Oracle® Construction and Engineering Intelligence

Security Guide

G14207-02
July 2025

Oracle Construction and Engineering Intelligence Security Guide,

G14207-02

Primary Author: Oracle Corporation

Contents

About This Guide

Provides important guidelines related to security in Construction and Engineering Intelligence.

Audience

This guide is intended for administrators and anyone who uses Construction and Engineering Intelligence.

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.

Conventions

The following text conventions are used in this document.

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1

Security Considerations

Authentication: How Users Sign On

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 may also enable 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.

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

Authorization: What Users Can Access

Authorization determines what users can access.

In Construction and Engineering Intelligence, users are managed using a combination of the following:

- **Roles**: Administrators can view and select one or more CIC roles for users.
- **Data Sources**: Administrators can give access to specific data sources to users and/or user groups
- **Workspaces**: Based on the user's role and access to data sources, administrators can give users access to specific workspaces in the Construction and Engineering Intelligence user interface.

Machine Learning

Some cautions unique to security in machine learning are discussed below.

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

Construction and Engineering Intelligence users don’t have visibility to the following data:

- Data in source applications outside their access purview
- Training data in Construction and Engineering Intelligence

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 Construction and Engineering Intelligence administrator role is very powerful and therefore must be granted judiciously.

The Construction and Engineering Intelligence administrator role grants access to the Administration module to manage Construction and Engineering Intelligence users and data. In addition to managing users specific to data sources, administrators can also add Construction and Engineering Intelligence-only users, to accommodate those users who are not necessarily associated with a specific data source. Therefore, granting access to administration module 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. Construction and Engineering Intelligence 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 Construction and Engineering Intelligence, which will also be used for training, opt in their target data appropriately.

  Unintended or misleading source data can affect outputs. Construction and Engineering Intelligence 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 (Construction and Engineering Intelligence administrator) which is role based permissions controlled by the client side. Since a regular user does not have access to the administration role (Construction and Engineering Intelligence administrator), they cannot poison the models by training it through introducing malicious scenarios.

  Training and prediction is also controlled by administrators (Construction and Engineering Intelligence 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 an ML model may be able to infer the training data. Similarly it is also prone to the Model Robustness Attack (MRA) where the user of an ML model may be able to skew the inputs imperceptibly to cause large errors in prediction. For better security, Construction and Engineering Intelligence 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 mechanisms such as, Regularization.

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

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

2

Endpoint Security

From laptops to cell phones, 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 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.

3

Privacy and Personal Information

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

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

Some Security Basics

We'll use the term *administrator* to refer to anyone who is 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 and Engineering Intelligence application to those who manage company servers.

An end user is anyone who uses Construction and Engineering Intelligence to do their job. This includes project managers, executives, and everyone else who logs into Construction and Engineering Intelligence 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.
- 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, see the Privacy and Security Feature Guidance information for Construction and Engineering Intelligence Service in the Industry Solutions (GBUs) section of Privacy and Security Feature Guidance for all Oracle Services (Doc ID 114.2).

4

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.

5

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 is important to also establish in-house security experts to whom other members can turn to 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.