ORACLE

Oracle CPQ Security Guide

March 2023

TABLE OF CONTENTS

INTRODUCTION

Oracle Configure, Price, and Quote (CPQ) enables companies to streamline the entire opportunity-to-quote-to-order process, including product selection, configuration, pricing, quoting, ordering, and approval workflows. The Oracle CPQ 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.

Oracle CPQ 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 Oracle CPQ. Refer to Oracle CPQ Administration Online Help and the Best Practice Overview topic for Oracle CPQ tips and videos.

ADMINISTRATION BEST PRACTICES

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

Passwords

Administrators have the ability to change password security settings for all Oracle CPQ user accounts from the General Site Options page. They can specify the number of login attempts allowed before locking a user account and the number of days a password is valid before it expires.

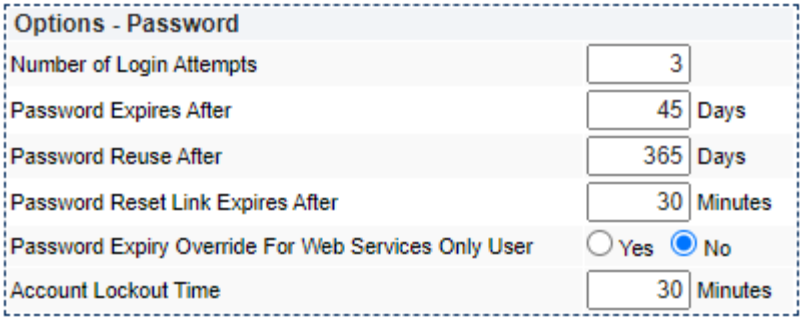
Complete the following steps:

1. Open the Oracle CPQ Administration Platform.
2. Under General, click **General Site Options**. The Options – General page opens.

NOTE: Beginning in Oracle CPQ 21B, support for low complexity password strength is discontinued and the **Password Strength** selection is removed from the Options – General page. Going forward, all new passwords require 8 – 31 characters, including at least one uppercase letter, at least one number, and at least one special character. This change will impact end users the first time they reset their password following the Oracle CPQ 21B upgrade.

3. 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.
4. 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 less than 90 days. This field cannot be left blank.
5. Use the **Password Reuse After** field to specify the number of days after which an expired password can be reused. Refer to your company policy and populate this field with the maximum value referenced. If not addressed in your company policy, Oracle recommends setting the value to 365 days.
6. Use the **Password Reset Link Expires After** field to specify the number of minutes the reset link is available to the user. 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 30.

7. Administrators can set the **Password Expiry Override For Web Services Only User** to **Yes** or **No**, the default setting for this is **No**. This option specifies if Web Services Only user passwords follow the CPQ site password options. Oracle recommends setting this value to **No**.
   - **Yes** - Passwords do not expire for SOAP and REST API Web Services users.
   - **No** - SOAP and REST API Web Services user passwords follow the password options set for all users on the CPQ site.
8. Use the **Account Lockout Time** field to specify the number of minutes an account is automatically locked after the number of invalid login attempts is exceeded. Once the lockout time has passed, the account is automatically unlocked and available for user login. Refer to your company policy and populate this field with the maximum value referenced. If not addressed in your company policy and you want to implement this feature, Oracle recommends setting the value to 30. If you do not want to implement this feature, set the value to 0.



BML

BigMachines Extensible Language (BML) is a powerful scripting language used by administrators to customize the functionality of Oracle CPQ. 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 current with industry standards 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, Oracle CPQ servers become an attack vector to other sites and issues occur with Oracle CPQ 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 side has performance problems.

Custom JavaScript and CSS

While Oracle CPQ does not endorse or guarantee the use of JavaScript customizations, we recognize that some customers have extended the Oracle CPQ. Customizations may conflict with new Oracle CPQ platform features, data may be corrupted or lost, maintenance and support may be difficult, cross-browser support must be verified, performance may be impaired, and testing is required for each upgrade. Customers should consider carefully the relative benefits of JavaScript customizations in light of the associated risks.

Customers are recommended to utilize the CPQJS APIs instead of manipulating the Document Object Model (DOM) structure or specific elements, classes or IDs.

If customers have added custom JavaScript that leverages the Document Object Model (DOM) structure or specific elements, classes or IDs, this customization should be thoroughly tested and may require refactoring.

Oracle CPQ 23A and later supports JET v12.1.0. Please note the following:

- Select One component (`<oj-select-one>`) is deprecated and has been replaced with Select Single (`<oj-select-single>`). The following are impacted by this change: Favorites List and Detail pages, Commerce Analytics graph, and Single Select Menu (SSM).
- Standard JET tables with data table cell tag (<td>) has updated id property syntax and the headers property is removed. For example:
  - JET v12.1.0 syntax: `<td class="oj-table-data-cell oj-form-control-inherit" id="mandatoryModels-table:48_0">Recommended Model 1</td>`
  - JET v10.0.0 syntax: `<td class="oj-table-data-cell oj-form-control-inherit" id="mandatoryModels-table:modelName_48" headers="mandatoryModels-table:modelName">Recommended Model 1</td>`
- For Configuration Array set read-only cells, `.oj-table-data-cell.oj-hover` styling has been updated from `{background-color: #f2f2f3;}` to `linear-gradient (rgb(242, 242, 243), rgb(242, 242, 243))`.
- When changing column selections for Simple List UIs and Configuration BOM panels, you need to hover over the columns to see the options list display. This change impacts Recommended Items List, Asset List, Performance Logs, and Eligibility Rules.
- In data tables, clicking on a table cell selects the current value in the table cell (all table cell contents are highlighted). If you begin typing, the newly entered content replaces the highlighted content.
- In the Commerce Layout Editor, the tooltip remains in view even after the applicable field is no longer visible.
- The error message text for required attributes is modified from "Enter a value" to "Select a value".
- When a sales user edits a date attribute, the date-picker tool will not automatically open. The user must either type in a value or click the date picker icon to select a value. On a mobile device, the user must select the date picker icon to select a value.

IMPORTANT: JET widget CSS applies to elements with class that starts with '.oj'. Oracle JET reserves this as a namespace. As such all customized elements that include '.oj' should be reviewed, tested, and refactored. Going forward no customized elements should include '.oj' in order to prevent future issues.

Oracle CPQ 22C upgraded jQuery to 3.6.0. Customers using earlier versions of jQuery need to upgrade and test their JavaScript customizations.

Refer to the following resources for more information:

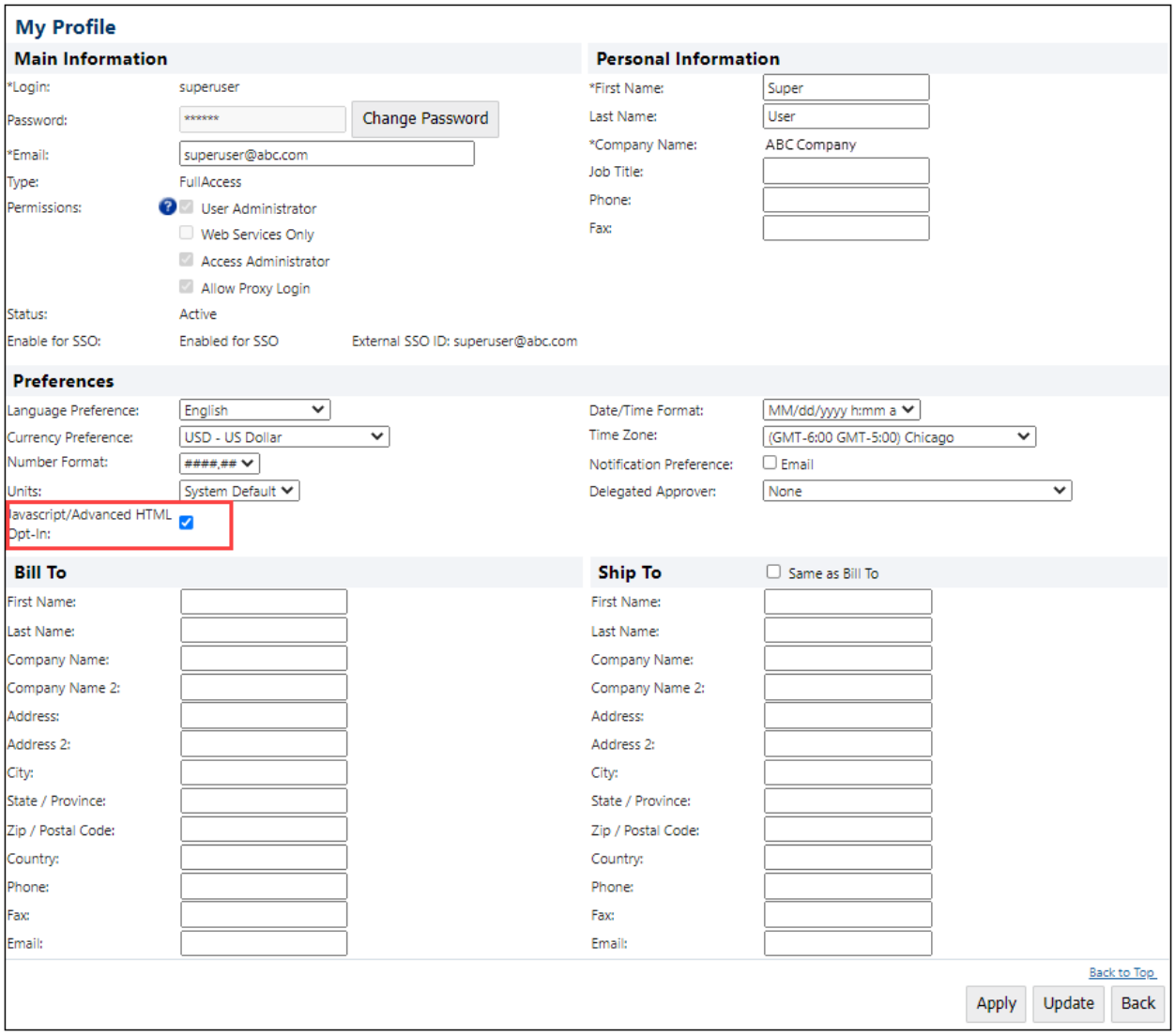
- Oracle CPQ Administration Online Help > Style & Templates > JavaScript Customizations for JET UIs
- Oracle CPQ JET Configuration and Transaction UI: Refactoring Existing JavaScript Customizations (Doc ID 2490016.1)
- JavaScript Extension Toolkit and JET v12.1.0 Release Notes

Beginning in Oracle CPQ 22B, administrators must opt in to add customized advanced HTML/JavaScript to the site. A new User Profile preference checkbox setting, **JavaScript/Advanced HTML Opt-In**, must be selected in order for customized JavaScript or Advanced HTML scripts to be added or modified.

If a user attempts to add custom advanced HTML without this setting selected, an error message displays indicating the opt-in setting is required. When this occurs the JavaScript/HTML content is blocked from entry. The user can remove the JavaScript/Advanced HTML content or opt in. This reminds users of the risks associated with JavaScript/Advanced HTML customizations and they must agree to take responsibility for the risks to their site.

To access the Opt-in for JavaScript/Advanced HTML setting, perform the following steps:

1. Navigate to the My Profile page by clicking the My Profile icon or selecting My Profile from the User Navigation Menu.
2. Select the **JavaScript/Advanced HTML Opt-In** checkbox within Preferences.



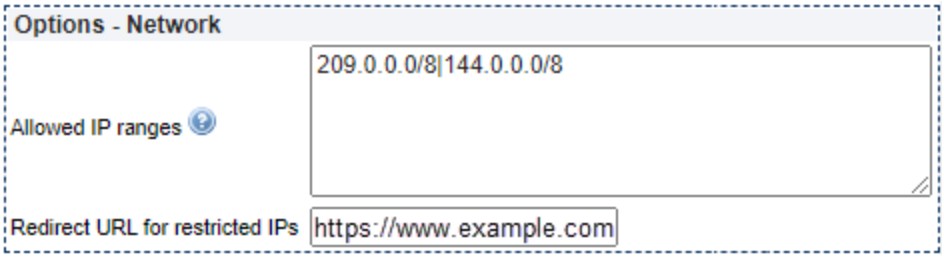
3. Click **Apply** or **Update**.

Restrict IP Range Access to Oracle CPQ

Beginning in Oracle CPQ 23B host company administrators can control which IP ranges can access their Oracle CPQ environments. This allows administrators to specify, for example, that CPQ environments can only be accessible from customer office networks or virtual private networks (VPNs).

This feature is only available for Oracle Cloud Infrastructure (OCI) environments. Customers need to analyze their business and security requirements before implementing this feature. If you determine restricting IP range access to Oracle CPQ fits your implementation needs, log a Service Request on My Oracle Support to enable the feature. When enabled, two new general site options are available from the General Site Options page, as follows:

- **Allowed IP Ranges** – List of all IP ranges, in IPv4 CIDR format, able to access the environment. You can enter multiple IP ranges using a pipe ("|") as the separator between ranges. For example, "173.227.23.2/32" indicates a single value and "173.227.23.2/32|92.168.0.0/24" indicates two values.
- **Redirect URL for restricted IPs** – The destination users are re-directed to if they are not allowed access. For example, a user may be re-directed to a corporate website home page or a dedicated access denied page.



Refer to the Network settings section of the General Site Options in the Oracle CPQ Administration Online Help for more information.

USER TYPE BEST PRACTICES

Oracle CPQ 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. This is based on the principle of least privilege (PoLP). You can find more information on this concept at https://www.cyberark.com/what-is/least-privilege/.

Host Company refers to the hosting company, which is designated as FullAccesswithESales company type. This company hosts companies, called Partner Organizations, which assist the Host Company in achieving its goals. 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 an Oracle CPQ site. They have access to both the Oracle CPQ Administration Console and the user side of Oracle CPQ. Administrative functions can only be performed by SuperUser or FullAccess users. Admin functions include making changes to Configuration (adding attributes, creating rules, etc.) and modifying Commerce Processes.
Sales Users	Sales users only have access to the user side of Oracle CPQ and use it to configure products, create Transactions, and create proposal documents. There are three types of sales users: SalesAgent, ChannelAgent, RestrictedAccess, and Sales Agent. For additional information, refer to the Oracle CPQ Administration Online Help.

A user can be setup to have Web Services only access. A Web Services Only user is granted access to make Web Services calls to the Oracle CPQ site but is not permitted to login through the web interface. Web Services only users are commonly used when integrating Oracle CPQ to other applications.

COMMERCE BEST PRACTICES

Commerce is one of the foundational pillars of Oracle CPQ 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 Oracle CPQ or 2) must be encrypted. Encryption is asymmetric.

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

When an Oracle CPQ 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 Oracle CPQ. The customer's system, located in their controlled database, handles data storage, security, and any further encryption and decryption.

Oracle CPQ 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

Administrators can utilize user roles to customize views and deny access to attributes and actions 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 and their participant profiles, 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. Administrators can create auto-forwarding rules for each workflow step and base them on any number of criteria.

NOTE: Use the defined user roles and steps to restrict all sensitive attributes from the view of users with no need to view them.

Approvals

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 some 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.

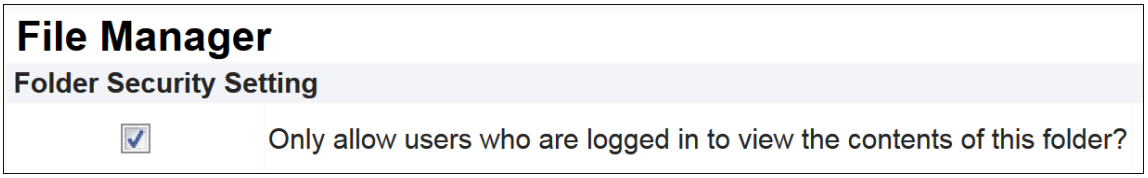
File Manager

File Manager is an integral part of Oracle CPQ. Customers can upload files to the File Manager, organize files into folders, and access files from anywhere on the Internet. The File Manager can store 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 Oracle CPQ 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.



5. Click **Save**.

HOME PAGE BEST PRACTICES

Administrators can customize the Oracle CPQ home page and use features on a customer's Oracle CPQ site to apply custom headers and footers, which are placed on the site without Oracle CPQ 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 allow listing for cross origin JavaScript calls is not setup for Oracle CPQ by default. If the functionality is needed for an Oracle CPQ site, open a Service Request (SR) on My Oracle Support.

API PROGRAMMING BEST PRACTICES

Oracle CPQ offers REST and SOAP APIs for interacting with Oracle CPQ objects. The Oracle CPQ 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, HTTP Basic Authorization (Basic Auth) headers, or a session cookie. Oracle does not recommend Basic Auth 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 Basic Auth, 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	Oracle CPQ 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 Oracle CPQ. To prevent unintentional information disclosure, Oracle strongly recommends that request attempts do not follow this transport method.
Oauth Provider	It is important that only trusted clients are allowed access to Oracle CPQ resources. Since Oracle CPQ 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:

- Oracle CPQ 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 Oracle CPQ objects. Most REST calls are synchronous and all REST calls are stateless.
- REST calls tax the Oracle CPQ system in an equivalent manner to a user performing the same operation through the Oracle CPQ 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 Oracle CPQ data tables for use in Oracle CPQ processing. Since the data can contain sensitive information, Oracle CPQ 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 Oracle CPQ 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 Oracle CPQ. 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 Oracle CPQ application, session cookies are maintained only for an active Oracle CPQ session. Once the active session is closed, tracking of cookies ends and all cookie-related data is deleted and not retained within the Oracle CPQ application.

CONNECT WITH US

Call +1.800.ORACLE1 or visit oracle.com.
Outside North America, find your local office at oracle.com/contact.

blogs.oracle.com facebook.com/oracle twitter.com/oracle