



Account-driven Enrollment Methods with Apple Devices using Cloudflare



Contents

Preface	3
Section 1: Creating a free Cloudflare account.	4
Section 2: Log into your existing Cloudflare account.....	7
Section 3: Adding Cloudflare name servers to your domain registration provider.	9
Section 4: Configuring DNS records in Cloudflare.....	11
Section 5: Creating a worker route	13



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.

A screenshot of the Cloudflare login page. At the top is the Cloudflare logo. Below it is the heading 'Log in to Cloudflare'. There are two input fields: 'Email' and 'Password'. To the right of the password field is a 'Show' link. Below the password field is a checkbox labeled 'Verify you are human' with the Cloudflare logo and 'Sign up' link next to it. Below the checkbox is a blue 'Log in' button. Below the button is an 'OR' separator. Below the separator are two buttons: 'Sign in with Google' and 'Sign in with Apple'. At the bottom are three links: 'Sign up', 'Forgot your password?', and 'Forgot your email?'.

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.

A screenshot of the Cloudflare sign-up page. At the top is the heading 'Get started with Cloudflare'. There are two input fields: 'Email' and 'Password'. The email field contains 'keith@hcstraining.net' and is annotated with a red line and the letter 'A'. The password field contains eight dots and is annotated with a red line and the letter 'B'. Below the password field is a section titled 'Password requirements met!' with four green checkmarks: '8 characters', '1 number', '1 special character e.g., \$, !, @, %, &', and 'No leading or trailing whitespace'. Below this is a section titled 'Let us know you're human' with a green checkmark and the word 'Success!' and the Cloudflare logo and 'Sign up' link. This section is annotated with a red line and the letter 'C'. Below this is a blue 'Sign up' button, annotated with a red line and the letter 'D'. Below the button is a link 'Log in' and the text 'Already have an account?'. At the bottom is a link to 'terms, privacy policy, and cookie policy'.



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.

Let's make your website or app fast & secure

Connect your domain to start sending web traffic through Cloudflare.

Enter an existing domain

hcstraining.net

Continue

Or register a new domain →

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

Cloudflare

Keith@hcstraining....

hcstraining.net

Setup Star Free plan

Phone + chat + ticket + community + developer docs

Free

\$0

Core Features

- Unmetered application layer DDoS protection
- IP-based rate limiting
- Protect against high severity and widespread vulnerabilities with WAF
- Detect and challenge common bots only
- Universal SSL certificate
- Fast, easy-to-use DNS
- Global CDN

Up to **65** Cloudflare Rules

5 WAF Rules

Support

Community + developer docs

Which plan is right for you?

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.

7

Cloudflare dashboard for **hcstraining.net**. The sidebar on the left shows the 'Overview' tab selected. The main content area displays the 'Overview' section for **hcstraining.net**, indicating that the domain is not yet active on Cloudflare. It provides instructions on how to activate the domain, including logging into the domain registrar, turning off DNSSEC, and updating the nameservers. The assigned Cloudflare nameservers are listed at the bottom: **joyce.ns.cloudflare.com** and **trey.ns.cloudflare.com**. A red box highlights the 'Overview' tab in the sidebar and the nameserver list at the bottom. A red arrow points from the number 7 to the 'Overview' tab, and another red arrow points from the number 8 to the nameserver list.

8

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>

The image shows the 'Log in to Cloudflare' page. It features a title 'Log in to Cloudflare' at the top. Below the title are two buttons: 'Continue with Google' and 'Continue with Apple'. Below these is an 'OR' separator. Then there are input fields for 'Email' and 'Password'. The password field has a 'Show' link. Below the password field is a checkbox labeled 'Verify you are human' with the Cloudflare logo and 'Privacy · Terms' link. At the bottom is a large blue 'Log in' button. Below the button are three links: 'Sign up', 'Forgot your password?', and 'Forgot your email?'.

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

The image shows the 'Two-Factor Authentication' page. It has a title 'Two-Factor Authentication'. Below the title is a text prompt 'Enter an authenticator app code or a recovery code:'. Below this is a text input field, which is highlighted with a red box and a red arrow labeled '2'. Below the input field is a link 'Lost all 2FA devices and backup codes? Try recovery'. At the bottom is a blue 'Log in' button, which is highlighted with a red box and a red arrow labeled '3'.

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

The image shows the 'Accounts' page. It has a title 'Accounts'. Below the title is a search bar with the placeholder text 'Search accounts...'. To the right of the search bar is a blue 'Search' button. Below the search bar is a list of accounts. The first account is 'HCS Technology Group', which is highlighted with a red box. The second account is 'Kmitnick@hconline.com's Account'.



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

Cloudflare Account Home - Websites

Select a domain to configure and monitor how Cloudflare processes its web traffic.

Search in HCS Technology Group...

Filter by: Starred

Name	Status	Plan	Plan Status
hcsarticles.com	✓ Active	Free	Active
hcsarticles.com	✓ Active	Free	Active

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.

Cloudflare Account Home - Overview

hcsarticles.com

Active

Star

Free plan

Overview

hcsarticles.com

Monitor security and performance for hcsarticles.com. Configure products and services from the menu.

[Review Cloudflare fundamentals](#)

DNS

DNS Setup: Full

[DNS Records](#)

This completes this section.

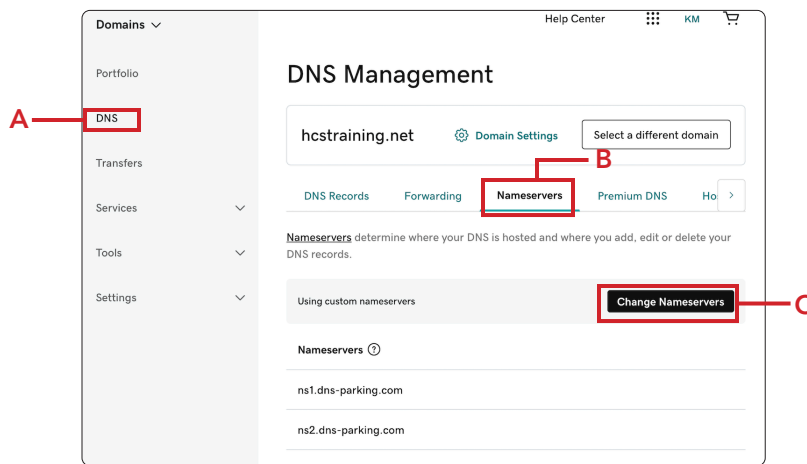


Section 3: Adding Cloudflare name servers to your domain registration provider.

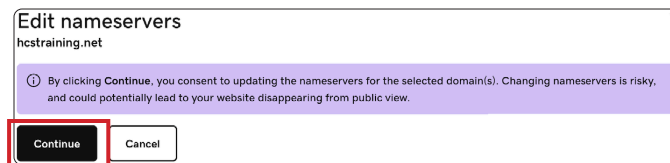
If you have an existing Cloudflare account and already configured your Cloudflare name servers, skip to Section 4 of this guide.

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.

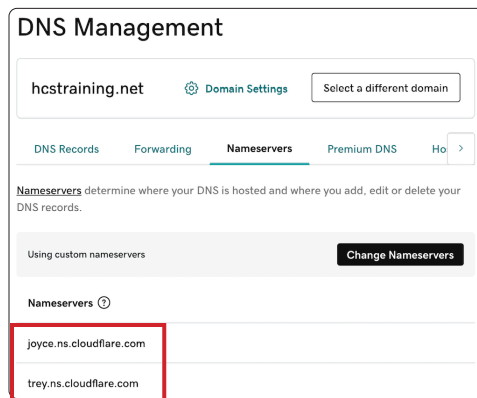


2. Click Continue.



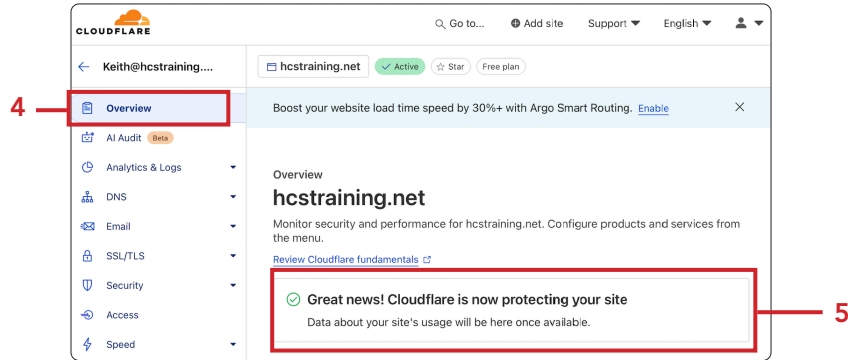
3. Verify the nameservers were changed.

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.



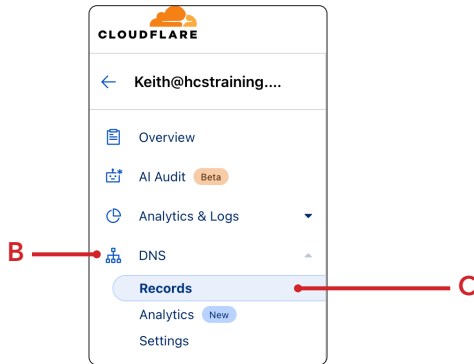
This completes this section.



Section 4: Configuring DNS records in Cloudflare.

1. Click DNS from the sidebar.

2. Click Records.



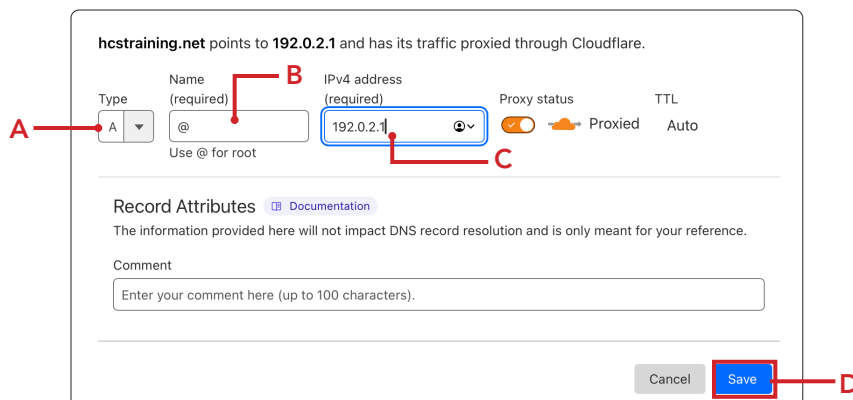
3. Click Add record.



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.

Search DNS Records					
Add filter		<input type="text"/>		Search	Add record
<input type="checkbox"/>	Type	Name	Content	Proxy status	TTL
<input type="checkbox"/>	A	hcstraining.net	192.0.2.1	Proxied	Auto
					Edit

This completes this section.

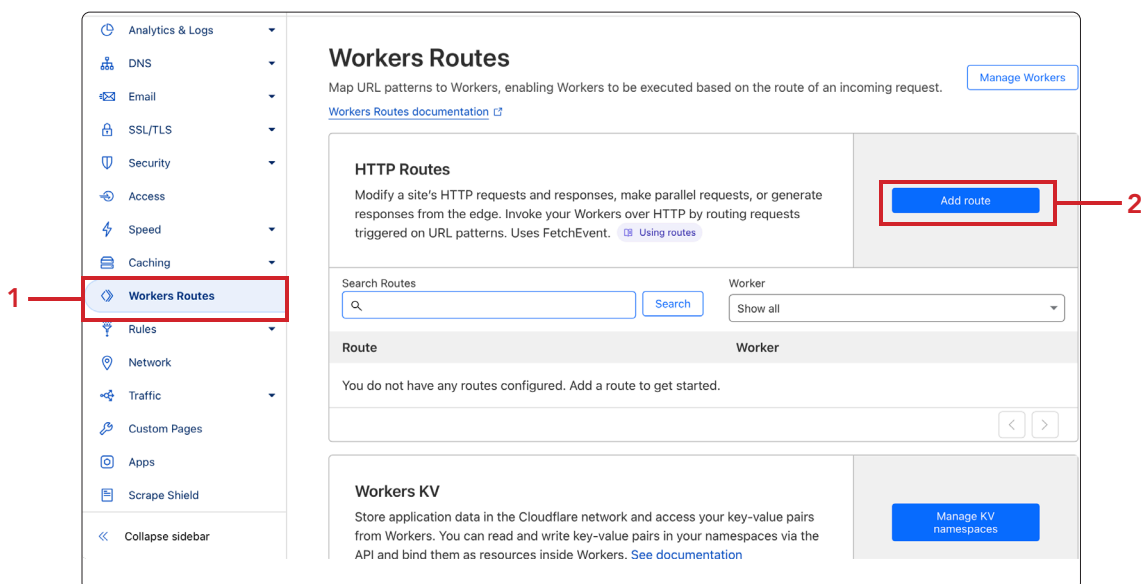


Section 5: Creating a worker route

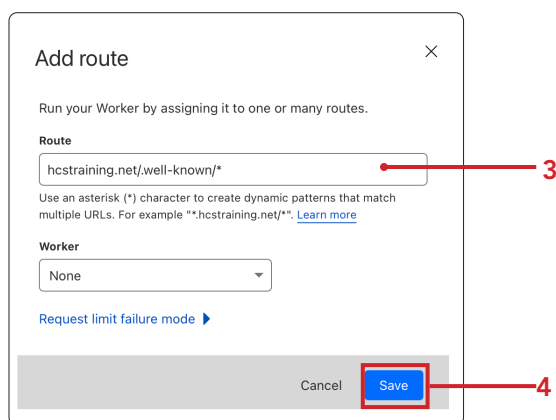
What is a worker route?

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://hconline.com>, and you have a page at <https://hconline.com/products>. You could set a Worker Route that runs custom code only when someone visits the hconline.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.

Workers Routes

Map URL patterns to Workers, enabling Workers to be executed based on the route of an incoming request.

[Workers Routes documentation](#)

HTTP Routes

Modify a site's HTTP requests and responses, make parallel requests, or generate responses from the edge. Invoke your Workers over HTTP by routing requests triggered on URL patterns. Uses FetchEvent. [Using routes](#)

[Add route](#)

Search Routes [Search](#) Worker [Show all](#)

Route	Worker
hctraining.net/well-known/*	Workers are disabled on this route Edit

< > 1 to 1 of 1 route

7. Click Create Worker.

Create a "Hello World" Worker and deploy across the globe

[Create Worker](#)

8. Click Deploy.

"Hello World" Worker

Create "Hello World" Worker

fragrant [🔗](#)

Your Worker will be deployed to: <https://fragrant-butterfly-0c6b.keith-ded.workers.dev>

worker.js

```
/**
 * Welcome to Cloudflare Workers! This is your first worker.
 *
 * - Run "npm run dev" in your terminal to start a development server
 * - Open a browser tab at http://localhost:8787/ to see your worker in a
 * - Run "npm run deploy" to publish your worker
 *
 * Learn more at https://developers.cloudflare.com/workers/
 */

export default {
  async fetch(request, env, ctx) {
    return new Response('Hello World!');
  },
};
```

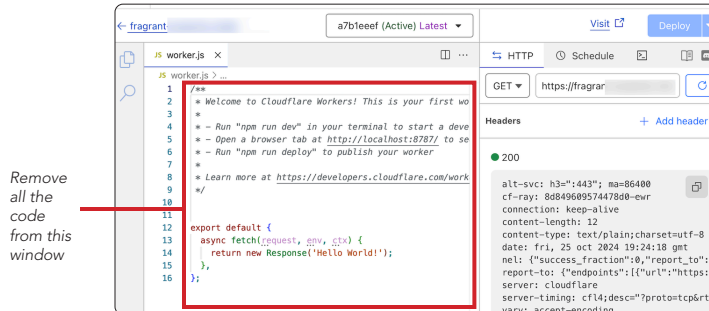
[Cancel](#) [Deploy](#)



9. Click Edit Code.



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

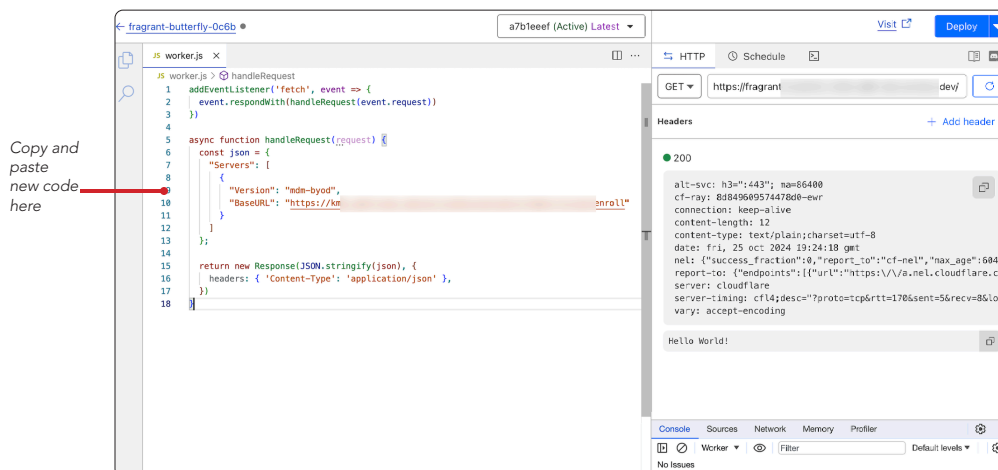


11. Paste in the code below. Make sure to change the BaseURL address to your mdm server address. Click Deploy.

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

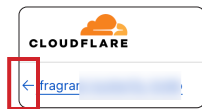
async function handleRequest(request) {
  const json = {
    "Servers": [
      {
        "Version": "mdm-byod",
        "BaseURL": "https://my.mdmserver.com/servicediscoveryenrollment/v1/userenroll"
      }
    ]
  };

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

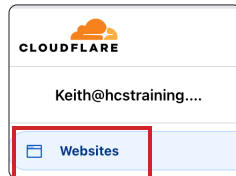




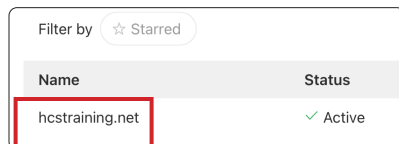
12. Click Previous (←) to return to the main screen.



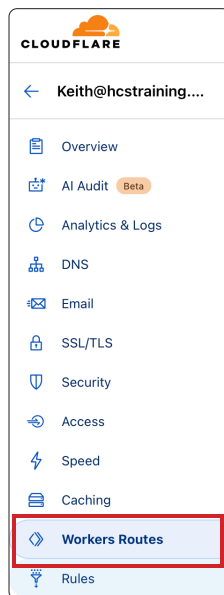
13. Select Websites.



14. Click on your domain to display the settings.



15. Select Worker Routes.





16. In the Route section, select Edit.

HTTP Routes
Modify a site's HTTP requests and responses, make parallel requests, or generate responses from the edge. Invoke your Workers over HTTP by routing requests triggered on URL patterns. Uses FetchEvent. [Using routes](#)

[Add route](#)

Search Routes [Search](#) Worker

Route	Worker
hcstraining.net/.well-known/*	Workers are disabled on this route

[Edit](#)

17. Configure the following:

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

Edit route ×

Run your Worker by assigning it to one or many routes.

Route
 A
Use an asterisk (*) character to create dynamic patterns that match multiple URLs. For example `**hcstraining.net/**`. [Learn more](#)

Worker
 B
[Request limit failure mode](#) ▶

[Remove](#) [Cancel](#) [Save](#) C

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

Route	Worker
hcstraining.net/.well-known/*	fragrai

[Edit](#)

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



Terminal

```
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.

```
work — zsh — 131x23
Last login: Wed Dec 18 11:03:15 on ttys000
work@keith ~ % curl -I https://hcstraining.net/.well-known/com.apple.remotemanagement
HTTP/2 200
date: Wed, 18 Dec 2024 16:04:48 GMT
content-type: application/json
content-length: 115
report-to: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v4?s=aBPvCJfQ3UzBKz9wSsu4l%2FU5JztYDSwHrGZUzNMkqEcYJPmIp6e8%2BUc6xr2mXyk6ckUKUum2%2FIibdjo1wKXx4cc0%2hel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
server: cloudflare
cf-ray: 8f40640bb9518c65-EWR
alt-svc: h3=":443"; ma=86400
server-timing: cfL4;desc="?proto=TCP&rtt=15275&min_rtt=14441&rtt_var=5311&sent=5&recv=1s=602&delivery_rate=147289&cwnd=243&unsent_bytes=0&cid=dcffb37369b9aced&ts=67&x=0"
```

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

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

This completes the guide.