

# BYO Identity

## Release Date:

Bring Your Own Identity (BYOI) will be available for non-government clients from 24 November 2021.

It will be available for government clients in early 2022.

BYOI is an improved way to log in to CloudCreator. Instead of using your CloudCreator username, password and one-time password, you can opt to use your existing corporate user credentials. It can also be used to supplement existing CloudCreator User Accounts. BYOI is based on the open SAML standard.

## Topics

- [Why Use BYOI?](#)
- [What are the Costs?](#)
- [Set up BYOI](#)
- [Access CloudCreator with BYOI](#)
- [One CloudCreator User Per Browser Application](#)
- [Create and Manage BYOI Users](#)
- [Use CloudCreator with Both Traditional and BYOI Users](#)
- [Access CloudCreator When BYOI is Down](#)
- [CCL Staff Managing Your Services with BYOI](#)
- [Unsubscribe from BYOI](#)

## Why Use BYOI?

The benefits of choosing to use BYOI include:

<b>Improved User Experience</b>	<ul style="list-style-type: none"><li>• Fewer credentials are needed. There's no need to remember a specific CloudCreator username and password. Simply use your usual corporate credentials.</li><li>• Less authentication tools. Instead of the usual CloudCreator PIN and one-time password, you can use your usual corporate multi-factor authentication tool.</li><li>• Consistent multi-cloud experience. If your company is using AWS and/or Azure, you can set up SAML with CloudCreator, AWS, and/or Azure. This will give you a consistent log in experience, using your corporate credentials across all three clouds.</li></ul>
<b>Reduced Cost</b>	<ul style="list-style-type: none"><li>• There is no monthly charge for BYOI users.</li><li>• Traditional CloudCreator users continue to come with a small monthly charge.</li></ul>
<b>Improved Security</b>	<ul style="list-style-type: none"><li>• When a new person joins your organisation, their corporate user credentials will immediately apply to CloudCreator. However, before they can do anything in CloudCreator, your Global Admin has to assign one or more CloudCreator roles to them.</li><li>• When a person leaves your organisation and their corporate user credentials are revoked, their ability to log into CloudCreator is also immediately revoked.</li></ul>

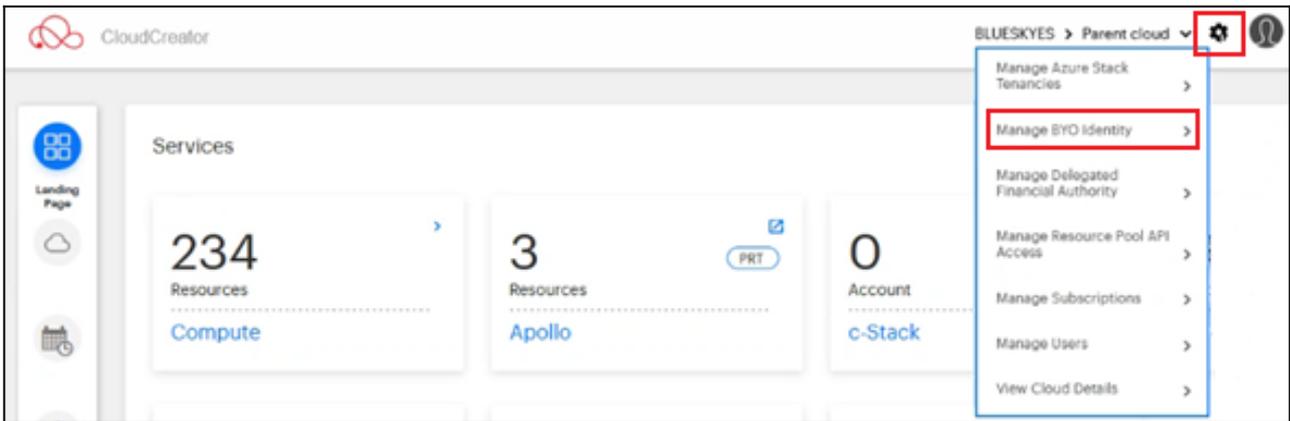
## What are the Costs?

BYOI is a free and optional feature of CloudCreator. The only associated cost is the time it takes for the initial set up. This is described below.

### Set Up BYOI

Follow the steps below to set up BYOI. These steps assume that your organisation already has 'traditional' CloudCreator users who log in with a username, password and one-time password.

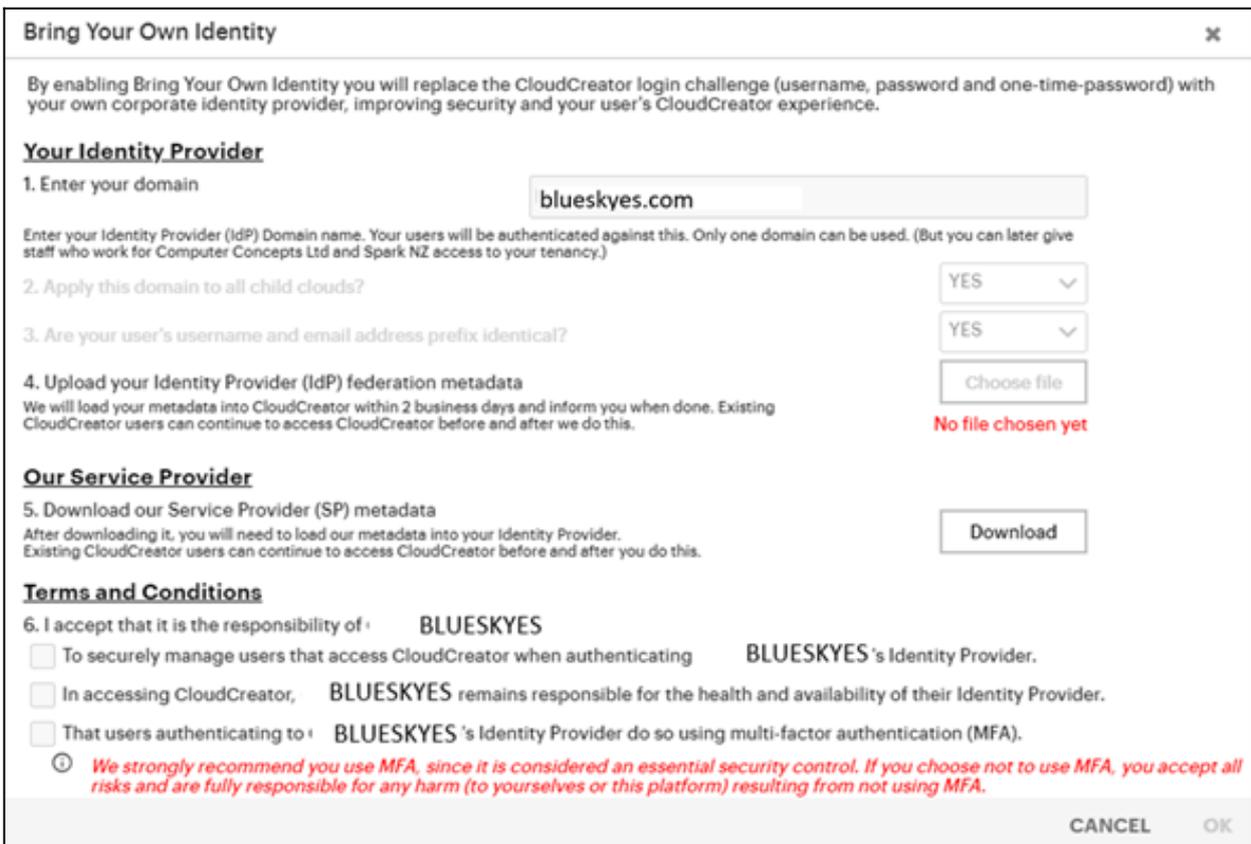
1. At the top of the CloudCreator screen, select the **Options Cog**  > **Manage BYO Identity**.



2. Complete the fields on the **Bring Your Own Identity** page. Use the table below as a guide.

**Note:**

- You must be logged in as a CloudCreator user with the Global Security Admin (GSA) role.
- In the screenshot below, 'BLUESKYES' is the name of the cloud that the BYOI functionality will be added to.

A screenshot of the 'Bring Your Own Identity' configuration page. The page is titled 'Bring Your Own Identity' and contains several sections: 'Your Identity Provider' with fields for domain (blueskyes.com), application to child clouds (YES), and identical username/email prefixes (YES); 'Our Service Provider' with a 'Download' button for SP metadata; and 'Terms and Conditions' with checkboxes for accepting responsibility and MFA. A red warning message states: 'We strongly recommend you use MFA, since it is considered an essential security control. If you choose not to use MFA, you accept all risks and are fully responsible for any harm (to yourselves or this platform) resulting from not using MFA.' The page ends with 'CANCEL' and 'OK' buttons.

3. Use this table to complete the fields:

Field	Description
1. Domain Name	The domain name of your identity provider.
2. Apply this domain to all child clouds?	Select whether all child clouds will be enabled at the same time. To understand the concept of child clouds, see <a href="#">About Virtual Clouds</a> . Child clouds can be linked later to the same domain if required. This option just allows the entire environment for a client to be updated in a single action.
3. Are your user's username and email address prefix identical?	This has no effect on the setup process but does affect the user management functions inside CloudCreator once the identity link is in place. Where the username and email prefix are different, you must also record a user's email address when they are enabled.
4. Upload your Identity Provider (IdP) federation metadata.	Upload your IdP file here. This will be loaded against your cloud environment as a separate manual step.
5. Download our Service Provider (SP) metadata.	Record our details on your Provider. This means that both parties have the relevant details of each other. This is a pre-requisite for establishing this trusted relationship.
6. Terms and Conditions	Review and accept the terms and conditions. By default, CloudCreator requires multi-factor authentication. CCL strongly recommends having this in place via your own Identity Management.

4. Complete the back end set up required with your identity access provider. For guidance see [Set Up Azure AD Identity Provider](#). If you have a different identity provider, this information may still be useful.

### Access CloudCreator with BYOI

Once BYOI is enabled, follow these steps to access CloudCreator:

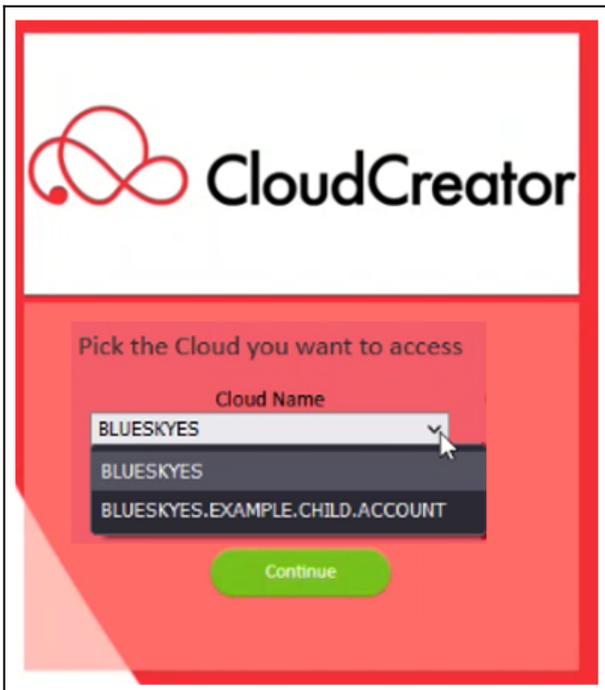
1. Browse to the URL for your domain. For example:

- Non-government clients: <https://myauth.cloudcreator.co.nz/blueskyes.com/> (your domain name will appear in the URL instead of 'blueskyes.com').
- Government clients: <https://myauth.homeland.revera.co.nz/blueskyes.com/> (your domain name will appear in the URL instead of 'blueskyes.com').

**Note:** A forward slash / appears at the end of these domains.

2. If you're not already logged in, you'll be redirected to your corporate login page. Once you have successfully completed this login process, and assuming your BYOI ID has access to exactly one cloud, you will be automatically redirected to the CloudCreator landing page.

3. If your BYO ID has been established as a user in more than one cloud, select the cloud you want to access.



4. If you don't already have a role assigned, you'll see an Access Permission Request (shown below). Complete the fields and click **Submit**.

The image shows a form titled "Access permission request" with a red header. Below the header, the text "Let your GA know why you need access to the CloudCreator Cloud" is displayed. The form contains three input fields: "First Name", "Last Name", and "Reason for access". At the bottom of the form, there is a "0/150" character count, a "Cancel" button, and a "SUBMIT" button.

5. Your Global Admin will assign the appropriate role, and ask you to log in again.

Inside CloudCreator users are assigned 'roles' that determine their rights of access to information and functions. To find out more, see [Roles and Permissions](#)

### One CloudCreator User Per Browser Application

Most people only have one CloudCreator user. But if you are an existing client implementing BYOI, your people may have both a traditional CloudCreator user and a BYOI CloudCreator user during a transition period of say a month.

It is important to know that CloudCreator only supports one CloudCreator user per browser application (not browser tab). To avoid problems, the simple rule is:

**If you are logged into CloudCreator as one user, and you want to log in CloudCreator as a different user, close the browser application (not tab), and re-open it.**

The reasons for this approach include security reasons, user experience reasons, and avoiding user confusion leading to mistakes. This approach applies to traditional CloudCreator users, and CloudCreator BYOI users also apply this approach. Having multiple different CloudCreator users (whether they are traditional users, BYOI users, or a mixture) logged in on different tabs within the same browser application doesn't work safely.

Once logged into CloudCreator, a user may use several tabs at the same time (to display dashboards or access service admin portals). When you are finished using CloudCreator, it is a good security practice to close **all** CloudCreator tabs (as they may be displaying sensitive data). An even better practice is to close the browser application. This is a good practice whether you only have one CloudCreator user or multiple CloudCreator users.

---

### **Create and Manage BYOI Users**

BYOI users are created and managed the same as 'traditional' users. See [Manage Users and Assign Roles](#)

#### **Create BYOI Users with Multiple Logins**

In rare cases, you may have a single user who needs two distinct logins to CloudCreator. For example, a user may log in as a Global Admin each day, but on rare occasions may need to log in as a Global Security Admin. Find out how to create these users here: [Create BYOI Users with Multiple Logins](#).

---

### **Use CloudCreator with Both Traditional and BYOI Users**

If you have traditional CloudCreator users set up, they can log in the same way before, during and after the BYOI set-up process.

Before deleting any traditional CloudCreator users, make sure that they have successfully logged into CloudCreator using their corporate credentials, and can use the functions related their role. This is to prove that BYOI is correctly set up and that the user has the correct roles assigned to them.

---

### **Access CloudCreator When BYOI is Down**

It is recommended that you retain 1 or 2 traditional CloudCreator users with the Global Admin role. These users would only be used in a 'break glass' situation, such as when your corporate identity system is down, and BYOI users can't log in to CloudCreator.

In an emergency, you can also contact the CCL Service Desk and have a traditional CloudCreator user with the Global Admin role created. However, this process includes security checks and will take time to be processed.

---

## **CCL Staff Managing Your Services With BYOI**

Once you have set up BYOI, your organisation can still use CCL staff to help manage its CCL services on an ongoing basis.

Our staff currently provide help by using a dedicated traditional CloudCreator user to log into your CloudCreator tenancy. In late 2021, these traditional CloudCreator users will be deleted and replaced by BYO Identity users. The way these users appear in CloudCreator and how they are managed will not change. The new users will:

- Have the same CloudCreator roles
- Appear the same way in the CloudCreator Manage Users page, and
- Be able to have roles added or removed to them in the CloudCreator Manage Users page.

---

## **Unsubscribe From BYOI**

Follow these steps to unsubscribe from BYOI.

1. Log a ticket with CCL to request that your Active Directory is unlinked from your CloudCreator accounts. You can request to unsubscribe individual CloudCreator accounts. For example, if you have a Parent account, and two Child accounts, you can unsubscribe one of the Child accounts.
  2. Allow a few days' notice for the request to be actioned.
  3. CCL will validate the request with senior contacts at your organisation and plan the date/time of the action.
-