

PRODUCT SPECIFICATIONS FOR COMPLIANCE DEPOT[®] SYSTEM

UPDATED: March 5, 2020

These Product Specifications describe the current functionality and certain dependencies of the above-referenced product center (the “Product Center”). Access to and use of the Product Center is governed by an underlying agreement and, as applicable, addendum (collectively, the “Agreement”) with RealPage, Inc. and, as applicable, its affiliates (collectively referred to herein as the “Provider” “we” or “us”). Capitalized terms used in these Product Specifications have the meanings provided in the Agreement unless otherwise defined herein.

Subject to the terms of the Agreement, these Product Specifications may be modified at any time. If we modify these Product Specifications, we will post the updated version at <http://www.specifications.controls.realpage.com> and update the “Updated” date above. We recommend that you review these Product Specifications periodically for any changes. Your continued access to or use of the Product Center will constitute your acceptance of the updated Product Specifications.

1. AUTHORIZED USERS AND PASSWORD

Provider will provide the licensee under the Agreement (“Licensee”) with a user name and password permitting Authorized Users to access the Product Center. Licensee is responsible for the protection and dissemination of such user name and password and for any activities or actions occurring under Licensee’s account or log-in credentials—including, without limitation, for any losses or damages resulting from the loss, theft or misuse of or failure to protect any such user name or password. Licensee will permit only Authorized Users to access the Product Center, will ensure that all Authorized Users comply with the terms and conditions set forth in the Agreement and herein, and will not permit any person that ceases to be an Authorized User to continue to use a user name or password.

2. OVERVIEW OF COMPLIANCE DEPOT

COMPLIANCE DEPOT is a vendor credentialing management service designed specifically to meet the needs of real estate owners and managers. It enables the sites to use only those vendors that have been properly evaluated in accordance with the client’s approved vendor criteria. The service includes a secure, web-based system that tracks vendor insurance documentation, licensing, owner/principal background screening, W9’s and other client-specific documentation as required. The system notifies site personnel when a vendor has fallen out of compliance or is due for an upcoming renewal. The Compliance Depot product may also be integrated with the company’s accounts payable system, and with RealPage’s web-based procurement software, OneSite Purchasing, and/or OpsTechnology, thereby preventing on-site staff from continued use of unauthorized vendors.

Note: The COMPLIANCE DEPOT Product Center was not designed to store electronic protected health information, as defined by Section 160.103 of the HIPAA Regulations, 45 CFR Parts 160, under the Health Information Portability and Accountability Act Omnibus Final Rule released on January 17, 2013. Users should not use any feature of the COMPLIANCE DEPOT Product Center to upload or to store any electronic protected health information.

3. DETAILED SPECIFICATIONS FOR COMPLIANCE DEPOT

This section outlines the major capabilities of COMPLIANCE DEPOT:

- Property List
- Vendor List
- System Notes
- Notification Service
- Vendor Document Management
- Sample Insurance Certificates
- Vendor-Specific Approval/Override Control
- Vendor Evaluation Status
- User Access Control
- Reports
- Integration
- Priority Vendor List
- Credential Key Program

3.1. The Property List feature of Compliance Depot permits the Authorized User to:

- a. Track a property's division, region, ownership group, database, address, phone number, fax number, email address, property class, property number, unit count, and year of construction.
- b. Search property listing by full or partial name, division, region, ownership group, database, or state.
- c. Link properties with the vendors used by that property.
- d. Control the access rights of the system Authorized Users so that they can only access information for selected properties.

3.2. The Vendor List feature of Compliance Depot permits the Authorized User to:

- a. Add new vendors to the system manually, through upload, or linking functionality. All vendors added to an individual property will be appended to the overall client vendor list.
- b. Remove vendors from the client vendor list.
- c. Link or unlink vendors from a specific property.
- d. Search existing vendors by full or partial name, Compliance Depot Vendor ID, client accounting ID (CVN), EIN, city, state, Zip Code, mileage range, industry code, minority-owned business designation, criteria/evaluation override flag, or status evaluation. The list can be searched at the property level, client level, or for Compliance Depot overall.
- e. Export a full vendor list at the property or client level to Excel.
- f. Apply an exempt status to specified vendors.
- g. View documents from a selected vendor.

3.3. System Notes feature of Compliance Depot permits the Authorized User to:

- a. View notes entered by the Compliance Depot staff such as summarized phone calls or vendor processing notations.
- b. View notes that describe each type of communication sent to the vendor from the Compliance Depot notification service.

3.4. The Notification Service feature of Compliance Depot permits the Authorized User to:

- a. Receive an email notification regarding vendor evaluation status changes which can be activated on an individual user basis.
- b. Receive an email notification regarding upcoming insurance expirations which can be activated on an individual user basis.
- c. Send notices automatically by email or fax using an approved letter format to the company's vendors regarding enrollment.

- 3.5. The Vendor Document Management feature of Compliance Depot permits the Authorized User to:
 - a. View and/or print all current vendor documentation including insurance certificates, endorsements, vendor requirements acknowledgement & agreements, W9, licenses, Workers' Compensation Exemption Forms, and any other client-specific documents.
 - b. Search, view, and print all historical vendor documentation.
 - c. Enlarge vendor documentation for viewing through the "full size" filter.
 - d. Save a copy of any vendor document.
- 3.6. The Document Storage feature of Compliance Depot is a self-serve option that permits the Authorized User to:
 - a. Upload PDF or TIF documents directly to the Compliance Depot web site with a maximum individual file size of 5 MB.
 - b. Assign an Ownership Group or Location Name to the document.
 - c. Enter an expiration date that may be associated with information contained in the document.
 - d. Search, view, and print all uploaded documents.
 - e. Export a listing of all documents by file name to Excel.
- 3.7. The Sample Insurance Certificate feature of Compliance Depot permits the Authorized User to:
 - a. View a vendor-specific sample insurance certificate. The applicable limits and additional insured language to be extracted based upon vendor's industry code designation and property links.
 - b. Print a vendor specific sample insurance certificate.
- 3.8. The Vendor-Specific Approval/Override Control feature of Compliance Depot permits the Authorized User to:
 - a. Enter an override for a specific criteria point. The override can be entered for a specific property(s). It may also be entered at the client level which becomes applicable for all current and future property links.
 - b. Grant the override for a specified amount of time or permanent basis.
- 3.9. The Vendor Evaluation Status Result feature of Compliance Depot permits the Authorized User to:
 - a. View the date/time stamped evaluation status result for all enrolled vendors.
 - b. Search for vendors by evaluation status result.
- 3.10. The User Access Control feature of Compliance Depot permits the Authorized User to:
 - a. Add new users.
 - b. Edit existing user access.
 - c. Grant portfolio wide, multi-property, or single property access to a single log-in.
 - d. Customize access by individual user or groups of users.
 - e. Retrieve lost/forgotten passwords directly from Compliance Depot web site.
- 3.11. The Reports feature of Compliance Depot permits the Authorized User to:
 - a. Generate, export, and print an alphabetical listing of all enrolled or account locked vendors, which indicates their current evaluation status result.
 - b. Generate, export, and print a vendor evaluation summary by status recommendation.
 - c. Generate, export, and print a criteria failure listing by individual insurance or business requirement category with applicable vendor summary.

- d. Generate, export, and print a listing of vendors that are missing fax or email contact information on a property-level basis.
 - e. Generate, export, and print a summary outlining the last log-in date for the Authorized Users linked to properties and their applicable client property numbers.
 - f. Generate, export, and print overall percentages for each evaluation status result. The expansion function enables drilling down to division, region, and property-level percentages. At the property level, a vendor summary with name, phone, fax, and email contact information is available per each evaluation status.
 - g. Generate, export, and print a listing of vendors with changed contact, evaluation status, or property links within a specified time frame.
 - h. Generate, export, and print a listing of vendors that are set for automatic removal from the client vendor list on a specified date.
 - i. Generate, export, and print a listing of vendors with Minority-Owned Business certifications and the type of minority certificate(s) they have on file
 - j. Generate, export and print a listing of vendors that have been assigned a status of Exempt and are not required to complete the credentialing process
 - k. Generate, export and print a listing of vendors that have requested no further contact with regard to the credentialing requirements for the Site Owner.
 - l. Generate and export a custom query full vendor list on the client or property level that includes:
 - (i) Compliance Depot ID
 - (ii) Client Accounting ID
 - (iii) Vendor Name
 - (iv) EIN (first 5 characters will be masked)
 - (v) Vendor Business & Remittance Addresses
 - (vi) Vendor Phone, Fax, Email
 - (vii) Current Evaluation Status
 - (viii) Vendor Tax Name & Company Type
 - (ix) Industry Code
 - (x) Insurance Expiration Dates by Policy Type
 - (xi) Date Vendor Added to Client List
 - (xii) Last Evaluation Date
 - (xiii) Number of Properties Vendor Services
 - (xiv) Annual Compliance Depot Renewal Date
- 3.12. Ability to integrate with RealPage Accounting, Yardi, or MRI accounting packages which includes:
- a. Addition of new approved or exempt vendors within the accounting system on a daily basis including the creation of a unique accounting ID number when applicable.
 - b. Activation/Deactivation of “inactive” or “pay-hold” flags.
 - c. Updates to existing vendor contact fields such as the address, phone, fax, and email on a daily basis.
 - d. Populating insurance policy expiration dates for general liability and workers’ compensation.
- 3.13. Ability to integrate with OneSite Purchasing which includes:
- a. Update to the OneSite Purchasing center with the Compliance Depot vendor evaluation result for each vendor on a daily basis.

- b. Ability to access additional real-time Compliance Depot updates directly from the OneSite Purchasing product center that includes the ability to view insurance and other pertinent documentation that has been submitted by the vendor.
 - c. Ability to prevent the generation of purchase orders, invoices, and credit memos for vendors when they have a “not approved” or “not enrolled” evaluation result.
 - d. Ability to warn users when generating a purchase order, invoice, or credit memo that the vendor’s evaluation result is “not approved” or “not enrolled.”
 - e. Ability to print a list of “approved” vendors from Compliance Depot,
- 3.14. Ability to integrate with the OpsTechnology center which includes:
- a. Update to the OpsTechnology center with the Compliance Depot vendor evaluation result for each vendor on a daily basis.
 - b. Ability to prevent the generation of purchase orders, invoices, and credit memos for vendors when they have a “not approved” or “not enrolled” evaluation result.
 - c. Ability to warn users when generating a purchase order, invoice, or credit memo that the vendor’s evaluation result is “not approved” or “not enrolled.”

4. PRIORITY VENDOR LIST

- 4.1. Site owners may select up to 5 vendors at a time to include on the Priority Vendor List. Once added to this list, RealPage staff will make proactive outreach to the vendor to assist with completion of the credentialing process. These attempts will be made on 5 occasions over a 2 week period. Each contact attempt will be documented in System Notes. Upon successful completion of the credentialing process or after all contact attempts have been made a vendor will be removed from the Priority Vendor List. Authorized Users may replace vendors on the Priority Vendor list with other vendors at any time.

5. CREDENTIAL KEY PROGRAM

The Credential Key Program offers Site Owners and vendors an expedited process to meet required proof of insurance requirements. Site Owners and vendors must opt into the program. Site Owner insurance requirements must be configured to accept ‘blanket’ policy endorsement documents to satisfy criteria for Additional Insured status, Waiver of Subrogation, Ongoing and Completed Operations. Vendors with insurance coverage that includes these types of ‘blanket’ endorsements are evaluated in a manner that reduces both the variety of insurance documents that must be submitted and the time required to complete the credentialing process.

6. CALIFORNIA CONSUMER PRIVACY ACT OF 2018 (“CCPA”) DATA PROCESSING STATEMENT

This CCPA Data Processing Statement applies to “Personal Information” of a “Consumer” as those terms are defined under the CCPA (referred to hereafter as “Personal Data”) that RealPage processes in the course of providing services under the Product Center (“Services”) governed by the Agreement to Customer.

RealPage understands the terms in this CCPA Data Processing Statement and agrees to comply with them. The terms of this CCPA Data Processing Statement will prevail in connection with the purpose and scope of this CCPA Data Processing Statement over any conflicting terms in the Agreement.

- 6.1. Customer’s Role. The Customer is a for profit entity that determines the purpose and means of processing Personal Data. Customer will provide Personal Data to RealPage solely for the purpose of RealPage performing the Services.
- 6.2. RealPage’s Role. RealPage shall provide the Services and process any Personal Data in accordance with the Agreement. RealPage may not retain, use, or disclose Personal Data for any other purpose other than for providing the Services and in performance of the Agreement.
- 6.3. Data Processing, Transfers, and Sales. RealPage will process Personal Data only as necessary to perform the Services, and will not, under any circumstances, collect, use, retain, access, share,

transfer, or otherwise process Personal Data for any purpose not related to providing such Services. RealPage will refrain from taking any action that would cause any transfers of Personal Data to or from RealPage to qualify as “selling personal information” as that term is defined under the CCPA.

- 6.4. Sub-Service Providers. Notwithstanding the restrictions in Section 2.3, Customer agrees that RealPage may engage other Service Providers (as defined under the CCPA), to assist in providing the Services to Customer (“Sub-Service Providers”). RealPage carries out appropriate due diligence on each Sub-Service Provider and the arrangement between RealPage and each Sub-Service Provider is governed by a written contract which includes terms substantially equivalent to those set out in this CCPA Data Processing Statement.
- 6.5. Security. RealPage will use commercially reasonable security procedures that are reasonably designed to maintain an industry-standard level of security, prevent unauthorized access to and/or disclosure of Personal Data.
- 6.6. Retention. RealPage will retain Personal Data in accordance with Customer instructions, the terms of the Agreement, or any applicable law(s), whichever requirement is controlling under the circumstances. At the termination of this CCPA Data Processing Statement, or upon Customer’s written request, RealPage will either destroy or return Personal Data to the Customer, unless legal obligations require storage of the Personal Data.
- 6.7. Assistance with Consumers’ Rights Requests. If RealPage, directly or indirectly, receives a request submitted by a Consumer to exercise a right it has under the CCPA in relation to that Consumer’s Personal Data, it will provide a copy of the request to the Customer. The Customer will be responsible for handling and communicating with Consumers in relation to such requests.
- 6.8. Enforceability. Any provision of this CCPA Data Processing Statement that is prohibited or unenforceable shall be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions hereof. The parties will attempt to agree upon a valid and enforceable provision that is a reasonable substitute and shall then incorporate such substitute provision into this CCPA Data Processing Statement.