Oracle® Retail Brand Compliance Management Cloud Service

Release Readiness Guide

Release 25.1.301.0
G36789-01
July 2025

Oracle Retail Brand Compliance Management Cloud Service Release Readiness Guide, Release 25.1.301.0

G36789-01

Contents

Preface

This guide outlines the information you need to know about Oracle Retail Brand Compliance Management Cloud Service new or improved functionality in this update, and describes any tasks you might need to perform for the update. Each section includes a brief description of the feature, the steps you need to take to enable or begin using the feature, any tips or considerations that you should keep in mind, and the resources available to help you.

Audience

This document is intended for the users and administrators of the Oracle Retail Brand Compliance Management Cloud Service.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

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
- Screen shots of each step you take

Oracle Help Center (docs.oracle.com)

Oracle Retail product documentation is available on the Oracle Help Center at https://docs.oracle.com/en/industries/retail/index.html.

(Data Model documents can be obtained through My Oracle Support.)

Comments and Suggestions

Please give us feedback about Oracle Retail Help and Guides. You can send an e-mail to: retail-doc_us@oracle.com

Oracle Retail Cloud Services and Business Agility

Oracle Retail Brand Compliance Management Cloud Service is hosted in the Oracle Cloud with the security features inherent to Oracle technology and a robust data center classification, providing significant uptime. The Oracle Cloud team is responsible for installing, monitoring, patching, and upgrading retail software.

Included in the service is continuous technical support, access to software feature enhancements, hardware upgrades, and disaster recovery. The Cloud Service model helps to free customer IT resources from the need to perform these tasks, giving retailers greater business agility to respond to changing technologies and to perform more value-added tasks focused on business processes and innovation.

Oracle Retail Software Cloud Service is acquired exclusively through a subscription service (SaaS) model. This shifts funding from a capital investment in software to an operational expense. Subscription-based pricing for retail applications offers flexibility and cost effectiveness.

1 Feature Summary

This chapter describes the feature enhancements in this release.

Noteworthy Enhancements

This guide outlines the information you need to know about new or improved functionality in the Oracle Retail Brand Compliance Management Cloud Service update and describes any tasks you might need to perform for the update. Each section includes a brief description of the feature, the steps you need to take to enable or begin using the feature, any tips or considerations that you should keep in mind, and the resources available to help you.

> **Note:**
>
> Where new fields, User Interface (UI) changes, or glossary entries are introduced as part of a change, the portal owner may need to apply their own translations of the core system text.

Column Definitions

- **Feature:** Provides a description of the feature being delivered.
- **Module Impacted:** Identifies the module impacted associated with the feature, if any.
- **Scale:** Identifies the size of the feature. Options are:
  - **Small:** These UI or process-based features are typically comprised of minor field, validation, or program changes. Therefore, the potential impact to users is minimal.
  - **Medium:** These UI or process-based features are typically comprised of field, validation, or program changes. Therefore, the potential impact to users is moderate.
  - **Large:** These UI or process-based features have more complex designs. Therefore, the potential impact to users is higher.
- **Delivered:** Is the new feature available for use immediately after upgrade or must the feature be enabled or configured? If no, the feature is non-disruptive to end users and action is required (detailed steps below) to make the feature ready to use.
- **Customer Action Required:** You must take action before these features can be used. These features are delivered disabled and you choose if and when to enable them.

Table 1-1 Noteworthy Enhancements

Feature	Module Impacted	Scale	Delivered	Customer Action Required?
Supplier and Site Address Validation	Supplier	Small	No	Yes

Table 1-1 (Cont.) Noteworthy Enhancements

Feature	Module Impacted	Scale	Delivered	Customer Action Required?
Ability for Retailer to Supplier Authorize Specifications	Product	Small	No	Yes
Project and Activity API Updates	Process	Medium	No	Yes

Supplier and Site Address Validation

Currently there is no validation of Supplier and Site addresses and phone numbers, meaning that this information is often not completed. This enhancement allows validation to be applied when the supplier is confirming that their details are up to date, making the fields mandatory.

The validation is optionally applied by three new system parameters, providing control over which of the individual address and phone number fields are to be mandatory when the *Confirm Details* action is used on the Supplier or Site record.

By default, in a new portal and in an upgraded portal, the system parameters will not be set, meaning that the mandatory validation will not be applied. Clients can choose to set the parameters to enable the validation. See Post Release Tasks.

The new system parameters are:

- The *Supplier & Site Local Address Validation* parameter allows selection of which of the Address fields mandatory validation is to be applied: Country, Address Line 1, Address Line 2, Address Line 3, Address Line 4, Post Code, GPS.
- The *Supplier & Site Business Language Address Validation* parameter allows selection of which of the Business Language Address fields mandatory validation is to be applied: Country, Address Line 1, Address Line 2, Address Line 3, Address Line 4, Post Code.
- The *Supplier & Site Phone Mandatory* parameter allows mandatory validation to be applied to the Phone fields.

If any of the selected fields fail the mandatory validation, the *Confirm Details* action will not take effect.

Ability for Retailer to Supplier Authorize Specifications

In certain circumstances, it is necessary for the retailer to be able to authorize Product Specifications on behalf of the Supplier, without the need to log on as a supplier user; for example, when it is necessary to progress a Specification rapidly, and the supplier themselves cannot do so, or in the case of retailer-managed Specifications, such as store-made products, where the retailer is the supplier.

This enhancement allows the retailer user to be given the ability to set a Specification to *Supplier Authorised* status through Permissions configuration. See Post Release Tasks.

If the feature is enabled, an *Authorise on Behalf of Supplier* status change action will be available to retailer users with the appropriate authority profile. The action will appear where the *Authorise Specification* action is available to supplier users (Collaborative Draft, Pack Copy Sent, and Ready for Authorisation). The option is not applicable to Produce specifications.

The action validates the Specification, and if successful prompts for the name, position and date, and the reason for authorizing on behalf of the supplier, before applying the status change.

If the feature is enabled, the corresponding Specification validation options will also be available:

- *Validate this Section for set to > Supplier Authorised*
- *Validate this Specification for set to > Supplier Authorised*

Project and Activity API Updates

The existing Project and Activity REST APIs are extended to allow for the update of Process (Project) and Activity records.

The following features are introduced:

- Project API Project Update function

  An inbound PROJECT UPDATE endpoint to perform a PATCH update of Project/Process records. This allows for updates to individual attributes without having to submit the full record.
- Activity API Activity Update function

  An inbound ACTIVITY UPDATE endpoint to perform a PATCH update of Activity records. This allows for updates to individual attributes without having to submit the full record.

  An inbound ACTIVITY STATUS UPDATE endpoint to update Activity status. The purpose of this endpoint is specifically to update the status, triggering any further updates to the associated Process or to other Activities within the Process.
- Support for JSON format payload

  While the XML payload format continues to be available, support for the JSON payload format is added for the Project and Activity APIs.

> **Note:**
>
> The enhancement does not include the facility to create (POST) Project/Process or Activity records.

Typical usage would be for the following updates from external systems:

- Process Schedule start or End Dates
- Process attributes, including Custom Fields and Process Briefs
- Activity Briefs
- Activity Dates, including planned (scheduled) Start and End dates and Actual Start and End dates
- Activity Status

Post Release Tasks & Impact on Existing Installation

The following post release tasks and impact on an existing installation must be taken into account as part of this release.

> **Note:**
>
> See the Noteworthy Resolved Issues document for 25.1.301.0 for additional post release tasks.

Permissions

The Ability for Retailer to Supplier Authorize Specifications feature is enabled by the following Permissions.

Add the entries below to the bottom of the Specification page of the Permissions spreadsheet.

Record (A)	Authority Profile (B)	Action (E)	Data Record (F)	Status - Record (J)	User Mode (L)	Access Level (M)
Product	ALL SPEC STATUS CHANG	SET TO SUPPLIER_AUTHORISED	Product Specification		NORMAL	Y
Product	Retailer Specification Editor	SET TO SUPPLIER_AUTHORISED	Product Specification	COLLABORATIVE_DRAFT	NORMAL	Y
Product	Retailer Specification Editor	SET TO SUPPLIER_AUTHORISED	Product Specification	PACK_COPY_SENT	NORMAL	Y
Product	Retailer Specification Editor	SET TO SUPPLIER_AUTHORISED	Product Specification	READY_FOR_AUTHORISATION	NORMAL	Y

The instructions for downloading and uploading the amended Permissions spreadsheet are as follows:

1. Log in as an Oracle Authorized Administrator user and go to Company > Admin > Roles & Permissions.
2. Open the Permissions page.
3. Download the active spreadsheet by selecting the row with *true* in the Active Permissions column, click *Download Selected*, and save locally.
4. Edit the downloaded spreadsheet, make the changes described above, then save the spreadsheet.
5. Upload the edited spreadsheet by clicking *Upload Permissions*, select the spreadsheet, and click *Ok*.
6. Apply the changes by selecting the uploaded spreadsheet row, click *Process Selected*, and then click *Ok* to confirm.

System Text

The following features include new system text:

- Supplier and Site Address Validation
- Ability for Retailer to Supplier Authorize Specifications

System text records are added automatically during the release process, however any translation overrides must be added manually, by the retailer administrator.

Post Release Configuration and Testing

The following feature has post release configuration and testing requirements.

Supplier and Site Address Validation

To enable the Supplier and Site Address Validation, set the following system parameters in the Registration page to apply the required mandatory validation:

- Supplier and Site Local Address Validation - select which Address fields are to have mandatory validation applied: Country, Address Line 1, Address Line 2, Address Line 3, Address Line 4, Post Code, GPS.
- Supplier and Site Business Language Address Validation - select which Business Language Address fields are to have mandatory validation applied: Country, Address Line 1, Address Line 2, Address Line 3, Address Line 4, Post Code.
- Supplier and Site Phone Mandatory - set if mandatory validation of the Phone fields is required.

Since this enhancement involves a change to the Specification workflow, it is advised to include a business test of Specification progression through the workflow when upgrading to a release where this enhancement is included.

Enabling Identity Management Notifications

As an IDCS or OCI IAM Administrator, verify that Notifications are enabled in the corresponding Stage / Production tenant.

Enabling User Roles

If they do not already exist, configure the *Power User*, *Account Administrator*, *Assistant Technologist*, and *Site Inspector* user roles, and assign to the appropriate users.

The instructions for downloading and uploading the amended Permissions spreadsheet are as follows:

1. Log in as an Oracle Authorized Administrator user and go to Company > Admin > Roles & Permissions.
2. Open the Permissions page.
3. Download the active spreadsheet by selecting the row with *true* in the Active Permissions column, click *Download Selected*, and save locally.
4. Edit the downloaded spreadsheet, make the changes described above, then save the spreadsheet.
5. Upload the edited spreadsheet by clicking *Upload Permissions*, select the spreadsheet, and click *Ok*.
6. Apply the changes by selecting the uploaded spreadsheet row, click *Process Selected*, and then click *Ok* to confirm.

Enabling Artwork with SSO

Artwork is not a core Brand Compliance module, but a third-party add-on application. This process enables the integration with the third-party Artwork application, where it is used.

For existing installations that use the Artwork module, in order to configure single sign on (SSO) between Brand Compliance and the Artwork solution (using IDCS or OCI IAM authentication), the following steps must be taken by the Customer or their Partner:

1. Ensure the MYARTWORK external system has been created in Brand Compliance PROD and STAGE.
2. Raise an SR service requesting for creation of the Artwork Application for PROD and STAGE. The call back URLs and IDCS or OCI IAM URLs must be provided in the SR.
3. Once created, you will be able to gather the Client ID and Client Secret from IDCS or OCI IAM.

IDCS Changes

As part of the updates from release 20.0 onwards, there are a few changes into various records within the IDCS configuration. These changes should be considered in instances where you have adopted your own changes and configuration within IDCS.

Oracle Cloud Service Records

This section within IDCS is only accessible to Admin users of the IDCS tenancy. A new Cloud Service record is created for the release 20+ instance and is now named using the following naming structure:

- STAGE: RGBU_BCCS_STG1_BC (from RGBU_BCCS_UAT_PROD_BC)
- PROD: RGBU_BCCS_PRD1_BC (from RGBU_BCCS_PRD_PROD_BC)
- DEV: RGBU_BCCS_DEV1_BC (from RGBU_BCCS_DEV_PROD_BC)

Where the OPAL Artwork is utilized, a new Cloud Service record is created for the release 20+ instance and is now using the following naming structure:

- STAGE: RGBU_BCCS_STG1_ARTWORK (from RGBU_BCCS_UAT_PROD_ARTWORK)
- PROD: RGBU_BCCS_PRD1_ARTWORK (from RGBU_BCCS_PRD_PROD_ARTWORK)

IDCS Group Records

These are created automatically by the Brand Compliance application and the naming of the groups is updated to be aligned with the Oracle Cloud Service record. Standard groups are created for . . . Artwork, . . . BC_User, . . . Reports_Admin, . . . Retailer, and . . . Supplier. For example, RGBU_BCCS_PRD1_BC_User is the new release 20+ group naming structure, RGBU_BCCS_PRD_PROD_BC_User being the previous naming structure.

> **Note:**
>
> When creating new groups within an IDCS tenant, avoid using the RGBU_BCCS_PRD1_ or RGBU_BCCS_STG1_ prefix for the name of groups. Any groups created with either prefix may have their users removed from the group as part of the hourly IDCS sync process.

2

Browser Requirements

> **Note:**
>
> Oracle Retail assumes that the retailer has ensured its Operating System has been patched with all applicable Windows updates.

The following browsers are supported:

- Mozilla Firefox
- Microsoft Edge
- Google Chrome (Desktop)

Microsoft has deprecated Internet Explorer 11 in Windows 10 and recommends using Edge as the default browser. Refer to the Oracle Software Web Browser Support Policy for additional information.

3 Noteworthy Resolved Issues

For the Noteworthy Resolved Issues document for this release, see the following on My Oracle Support (MOS): Oracle Retail Brand Compliance Management Cloud Service Documentation Library at Doc ID 2400174.1.

4
Deprecated Features

As part of the continuous delivery model for cloud services, features and technical components of a solution may be removed or replaced to enhance the security, performance, and overall quality of the cloud service. When this occurs, the deprecation of a feature or component will be announced in advance, allowing customers sufficient time to anticipate the change and transition to any enhanced replacement feature/component. After the deprecation is announced, the deprecated feature or component will remain in the solution until the planned removal date and will not be enhanced or made compatible with other new features.

In this release, the following changes are made for the previously announced deprecations:

- **Removal of Basic Authentication**

  The ability to use Basic Authentication to access the APIs is removed.
- **Removal of SOAP APIs**

  The SOAP APIs are removed.

For the full schedule of planned deprecations for this product, see the Deprecation Advisory accessed from the following MOS Documentation Library: Oracle Retail Brand Compliance Management Cloud Service Documentation Library at Doc ID 2400174.1.