

ORACLE®

**CONFIGURE, PRICE,
AND QUOTE
CLOUD**

CPQ Cloud Security Guide

MARCH 2018

ORACLE®



Table of Contents

Introduction.....	1
Administration Best Practices.....	1
<i>Passwords</i>	1
<i>BML</i>	2
User Type Best Practices.....	3
Commerce Best Practices.....	3
<i>Secure Attributes</i>	3
<i>Workflow</i>	4
<i>Approvals</i>	5
<i>Integrations</i>	5
<i>File Manager</i>	5
Home Page Best Practices	6
API Programming Best Practices.....	6
Data Table Best Practices.....	7
Data Use Best Practices	7

Introduction

Oracle Configure, Price, and Quote (CPQ) Cloud enables companies to streamline the entire opportunity-to-quote-to-order process, including product selection, configuration, pricing, quoting, ordering, and approval workflows. The CPQ Cloud product provides a flexible, scalable, enterprise-ready solution ideal for companies of all sizes that sell products and services across direct, indirect, and e-commerce sales channels.

CPQ Cloud is a highly customizable product and provides administrators with numerous configuration options. The purpose of this Security Guide is to provide administrators with tips and best practices to aid in the secure deployment and usage of CPQ Cloud.

Administration Best Practices

The CPQ Cloud **Administration Platform**, often referred to as the Admin Home page, is the area within CPQ Cloud used by administrators to setup a secure configuration for CPQ Cloud. Oracle recommends administrators comply with the administration best practices identified within this section.

Passwords

Administrators have the ability to set the password strength for all CPQ Cloud user accounts from the **Options – General** page. They can also specify the number of login attempts allowed before locking a user account and the number of days a password is valid before it expires.

Complete the following steps:

1. Open the CPQ Cloud **Administration Platform**.
2. Under **General**, click **General Site Options**.
The **Options – General** page opens.
3. While administrators can set the password strength to **Low** or **High**, Oracle recommends setting the password strength to **High** for greater security.
 - **Low** - Requires 4-30 characters without special requirements.
 - **High** - Requires 8-31 characters, including at least one uppercase letter, at least one number, and at least one special character.
4. Use the **Number of Login Attempts** field to specify the number of login attempts allowed before locking a user account. Refer to your company policy and populate this field with the minimum value referenced. If not addressed in your company policy, Oracle recommends setting the value to 3.
5. Use the **Password Expires After** field to specify the number of days after which the password expires. Refer to your company policy and populate the value with the minimum value referenced. If not addressed by your company policy, Oracle recommends setting the value to 180.

6. In the **Password Reuse After** field, Oracle recommends entering **365** days. The value entered specifies the number of days after which an expired password can be reused.

Options - Password

Password Strength	<input type="radio"/> Low <input checked="" type="radio"/> High
Number of Login Attempts	<input type="text" value="3"/>
Password Expires After	<input type="text" value="180"/> Days
Password Reuse After	<input type="text" value="365"/> Days

Figure 1: Password Options on Options – General Page

7. Click **Apply**.

BML

BigMachines Extensible Language (BML) is a powerful scripting language used by administrators to customize the functionality of CPQ Cloud. Oracle recommends that administrators who write BML comply with the following best practices.

Best Practice	Description
BMQL	BMQL takes in a query string that can have inputs passed in as \$ defined variables, which is the Oracle recommended best practice. While administrators can also build the string with variables hardcoded in the string, Oracle does not recommend this method as the query string has a higher likelihood of being vulnerable to attack.
Input	Oracle recommends sanitizing all BML input before the input goes through sensitive processing. For example: If using a numeric drop-down for input in BML, do not assume the content coming in is from the drop-down. If you take content and, for example, do a loop based upon this, an attacker could send in an input of more than a million, potentially compromising site stability.
HTTP	Oracle recommends using URL Data methods to make HTTP calls from BML. URL data methods can make an HTTP call to a third party site and is an easy way to do integrations.

NOTES:

- When sending sensitive content, use HTTPS and not HTTP when making these calls.
- If the URL and the parameters list comes from user content, they must either come from administrator-defined values or undergo validation. By not complying with this best practice, CPQ Cloud servers become an attack vector to other sites and issues occur with CPQ Cloud deployments.
- Oracle recommends putting in a timeout value for every HTTP call made from BML, so there are no hanging threads waiting for server responses when a third party site has performance problems.

User Type Best Practices

CPQ Cloud offers multiple user types for different roles. Oracle recommends assigning users to the correct user type, so users only have access to the functionality they need. As described in the following table, all host company users fall into two general categories of user type: admin users and sales users.

User Type	Description
Admin Users	Admin users are responsible for implementing and maintaining a CPQ Cloud site. They have access to both the CPQ Cloud Administration Console and the user side of CPQ Cloud.
Sales Users	<p>Sales users only have access to the user side of CPQ Cloud and use it to configure products, create Transactions, and create proposal documents.</p> <p>There are three types of sales users: Full Access, Restricted Access, and Sales Agent. For additional information, refer to the CPQ Cloud Administrator Online Help.</p>


Commerce Best Practices

Commerce is one of the foundational pillars of CPQ Cloud and is where a configuration turns into a quote, which can flow through approvals and into other systems. Commerce uses secure attributes, workflows, and approvals to help process data in a secure way.

Secure Attributes

Secure attributes are available to administrators when they need information encrypted in the system that 1) should not be persisted in CPQ Cloud or 2) must be encrypted. Encryption is asymmetric.

With a **Secure Attribute** field on a Commerce layout, CPQ Cloud can capture values as users input them. CPQ Cloud masks the entry as if it were a password. In addition, CPQ Cloud uses the Java RSA encryption standard to encrypt the data without ever storing the original value in CPQ Cloud. CPQ Cloud only stores the masked data, which cannot be converted back to its original value.



When a CPQ Cloud action (such as Save) is active, the encrypted data is temporarily stored in memory and can be transferred to the customer's system via an integration call from CPQ Cloud. The customer's system, located in their controlled database, handles data storage, security, and any further encryption and decryption.

CPQ Cloud encryption uses standard Java libraries, including RSA standard with Optimal Asymmetric Encryption Padding. The public key (an SSL certificate with a minimum key length of 2048) must be uploaded to the Commerce process.

Workflow

Workflow administration is the final step in setting up a Commerce process. Administrators can utilize user roles to customize views and deny access to attributes when a quote enters specific states. Layout customizations allow administrators to remove sensitive attributes from the interface when non-cleared users can view the quote.

A workflow consists of steps, which define document permissions, routing, and the different states of a Transaction. Commerce processes can have any number of workflow steps.

For example: A Request for Quote (RFQ) process could have steps such as "Submitted", "Quoted", "Accepted", "Declined", and "Expired". These steps could transition a Transaction from an RFQ document, to a Quote document, to a purchase order document.

Workflow steps use profiles to define access rights, transition notifications, and Transaction views. The Commerce system automatically creates a default profile for each workflow step. Administrators can customize the default profile and create additional ones to support different Transaction access rights.

Administrators grant profile permissions based on user access type, user group, or previous performers. In addition to these permissions, administrators can also add auto-forwarding rules to workflow steps to support a collaborative sales environment where multiple users can work on the same Transaction. Auto-forwarding rules direct the system to share Transactions between members of certain user groups. Administrators can create auto-forwarding rules for each workflow step and base them on any number of criteria.

Notes:

- Use the defined user roles and steps to restrict all sensitive attributes from the view of users with no need to view them.
- Administer all workflow steps in undeployed Commerce processes. After deploying a Commerce process, functionality including the ability to add, order, and delete steps becomes hidden from view. To perform any of these actions when they are not visible, contact a CPQ Cloud implementation engineer.

Approvals

Upon finalizing a quote, the quote enters the approval process. The approval process defines how the business hierarchy signs off on the validity of quote, allowing the quote to proceed to the next step. Approvers can evaluate quote values during the approval process to ensure the values are as expected.

Integrations

Integrations with third party sites use integration XSLs. In Commerce, this transforms the quote data and sends the transformed object to the connected CRM system. These XSLs can use XSL library functions and the full functionality of the language.

Note: Non-standard extension libraries are not supported.

File Manager

File Manager is an integral part of CPQ Cloud. Customers can upload files to the File Manager, organize files into folders, and access files from anywhere on the Internet. The File Manager stores external images, JavaScript files linked to various areas on the site, CSS Stylesheets for Configuration flow templates, and Excel spreadsheets used to hold master data.

Unless administrators apply folder security, the File Manager files are available publicly. Oracle recommends administrators place all sensitive content in a secure folder. Administrators can designate any folder they have added to File Manager as secure. Once an administrator designates a folder as secure, the security settings apply to all files within that folder.

Complete the following steps:

1. Open the CPQ Cloud Administration Platform.
2. Under **Utilities**, select **File Manager**.
The **File Manager** opens.
3. Select a folder from the **Folders** panel.
4. Select the **Folder Security Setting** checkbox to make the folder secure.

File Manager	
Folder Security Setting	
<input checked="" type="checkbox"/>	Only allow users who are logged in to view the contents of this folder?

5. Click **Save**.

Home Page Best Practices

Administrators can customize the CPQ Cloud home page and use features on a customer's CPQ Cloud site to apply custom headers and footers, which are placed on the site without CPQ Cloud processing. Oracle advises administrators to carefully place content in the header and footer, ensuring not to expose insecure or performance impacting JavaScript.

The home page can also have access restrictions applied to various elements. In the administration section on the homepage link, administrators can introduce smart restrictions based upon user account values, allowing models to shown to specific users only if they are in a specific user group. In this way, homepage views are customized to the permission of each user.

Note: Domain whitelisting for cross origin JavaScript calls is not setup for CPQ Cloud by default. If the functionality is needed for a CPQ Cloud site, open a Service Request (SR) on My Oracle Support.

API Programming Best Practices

CPQ Cloud offers REST and SOAP APIs for interacting with CPQ Cloud objects. The CPQ Cloud Administration Online Help contains documentation about both the REST and SOAP APIs.

REST APIs allow authentication via the following options, listed in preferred order: an OAuth token, BaseAuth headers, or a session cookie. Oracle does not recommend BaseAuth as the integration site is responsible for securely managing the credentials. Using a session cookie is a browser-based authentication mechanism where REST calls are usually server-to-server. For this reason, Oracle does not recommend using a session cookie. The preferred usage for SOAP APIs is to use a WS-Security header for login.

Best Practice	Description
Password Storage	Regardless of the authentication method used, administrators must securely store the secret values for authentication. If using BaseAuth, administrators must keep user credentials safe on a trusted server. If using OAuth, administrators must keep the client secret safe on the callback server. Any compromise of these credentials should trigger an immediate credential change or deactivation of the user or client record.
Client Registration	Registration of OAuth clients occurs via a REST endpoint. Administrators should correctly choose the time to live values for access and refresh token time to live values. The default values are 30 minutes and 24 hours respectively. Oracle recommends not setting the access token lifetime at more than an hour.
HTTPS Only	CPQ Cloud only responds over HTTPS calls, which are the only calls Oracle recommends making. If attempting to pass credentials or sensitive information over HTTP, the data can be read from intermediate servers processing the request on its way to CPQ Cloud. To prevent unintentional information disclosure, Oracle strongly recommends that request attempts do not follow this transport method.

Best Practice	Description
OAuth Provider	It is important that only trusted clients are allowed access to CPQ Cloud resources. Since CPQ Cloud implicitly trusts OAuth Provider credentials as a trusted identity and passes along that signature authority, ensure that only trusted services have access to get signature from the OAuth Provider. With this in mind, also ensure proper security privileges are established for the OAuth provider.

Notes:

- CPQ Cloud supports the use of REST APIs for communication between clients and servers. In general, Oracle recommends making calls to support standalone user interfaces or server processing of CPQ Cloud objects. Most REST calls are synchronous and all REST calls are stateless.
- REST calls tax the CPQ Cloud system in an equivalent manner to a user performing the same operation through the CPQ Cloud interface. Oracle recommends administrators make sure the system is not flooded with REST calls. To maintain a lighter load of REST calls, request only the portion of attributes needed for extra processing in the REST endpoint. For additional information, refer to the REST metadata documentation.

Data Table Best Practices

Data tables allow for the storage of spreadsheet like data in the system. Customers upload a large amount of data into CPQ Cloud data tables for use in CPQ Cloud processing. Since the data can contain sensitive information, CPQ Cloud allows administrators to impose security layers on the data tables.

Secure columns encrypt the data entered into them and provide a good way to keep confidential information (i.e. passwords to external systems, secret keys, or tokens) in data tables. Once entered, the data remains encrypted in the CPQ Cloud database and is only accessible via BMQL.

Administrators can use the secure data type option for new columns in both new and existing data tables. Confidential client credentials are required to connect to other Oracle products and applications. Secure data table columns provide a method for securely storing confidential credentials in CPQ Cloud. Secure columns always store the encrypted form of the data in the data table. The only way to access this data in its original, decrypted form is through BMQL.

Note: Secure columns are not designed to store very sensitive data such as credit card numbers or social security numbers.

Data Use Best Practices

Within the CPQ Cloud application, session cookies are maintained only for an active CPQ Cloud session. Once the active session is closed, tracking of cookies ends and all cookie-related data is deleted and not retained within the CPQ Cloud application.



Oracle is committed to developing practices and products that help protect the environment

Copyright © 2018 Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

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.

Integrated Cloud Applications & Platform Services