Oracle

Construction Intelligence Cloud Advisor Security Guide

December 2023

Oracle Construction Intelligence Cloud Advisor Security Guide

Primary Author: Oracle Corporation

Contents

Security Considerations

For any company that deals with sensitive data, keeping it secure is crucial to success. While hosting Construction Intelligence Cloud Advisor data on Oracle Cloud provides security measures, it can't do everything. It is the responsibility for all users working in Construction Intelligence Cloud Advisor and all source products to work in a secure manner to ensure the safety, correctness, and security of their data.

Security is everyone's business. This information is for anyone who uses, manages, or is just interested in Construction Intelligence Cloud Advisor for making decisions. If you're a security expert or administrator, this is a good place to start. It should help you see the big security picture and understand the most important guidelines related to security in Construction Intelligence Cloud Advisor.

In This Section

Authentication: How Users Sign On

If your Construction Intelligence Cloud Advisor environment is provisioned in Oracle Cloud Infrastructure (OCI), it comes with an identity management domain for access management.

Authentication refers to the way users sign on. Administrators can—and should—implement Single Sign-on (SSO). SSO reduces the number of passwords users have to remember. It also enables multi-factor login, which is when users are asked to provide some verification in addition to their passwords, like a code that they receive via text or email.

Authorization: What Users can Access

Authorization determines what users can access. There are several ways to manage this in CIC Advisor.

Permission Sets: In CIC Advisor, permission sets help administrators view and set permissions for many users by listing permissions in multi-dimensional tables.

Groups: Security groups make it easier for administrators to assign permission sets to multiple users at the same time. CIC Advisor users need to be assigned access to P6 EPPM, and in Primavera Administration, CIC Advisor users should be assigned the roles of **CIC Production Administrator** and **CIC Production.** For more details, see *Manage Application Access* topic in the *Primavera Administration Identity Management Administration Guide* .

Machine Learning Security Considerations

It is important to understand the following security considerations while providing access to administrators and users.

CIC Advisor users don't have visibility to the following data:

- Data in source applications outside their access purview
- Training data in CIC Advisor

Furthermore, they don't have access to personal information (PI) data, ML models, and cannot change model code. At no point are the models exposed to organizations that could change access or inject malicious adjustments. Additionally, no PI is used in training or testing.

However, some cautions unique to security in machine learning are in order and discussed below:

- The CIC Advisor administrator role is very powerful and therefore must be granted judiciously.

  The CIC Advisor administrator role grants access to the **CIC Advisor Administration** application. This administration application gives CIC Advisor administrators access to the **ML Workbench** page. On the **ML Workbench** page, administrators can explore and see the models to be trained or retrained and determine which feature selections to enable or disable for each model. When a model is retrained, if new data has been added into the training set, it could cause current predictions to change. Therefore, granting access to administration application and **ML Workbench** page should be limited and restricted.
- Administrators should be cautious of input poisoning.

  Data used in training shapes future predictions. Malicious or bad data can lead to bad future predictions. CIC Advisor administrators should be aware of the projects opted into the system and also aware of which projects are used for training the models that leads to prediction accuracy. Use security best practices such as Separation of Duty controls outlined in the *Product/Service Feature Guide of Oracle CIC Advisor (Doc ID 114.2)* on My Oracle Support to ensure that those choosing the projects for CIC Advisor, which will also be used for training, opt in their target data appropriately.

  Unintended or misleading source data can affect outputs. CIC Advisor is delivered with multiple off-the-shelf *Seed Models*, which are trained with sample data. These are not ideal models to use, but they give your organization a good starting point for enabling the system, and to see a first round of predictions while you understand how to train with your data.
- Irrelevant features can precipitate confounding and spurious correlations.

  It is important to understand how certain features affect your predictions or how your data is reflected in the feature set. For example, if you are an organization without costs, you may want to make sure no cost features are selected. To get a basic implementation with the models you can choose *SeedModel customerData*. This model will use the Seed Model features with your data. Therefore select only the relevant features applicable for your data.
- Data Privacy and Access Controls

  The models are protected for data used in training, and users have no access to this data.

Users have access to the dashboard unless they are administrators (CIC Advisor administrator) which is role based permissions controlled by the client side. Since a regular user does not have access to the administration role (CIC Advisor administrator), they cannot poison the models by training it through introducing malicious scenarios.

Training and prediction is also controlled by administrators (CIC Advisor administrator) which enables controlled training and model executions.

- Membership Inference Attack (MIA) / Model robustness attack (MRA)

  This is an inherent weakness in machine learning.

  Machine learning is prone to new attack vectors such as the Membership Inference Attack (MIA) where the user of a ML model may be able to infer the training data. Similarly it also prone to the Model Robustness Attack (MRA) where the user of a ML model may be skew the inputs imperceptibly to cause large errors in prediction. For better security, CIC Advisor makes such attempts difficult by not exposing the model code or its hyperparameters. To further enhance the product for good privacy-preservation, continuous attempts are being made to have models learn from the training data, but do not have them memorize it and enabling defense mechanism such as, Regularization.

  Additionally, models continuously enhance to be robust by multiple tests to ensure that the accuracy does not change significantly from the base line accuracy under various conditions.

  They evolve with multiple trainings and testing on similar data but different scenarios and data points with simultaneous customer usage.

Endpoint Security

From laptops to cellphones, organizations have to keep track of data on more devices than ever, and more devices means more risk.

Inherent Risks and Practical Policies

No automated security system or protocol can make a system fully secure if those with legitimate access exploit it for illegitimate purposes or if a device falls into the wrong hands. Here are some general "common sense" guidelines you should follow when it comes to endpoint security:

Grant security permission conservatively. Don't give everyone permission to everything just to avoid perceived complexity. Remember, one breach can be many times more costly and time consuming than setting and following standard security protocols.

Organize permission sets and credentials so they can be edited quickly. Keep user groups and their permissions organized and easy to manage. Use descriptive names for permission sets, and organize them logically to make it easier for you or anyone else to manage them quickly and confidently.

Keep up with organizational changes. If a user no longer needs access to a part of the app, for whatever reason, update that user's permissions accordingly.

Privacy and Personal Information

Closely related to security are matters of privacy and personal information.

View the section *Managing Personal Information* in Construction Intelligence Cloud Advisor in the *Construction Intelligence Cloud Advisor Administration Guide* to learn about what information is collected and what you can do to monitor personal information in Construction Intelligence Cloud Advisor.

Some Security Basics

We'll use the term **administrator** to refer to anyone who's responsible for managing a company's data and who can access that data. For our purposes, administrators includes a wide variety of IT professionals, from those who define roles in the Construction Intelligence Cloud Advisor application to those who manage company servers.

An **end user** is anyone who uses Construction Intelligence Cloud Advisor to do their job. This includes project managers, executives, and everyone else who logs into Construction Intelligence Cloud Advisor from an office or jobsite to get their work done.

Administrators should...

- **Set up Single Sign-On (SSO) and enable multi-factor authentication** to minimize the number of passwords that users have to remember and to consolidate risk.
- **Kindly educate users** on how they can avoid unwittingly helping hackers. One of the best ways application administrators and security advocates can help users is by helping them to prevent security breaches.
- **Use a VPN** to encrypt data being sent over the internet.
- **Stay up-to-date** about security trends and best practices.

End users should...

- **Follow security guidelines** created by their companies and the administrators of any network applications they use.
- **Use strong passwords**. The more random-looking the better.Avoid reusing passwords to reduce the risk of intruders gaining access through exploitation of user accounts.
- **Learn to recognize phishing**. Phishing is when someone disguises an email or some other transmission as a legitimate message in an attempt to get a user to reveal sensitive information. For example, a hacker may send you an email disguised to look like an email from your employer requesting login information. These attacks are becoming more sophisticated, but you can still protect yourself by making sure any emails you receive or websites you visit are legitimate before using them to share sensitive information.

For more details, refer to the Privacy and Security Feature Guidance information for Construction Intelligence Cloud Service in the Industry Solutions (GBUs) section of Privacy and Security Feature Guidance for all Oracle Services Doc ID 114.2.

Integration with Other Applications

The ability to connect and exchange information with other applications is powerful, but it also presents some potential security issues that administrators must manage. It is important to understand which data flows between applications to ensure compliance with policies and regulations related to security and privacy.

Establishing Security Contacts

While the apps used by your organization may have some security features of their own, most security issues ultimately come down to the people who use them. When your company establishes its security procedures, it's important to also establish in-house security experts to whom other members can turn when they have security questions. Security points of contact should be continuously learning about security trends and how they can educate users to keep their data and network secure. Security contacts should also routinely update and maintain protocols that suit the security needs of their organizations.