Oracle

Construction Intelligence Cloud Analytics Security Guide

December 2023

Oracle Construction Intelligence Cloud Analytics 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 Analytics data on Oracle Cloud provides security measures, it can't do everything. It is the responsibility for all users working in CIC Analytics 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 CIC Analytics 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 CIC Analytics.

In This Section

Authentication: How Users Sign On

If your CIC Analytics Cloud 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 Analytics.

Permission Sets: In CIC Analytics, 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 Analytics users need to be assigned access to the Analytics module within P6 and Unifier application respectively**.** For more details, see *Manage Application Access* topic in the *Primavera Administration Identity Management Administration Guide*

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 CIC Analytics in the *Construction Intelligence Cloud Analytics Administration Guide* to learn about what information is collected and what you can do to monitor personal information in CIC Analytics.

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 CIC Analytics application to those who manage company servers.

An **end user** is anyone who uses CIC Analytics to do their job. This includes project managers, executives, and everyone else who logs into CIC Analytics 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.