2-256-etm	rsa-sha2
aes256-ctr	ecdh-sha2-nistp384	hmac-sha1-etm	rsa-sha2
aes256-cbc	ecdh-sha2-nistp521	hmac-sha2-512-etm	ecdsa-sh
aes128-gcm	diffie-hellman-group-exchange-sha256	hmac-sha2-256	
aes128-ctr	diffie-hellman-group14-sha256	hmac-sha1	
aes128-cbc	diffie-hellman-group16-sha512	hmac-sha2-512	
	diffie-hellman-group18-sha512		

- A device without a physical keyboard, using only an on-screen keyboard will have severe limitations in functionality and performance, when used with the Mobile RF WMS application. The Control key is required. The standard on-screen keyboards may not expose this key and third party software keyboards may need to be installed. Even with that, it will be quite inefficient to use an on-screen keyboard.

> **Note:** WebRF isn't intended to be a production or high volume solution for RF. It's designed for testing purposes *only*. Customers using WebRF for testing should use Redwood Mobile WMS. WebRF will be retired soon.

Connection Stabilizing Software

Some customers have used connectivity stabilizing software to handle spotty WiFi in warehouse where the handheld device connects to the connection stabilization software, which in turn connects to Oracle WMS Cloud. Oracle does not test or certify such solutions and customers would be responsible for making sure it performs per their needs. Oracle will not be able to debug any issues related to such software.

Computers

To access the RF application from a desktop or laptop, PuTTY is typically used.

> **Note:** The devices and applications mentioned here are for reference. The customer is responsible for acquiring proper licenses etc, if any, as may be required.

Redwood Mobile WMS

Built using Oracle's latest mobile application technology, VBCS (Visual Builder Cloud Service), the Redwood Mobile WMS application features modern, graphical, mobile screens that can display images, capture photos, and scan barcodes using either the device camera or integrated scanners.

Originally released as Android and iOS apps, Redwood Mobile WMS has been converted to a progressive web application (PWA). PWA applications run using browser technology but still have the advantages of mobile apps in being able to access device features like cameras. They also have the flexibility of web applications since they can be directly downloaded and installed, without going through an app store. Updates can be provided more frequently.

Redwood Mobile WMS will run on mobile devices based on Android and iOS, as well as on desktop systems like Windows and Mac (works best on Chrome). The PWA is accessed via a URL that is available in the main web application. They can be installed on the device home screen similar to a traditional app.

Android

- Android 13 or newer is required
- Works on regular Android phones and ruggedized Android warehouse devices

iOS

- iOS 16 and higher is recommended but may work on older versions

Additional Notes

- Each WMS environment has a different URL for the PWA, and can be installed as separate apps, one per environment. The user has the ability to customize the name for the app icon.
- Barcode scanning using the camera works on both Android and iOS devices, but is optimized for Android in terms of performance. It may be slightly slower in iOS. This is due to PWA technical limitations of the platform.
- Barcode scanning with a scanner (attached or integrated) gives the best performance. This works equally well on Android and iOS.
- The app supports both single and multi-field barcodes using the existing configuration available in the WMS Cloud service.
  - The app can use the device's camera to scan barcodes or can also work with a barcode scanner attachment that converts the barcode into keyboard input.
- The app supports the same literals and language translation configuration and features available with the WMS Cloud web UI and the text based Mobile RF.
- The app supports display and upload of images.
  - The app layout is optimized for phone sized screens rather than tablet sized screens.

Label Printers

Oracle Warehouse Management Cloud supports the Zebra Printing Language (ZPL). Printers manufactured by Zebra as well as many other companies that support the ZPL printing language should work. The customer is required to test and verify that label printing works as expected. Some typical models in use by some customers are Zebra / ZM400, Zebra 105SL, Zebra R110Xi4 and INTERMEC /PD42.

The Oracle Warehouse Management Cloud application prints to label printers at customer locations via network access that must be configured as described in *Network Configuration*. These printers must be configured in the Oracle Warehouse Management Cloud application.

Laser Printers

Report documents are typically generated as a PDF by the Oracle Warehouse Management Cloud application desktop web interface and can be printed to a local printer by the user. As such these printers typically do not need to be configured in the Oracle Warehouse Management Cloud application.

If the ability to print certain PDF documents from the handheld RF interface is used, then laser printers also need to be setup in the application and accessed by the Oracle Warehouse Management Cloud application over the network similar to label printers.

Dot Matrix Printers

These are used for certain shipping documents such as GDD documents common in South American countries. These must be setup as network accessible printers similar to laser printers. Printers that support the ESC-P language are supported. Some sample models used by current clients are:

- PRINTRONIX/P7220
- EPSON / DFX 9000
- EPSON / FX890
- OKI/Pacemark 4410

Print Servers

We recommend that clients use a print server to manage printers that the Oracle Warehouse Management Cloud application needs to access. Printers connected to an external dedicated print server (typically a Windows Server or a Linux Server) are more robust and can handle larger volumes of labels. Printers that use a built in print server (network card or dongle) may have trouble with higher volumes and may have issues with lost labels or repeated labels etc.

Users should base printing choices on the expected volume and type of use. For example, if they are going to routinely print dozens or hundreds of labels at a time from the wave, they should have a dedicated print server to avoid problems. In addition, print servers avoid the need to have multiple public IP addresses for printers.

> **Note:**
>
> - It is also possible for WMS Cloud to directly communicate with individual printers without a print server. The process for setting this up is basically the same as with a print server as long as each printer has a unique public IP address. This is only recommended for smaller sites that may have just one or two printers.
> - Print requests from WMS Cloud will originate from certain IP addresses (or a range), and this can be used by customers to control access to their printer servers or printers.

Network Configuration

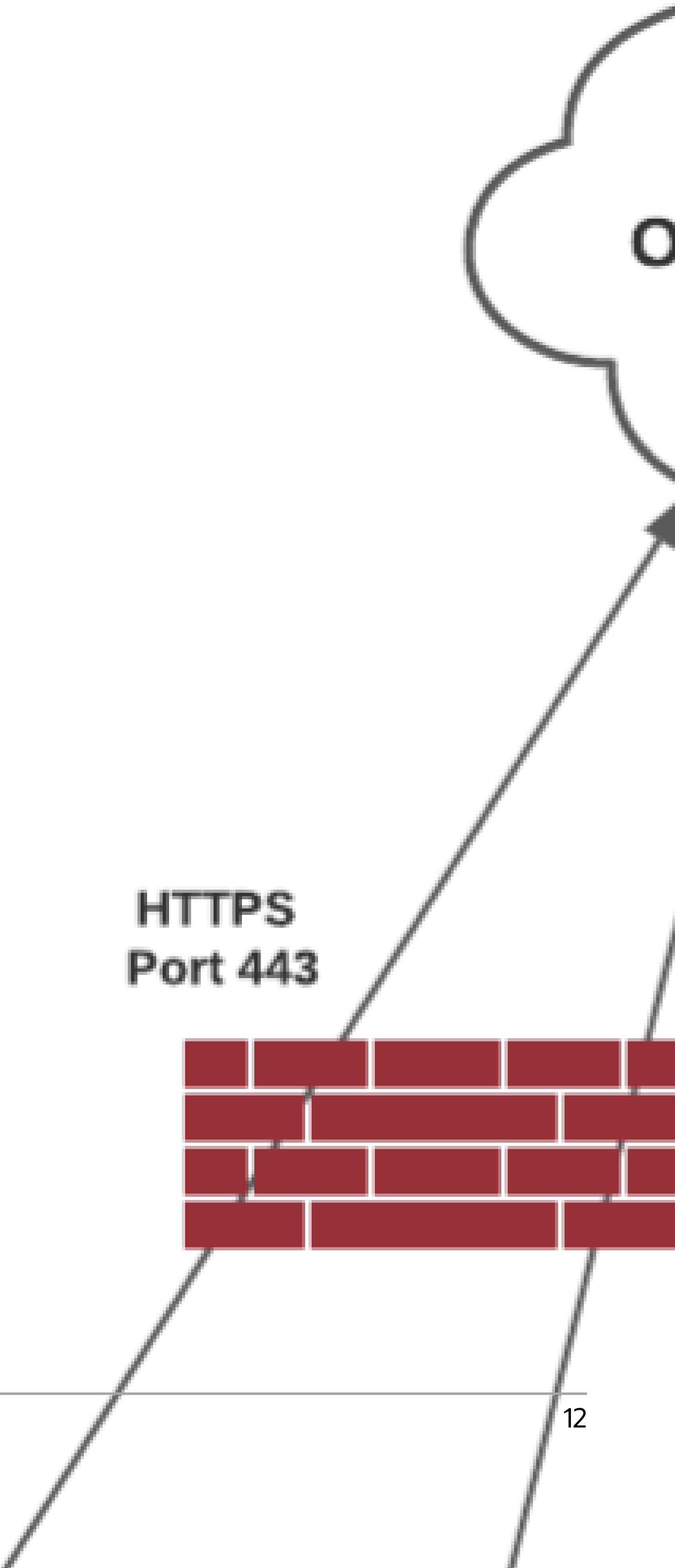
The following diagram describes a typical configuration of how the various hardware devices in a facility running the Oracle Warehouse Management Cloud application access the Oracle Warehouse Management Cloud application. WMS Cloud can be setup to communicate to printers via HTTPS, LPD, or Socket protocols.

Access to Printers

Customers will need to allow access from WMS Cloud to their printers. WMS Cloud publishes IP addresses from which print requests will originate. Customers can configure this on their firewalls to selectively allow access. Using one print server handling multiple printers will usually be easier for network administrators to manage.

Secure Printing

WMS Cloud supports HTTPS as a communication protocol for printing. Customers wanting to encrypt the data being sent from WMS Cloud to their printers can use this option.



O
HTTPS
Port 443

5 Interfaces

Interfaces

Oracle Warehouse Management Cloud supports multiple standard communication mechanisms in addition to client specific custom ones. Standard data formats are XML and flat files. Standard communication methods are Web Services (XML data) or secure FTP (SFTP) for XML or flat files.

> **Note:** To access the latest Interface Specifications, go to the *Oracle WMS Cloud Information Center* From the top of the page, click on the **Documentation** tab at the top, then click the link under **Current Documentation.**

> **Note:** WMS Cloud no longer hosts an SFTP site, though it has the capability to get and put files from and to an external SFTP site via scheduled jobs.

The following table lists the supported Ciphers, Key Exchange Algorithms, Digests and Host Key Algorithms:

Supported Options in SFTP Output Interface

Ciphers	Key Exchanges	Macs	Host Ke
aes128-ctr	curve25519-sha256	hmac-sha2-256	ssh-ed2
aes192-ctr	ecdh-sha2-nistp256	hmac-sha2-512	ecdsa-sh
aes256-ctr	ecdh-sha2-nistp384	hmac-sha2-256-etm	ecdsa-sh
aes128-cbc	ecdh-sha2-nistp521	hmac-sha2-512-etm	ecdsa-sh
aes192-cbc	diffie-hellman-group16-sha512	hmac-sha1	ssh-rsa
aes256-cbc	diffie-hellman-group-exchange- sha256	hmac-md5	ssh-dss
3des-cbc	diffie-hellman-group14-sha256	hmac-sha1-96	ssh-rsa-
rijndael-cbc	diffie-hellman-group-exchange- sha1	hmac-md5-96	ssh-dss-
aes128-gcm	diffie-hellman-group14-sha1	umac-64	ssh-ed2
aes256-gcm	diffie-hellman-group1-sha1	umac-128	ecdsa-sh
chacha20-poly1305	diffie-hellman-group18-sha512	hmac-sha1-etm	ecdsa-sh
		hmac-sha1-96-etm	ecdsa-sh
		hmac-md5-etm	
		hmac-md5-96-etm	

Note:

1. The host key types "rsa-sha2-512" and "rsa-sha2-256" are additionally supported from 23C onward.
2. The cipher "blowfish-cbc" is not supported.

REST WebService XML Payload Size: We recommend XML payloads no larger than 10MB, and preferably less than 5MB, to minimize performance issues. You can achieve this by splitting a data payload into multiple requests. Multiple interface requests can be made in parallel, but we recommend less than 10 simultaneously. The size of output interface payloads sent via REST WebServices can be controlled via the data filtering feature in output interfaces config. Payload limits on the output side, are more dictated by the target system, however there is a hard limit of 20MB in WMS Cloud and it is recommended that payloads be no larger than 10MB.

All languages are supported. We recommend that you use Web Services rather than SFTP as it offers several advantages. It is recommended that UTF-8 encoding is used for data in order to have the widest language compatibility, but other encodings are supported as well such as latin-1 (for western European languages only).

Whichever encoding is chosen must be configured in the Oracle Warehouse Management Cloud system so that data is interpreted accurately. If you have further question please contact The *Oracle Warehouse Management Cloud services and support team*.

6 Authentication

Authentication

Oracle WMS Cloud includes a built-in authentication mechanism using with users can be setup with their own user-id and passwords to access the WMS Web UI, WMS Cloud Mobile App and Mobile RF applications. In addition, it also supports authenticating users against external identity providers (IDP) such as Oracle IDCS or Microsoft Azure AD. It supports multiple authentication mechanisms:

- SAML2 Single Sign On, or SSO in short
  - A web-based authentication standard that can be used only to login to the WMS Web UI
- OAuth2
  - Another authentication standard that can be used for the WMS Web UI, the WMS Cloud Mobile App and Mobile RF.

For more information, refer to the *SSO and Alternate Authentication Setup Guide.*

API Authentication

Incoming REST APIs support the following authentication methods:

- basic auth (username and password)
- simple token based authentication
- OAuth2 token based authentication (for grant types ROPC and Authorization Code to obtain a token)

There are also API related permissions to be setup within the WMS that controls the ability to read, modify or delete data.

Outgoing REST API’s support only basic auth. Outgoing touch points can also be configured to send the payload to external SFTP or SFTP sites.