Account-driven Enrollment Methods with Apple Devices using Cloudflare

Rev. 20241226

Contents

Preface

What is the purpose of this guide?
This guide offers an alternative for organizations that prefer not to host the com.apple.remotemanagement file on their public web server for Account-driven enrollment. By leveraging Cloudflare, you can manage the com.apple.remotemanagement file externally while maintaining secure access. To implement this configuration, you'll need to update your domain's DNS name servers through your domain registrar and configure DNS records in Cloudflare to ensure proper routing for your web server, mail server, and any other critical services linked to your domain. This guide uses Jamf Pro as the MDM server however, the process is compatible with any MDM server supporting Account-driven enrollment.

CAUTION: USE THIS GUIDE AT YOUR OWN RISK.

This guide requires a Cloudflare account and changing your current DNS name servers to Cloudflare name servers. If that is not an option for your organization, this guide is not for you. If you decide to go forward with this guide, we highly recommend using a non production domain as a Proof of Concept test to ensure you get the desired results.

What is Cloudflare?
Cloudflare is a global network service provider that offers a range of solutions for website security, performance, and reliability. Primarily known for its content delivery network (CDN) and DNS services, Cloudflare improves website speed by caching content on its global network and reducing load times for visitors across the world. By offering these tools and a global network, Cloudflare supports websites and applications, helping them stay fast, secure, and resilient against attacks. Cloudflare offers free and paid accounts.

What is Account-driven enrollment?
Account-driven enrollment is intended for organizations that require personal devices to be enrolled in a Mobile Device Management (MDM) solution, particularly for Bring Your Own Device (BYOD) scenarios. This enrollment method allows users to maintain ownership of their devices while still providing secure access to the organization's resources. It achieves a balance between organizational security and user privacy. A key requirement of Account-driven enrollment, is ensuring the com.apple.remotemanagement file is accessible remotely.

NOTE: Account-driven enrollment is for both device and user enrollment. This guide will cover Account-driven user enrollment only.

What is the purpose of the com.apple.remotemanagement file?
When a device attempts to initiate Account-driven enrollment, it checks for the presence of the com.apple.remotemanagement file hosted on the organization's domain in a directory named .well-known. This file confirms that the domain supports Account-driven enrollment, allowing the user to proceed with device enrollment..

What you will need to following along with this guide:
- Administrative access to your MDM server (this guide uses Jamf Pro).
- Administrative access to your domain registration provider.
- Administrative access to Cloudflare.

Additional Resources:
https://learn.jamf.com/en-US/bundle/technical-articles/page/Prepare_for_Account-Driven_Enrollment_with_Managed_Apple_IDs_and_Service_Discovery.html

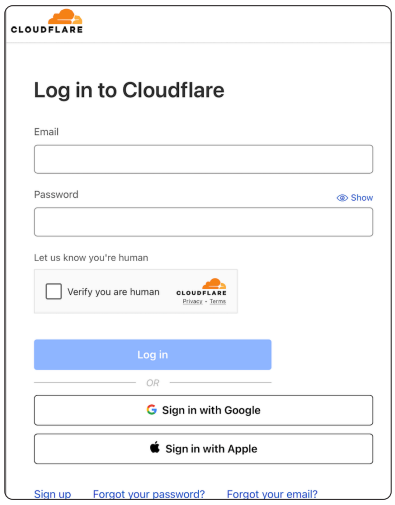
https://hcsonline.com/support/resources/white-papers/how-to-configure-account-driven-enrollment-and-enroll-a-personal-device-in-jamf-pro

https://support.apple.com/guide/deployment/account-driven-enrollment-methods-dep4d9e9cd26/web

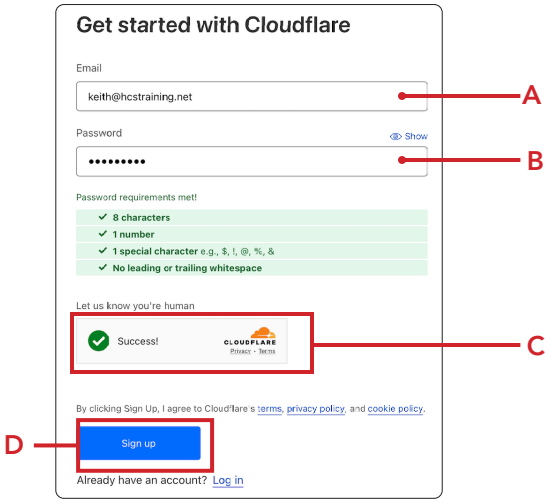
Section 1: Creating a free Cloudflare account.

NOTE: If you already have a Cloudflare account, move on to Section 2 of this guide.

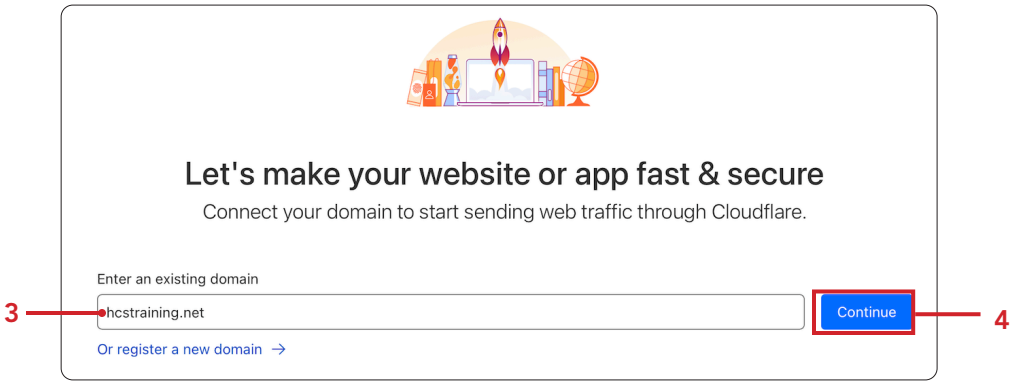
1. Create a Cloudflare free account here: https://dash.cloudflare.com/login. Click Sign up.



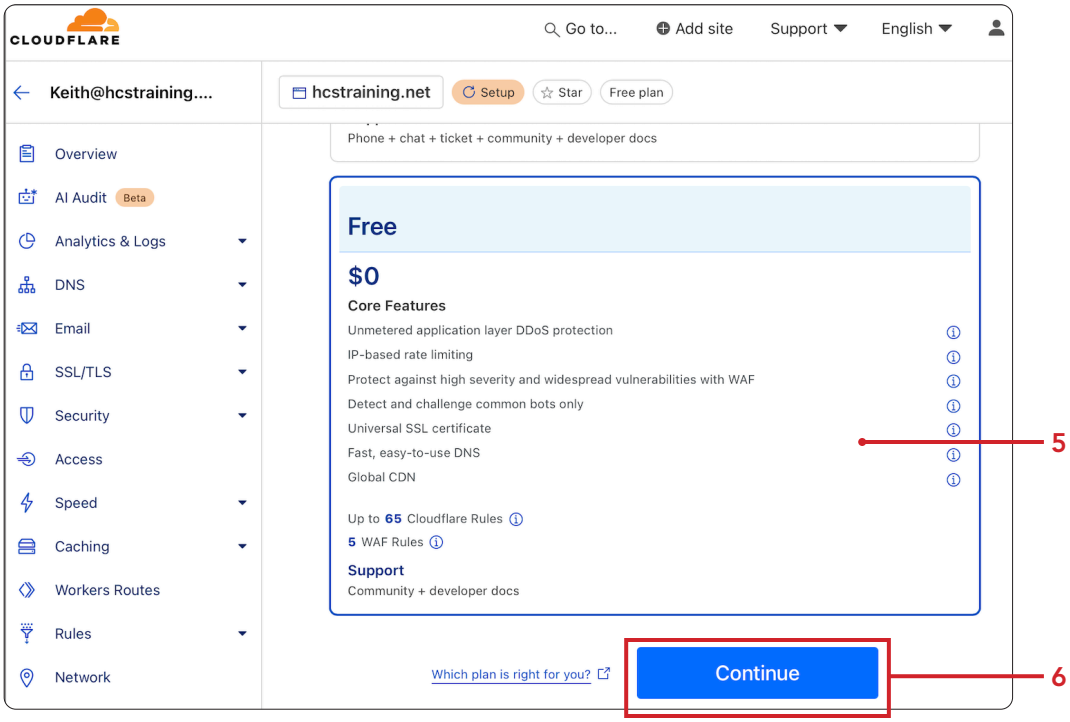
2. Enter the following:
   A. Email: Enter your email address.
   B. Password: Enter your password.
   C. Select the checkbox for the CAPTCHA verification (Under Let us know you're human).
   D. Click Sign up.
   E. Check your email account for a verification email from Cloudflare.



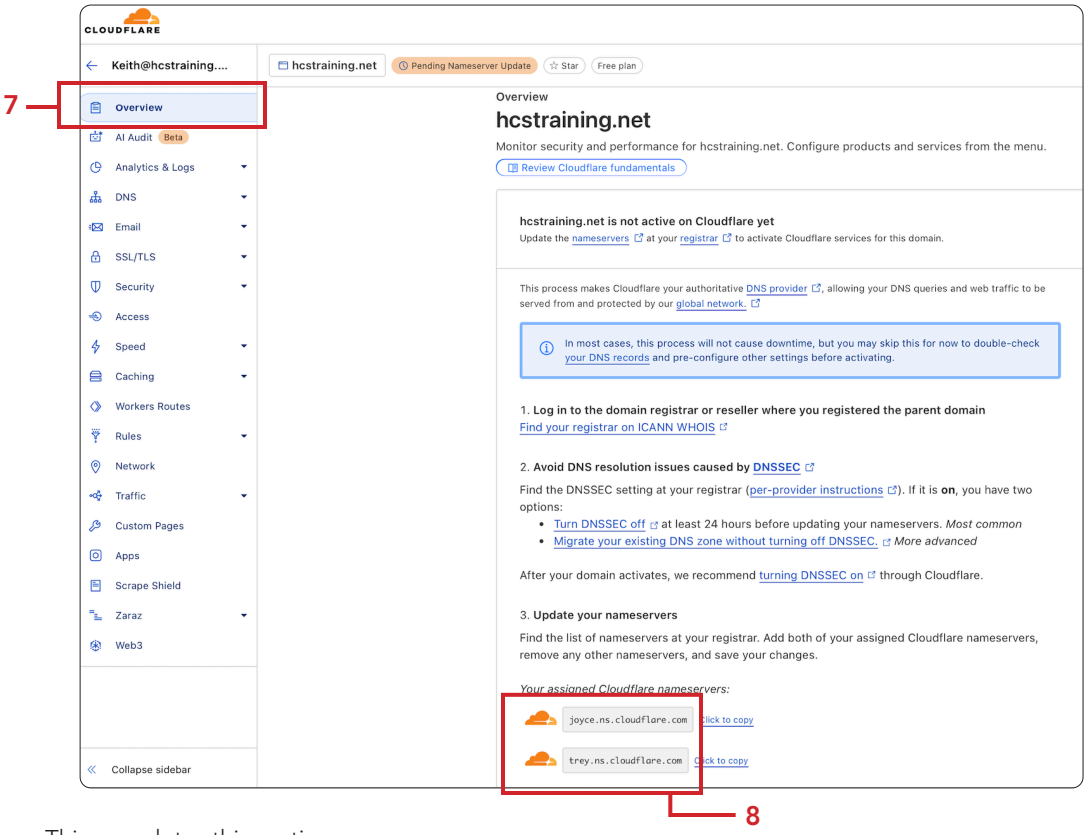
3. Enter an existing domain.
4. Click Continue. This will be the domain name that you want to use for Account Driven user enrollment. This guide will use hcstraining.net.



5. Scroll down and select the Free plan.
6. Click Continue.



7. Click Overview from the sidebar.
8. Copy your assigned Cloudflare nameservers to a text document. You will need them in section three of this guide.

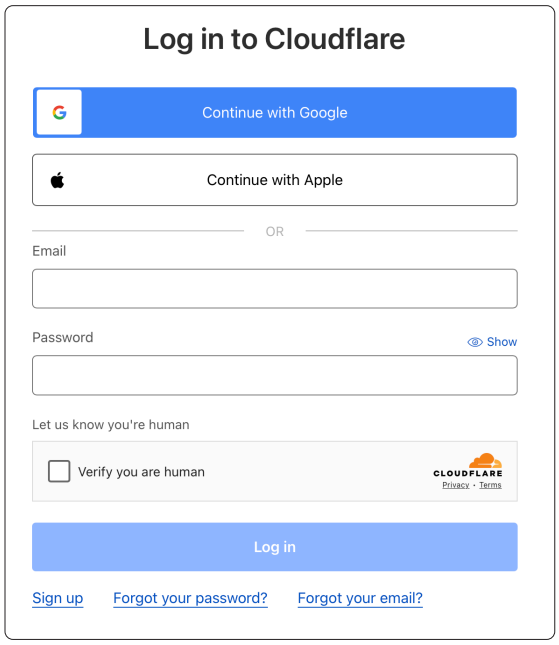


This completes this section.

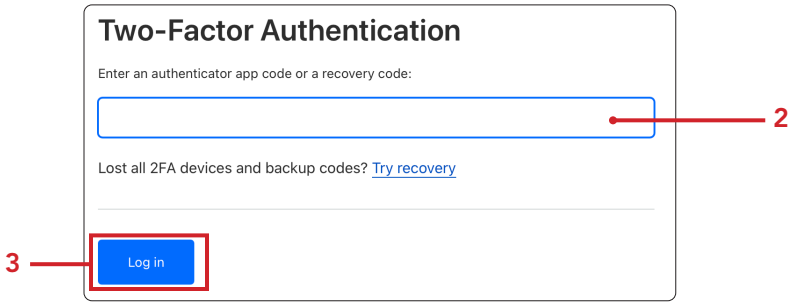
Section 2: Log into your existing Cloudflare account

NOTE: Skip this section if you created a free Cloudflare account in Section 1 of this guide.

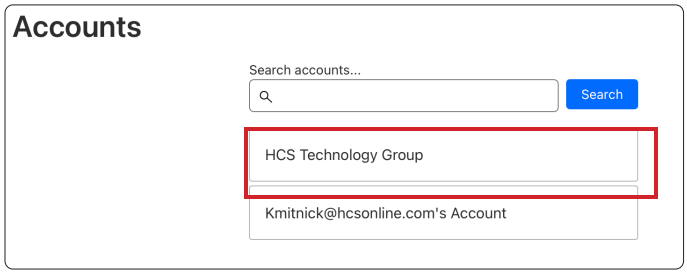
1. Log into Cloudflares with administrative credentials. http://cloudflare.com



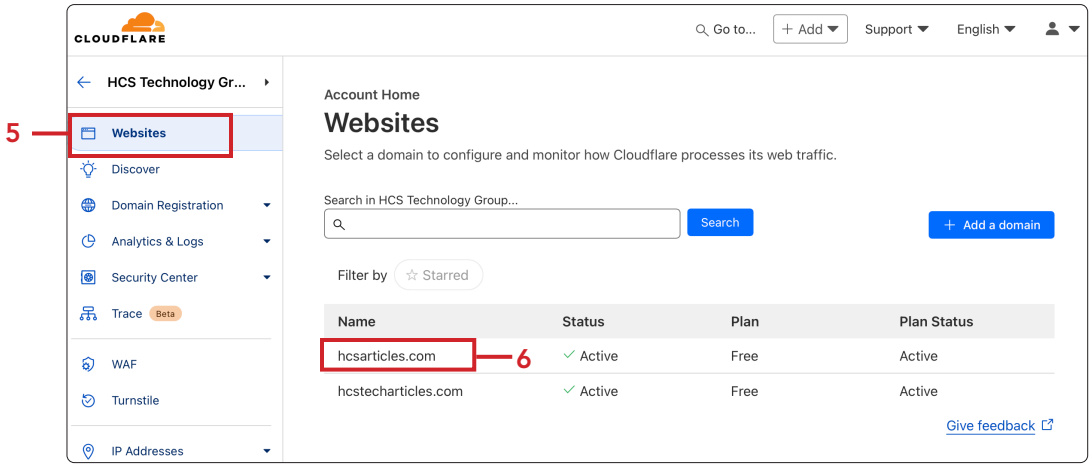
2. If you have Two-Factor Authentication enabled, enter your code.
3. Click Log in.



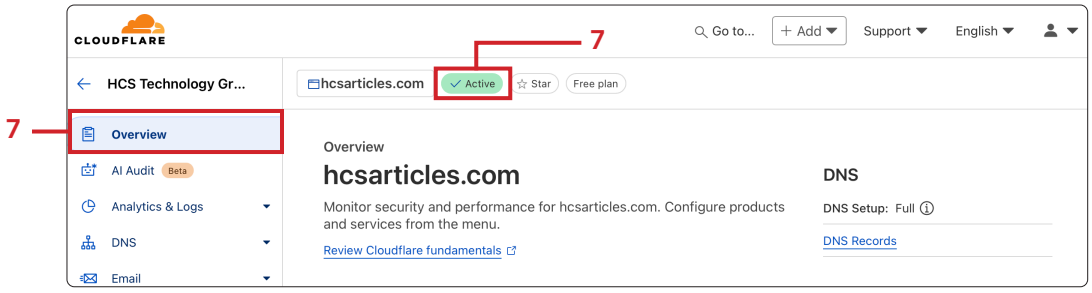
4. Select the account you want to use. This guide will select HCS Technology Group.



5. If not already selected, select Websites from the sidebar.
6. Select the website that you want to configure.



7. Select Overview from the sidebar.
8. Confirm the Active button is green which indicates your Cloudflare name servers are configured at your domain registration provider.
   NOTE: If the Active button is NOT green, you will need to configure your Cloudflare name servers at your domain registration provider.



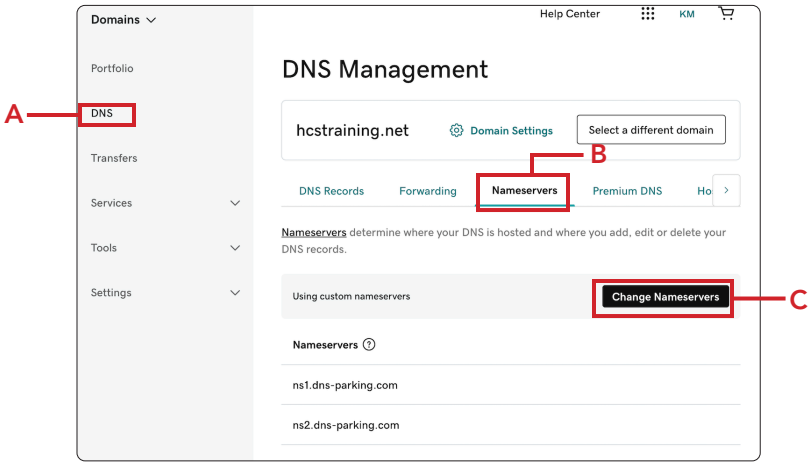
This completes this section.

Section 3: Adding Cloudflare name servers to your domain registration provider.

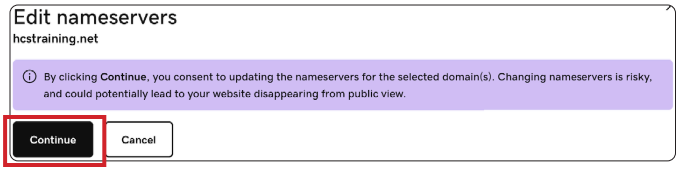
If you have an existing Cloudflare account and already configured your Cloudflare name servers, skip to Section 4 of this guide.

1. Log into your domain registration provider. This guide will use godaddy.com as the domain registration provider.
   A. Click DNS
   B. Click Nameservers
   C. Click Change Nameservers

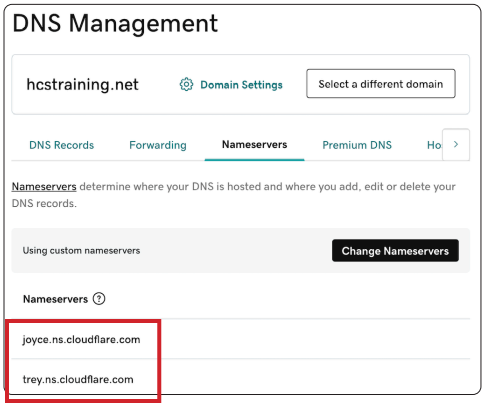
   NOTE: If you're not using godaddy.com as your provider, you will need to find the DNS management section for your provider.



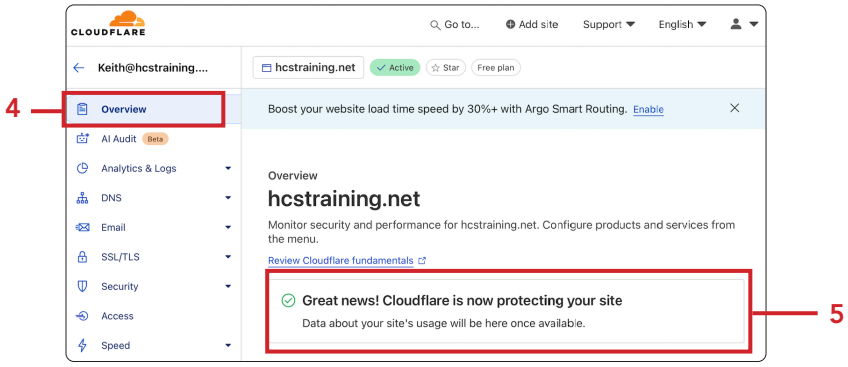
2. Click Continue.



3. Verify the nameservers were changed.
   NOTE: You may need to refresh your web browser to see the name server changes.



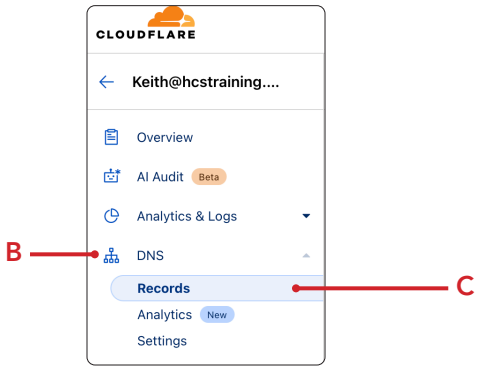
4. Switch back to Cloudflare. Click Overview.
5. Confirm your site is protected by Cloudflare and have a green Active symbol.
   NOTE: It can take a few hours for your site to show as active in Cloudflare.



This completes this section.

Section 4: Configuring DNS records in Cloudflare.

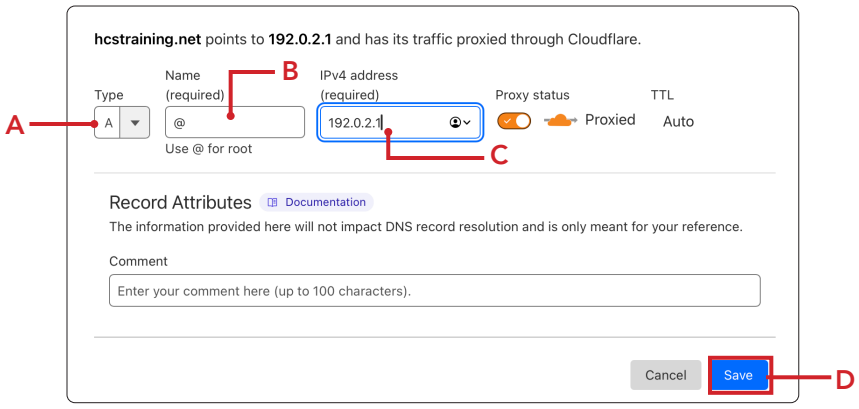
1. Click DNS from the sidebar.
2. Click Records.



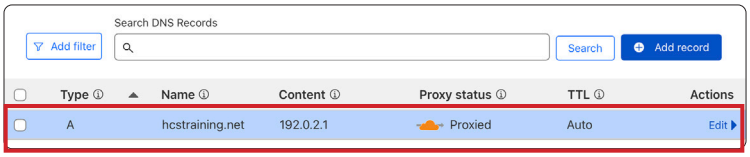
3. Click Add record.

4. Configure the following:
   A. Type: A
   B. Name: @
   C. IPv4 address: 192.0.2.1
   D. Click Save

Cloudflare uses the IP address "192.0.2.1" as a placeholder IP address to represent their network when a website is using their proxy service.



5. Confirm the A record was created.
   NOTE: Depending on your environment, you may need to add additional records in your Cloudflare for mail and other internet services. This guide only covers adding one A record.

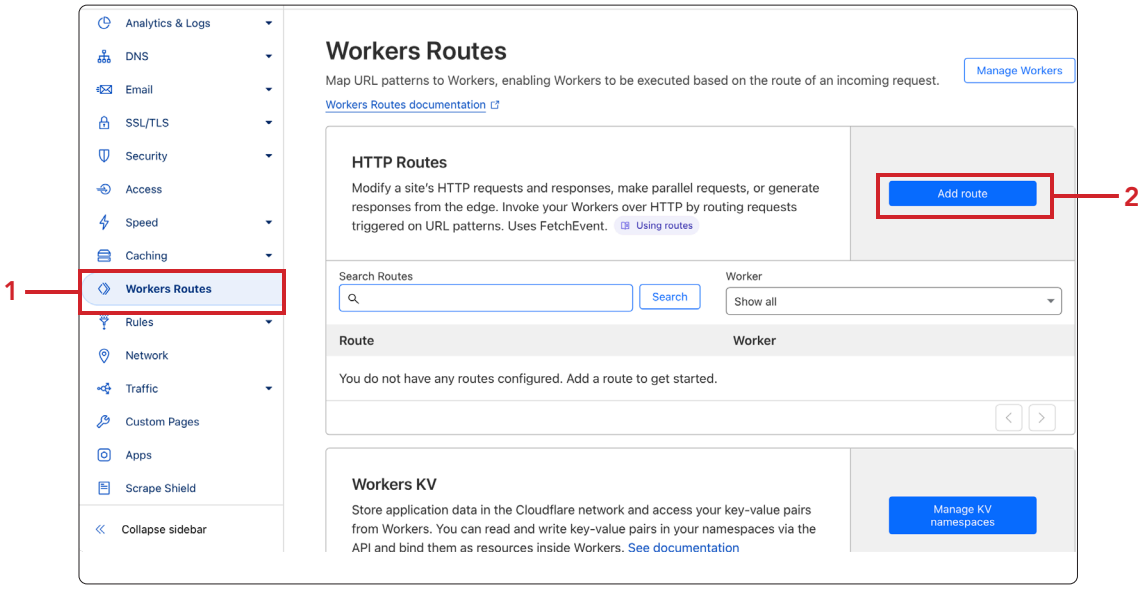


This completes this section.

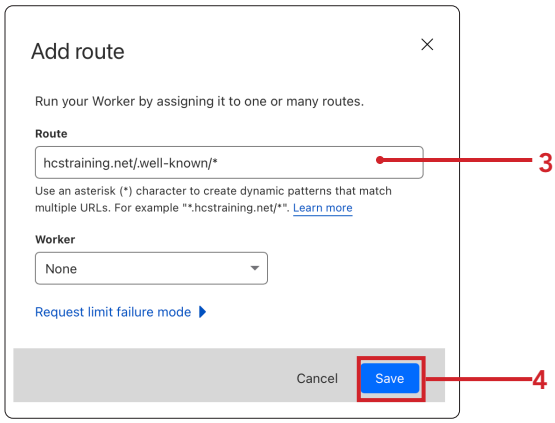
Section 5: Creating a worker route

What is a worker route?
A Worker Route in Cloudflare tells Cloudflare where to run your custom code on your website. Think of it as a rule that says, "When someone visits this part of my website, run this special program". For example, If your website is https://hcsonline.com, and you have a page at https://hcsonline.com/products. You could set a Worker Route that runs custom code only when someone visits the hcsonline.com/products page

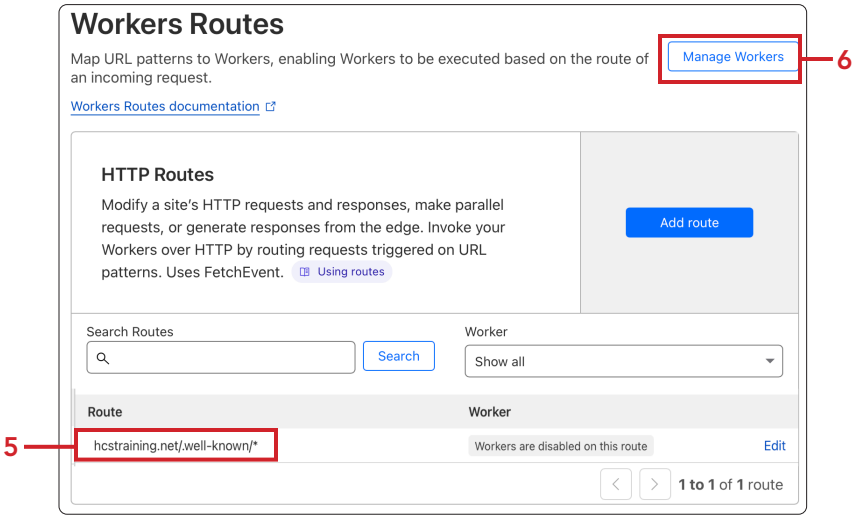
1. Click Workers Routes
2. Click Add route



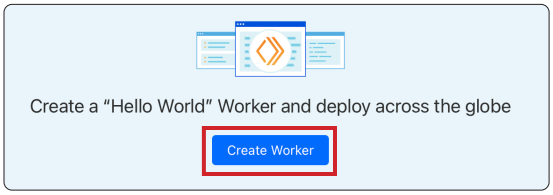
3. In the Route field, add your domain as shown below. This guide will use: hcstraining.net/.well-known/*
4. Click Save.



5. Verify your route was created.
6. Click Manage Workers.



7. Click Create Worker.



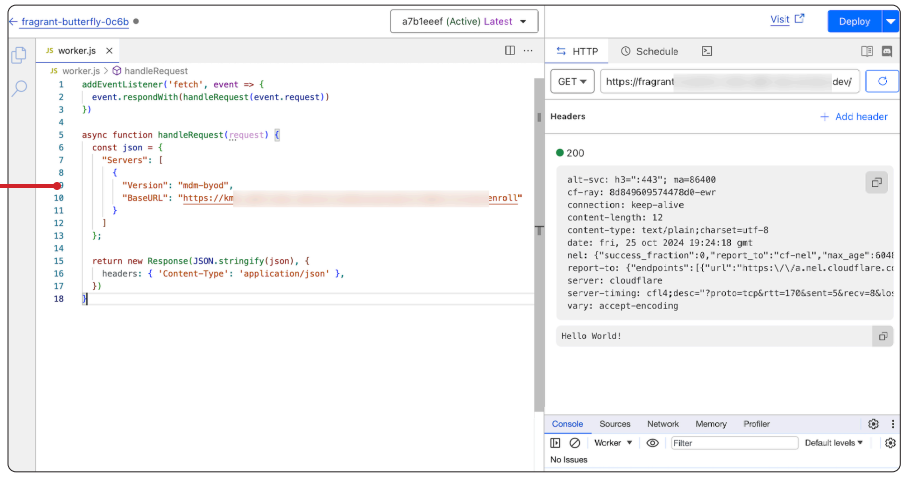
8. Click Deploy.

9. Click Edit Code.

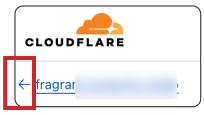
10. Remove all the code in the window on the left side.

11. Paste in the code below. Make sure to change the BaseURL address to your mdm server address. Click Deploy.

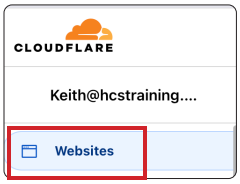
```
addEventListener('fetch', event => {
  event.respondWith(handleRequest(event.request))
})

async function handleRequest(request) {
  const json = {
    "Servers": [
      {
        "Version": "mdm-byod",
        "BaseURL": "https://my.mdmserver.com/servicediscoveryenrollment/v1/userenroll"
      }
    ]
  };

  return new Response(JSON.stringify(json), {
    headers: { 'Content-Type': 'application/json' },
  })
}
```



12. Click Previous (←)to return to the main screen.

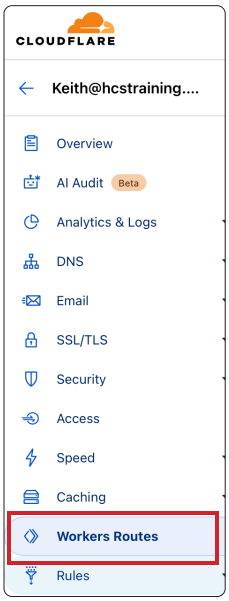


13. Select Websites.

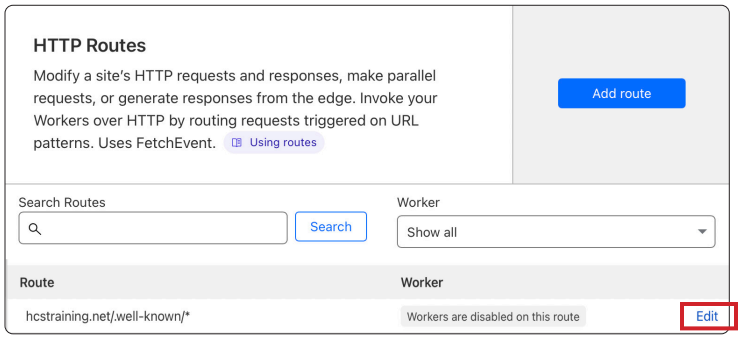


14. Click on your domain to display the settings.

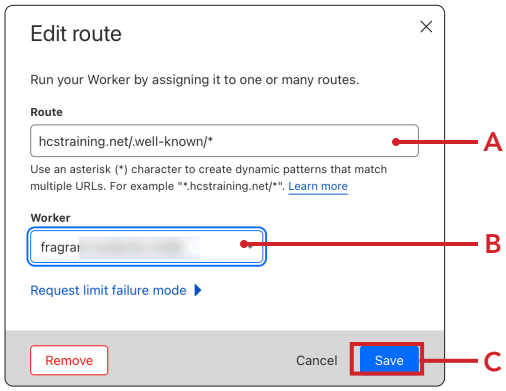
15. Select Worker Routes.



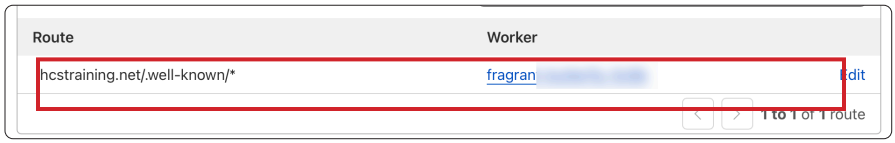
16. In the Route section, select Edit.



17. Configure the following:
    A. Select the Worker dropdown menu
    B. Select the worker we created in step 7. (For example: fragrant-xxxxxxxx-xxxx Your worker name will be different.)
    C. Click Save



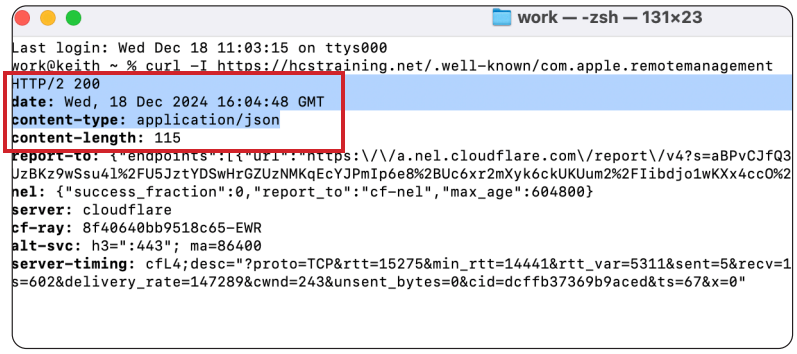
18. Confirm the Route and Worker information are both configured.



19. Open the Terminal application and enter the command below. Change the url to from https://hcstraining.net to your URL.


```
curl -I https://hcstraining.net/.well-known/com.apple.remotemanagement
```

20. You will receive a response similar to what is shown below. Confirm you see HTTP/2 200 and content-type shows as application/json.



The com.apple.remotemanagement file is ready for testing. Use the link below to test a complete Account-driven enrollment.

https://hcsonline.com/support/white-papers/how-to-configure-account-driven-enrollment-and-enroll-a-personal-device-in-jamf-pro

This completes the guide.