Cloud Hosted Content Manager with Information Proficiency

Frequently Asked Questions

What is Cloud Hosting?
Cloud hosting is when software is installed on infrastructure that is not within your office network.

The servers used are typically deployed by Microsoft Azure or Amazon Web Services.

What ways can Content Manager be Cloud Hosted?
CM can be implemented in the cloud in a few ways. Here are the common approaches:

If your internal IT already have a cloud infrastructure deployment, then Content Manager can be hosted within this infrastructure. This is the equivalent of "renting" a server. Your IT department will still need to maintain the servers and the application. Information Proficiency can assist to install and configure the application with or for you.

If you don't want to manage the infrastructure or application, then we can host the application for you. We rent the server, install the application, and configure connectivity between you and the cloud server. We also maintain the servers and the application.

NOTE: The remainder of this document assumes that Information Proficiency are hosting Content Manager for you.

What type of CM licence do I need?
You can use your *existing* perpetual licence, or a CM Select licence. When you use Information Proficiency as your Cloud Hosting provider you can BYO your existing licences, we have no requirement to convert your existing licences to a subscription model.

What version of Content Manager will I be running?
We can host Content Manager versions 9.3 and later in the cloud. The version deployed is specifically for you, so we have no constraints based on what other customers are doing.

Where is my data stored?
We only use Microsoft Azure infrastructure, located within Australia. Our preference is to utilise datacentres that are closest to your physical office.

Do I have access to my data?
You will have access to all your records through Content Manager as per normal. As the infrastructure is managed by us through the agreement we have in place with you, remote desktop protocol (RDP) access is not provided.

Is my data secure?
In short, yes. All access to machines hosting your data requires two-factor authentication.

All data is "encrypted at rest" and in transit, which means that not even Microsoft can access your data.

How does authentication work?
We configure "Azure AD" authentication for the desktop client and the web client.

This prompts users to log in using their Microsoft account, which will be linked to your Office 365 deployment.

The existing Single Sign On (SSO) using domain credentials is not possible, since our servers are not joined to your IT domain.

Will I have access to Content Manager from outside my office network?
Absolutely, if that's an option you'd like. The cloud hosted solution provides the flexibility to work both onsite and offsite, and the Microsoft authentication is available everywhere.

What if I have integrations in place?
Most common integrations utilise the cloud API for Content Manager, or a desktop client API. Both are supported by a cloud deployment of CM. We would need to understand your integrations as part of quoting and deployment planning.

What do we need to do to get it set up?
The basic transition plan involves these steps:

1) Size and deploy the infrastructure (we set up the servers and ensure enough space is configured);
2) Implement the pre-production environment (install software and take an initial copy of your data);
3) Test the pre-production infrastructure (this involves functionality, performance, and security testing);
4) Transition the current environment to the cloud environment (this involves the rollout of desktop clients, suspending the existing servers, transferring data to the cloud, and bringing up the cloud environment in production mode); then it's ….
5) Business as usual

What about backups?
We ensure that Content Manager is backed up according to best-practice.

We have a well documented and tested disaster recovery plan in place and in the event of it being required, your data is able to be recovered quickly with minimum disruption.

The backups maintained by Information Proficiency are primarily intended for us to maintain a level of service to you as we perform disaster recovery on your behalf. If required, we can work with your IT department to ensure the backups are captured using your preferred backup system. If your IT Department are performing the backups outside of the cloud service this can lead to delays if disaster recovery is required.

What if I don't want to continue with the cloud service?
We can work with your IT Department to execute a transition-out programme, where the cloud service is retired, and the data is returned to you to manage accordingly. This process can involve several phases as the implementation and testing of an alternative solution are executed.