A Guide to
Creating a Jamf Pro
Cloud Distribution Point with
Amazon Web Services (AWS)
and Simple Storage Service (S3)

REV20180601

Requirements
- Root Identity and Access Management (IAM) AWS account to obtain the appropriate keys for signed URLs (Optional) An AWS account (you can use the Root AWS account)
- A Jamf Pro instance
- A Jamf Pro administrator user

This guide was created using the following resources:
- A free AWS account
- The Root IAM AWS user
- A Jamf Pro 10.17 cloud instance hosted by Jamf Software

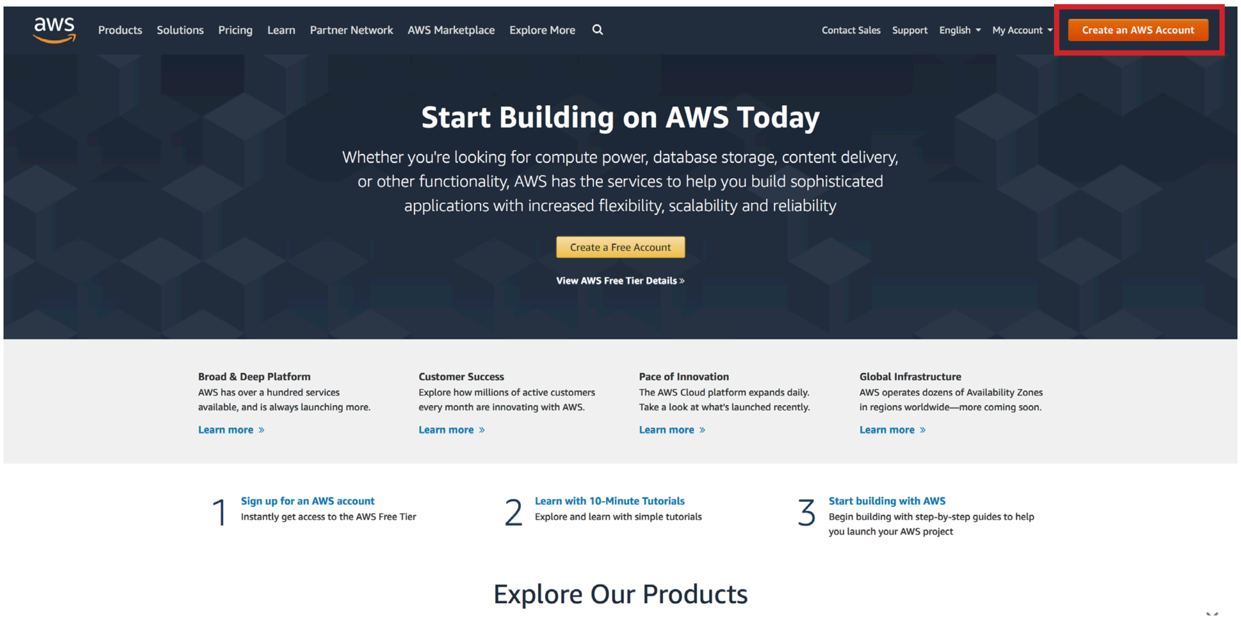
What's covered
1. Creating an AWS account if you do not already have one.
2. Setting the needed permissions inside of AWS for Jamf Pro
3. Testing your Cloud Distribution Point
4. Configuring Signed URLs

Sections
- Create an AWS Account - covers creating an AWS account if you do not already have one
- Configure AWS Permissions for Jamf Pro - covers creating the necessary permissions for a Jamf Pro AWS IAM user to be able to create and configure its S3 bucket
- Configure an AWS Distribution Point in Jamf Pro - covers configuring the Jamf Pro server with the previously created services
- Verify that Jamf Pro created an S3 bucket - covers verifying successful bucket creation inside of the AWS S3 service

Create an AWS Account

NOTE: If you already have an AWS account, skip to Configure AWS Permissions for Jamf Pro.

1.In a modern web browser open aws.amazon.com then select “Create an AWS account” in the upper-right corner.



Start Building on AWS Today

Whether you're looking for compute power, database storage, content delivery, or other functionality, AWS has the services to help you build sophisticated applications with increased flexibility, scalability and reliability

Broad & Deep Platform AWS has over a hundred services available, and is always launching more.

Customer Success Explore how millions of active customers every month are innovating with AWS.

Pace of Innovation The AWS Cloud platform expands daily. Take a look at what's launched recently.

Global Infrastructure AWS operates dozens of Availability Zones in regions worldwide—more coming soon.

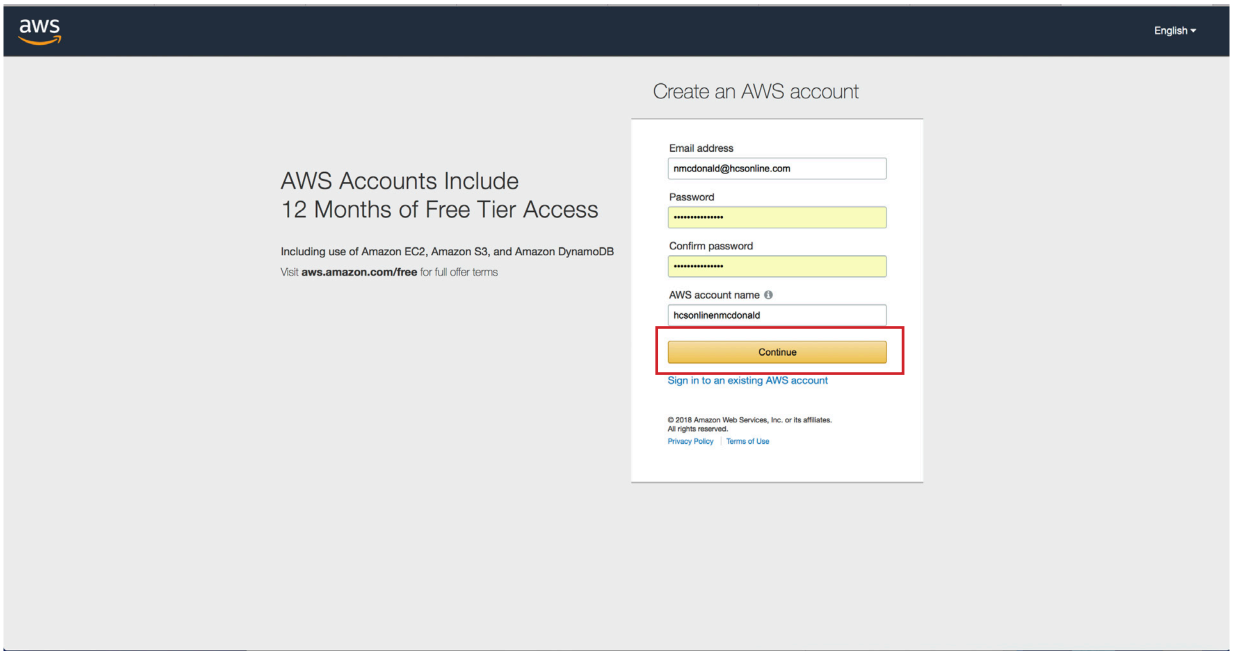
1 Sign up for an AWS account — Instantly get access to the AWS Free Tier

2 Learn with 10-Minute Tutorials — Explore and learn with simple tutorials

3 Start building with AWS — Begin building with step-by-step guides to help you launch your AWS project

Explore Our Products

2. Enter the required fields to create your Amazon Web Service account, then click Continue.



Create an AWS account

AWS Accounts Include
12 Months of Free Tier Access

Including use of Amazon EC2, Amazon S3, and Amazon DynamoDB
Visit **aws.amazon.com/free** for full offer terms

Email address: nmcdonald@hcsonline.com

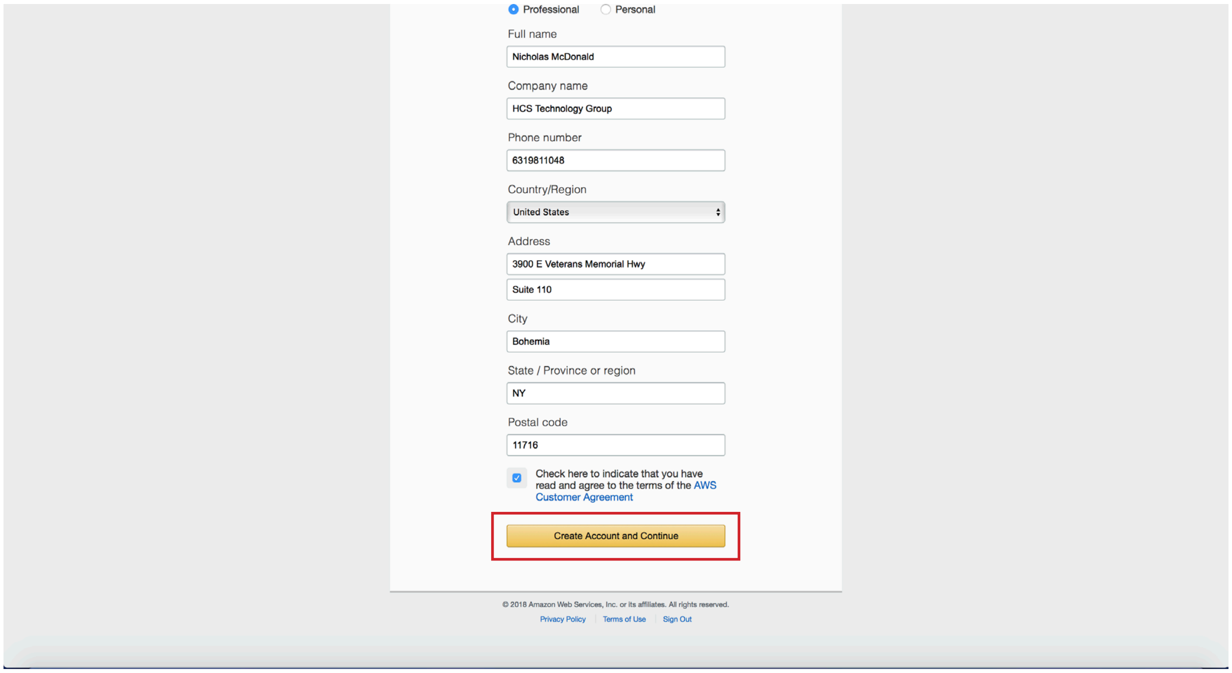
Password: •••••••••••••••

Confirm password: •••••••••••••••

AWS account name: hcsonlinenmcdonald

© 2018 Amazon Web Services, Inc. or its affiliates. All rights reserved.

3. Enter your organization’s details, then click “Create Account and Continue.”



● Professional ○ Personal

Full name
Nicholas McDonald

Company name
HCS Technology Group

Phone number
6319811048

Country/Region
United States

Address
3900 E Veterans Memorial Hwy
Suite 110

City
Bohemia

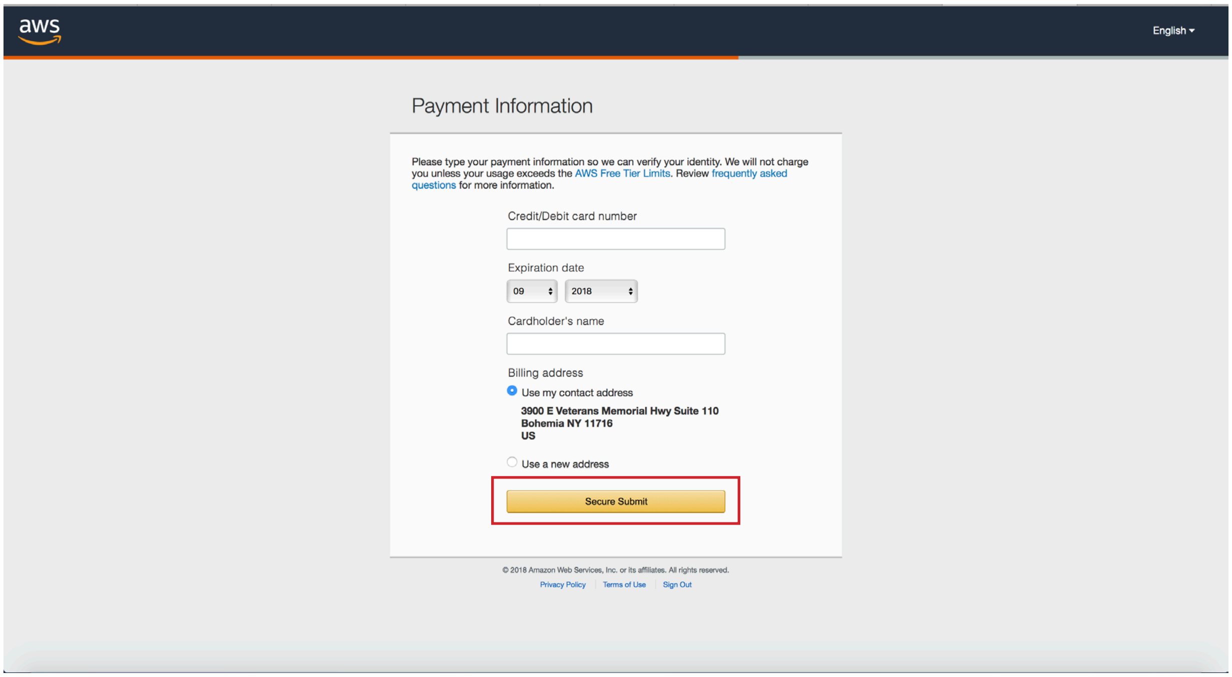
State / Province or region
NY

Postal code
11716

☑ Check here to indicate that you have read and agree to the terms of the AWS Customer Agreement

© 2018 Amazon Web Services, Inc. or its affiliates. All rights reserved.

4. Enter your organization’s payment information. You will not be charged unless your organization exceeds Amazon’s Free Tier usage. If your organization does not allow you to use a credit card, contact Amazon Web Services directly to create your account. After you enter your payment information click Secure Submit.



Payment Information

Please type your payment information so we can verify your identity. We will not charge you unless your usage exceeds the AWS Free Tier Limits. Review frequently asked questions for more information.

Credit/Debit card number

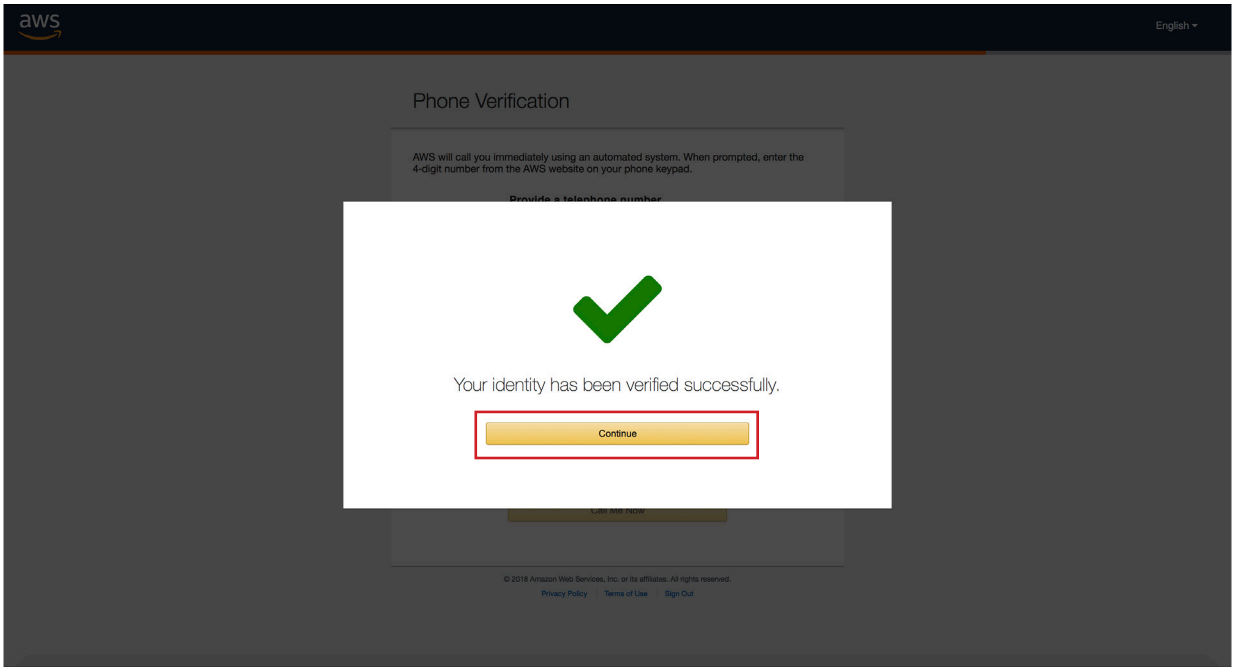
Expiration date
09 2018

Cardholder's name

Billing address
● Use my contact address
3900 E Veterans Memorial Hwy Suite 110
Bohemia NY 11716
US
○ Use a new address

© 2018 Amazon Web Services, Inc. or its affiliates. All rights reserved.

5. Enter your phone number, then click Call Me Now.
6. The web page displays a 4-digit number. Answer the call from AWS and, when prompted, enter the 4-digit number on your phone keypad.
7. When you see the message, “Your identity has been successfully verified,” click Continue.



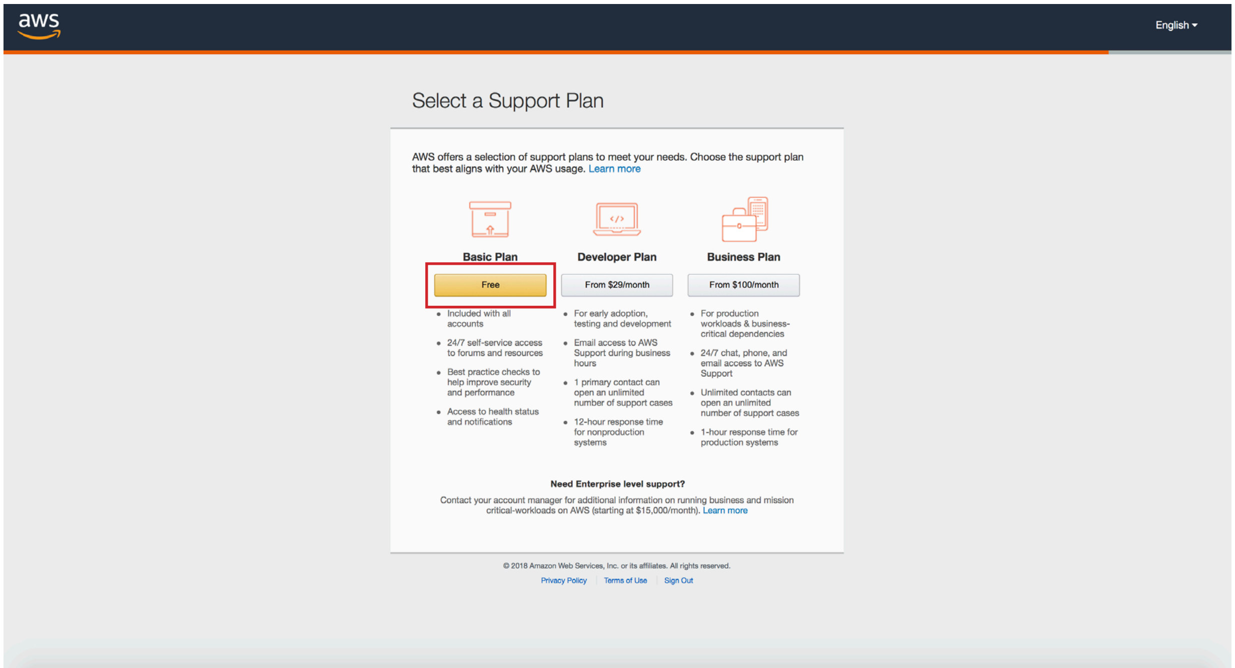
Phone Verification

AWS will call you immediately using an automated system. When prompted, enter the 4-digit number from the AWS website on your phone keypad.

Your identity has been verified successfully.

© 2018 Amazon Web Services, Inc. or its affiliates. All rights reserved.

8. Select the support plan that best meets the needs of your organization. This guide uses the free Basic Plan.



Select a Support Plan

AWS offers a selection of support plans to meet your needs. Choose the support plan that best aligns with your AWS usage. Learn more

Basic Plan

- Included with all accounts
- 24/7 self-service access to forums and resources
- Best practice checks to help improve security and performance
- Access to health status and notifications

Developer Plan

- For early adoption, testing and development
- Email access to AWS Support during business hours
- 1 primary contact can open an unlimited number of support cases
- 12-hour response time for nonproduction systems

Business Plan

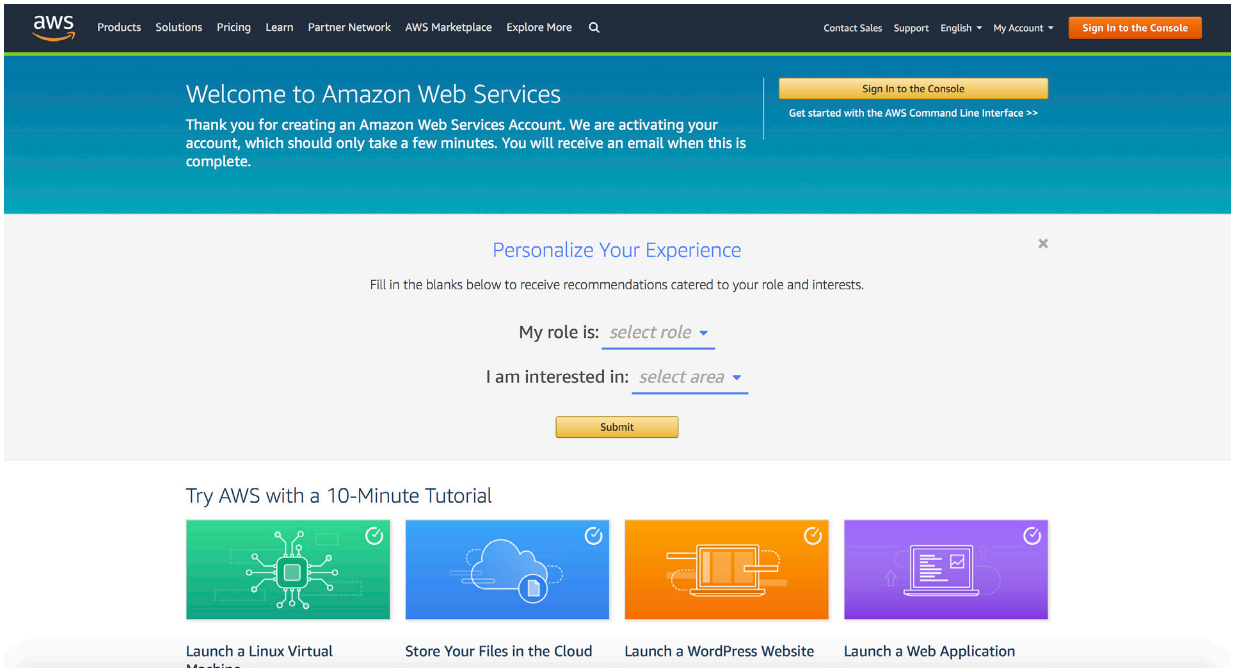
- For production workloads & business-critical dependencies
- 24/7 chat, phone, and email access to AWS Support
- Unlimited contacts can open an unlimited number of support cases
- 1-hour response time for production systems

Need Enterprise level support?

Contact your account manager for additional information on running business and mission critical-workloads on AWS (starting at $15,000/month). Learn more

© 2018 Amazon Web Services, Inc. or its affiliates. All rights reserved.

9. Check your email for verification. You may need to wait a few minutes while AWS activates your account.



Welcome to Amazon Web Services

Thank you for creating an Amazon Web Services Account. We are activating your account, which should only take a few minutes. You will receive an email when this is complete.

Personalize Your Experience

Fill in the blanks below to receive recommendations catered to your role and interests.

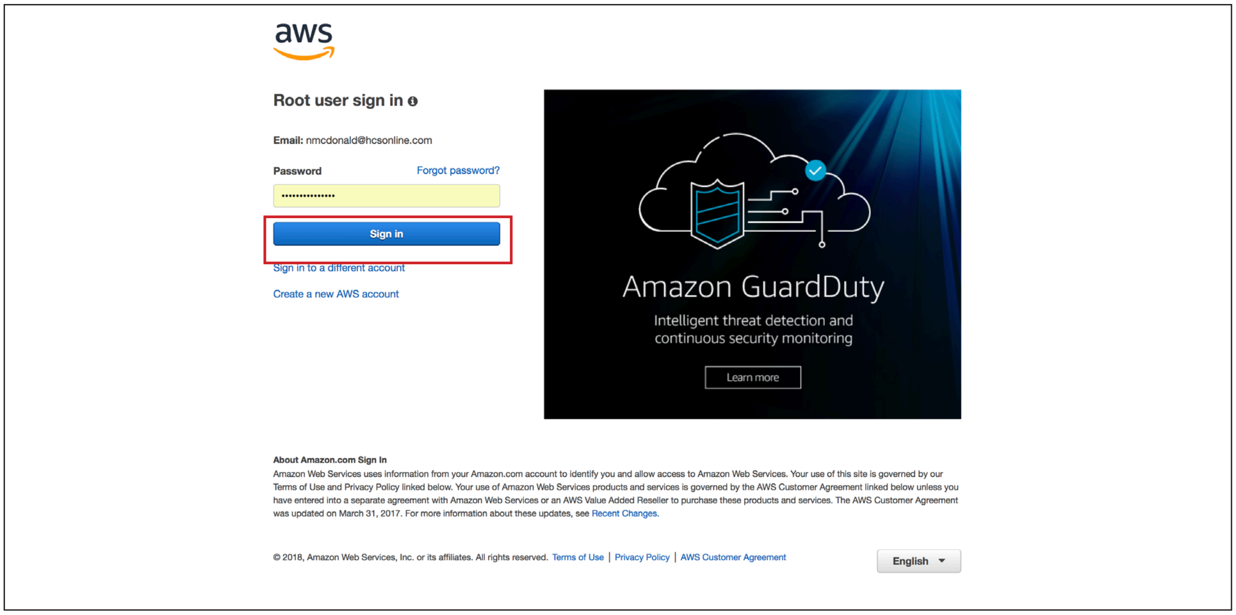
My role is: select role

I am interested in: select area

Submit
Try AWS with a 10-Minute Tutorial
Launch a Linux Virtual Machine
Store Your Files in the Cloud
Launch a WordPress Website
Launch a Web Application

Configure AWS Permissions for Jamf Pro

1. In a modern web browser, open console.aws.amazon.com then log in with your AWS account.
2. If you see the “Root user sign in” screen, enter the IAM Root user credentials then click “Sign in.”



aws

Root user sign in

Email: nmcdonald@hcsonline.com

Password Forgot password?

Sign in

Sign in to a different account

Create a new AWS account

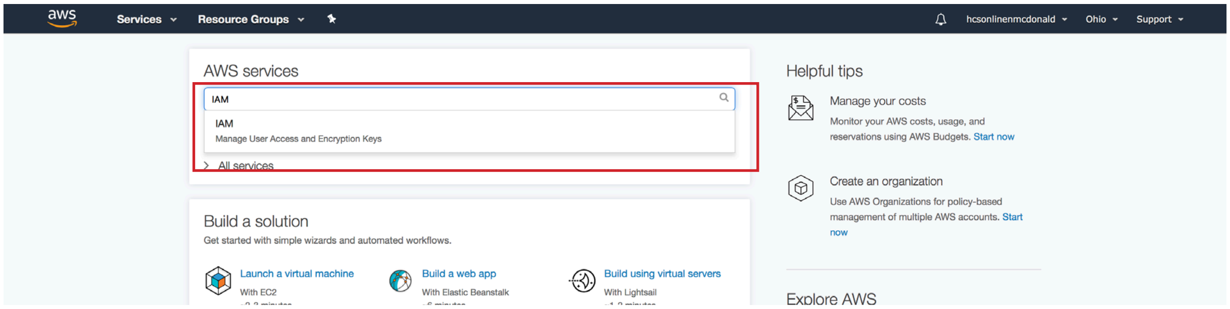
Amazon GuardDuty
Intelligent threat detection and continuous security monitoring
Learn more

About Amazon.com Sign In
Amazon Web Services uses information from your Amazon.com account to identify you and allow access to Amazon Web Services. Your use of this site is governed by our Terms of Use and Privacy Policy linked below. Your use of Amazon Web Services products and services is governed by the AWS Customer Agreement linked below unless you have entered into a separate agreement with Amazon Web Services or an AWS Value Added Reseller to purchase these products and services. The AWS Customer Agreement was updated on March 31, 2017. For more information about these updates, see Recent Changes.

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved. Terms of Use | Privacy Policy | AWS Customer Agreement

English

3. In the AWS services search field, enter IAM, then choose IAM from the results list.



AWS services

IAM

IAM
Manage User Access and Encryption Keys

All services

Build a solution
Get started with simple wizards and automated workflows.

Launch a virtual machine
With EC2

Build a web app
With Elastic Beanstalk

Build using virtual servers
With Lightsail

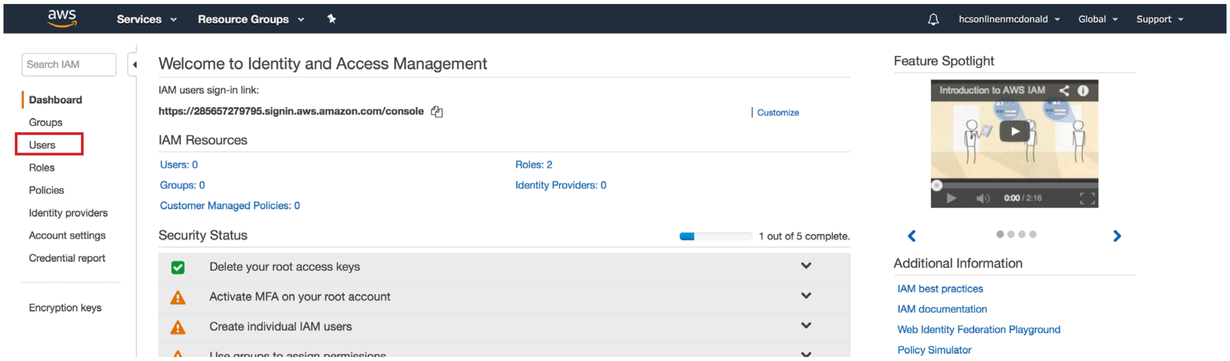
Helpful tips

Manage your costs
Monitor your AWS costs, usage, and reservations using AWS Budgets. Start now

Create an organization
Use AWS Organizations for policy-based management of multiple AWS accounts. Start now

Explore AWS

4. In the sidebar, click Users.



Welcome to Identity and Access Management

IAM users sign-in link:
https://285657279795.signin.aws.amazon.com/console | Customize

IAM Resources

Users: 0 Roles: 2
Groups: 0 Identity Providers: 0
Customer Managed Policies: 0

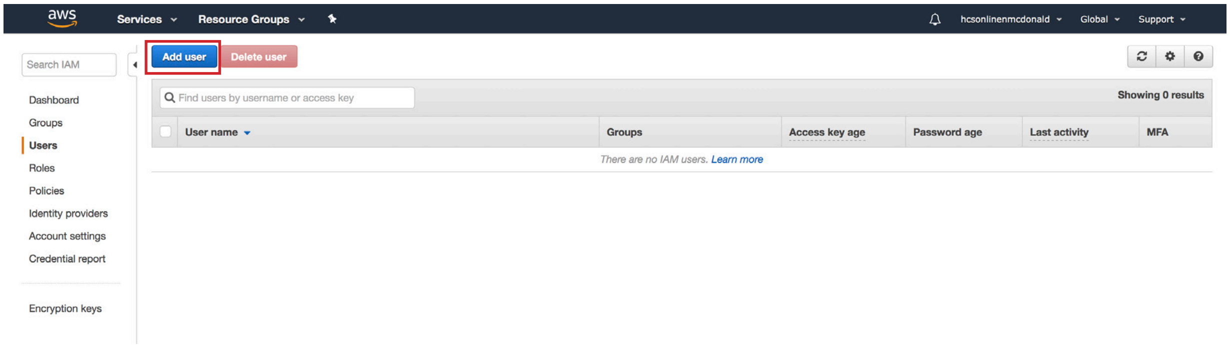
Security Status 1 out of 5 complete.

Delete your root access keys
Activate MFA on your root account
Create individual IAM users
Use groups to assign permissions

Feature Spotlight

Additional Information
IAM best practices
IAM documentation
Web Identity Federation Playground
Policy Simulator

5. Alick “Add Users.”



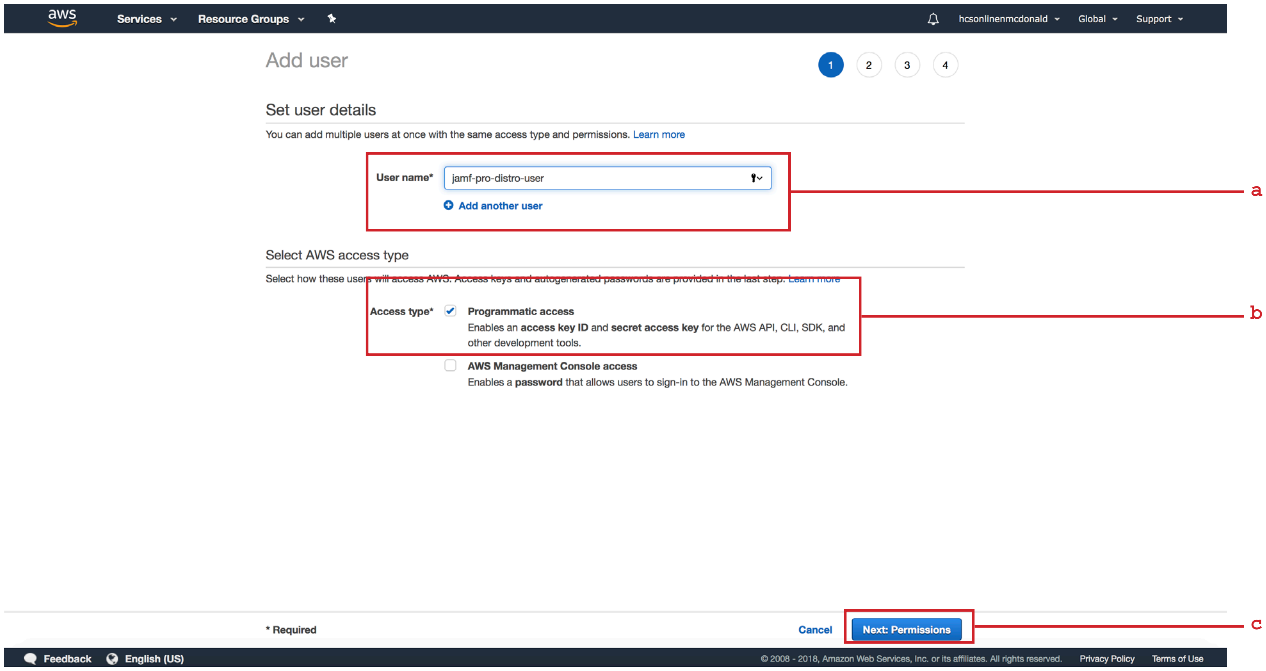
There are no IAM users. Learn more

6. Configure the following details:

a. User name: jamf-pro-distro-user

b. Access Type: Programmatic access

c. Click “Next: Permissions”



Set user details

You can add multiple users at once with the same access type and permissions. Learn more

User name* jamf-pro-distro-user

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. Learn more

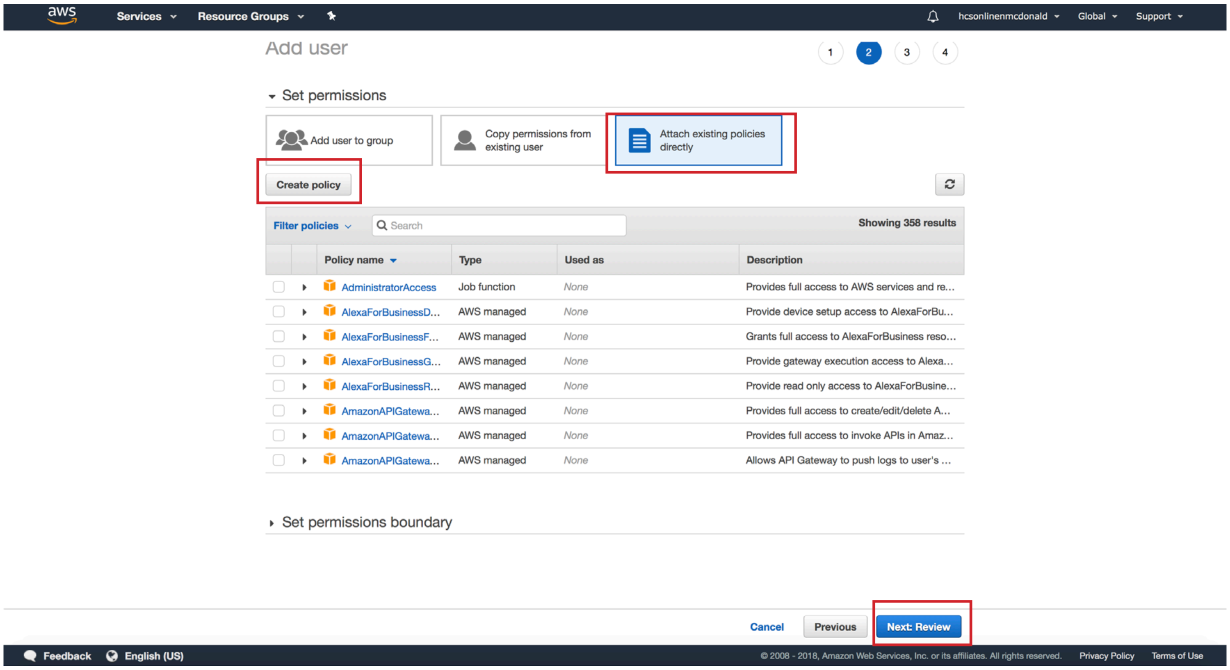
Access type* ☑ Programmatic access
Enables an access key ID and secret access key for the AWS API, CLI, SDK, and other development tools.

□ AWS Management Console access
Enables a password that allows users to sign-in to the AWS Management Console.

* Required

© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

7. Select “Attach existing policies directly”, then click “Create policy.” Click “Next: Review” to continue.



Add user

Set permissions

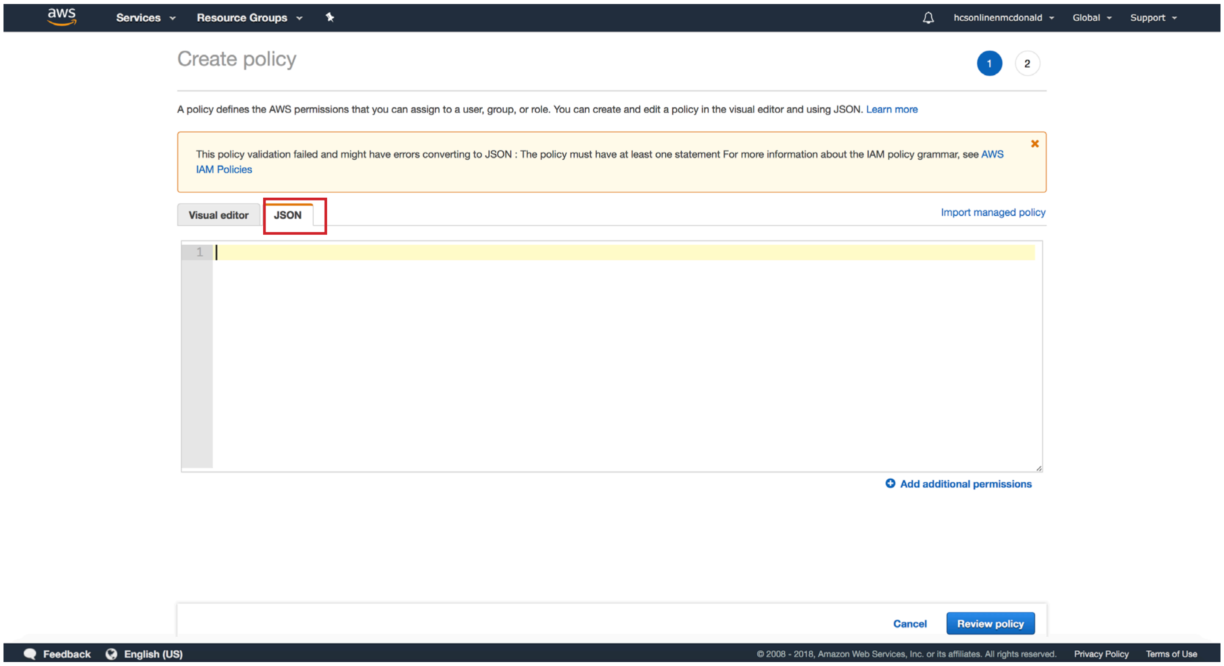
Showing 358 results

Policy name	Type	Used as	Description
AdministratorAccess	Job function	None	Provides full access to AWS services and re...
AlexaForBusinessD...	AWS managed	None	Provide device setup access to AlexaForBu...
AlexaForBusinessF...	AWS managed	None	Grants full access to AlexaForBusiness reso...
AlexaForBusinessG...	AWS managed	None	Provide gateway execution access to Alexa...
AlexaForBusinessR...	AWS managed	None	Provide read only access to AlexaForBusine...
AmazonAPIGatewa...	AWS managed	None	Provides full access to create/edit/delete A...
AmazonAPIGatewa...	AWS managed	None	Provides full access to invoke APIs in Amaz...
AmazonAPIGatewa...	AWS managed	None	Allows API Gateway to push logs to user's ...

Set permissions boundary

© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

8. Click JSON.
9. Remove the existing datatext from the windowJSON field.



Create policy

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. Learn more

This policy validation failed and might have errors converting to JSON : The policy must have at least one statement For more information about the IAM policy grammar, see AWS IAM Policies

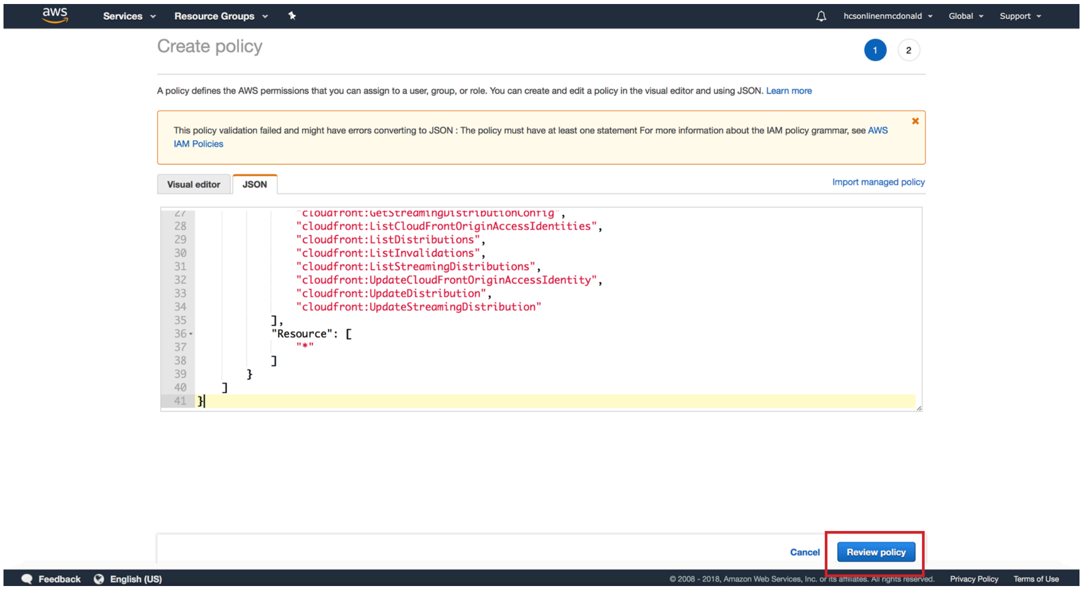
© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

10. Go to this Link: https://goo.gl/eJfXzH

    From the viewable page, copy the text and paste it into the JSON field (The text below is only for reference and will not work):

```
{
    “Version”: “2012-10-17”,
    “Statement”: [
        {
            “Sid”: “AllowFullS3JAMFBucketsOnly”,
            “Effect”: “Allow”,
            “Action”: [
                “s3:*”
            ],
            “Resource”: [
                “arn:aws:s3:::jamf*”
            ]
        },
        {
            “Effect”: “Allow”,
            “Action”: [
                “cloudfront:CreateCloudFrontOriginAccessIdentity”,
                “cloudfront:CreateDistribution”,
                “cloudfront:CreateInvalidation”,
                “cloudfront:CreateStreamingDistribution”,
                “cloudfront:GetCloudFrontOriginAccessIdentity”,
                “cloudfront:GetCloudFrontOriginAccessIdentityConfig”,
                “cloudfront:GetDistribution”,
                “cloudfront:GetDistributionConfig”,
                “cloudfront:GetInvalidation”,
                “cloudfront:GetStreamingDistribution”,
                “cloudfront:GetStreamingDistributionConfig”,
                “cloudfront:ListCloudFrontOriginAccessIdentities”,
                “cloudfront:ListDistributions”,
                “cloudfront:ListInvalidations”,
                “cloudfront:ListStreamingDistributions”,
                “cloudfront:UpdateCloudFrontOriginAccessIdentity”,
                “cloudfront:UpdateDistribution”,
                “cloudfront:UpdateStreamingDistribution”
            ],
            “Resource”: [
                “*”
            ]
        }
    ]
}
```

11. Ignore the warning that the policy must have at least one statement.
12. Click “Review policy.”



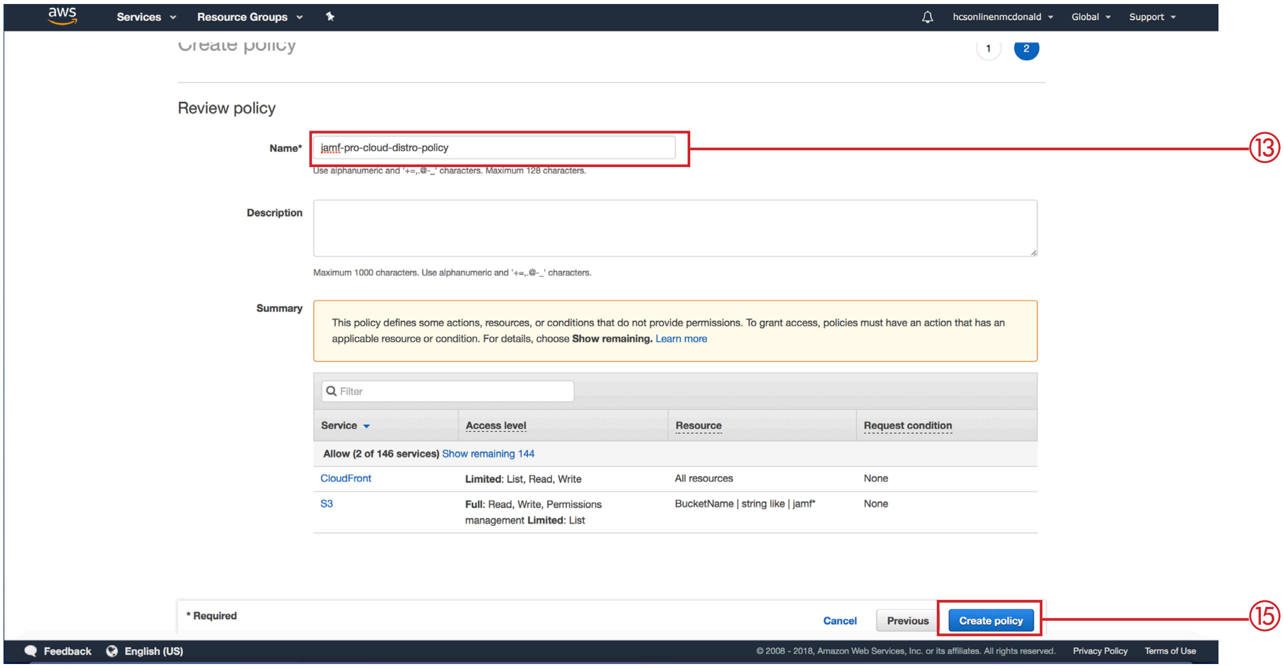
Create policy

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. Learn more

This policy validation failed and might have errors converting to JSON : The policy must have at least one statement For more information about the IAM policy grammar, see AWS IAM Policies

```
                "cloudfront:GetStreamingDistributionConfig",
                "cloudfront:ListCloudFrontOriginAccessIdentities",
                "cloudfront:ListDistributions",
                "cloudfront:ListInvalidations",
                "cloudfront:ListStreamingDistributions",
                "cloudfront:UpdateCloudFrontOriginAccessIdentity",
                "cloudfront:UpdateDistribution",
                "cloudfront:UpdateStreamingDistribution"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

13. In the Name field enter jamf-pro-cloud-distro-policy.
14. You can leave the Description field blank.
15. Click “Create policy.”



Review policy

Name* jamf-pro-cloud-distro-policy

Use alphanumeric and '+=,.@-_' characters. Maximum 128 characters.

Description

Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

Summary

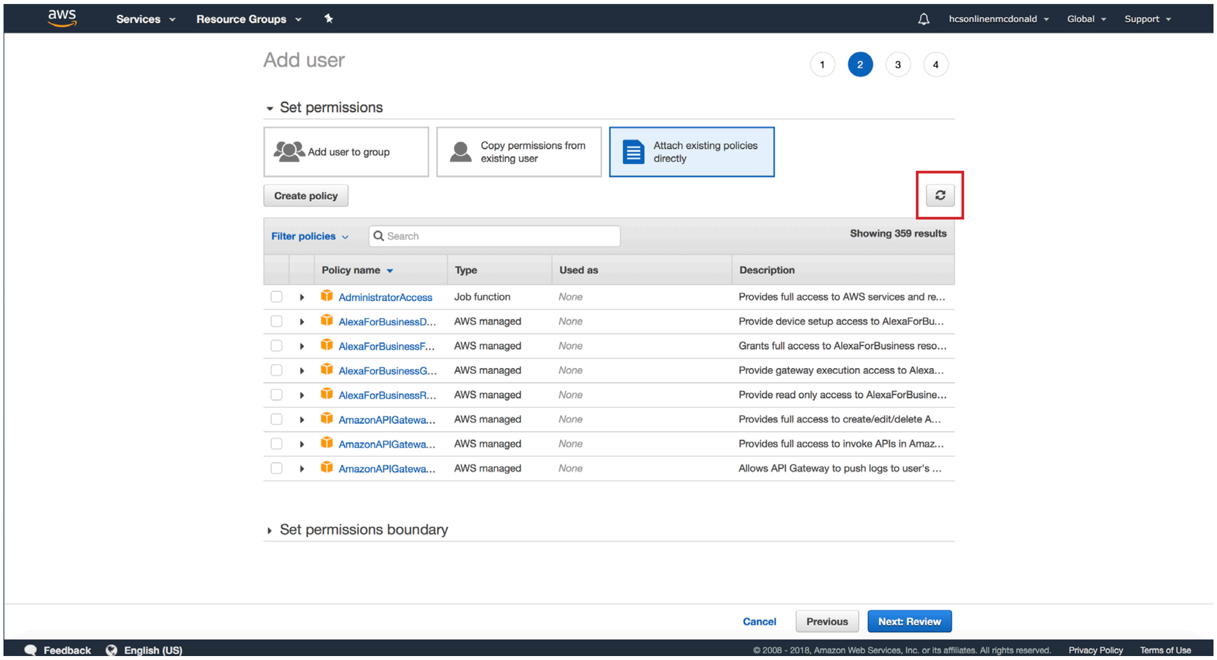
This policy defines some actions, resources, or conditions that do not provide permissions. To grant access, policies must have an action that has an applicable resource or condition. For details, choose **Show remaining.** Learn more

Service	Access level	Resource	Request condition
Allow (2 of 146 services) Show remaining 144			
CloudFront	**Limited**: List, Read, Write	All resources	None
S3	**Full**: Read, Write, Permissions management **Limited**: List	BucketName | string like | jamf*	None

* Required

Cancel | Previous | Create policy

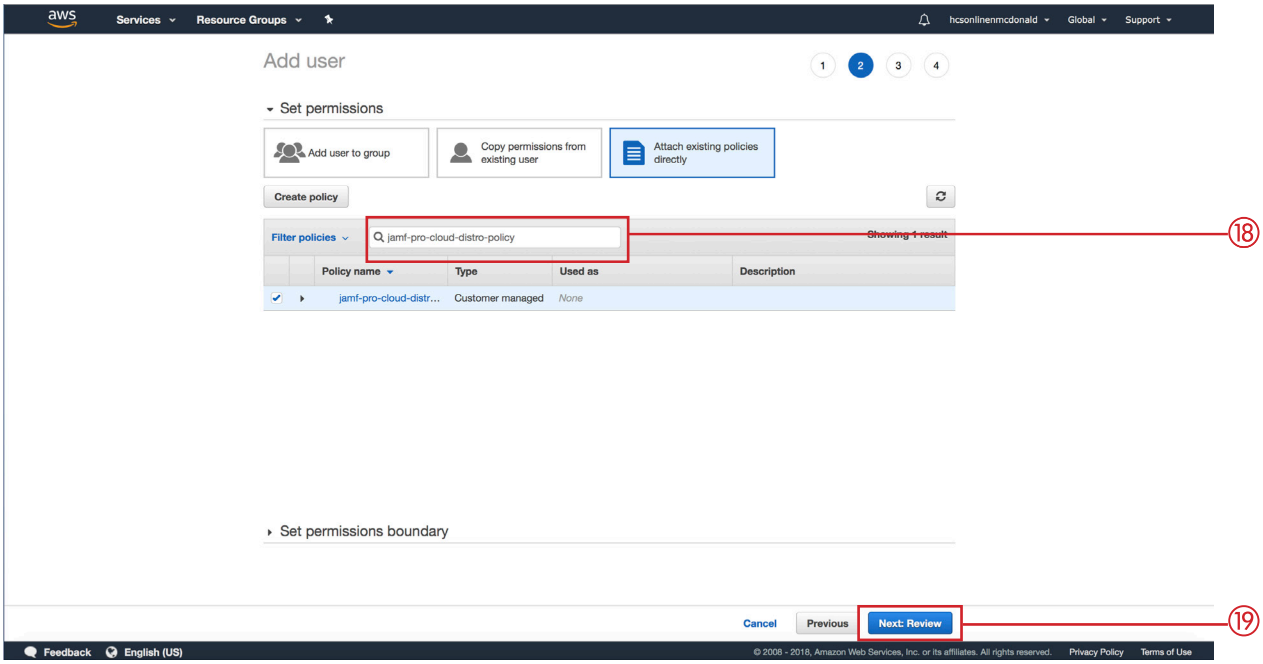
16. Close the IAM Management Console tab.
17. Your web browser should display the Add User screen. Click the Refresh button (looks like two arrows in a circular outline).



Showing 359 results

		Policy name	Type	Used as	Description
□	▸	AdministratorAccess	Job function	*None*	Provides full access to AWS services and re...
□	▸	AlexaForBusinessD...	AWS managed	*None*	Provide device setup access to AlexaForBu...
□	▸	AlexaForBusinessF...	AWS managed	*None*	Grants full access to AlexaForBusiness reso...
□	▸	AlexaForBusinessG...	AWS managed	*None*	Provide gateway execution access to Alexa...
□	▸	AlexaForBusinessR...	AWS managed	*None*	Provide read only access to AlexaForBusine...
□	▸	AmazonAPIGatewa...	AWS managed	*None*	Provides full access to create/edit/delete A...
□	▸	AmazonAPIGatewa...	AWS managed	*None*	Provides full access to invoke APIs in Amaz...
□	▸	AmazonAPIGatewa...	AWS managed	*None*	Allows API Gateway to push logs to user's ...

18. In the policy Search field, enter jamf-pro-cloud-distro-policy.
19. Select the jamf-pro-cloud-distro-policy policy weyou recently created then click “ earlier and click “Next: Review.”



Add user

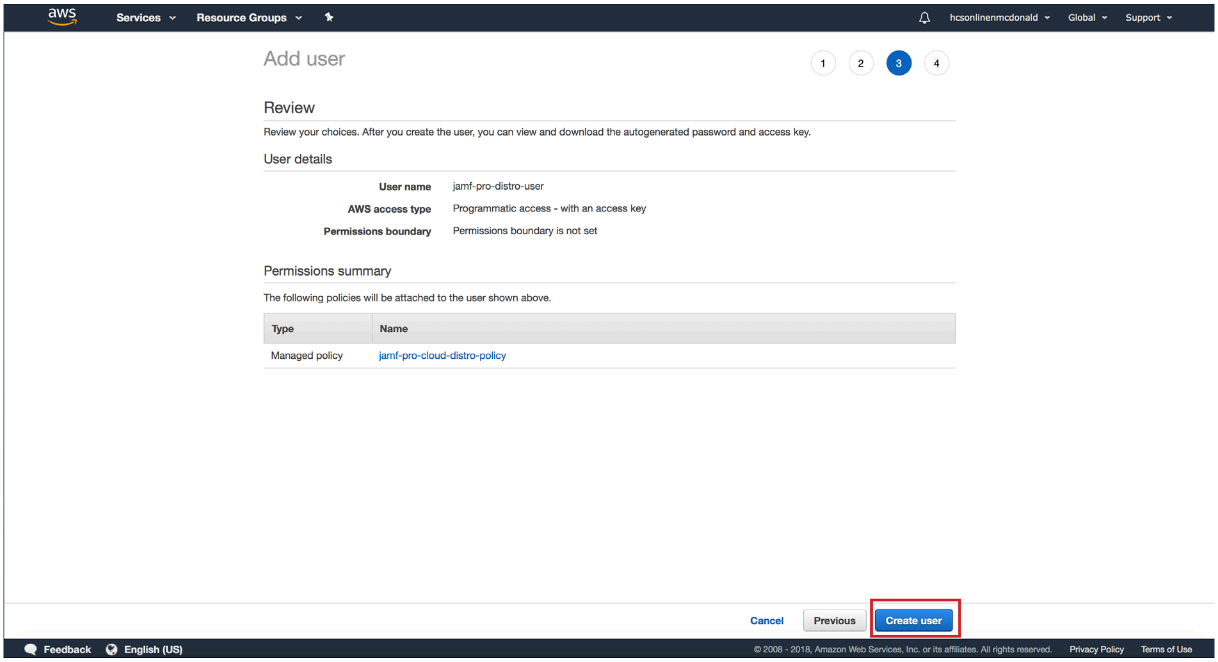
Set permissions

jamf-pro-cloud-distro-policy

		Policy name	Type	Used as	Description
☑	▸	jamf-pro-cloud-distr...	Customer managed	None	

Set permissions boundary

20. Review your information then click “Create user.”



Add user

Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

User details

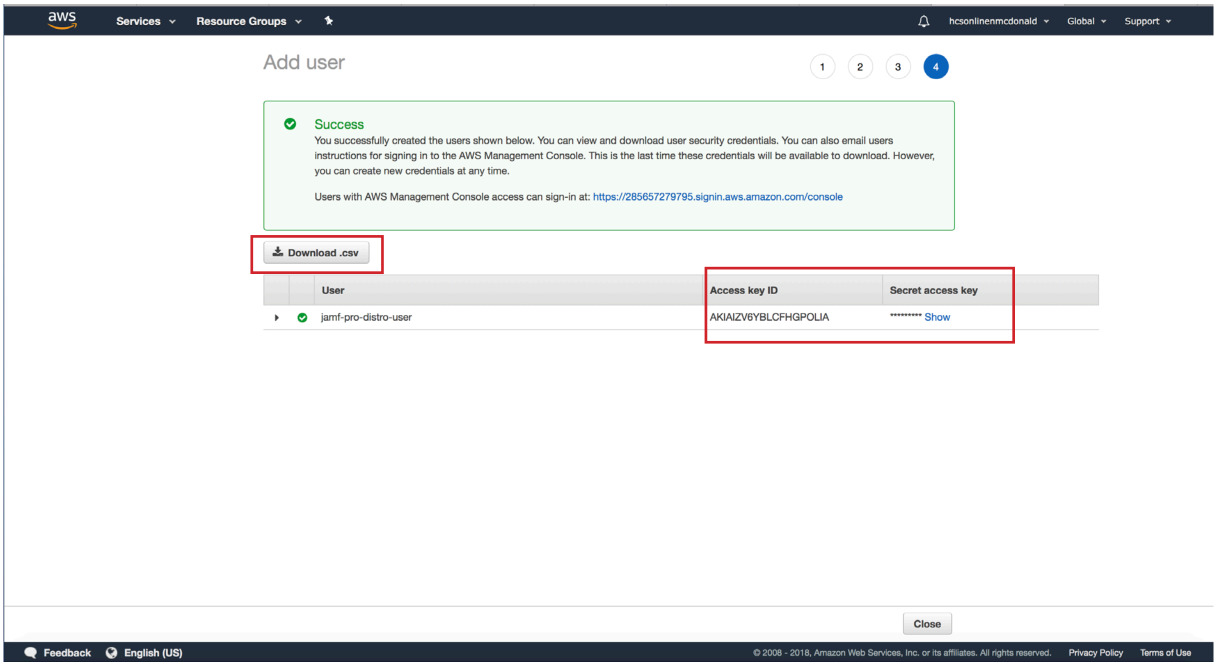
User name	jamf-pro-distro-user
AWS access type	Programmatic access - with an access key
Permissions boundary	Permissions boundary is not set

Permissions summary

The following policies will be attached to the user shown above.

Type	Name
Managed policy	jamf-pro-cloud-distro-policy

21. At the success screen, click “Show” (which is displayed below the Secret access key).



Add user

Success

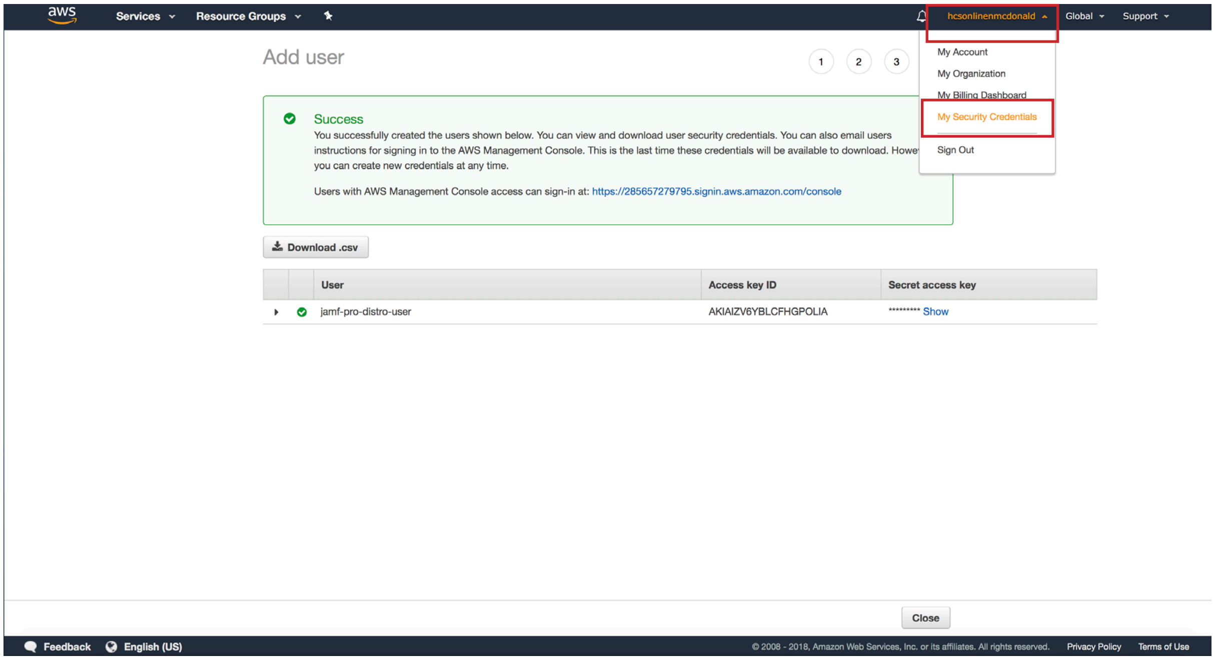
You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: https://285657279795.signin.aws.amazon.com/console

User	Access key ID	Secret access key
jamf-pro-distro-user	AKIAIZV6YBLCFHGPOLIA	********* Show

22. Write down both the Access key ID and “Secret access key.” You need these pieces of information in the next section. Or you can click “Download .csv” to download the information. If you do not wish to use signed URLs in Jamf Pro you can skip to the next section, “Configure an AWS Distribution Point in Jamf Pro.”

23. To use Signed URLs, click your account name in the upper right hand corner, then choose “My Security Credentials.”



Add user

Success

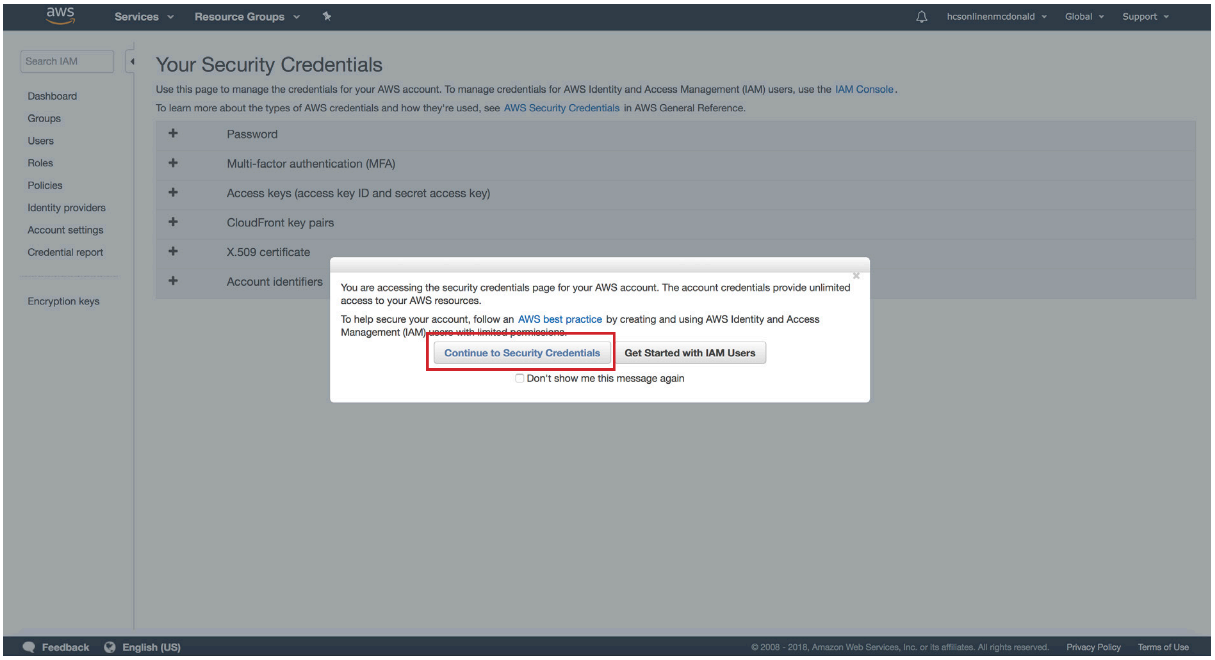
You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. Howe

you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: https://285657279795.signin.aws.amazon.com/console

User	Access key ID	Secret access key
jamf-pro-distro-user	AKIAIZV6YBLCFHGPOLIA	********* Show

24. Select “Continue with Security Credentials”.



Your Security Credentials

Use this page to manage the credentials for your AWS account. To manage credentials for AWS Identity and Access Management (IAM) users, use the IAM Console.

To learn more about the types of AWS credentials and how they're used, see AWS Security Credentials in AWS General Reference.

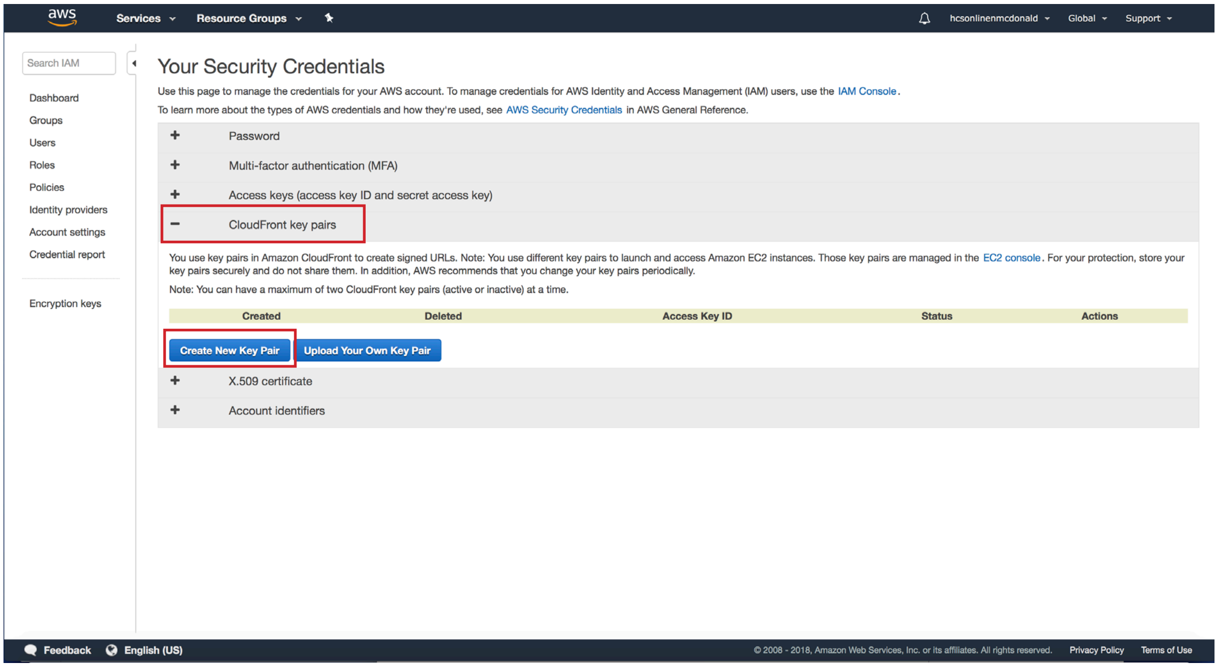
- Password
- Multi-factor authentication (MFA)
- Access keys (access key ID and secret access key)
- CloudFront key pairs
- X.509 certificate
- Account identifiers

You are accessing the security credentials page for your AWS account. The account credentials provide unlimited access to your AWS resources.

To help secure your account, follow an AWS best practice by creating and using AWS Identity and Access Management (IAM) users with limited permissions.

Continue to Security Credentials
Get Started with IAM Users
□ Don't show me this message again

25. Select “CloudFront key pairs” then click “Create New Key Pair.”



Your Security Credentials

Use this page to manage the credentials for your AWS account. To manage credentials for AWS Identity and Access Management (IAM) users, use the IAM Console.

To learn more about the types of AWS credentials and how they're used, see AWS Security Credentials in AWS General Reference.

- Password
- Multi-factor authentication (MFA)
- Access keys (access key ID and secret access key)
- CloudFront key pairs

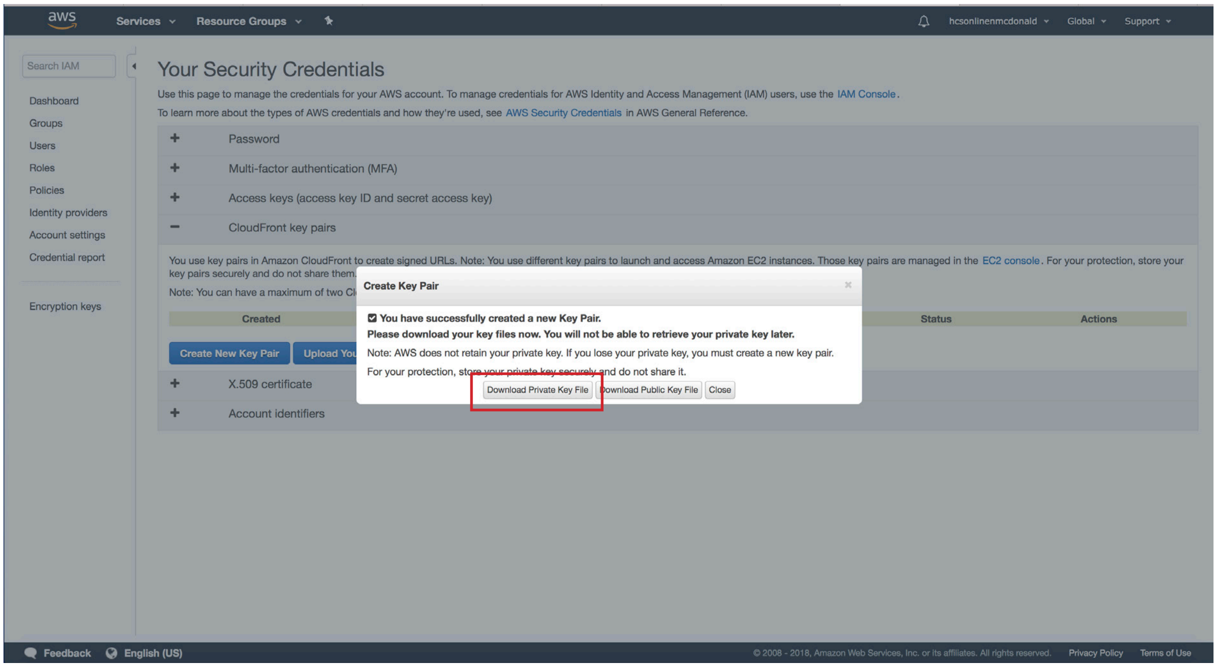
You use key pairs in Amazon CloudFront to create signed URLs. Note: You use different key pairs to launch and access Amazon EC2 instances. Those key pairs are managed in the EC2 console. For your protection, store your key pairs securely and do not share them. In addition, AWS recommends that you change your key pairs periodically.

Note: You can have a maximum of two CloudFront key pairs (active or inactive) at a time.

Created	Deleted	Access Key ID	Status	Actions

- X.509 certificate
- Account identifiers

26. Click “Download Private Key File”. Your private key will start with pk-. Note: Your file will download with a filename suffix of .pem.txt. You must change the filename suffix to .pem only.



Your Security Credentials

Use this page to manage the credentials for your AWS account. To manage credentials for AWS Identity and Access Management (IAM) users, use the IAM Console.

To learn more about the types of AWS credentials and how they're used, see AWS Security Credentials in AWS General Reference.

You use key pairs in Amazon CloudFront to create signed URLs. Note: You use different key pairs to launch and access Amazon EC2 instances. Those key pairs are managed in the EC2 console. For your protection, store your key pairs securely and do not share them.

Note: You can have a maximum of two Cl

☑ **You have successfully created a new Key Pair.**

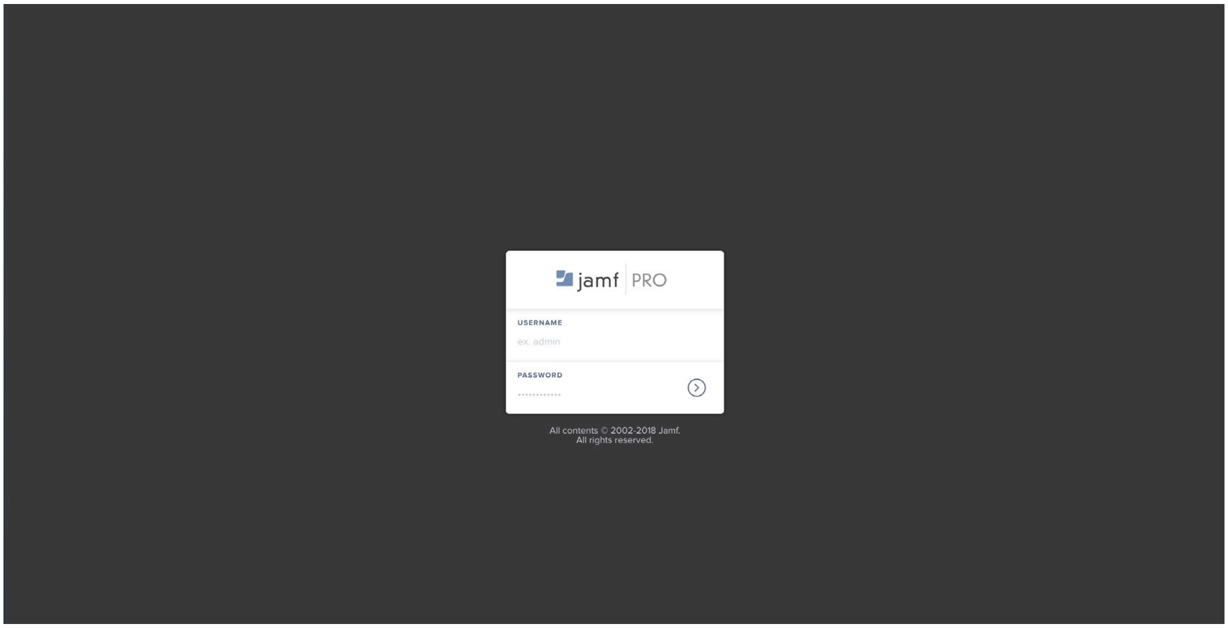
Please download your key files now. You will not be able to retrieve your private key later.

Note: AWS does not retain your private key. If you lose your private key, you must create a new key pair.

For your protection, store your private key securely and do not share it.

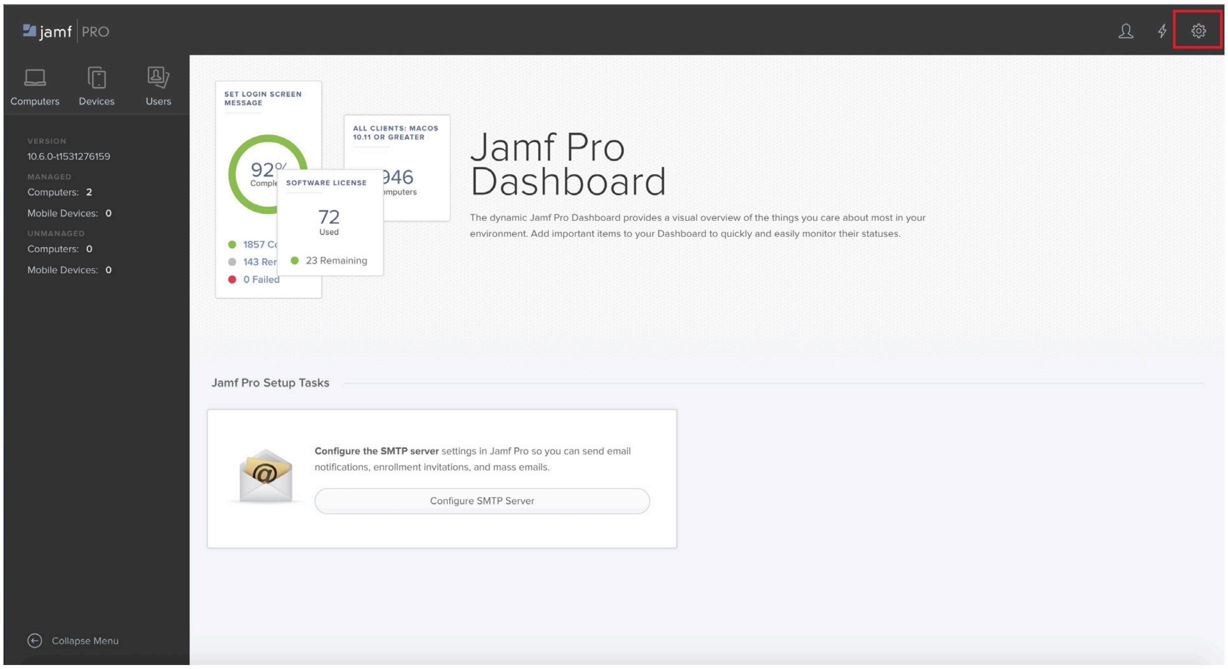
Configure an AWS Distribution Point in Jamf Pro

1. Navigate to your Jamf Pro Server, for example, https://hcsjamf.hcsonline.com



All contents © 2002-2018 Jamf.
All rights reserved.

2. Sign in with an Administrative account.
3. Click the Settings button (looks like a gear) in the upper- right hand corner.



VERSION: 10.6.0-t1531276159

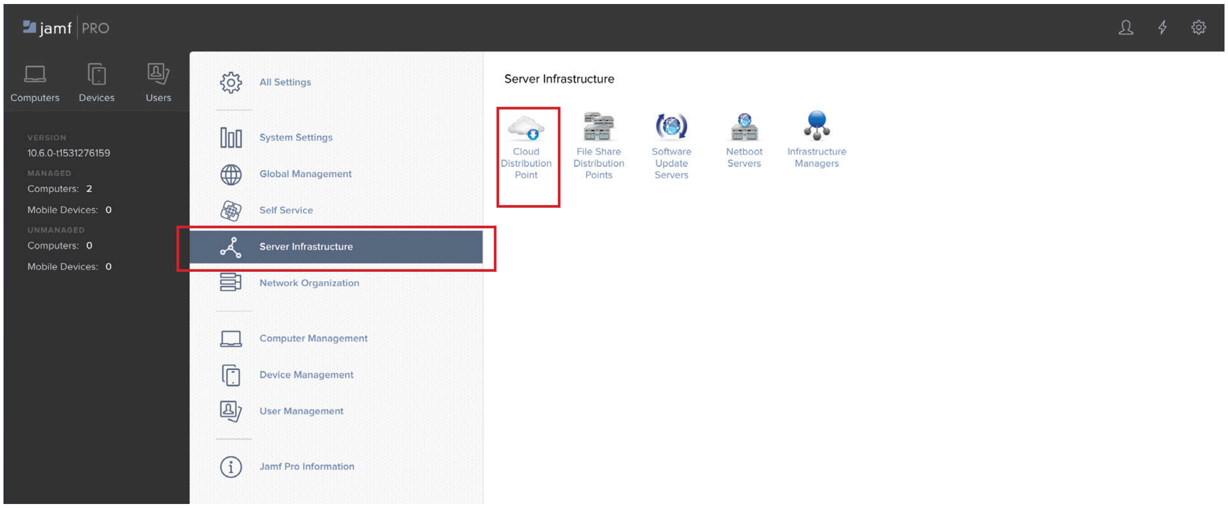
MANAGED
Computers: 2
Mobile Devices: 0

UNMANAGED
Computers: 0
Mobile Devices: 0

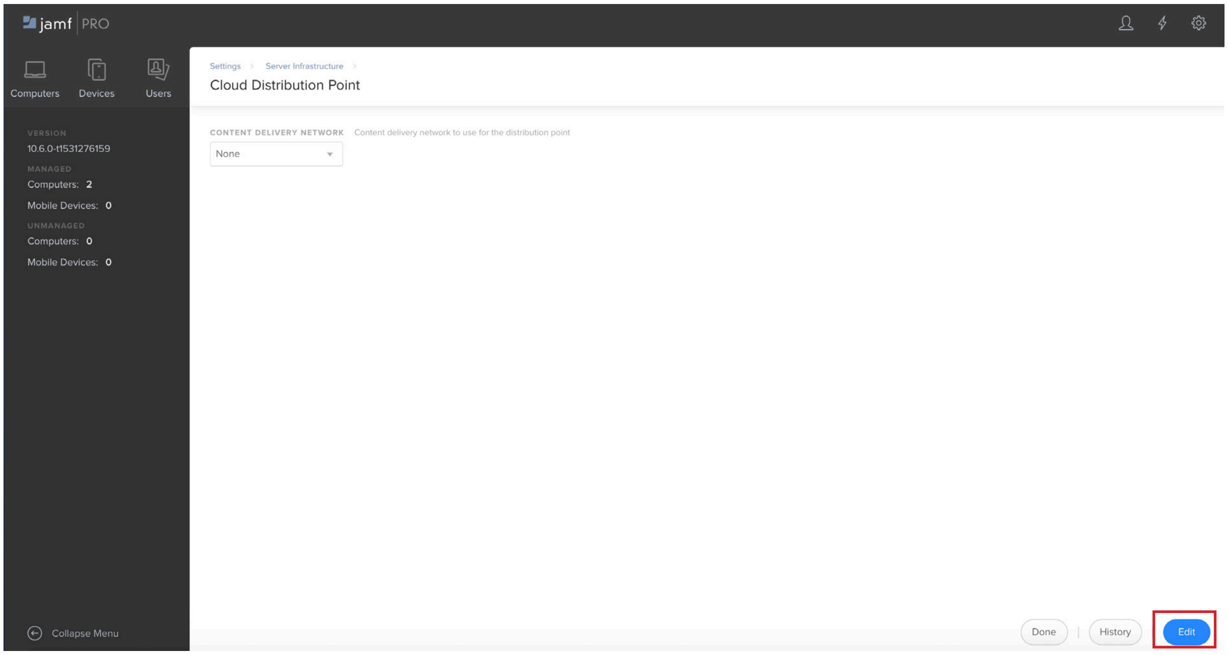
The dynamic Jamf Pro Dashboard provides a visual overview of the things you care about most in your environment. Add important items to your Dashboard to quickly and easily monitor their statuses.

Configure the SMTP server settings in Jamf Pro so you can send email notifications, enrollment invitations, and mass emails.

4. In the middle column, select “Server Infrastructure,” then click “Cloud Distribution Point.



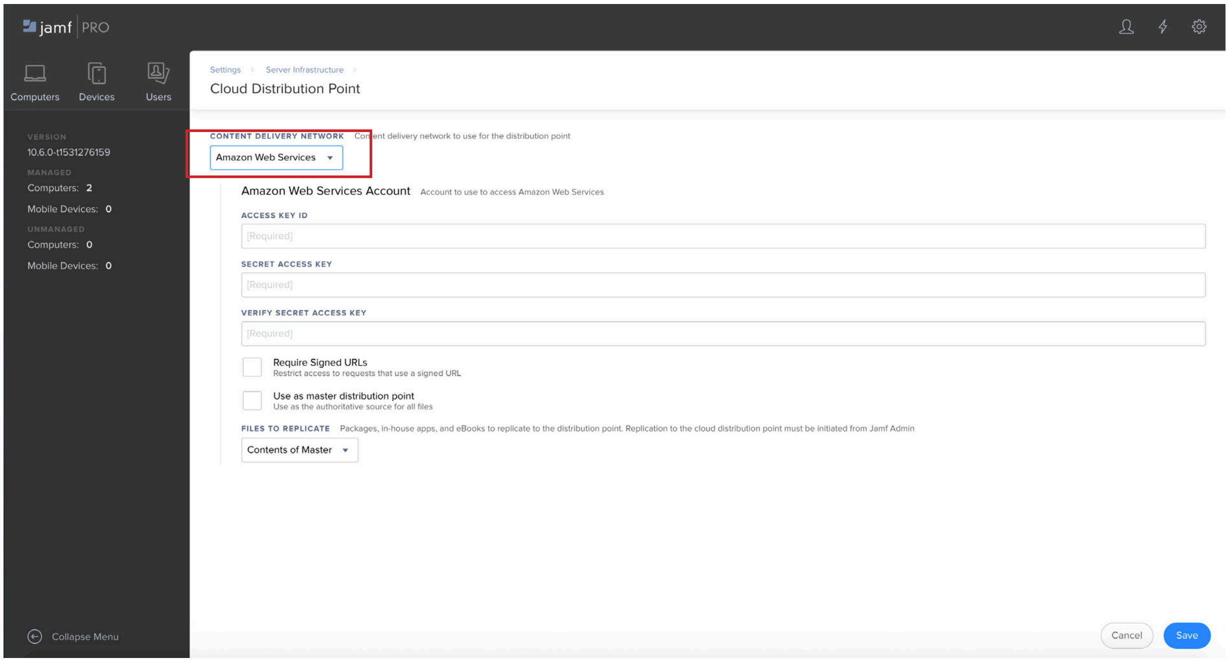
5. Select “Edit” from the lower right hand corner.



CONTENT DELIVERY NETWORK Content delivery network to use for the distribution point

None

6. Click the Content Delivery Network pop-up menu then choose “Amazon Web Services”.



VERSION 10.6.0-t1531276159
MANAGED
Computers: 2
Mobile Devices: 0
UNMANAGED
Computers: 0
Mobile Devices: 0

Settings > Server Infrastructure >

Cloud Distribution Point

CONTENT DELIVERY NETWORK Content delivery network to use for the distribution point
Amazon Web Services

Amazon Web Services Account Account to use to access Amazon Web Services

ACCESS KEY ID
[Required]

SECRET ACCESS KEY
[Required]

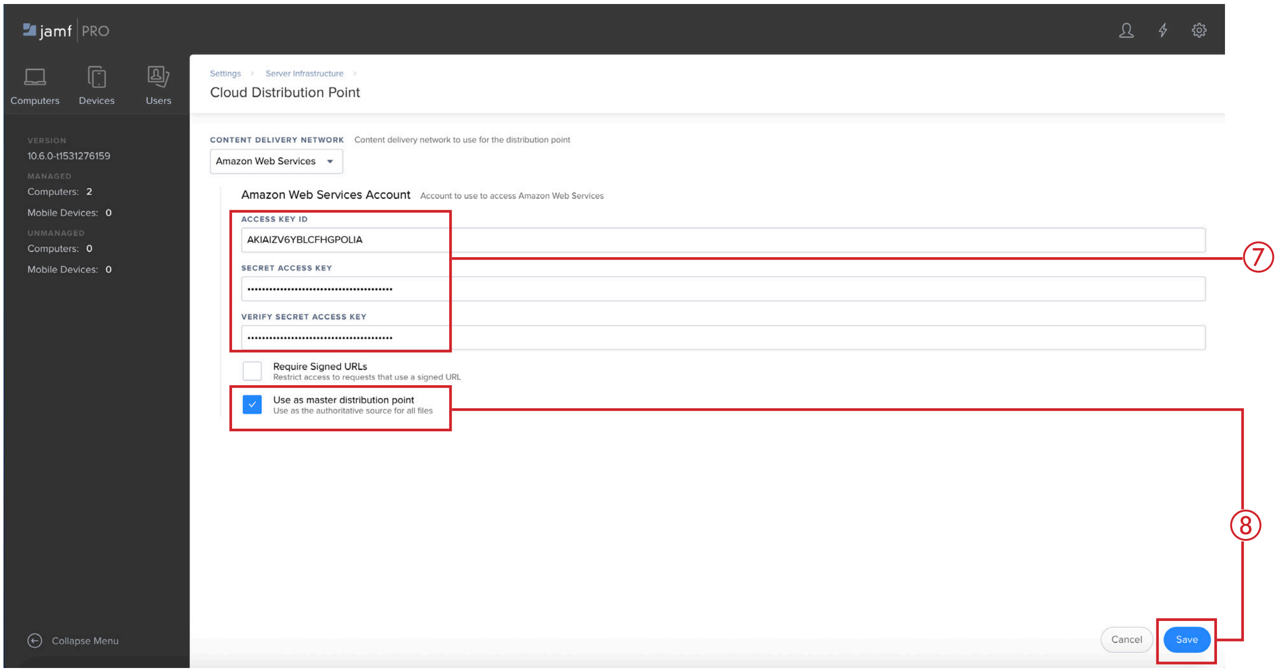
VERIFY SECRET ACCESS KEY
[Required]

□ Require Signed URLs
Restrict access to requests that use a signed URL

□ Use as master distribution point
Use as the authoritative source for all files

FILES TO REPLICATE Packages, in-house apps, and eBooks to replicate to the distribution point. Replication to the cloud distribution point must be initiated from Jamf Admin
Contents of Master

7. Click the Content Delivery Network pop-up menu then choose “Amazon Web Services”.
8. If you wish for your “Cloud Distribution Point” to also be your “Master Distribution Point,” select the checkbox labeled “Use as Master Distribution Point.” By default all contents of your Master Distribution Point will be replicated to any additional cloud distribution points you have. If you do not wish to use signed URLs, click Save in the lower-right corner.



VERSION 10.6.0-t1531276159
MANAGED
Computers: 2
Mobile Devices: 0
UNMANAGED
Computers: 0
Mobile Devices: 0

Settings > Server Infrastructure >

Cloud Distribution Point

CONTENT DELIVERY NETWORK Content delivery network to use for the distribution point
Amazon Web Services

Amazon Web Services Account Account to use to access Amazon Web Services

ACCESS KEY ID
AKIAIZV6YBLCFHGPOLIA

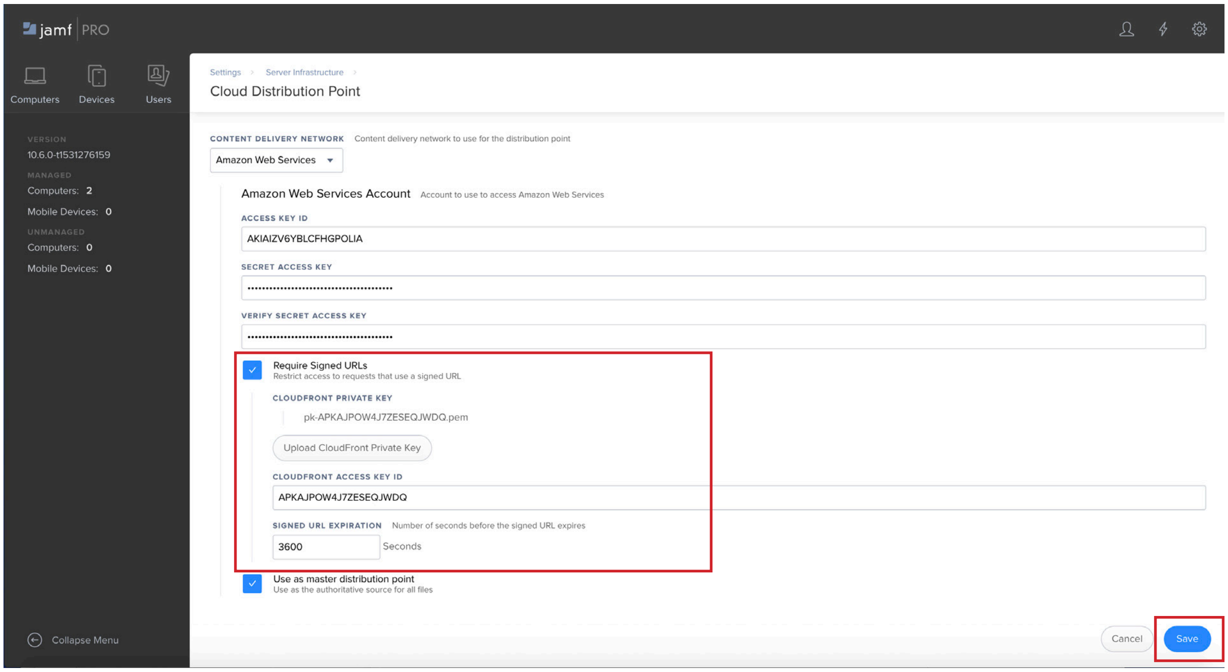
SECRET ACCESS KEY
••

VERIFY SECRET ACCESS KEY
••

□ Require Signed URLs
Restrict access to requests that use a signed URL

☑ Use as master distribution point
Use as the authoritative source for all files

9. If you wish to require signed URLs, ensure that you followed steps 24-26 in the previous section, then select the checkbox labeled "Require Signed URLs", click "Upload CloudFront Private Key," then select the private key you downloaded and renamed earlier. Confirm that your CloudFront Access Key ID should auto-populates, then click Save.



VERSION
10.6.0-t1531276159
MANAGED
Computers: 2
Mobile Devices: 0
UNMANAGED
Computers: 0
Mobile Devices: 0

Cloud Distribution Point

CONTENT DELIVERY NETWORK Content delivery network to use for the distribution point
Amazon Web Services

Amazon Web Services Account Account to use to access Amazon Web Services

ACCESS KEY ID
AKIAIZV6YBLCFHGPOLIA

SECRET ACCESS KEY
•••

VERIFY SECRET ACCESS KEY
•••

☑ Require Signed URLs
Restrict access to requests that use a signed URL

CLOUDFRONT PRIVATE KEY
pk-APKAJPOW4J7ZESEQJWDQ.pem

Upload CloudFront Private Key

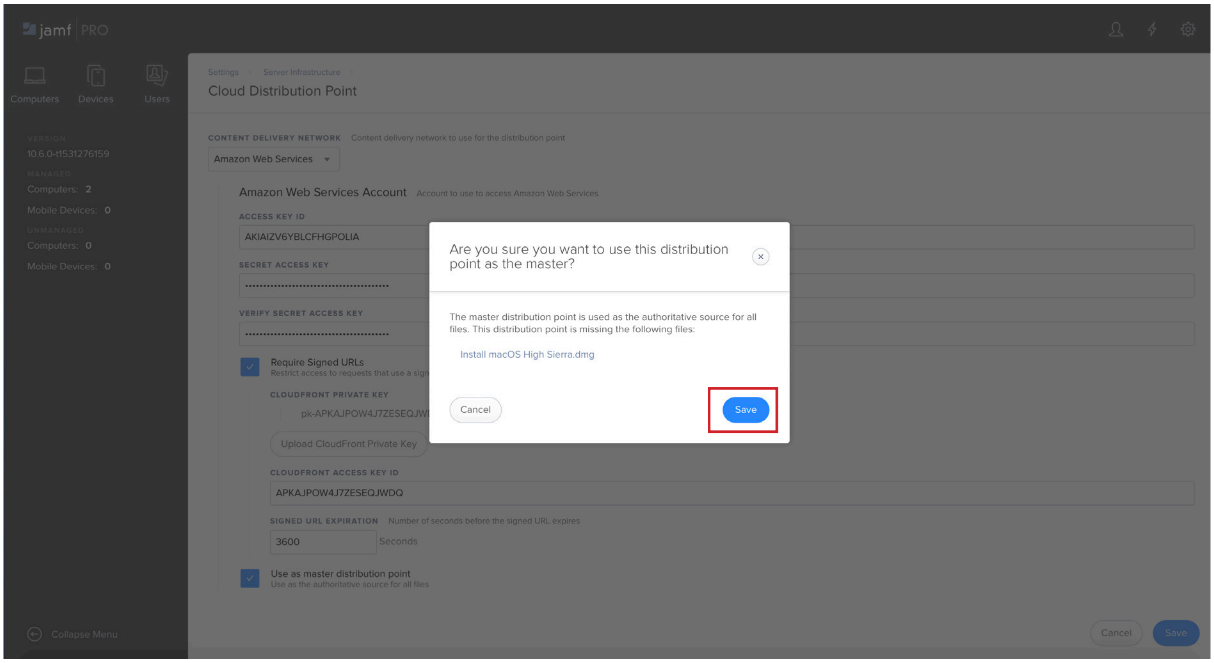
CLOUDFRONT ACCESS KEY ID
APKAJPOW4J7ZESEQJWDQ

SIGNED URL EXPIRATION Number of seconds before the signed URL expires
3600 Seconds

☑ Use as master distribution point
Use as the authoritative source for all files

Cancel Save

10. If you receive a warning labeled "Are you sure you want to use this distribution point as the master?" This means that you already have packages in your old Master Distribution Point; if this is the case, you can use the Mac app Jamf Admin to copy packages to your new Master Distribution Point after you complete this guide.

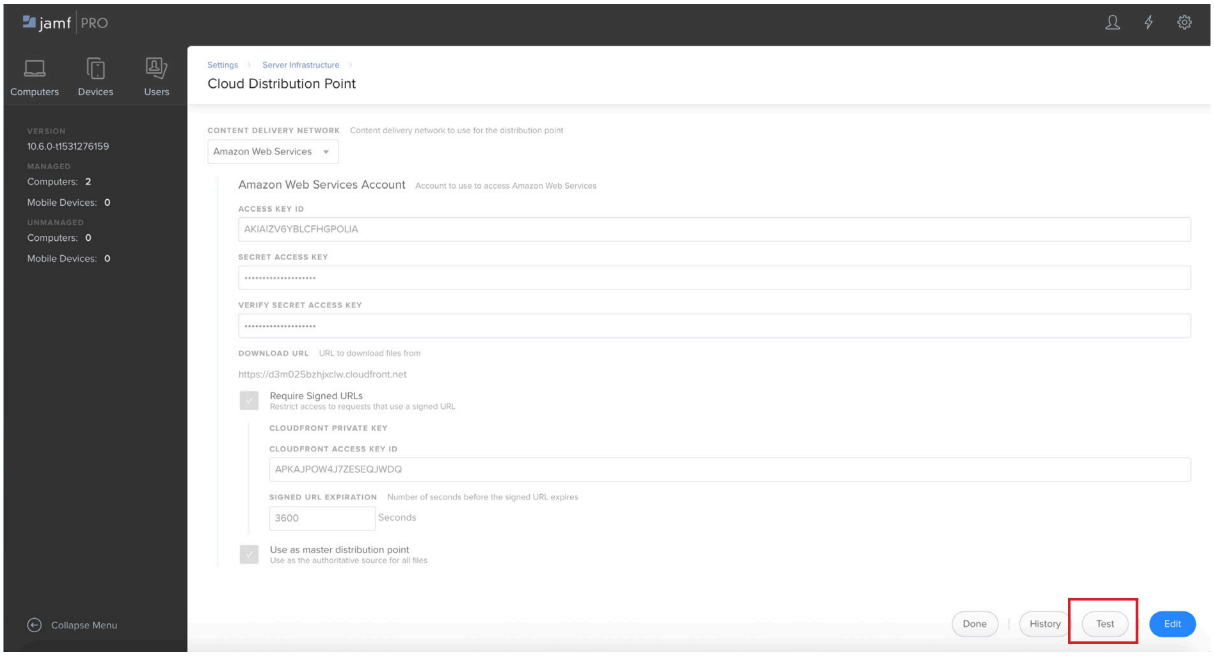

Are you sure you want to use this distribution point as the master?

The master distribution point is used as the authoritative source for all files. This distribution point is missing the following files:

Install macOS High Sierra.dmg

Cancel Save

11. Click “Test” in the lower-right corner.



VERSION
10.6.0-t1531276159
MANAGED
Computers: 2
Mobile Devices: 0
UNMANAGED
Computers: 0
Mobile Devices: 0

Settings > Server Infrastructure >

Cloud Distribution Point

CONTENT DELIVERY NETWORK Content delivery network to use for the distribution point
Amazon Web Services

Amazon Web Services Account Account to use to access Amazon Web Services

ACCESS KEY ID
AKIAIZV6YBLCFHGPOLIA

SECRET ACCESS KEY
••••••••••••••••••••

VERIFY SECRET ACCESS KEY
••••••••••••••••••••

DOWNLOAD URL URL to download files from
https://d3m025bzhjxclw.cloudfront.net

☑ Require Signed URLs
Restrict access to requests that use a signed URL

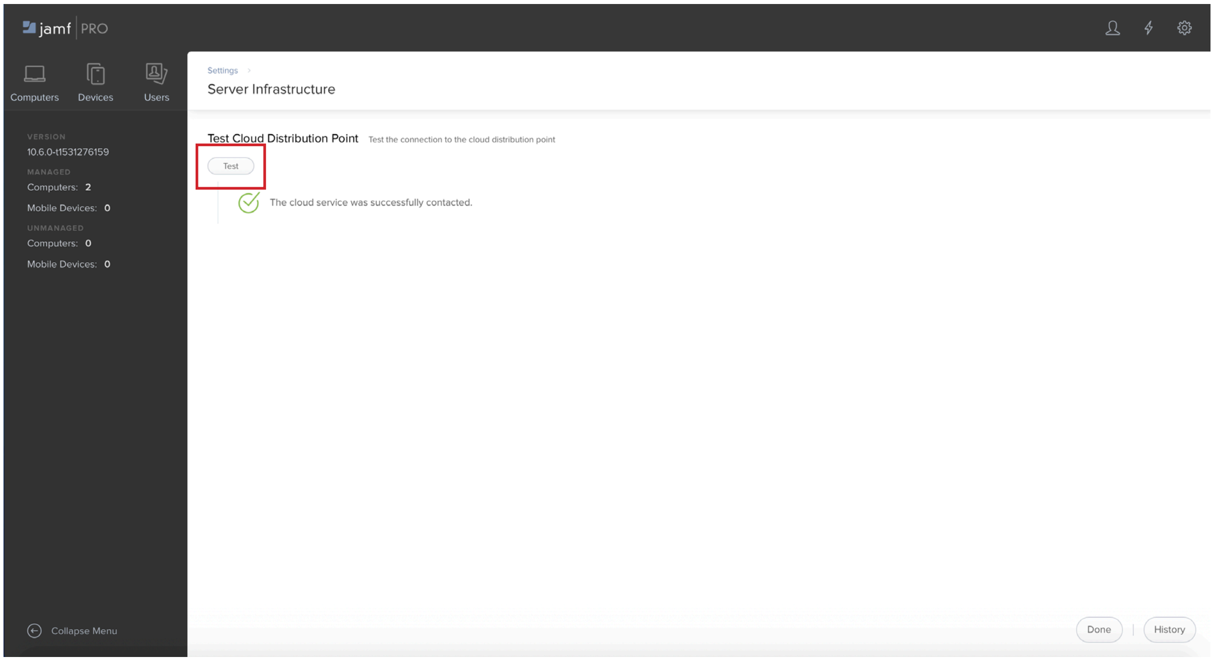
CLOUDFRONT PRIVATE KEY

CLOUDFRONT ACCESS KEY ID
APKAJPOW4J7ZESEQJWDQ

SIGNED URL EXPIRATION Number of seconds before the signed URL expires
3600 Seconds

☑ Use as master distribution point
Use as the authoritative source for all files

12. Click “Test,” then confirm you see the following success message, otherwise go back and check your settings.



VERSION
10.6.0-t1531276159
MANAGED
Computers: 2
Mobile Devices: 0
UNMANAGED
Computers: 0
Mobile Devices: 0

Settings >

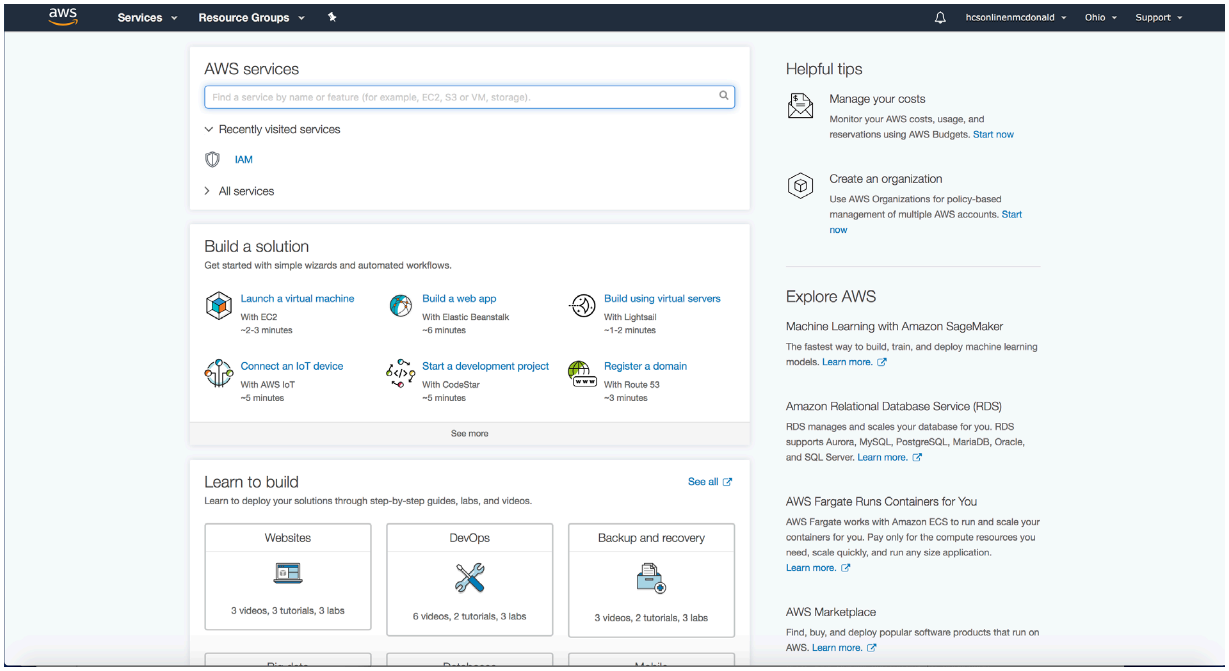
Server Infrastructure

Test Cloud Distribution Point Test the connection to the cloud distribution point

✓ The cloud service was successfully contacted.

Verify Jamf Pro Created an S3 Bucket

1. Navigate back to your Amazon Web Services Console (https://console.aws.amazon.com) and sign in again if needed.



AWS services

Find a service by name or feature (for example, EC2, S3 or VM, storage).

Recently visited services

IAM

All services

Build a solution

Get started with simple wizards and automated workflows.

Launch a virtual machine
With EC2
~2-3 minutes

Build a web app
With Elastic Beanstalk
~6 minutes

Build using virtual servers
With Lightsail
~1-2 minutes

Connect an IoT device
With AWS IoT
~5 minutes

Start a development project
With CodeStar
~5 minutes

Register a domain
With Route 53
~3 minutes

See more

Learn to build

See all

Learn to deploy your solutions through step-by-step guides, labs, and videos.

Websites
3 videos, 3 tutorials, 3 labs

DevOps
6 videos, 2 tutorials, 3 labs

Backup and recovery
3 videos, 2 tutorials, 3 labs

Helpful tips

Manage your costs
Monitor your AWS costs, usage, and reservations using AWS Budgets. Start now

Create an organization
Use AWS Organizations for policy-based management of multiple AWS accounts. Start now

Explore AWS

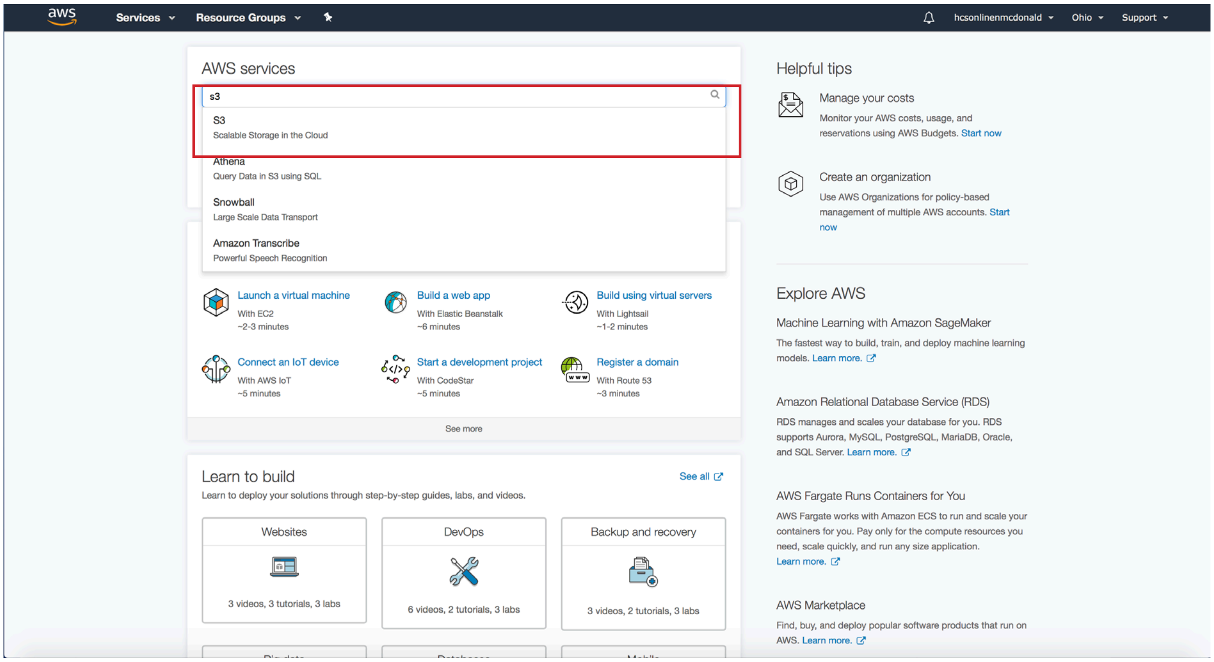
Machine Learning with Amazon SageMaker
The fastest way to build, train, and deploy machine learning models. Learn more.

Amazon Relational Database Service (RDS)
RDS manages and scales your database for you. RDS supports Aurora, MySQL, PostgreSQL, MariaDB, Oracle, and SQL Server. Learn more.

AWS Fargate Runs Containers for You
AWS Fargate works with Amazon ECS to run and scale your containers for you. Pay only for the compute resources you need, scale quickly, and run any size application.
Learn more.

AWS Marketplace
Find, buy, and deploy popular software products that run on AWS. Learn more.

2. In the AWS Services Search bar search for S3 and choose the first result as shown below.



AWS services

s3

S3
Scalable Storage in the Cloud

Athena
Query Data in S3 using SQL

Snowball
Large Scale Data Transport

Amazon Transcribe
Powerful Speech Recognition

Launch a virtual machine
With EC2
~2-3 minutes

Build a web app
With Elastic Beanstalk
~6 minutes

Build using virtual servers
With Lightsail
~1-2 minutes

Connect an IoT device
With AWS IoT
~5 minutes

Start a development project
With CodeStar
~5 minutes

Register a domain
With Route 53
~3 minutes

See more

Learn to build

See all

Learn to deploy your solutions through step-by-step guides, labs, and videos.

Websites
3 videos, 3 tutorials, 3 labs

DevOps
6 videos, 2 tutorials, 3 labs

Backup and recovery
3 videos, 2 tutorials, 3 labs

Helpful tips

Manage your costs
Monitor your AWS costs, usage, and reservations using AWS Budgets. Start now

Create an organization
Use AWS Organizations for policy-based management of multiple AWS accounts. Start now

Explore AWS

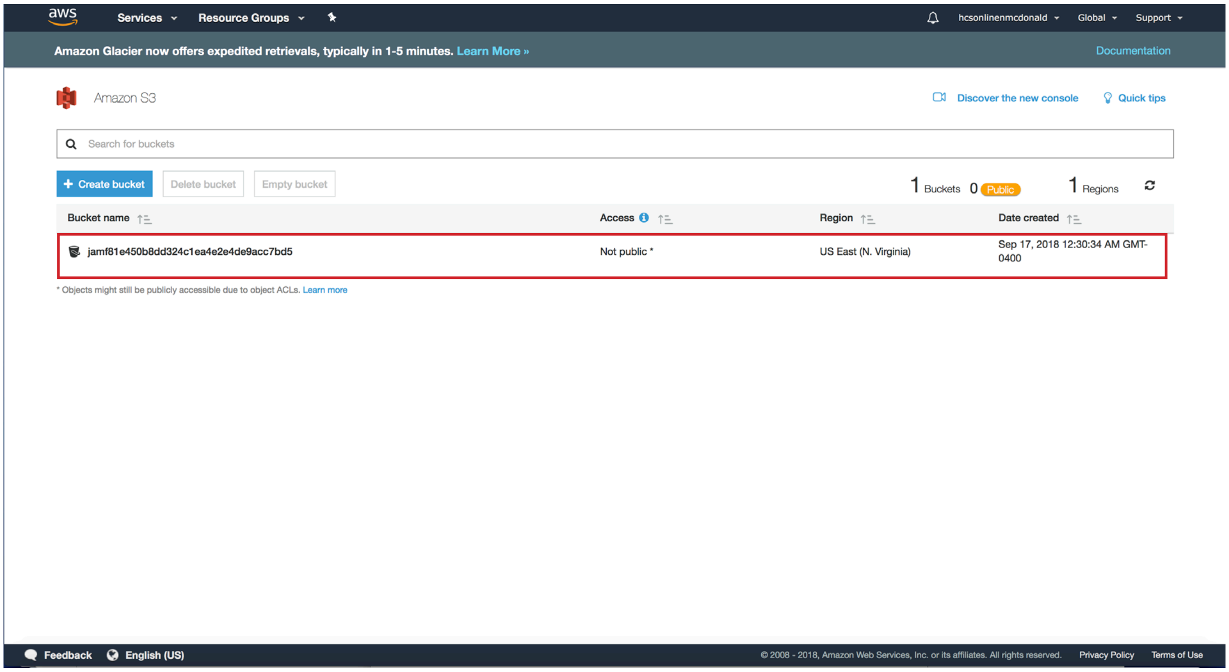
Machine Learning with Amazon SageMaker
The fastest way to build, train, and deploy machine learning models. Learn more.

Amazon Relational Database Service (RDS)
RDS manages and scales your database for you. RDS supports Aurora, MySQL, PostgreSQL, MariaDB, Oracle, and SQL Server. Learn more.

AWS Fargate Runs Containers for You
AWS Fargate works with Amazon ECS to run and scale your containers for you. Pay only for the compute resources you need, scale quickly, and run any size application.
Learn more.

AWS Marketplace
Find, buy, and deploy popular software products that run on AWS. Learn more.

3. Confirm that you see a bucket beginning with “jamf.” This is a final confirmation that the Jamf Pro Server was able to successfully contact AWS and create an S3 bucket for storage.



Amazon Glacier now offers expedited retrievals, typically in 1-5 minutes. Learn More »

Bucket name	Access	Region	Date created
jamf81e450b8dd324c1ea4e2e4de9acc7bd5	Not public *	US East (N. Virginia)	Sep 17, 2018 12:30:34 AM GMT-0400

* Objects might still be publicly accessible due to object ACLs. Learn more

© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

4. You are now finished!