



# 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/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.

UDFLARE	
Log in to Cloudflare	
Email	
Password	@ Sł
Let us know you're human	
Brivery - Terme	
Log in	
G Sign in with Google	

#### 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.

Email  keith@hcstraining.net  Password  Show  Password  Show  Password Show  Password requirements mett  Show  A Show  Let us know you're human  Show  Let us know you're human  Show  Courter Amage  Cou	Get started with Cloudflare	
Password   Password   Password requirements mett  Password requirements mett  S characters  I number  I special character e.g., §, [], %, &  V to leading or trailing whitespace  Let us know you're human  S Success1  E.cover.tat	Email	
Password requirements mett  Password requirements mett  Standarders  No leading or trailing whitespace Let us know you're human  Standarder Success1  Let us know you're human  Standarder Success1  Let us know you're human	keith@hcstraining.net	——A
Password requirements mett ✓ 8 characters ✓ 1 number ✓ 1 special character e.g., \$. L. @. %, & ✓ No leading or trailing whitespace Let us know you're human € Success!	Password (1) Show	
	••••••	—— B
✓ 1 number     ✓ 1 special character e.g., \$, I. @, %, &     ✓ No leading or trailing whitespace Let us know you're human     ✓ Success!	Password requirements met!	
✓ 1 special character e.g., \$, I, @, %, &     ✓ No leading or trailing whitespace Let us know you're human     ✓ Success!	✓ 8 characters	
Voleading or trailing whitespace Let us know you're human Success! Course to the second seco		
Let us know you're human		
	<ul> <li>No leading or trailing whitespace</li> </ul>	
	Let us know you're human	
		— c
	By clicking Sign Up, I agree to Cloudflare's terms, privacy policy, and cookie policy.	
By cicking sign op, ragree to cloud rate s terms, privacy policy, and cooke policy.	Sign up	
	Already have an account? Log in	



- 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.

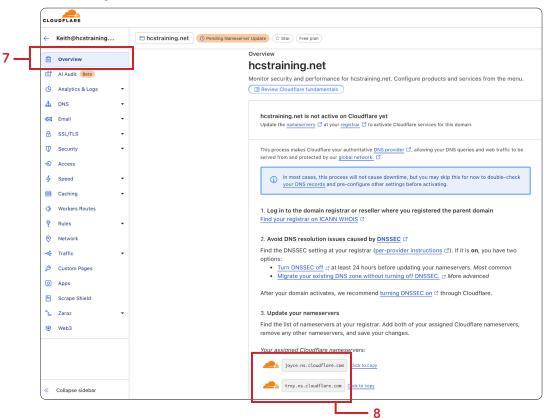
	Let's make your website or app fast & secure Connect your domain to start sending web traffic through Cloudflare.	
3 —	Enter an existing domain ●hcstraining.net Or register a new domain →	4

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

CLO	UDFLARE		Q Go to ⊕ Add site Support ▼ English ▼	*
←	Keith@hcstraining		☐ hcstraining.net       C Setup     ☆ Star     Free plan	
Ē	Overview		Phone + chat + ticket + community + developer docs	
Ċ	Al Audit Beta			
O	Analytics & Logs	•	Free	
ሔ	DNS	•	\$0	
	Email	-	Core Features	
	EIIIdii	•	Unmetered application layer DDoS protection	
₽	SSL/TLS	-	IP-based rate limiting Protect against high severity and widespread vulnerabilities with WAF	
			Detect and challenge common bots only	-
Φ	Security	•	Universal SSL certificate	
0			Fast, easy-to-use DNS	
Ð	Access		Global CDN	
4	Speed	•		-
<i>.</i>			Up to <b>65</b> Cloudflare Rules ()	
	Caching	•	5 WAF Rules ①	
~			Support	
$\langle\rangle$	Workers Routes		Community + developer docs	
Ψ̈́	Rules	•	<b></b>	_
*				
0	Network		Which plan is right for you? [가 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.





## 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

Log in to Cloudflar	re
G Continue with Google	
Continue with Apple	
Email OR	
Password	@ Show
Let us know you're human	
Verify you are human	CLOUDFLARE Privacy · Terms
Log in	
Sign up Forgot your password? Forgot your e	email?

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

	Two-Factor Authentication	
	Enter an authenticator app code or a recovery code:	
		2
	Lost all 2FA devices and backup codes? Try recovery	
3 —	Log in	

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

Accounts	
	Search accounts
	HCS Technology Group Kmitnick@hcsonline.com's Account



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

				Q Go to + Add	▼ Support ▼ English ▼ 🛓 ▼
	← HCS Technology Gr →	Account Home			
5 —	🗂 Websites	Websites			
	-∵ਊ- Discover	Select a domain to configure and I	monitor how Cloudflar	e processes its web traffic	).
	Domain Registration	Search in HCS Technology Group		Search	+ Add a domain
	🕒 Analytics & Logs 🔹				
	Security Center •	Filter by 🛱 Starred			
	品 Trace Beta	Name	Status	Plan	Plan Status
	WAF	hcsarticles.com 6	✓ Active	Free	Active
	🖏 Turnstile	hcstecharticles.com	✓ Active	Free	Active
	IP Addresses				<u>Give feedback</u> ⊡ੈ

- 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		<b>7</b> Q Go to +	Add  Support	English 🔻	<b>.</b> -
	- HCS Technology (	Gr	☐hcsarticles.com			
🖹 Overview			Overview			
	📩 Al Audit 📴		hcsarticles.com	DNS		
	Analytics & Logs	•	Monitor security and performance for hcsarticles.com. Configure products and services from the menu.	DNS Setup: Full (j)		
	品 DNS	•	Review Cloudflare fundamentals	DNS Records		
l	🖾 Email	-				



# 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.

Domains 🗸		Help Center 🚻 KM 🖵
Portfolio		DNS Management
DNS		hcstraining.net
Transfers		DNS Records Forwarding Nameservers Premium DNS Ho
Services	$\sim$	
Tools	~	Nameservers determine where your DNS is hosted and where you add, edit or delete your DNS records.
Settings	~	Using custom nameservers Change Nameservers
		Nameservers ⑦
		ns1.dns-parking.com
		ns2.dns-parking.com

2. Click Continue.

	dit name straining.net	eservers	~
C	<i>.</i> , .	Continue, you consent to updating the nameservers for the selected domain(s). Changing nameservers is risky, stentially lead to your website disappearing from public view.	
	Continue	Cancel	

3. Verify the nameservers were changed.

NOTE: You may need to refresh your web browser to see the name server changes.

DNS Mar	nage	mer	nt			
hcstraining.net		۵ (	Domain Settings	Select a different domain		
DNS Records	Forwa	rding	Nameservers	Premium DNS	Ho→	
Nameservers determ DNS records.	nine where	e your DN	NS is hosted and w	here you add, edit or d	elete your	
Using custom names	ervers			Change Nam	eservers	
Nameservers 🕐						
joyce.ns.cloudflare	e.com					



- 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.

[	CLO	UDFLARE	Q, Go to 🔮 Add site Support 👻 English 👻 💄	•
	←	Keith@hcstraining	E hcstraining.net	
4 —		Overview	Boost your website load time speed by 30%+ with Argo Smart Routing. Enable $\qquad \qquad \qquad$	
1	đ	Al Audit Beta		
	Q	Analytics & Logs	Overview	
	ሔ	DNS	hcstraining.net	
	⊠	Email	Monitor security and performance for hcstraining.net. Configure products and services from the menu.	
	₿	SSL/TLS	Review Cloudflare fundamentals 🗗	
	Φ	Security	⊘ Great news! Cloudflare is now protecting your site	1
	Ð	Access	Data about your site's usage will be here once available.	ŀ
	4	Speed		



## Section 4: Configuring DNS records in Cloudflare.

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



3. Click Add record.

	Se	earch DNS Reco	rds			
		۹		Sear	ch 🕀	Add record
🗌 Type 🛈		Name (i)	Content ①	Proxy status ①	TTL ①	Actions

- 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.

A—	hcstraining.net points to 192.0.2.1 and has its traffic proxied through Cloudflare. Name B IPv4 address (required) Proxy status TTL (required) Or proxied Auto Use @ for root C	
	Record Attributes III Documentation The information provided here will not impact DNS record resolution and is only meant for your reference. Comment	
	Enter your comment here (up to 100 characters). Cancel Save	-D



#### 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				
7	Add filter	٩				Search	Add record
0	Туре 🛈		Name (1)	Content (1)	Proxy status ③	TTL ①	Actions
	А		hcstraining.net	192.0.2.1	- Proxied	Auto	Edit 🕨



## 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

Analytics & Logs	•
战 DNS	- Workers Routes
≢⊠ Email	Map URL patterns to Workers, enabling Workers to be executed based on the route of an incoming request.
🔒 SSL/TLS	
	HTTP Routes Modify a site's HTTP requests and responses, make parallel requests, or generate
4 Speed	Modiny a site SH I IP requests and responses, make parallel requests, or generate     responses from the edge. Invoke your Workers over HTTP by routing requests     trigaered on URL patterns. Uses FetchEvent. (B Using routes
aching	•
♦ Workers Routes	Search Routes Worker Q. Search Show all V
Y Rules	Route Worker
Network	Route Worker
⊶o∯ Traffic	You do not have any routes configured. Add a route to get started.
Custom Pages	
O Apps	
E Scrape Shield	Workers KV
Collapse sidebar	Store application data in the Cloudflare network and access your key-value pairs       Manage KV         from Workers. You can read and write key-value pairs in your namespaces via the       API and bind them as resources inside Workers. See documentation

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

Run your Worker by as	signing it to one or	many routes.		
Route				
hcstraining.net/.well-	known/*		•	
Use an asterisk (*) charac multiple URLs. For examp			atch	
Worker None	•			
Request limit failure m	ada N			



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

an incoming request.	Workers to be executed based or	n the route of	hage Workers
Vorkers Routes documentation			
HTTP Routes			
Modify a site's HTTP requests and requests, or generate responses fr Workers over HTTP by routing requ patterns. Uses FetchEvent. (19 Usi	om the edge. Invoke your uests triggered on URL	Add rou	ite
Search Routes	Worker Search Show all		~
Route	Worker		
hcstraining.net/.well-known/*		bled on this route	Edi

7. Click Create Worker.

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

8. Click Deploy.

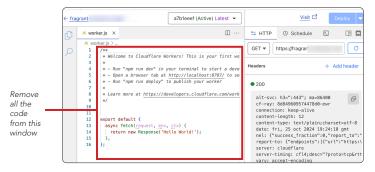
"Hello World" Worker
Create ""Hello World" Worker" Worker
fragrant 🥥
Your Worker will be deployed to: https://fragrant-butterfly-Oc6b.keith-ded.workers.dev
worker.js
/** * Welcome to Cloudflare Workers! This is your first worker. * * Run "npm run dev" in your terminal to start a development server * - Open a browser tab at http://cloudinast:8787/ to see your worker in a - Run "npm run deploy" to publish your worker * * Learn more at https://developers.cloudflare.com/workers/ */
<pre>export default {   async fetch(request, env, ctx) {   return new Response('Hello World!');   }; };</pre>
Cancel



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"
                             }
                         1
                     };
                     return new Response(JSON.stringify(json), {
                         headers: { 'Content-Type': 'application/json' },
                     })
                 }
                                                                                     a7b1eeef (Active) Latest 👻
                                                                                                                                                       Visit 🗳
                    fragrant-butterfly-0c6b
                        JS worker.js ×
                             orker.js > ② handleRequest

addEventListener('fetch', event ⇒ (

event.respondWith(handleRequest(event.request))

})
                                                                                                        ....
                                                                                                                 Schedule
                                                                                                                                                                      dev/ 🔿
                                                                                                                  GET - https://fragrant
                                                                                                                 Headers
                                                                                                                                                                + Add header
                              Copy and
                                                                                                                 200
paste
                                                                                                                   alt-svc: h3=":443"; na=66400
cf-ray: ddd4960957447800-ewr
connection: keep-alue
content-length: 12
content-type: text/plain;charset=utf-8
date: fri, 25 oct 2024 19:24:18 gwt
nel: {"success_fraction":0, "report_c0": "cf-nel", "nax_age":6041
report-t0: "dengonis": {"tru"': "https://la.mel.cloudflare.cr
server: loudflare
server: loudflare : "proto=tcp&rtt=1786sent=56recv=86\or
vary: accept-encoding
new code
                                                                                          enroll"
here
                          10
11
12
                                   }
                          13
14
15
16
17
18
                                - 33
                               return new Response(JSON.stringify(json), {
    headers: { 'Content-Type': 'application/json' },
                             )
})
                                                                                                                  Hello World!
                                                                                                                                                                     ø
                                                                                                                      le Sources Network Memory Profiler
                                                                                                                                                                      .
                                                                                                                🕒 🖉 Worker 🔻 🕲 Filter
                                                                                                                                                         Default levels *
                                                                                                                                                                           8
                                                                                                                 No Issues
```



12.Click Previous ( $\leftarrow$ )to return to the main screen.



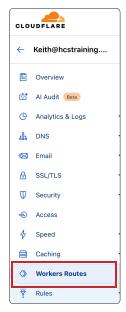
13.Select Websites.



14.Click on your domain to display the settings.

ſ	Filter by 🗍 🛱 Sta	rred
	Name	Status
	hcstraining.net	✓ Active

15. Select Worker Routes.





16.In the Route section, select Edit.

HTTP Routes Modify a site's HTTP requests and responses, ma requests, or generate responses from the edge. I Workers over HTTP by routing requests triggered patterns. Uses FetchEvent. B Using routes	nvoke your Add route
Search Routes	Worker Show all
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-xxxxxxxx Your worker name will be different.)
  - C. Click Save

Edit route		×	
Run your Worker by assigning	t to one or many routes.		
Route			
hcstraining.net/.well-known/*			— A
Use an asterisk (*) character to cre multiple URLs. For example "*.hcst		natch	
Worker			
fragra	•		— B
Request limit failure mode 🕨			
Remove	Cancel	Save	

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

Route	Worker	
hcstraining.net/.well-known/*	fragran	lidi

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.

	🚞 work — -zsh — 131×23
_ast login: Wed Dec 18 11:03:15 on <u>vork©keith ~ % curl -I https://hcst</u> HTTP/2 200 <b>jate:</b> Wed, 18 Dec 2024 16:04:48 GMT	raining.net/.well-known/com.apple.remotemanagement
<pre>content-type: application/json content-length: 115</pre>	tos:\/\/a.nel.cloudflare.com\/report\/v4?s=aBPvCJfQ
	cYJPmIp6e8%2BUc6xr2mXyk6ckUKUum2%2FIibdjo1wKXx4cc0%
alt-svc: h3=":443"; ma=86400 server-timing: cfL4;desc="?proto=TC	P&rtt=15275&min_rtt=14441&rtt_var=5311&sent=5&recv= &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://hcsonline.com/support/white-papers/how-to-configure-account-driven-enrollment-and-enroll-a-personal-device-in-jamf-pro

This completes the guide.