

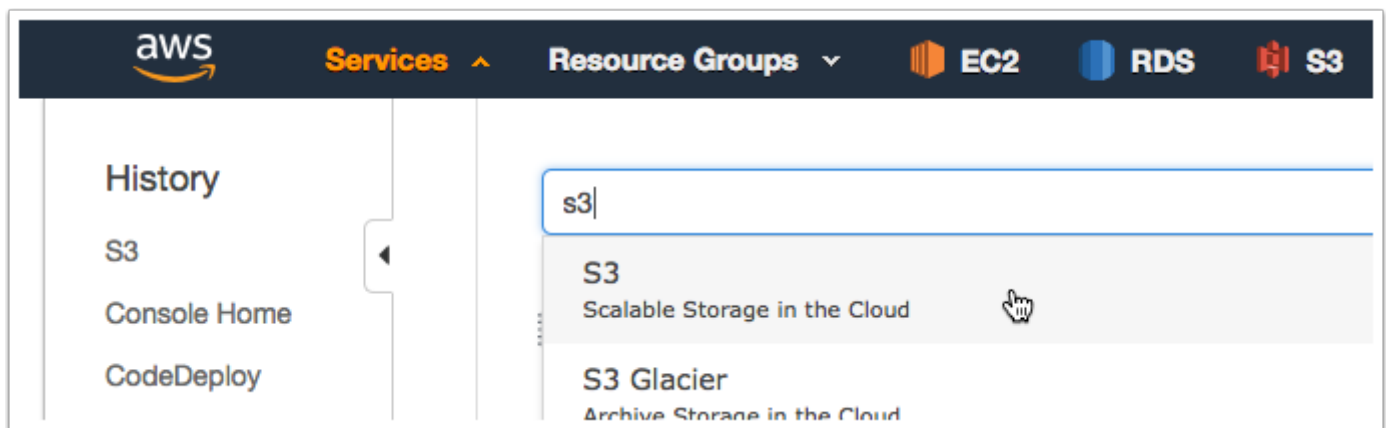
Setting Up an Amazon S3™ Bucket for WHMCS

If you want to use Amazon S3™ as the storage provider for your WHMCS installation, you will need to create an S3 bucket.

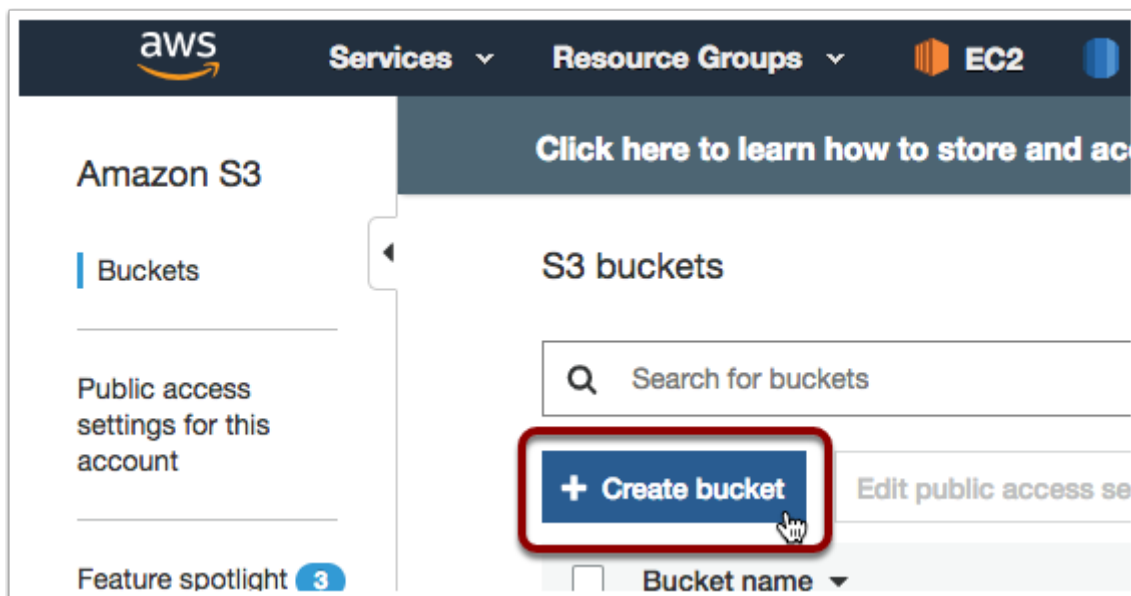
Create an S3 Bucket

To create an Amazon S3 bucket:

1. Log in to your Amazon account at <https://aws.amazon.com/>.
2. Go to S3.

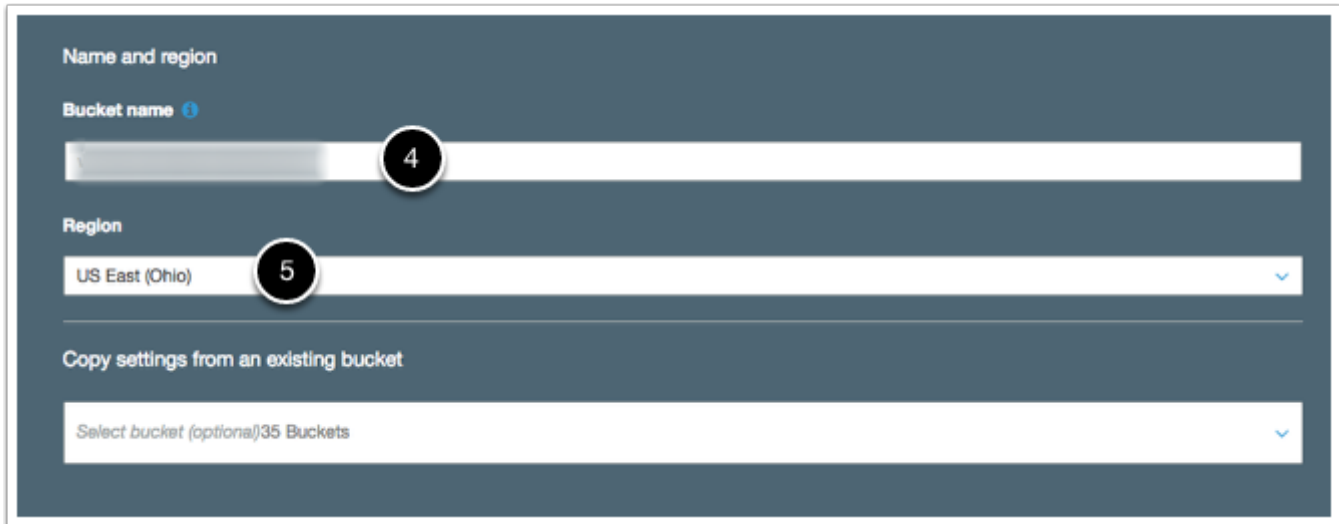


3. Click **Create bucket**.



4. Enter a name for your bucket.

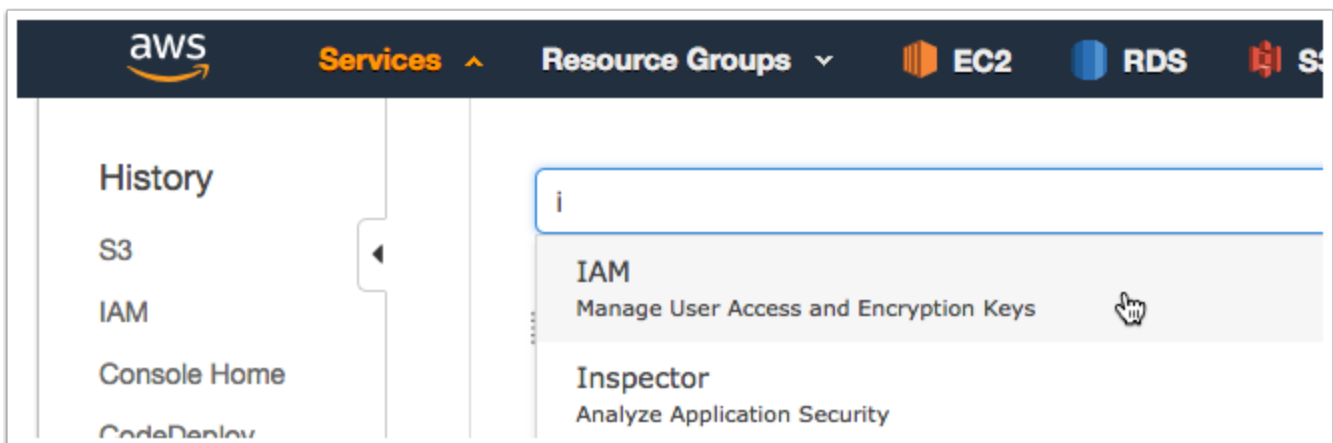
5. Choose your desired region.



The screenshot shows the 'Create bucket' page in the AWS Management Console. The 'Name and region' section is visible. The 'Bucket name' field is highlighted with a circled '4'. The 'Region' dropdown menu is highlighted with a circled '5' and shows 'US East (Ohio)' selected. Below this, there is a section for 'Copy settings from an existing bucket' with a dropdown menu showing 'Select bucket (optional) 35 Buckets'.

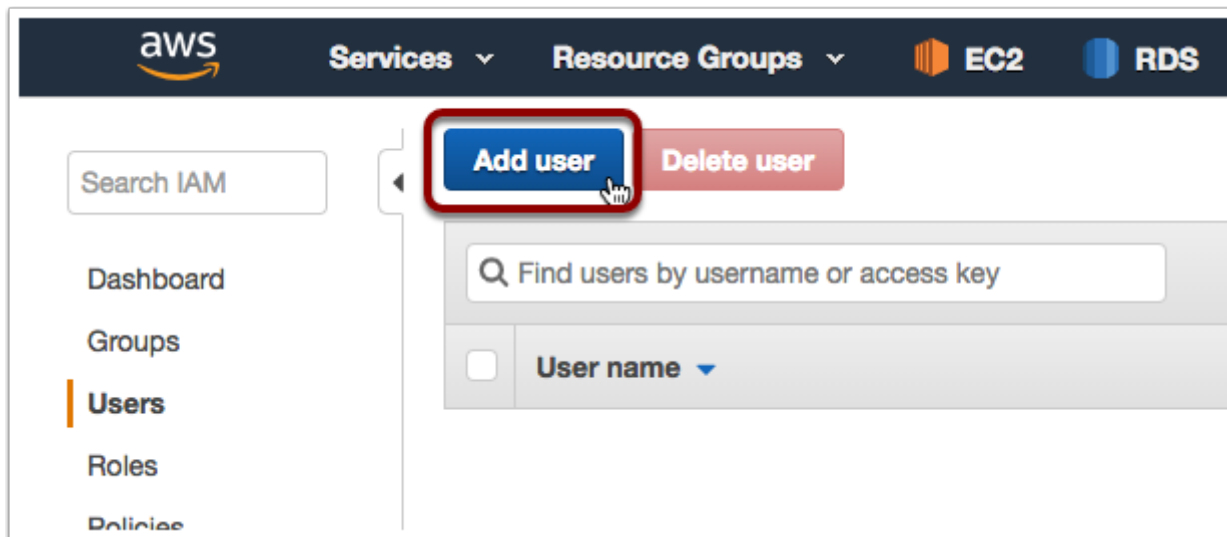
6. Configure the other bucket settings according to your needs. In most cases, for private buckets, you use the default settings.

7. Go to IAM.



8. Select **Users** in the left side menu.

9. Click **Add user**.



10. Enter a username.

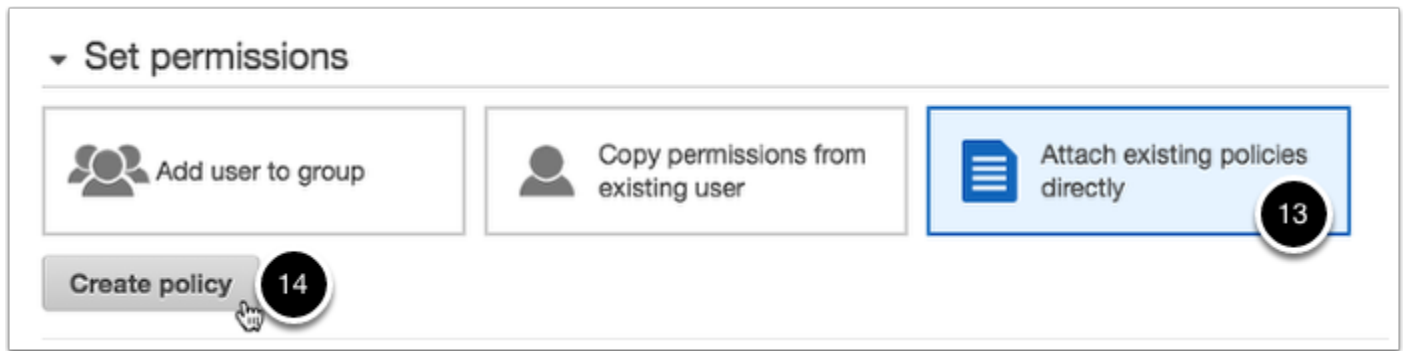
11. Check *Programmatic access* for **Access Type**.

12. Click **Next**.

 This screenshot shows the 'Add user' wizard in the AWS IAM console. The wizard has five steps: 1. Set user details, 2. Select AWS access type, 3. Attach existing policies directly, 4. Create policy, and 5. Review. Step 1 is currently active. It includes a 'User name*' field with a text input and a circular callout with the number 10. Below the field is a link '+ Add another user'. Step 2 is 'Select AWS access type', which includes a section 'Access type*' with two radio buttons: 'Programmatic access' (selected) and 'AWS Management Console access'. The 'Programmatic access' option has a circular callout with the number 11. Below the radio buttons are descriptions for each access type. At the bottom right, there is a 'Cancel' button and a 'Next: Permissions' button, which is highlighted with a red circle and the number 12. A legend at the bottom left indicates '* Required'.

13. Select **Attach existing policies directly**.

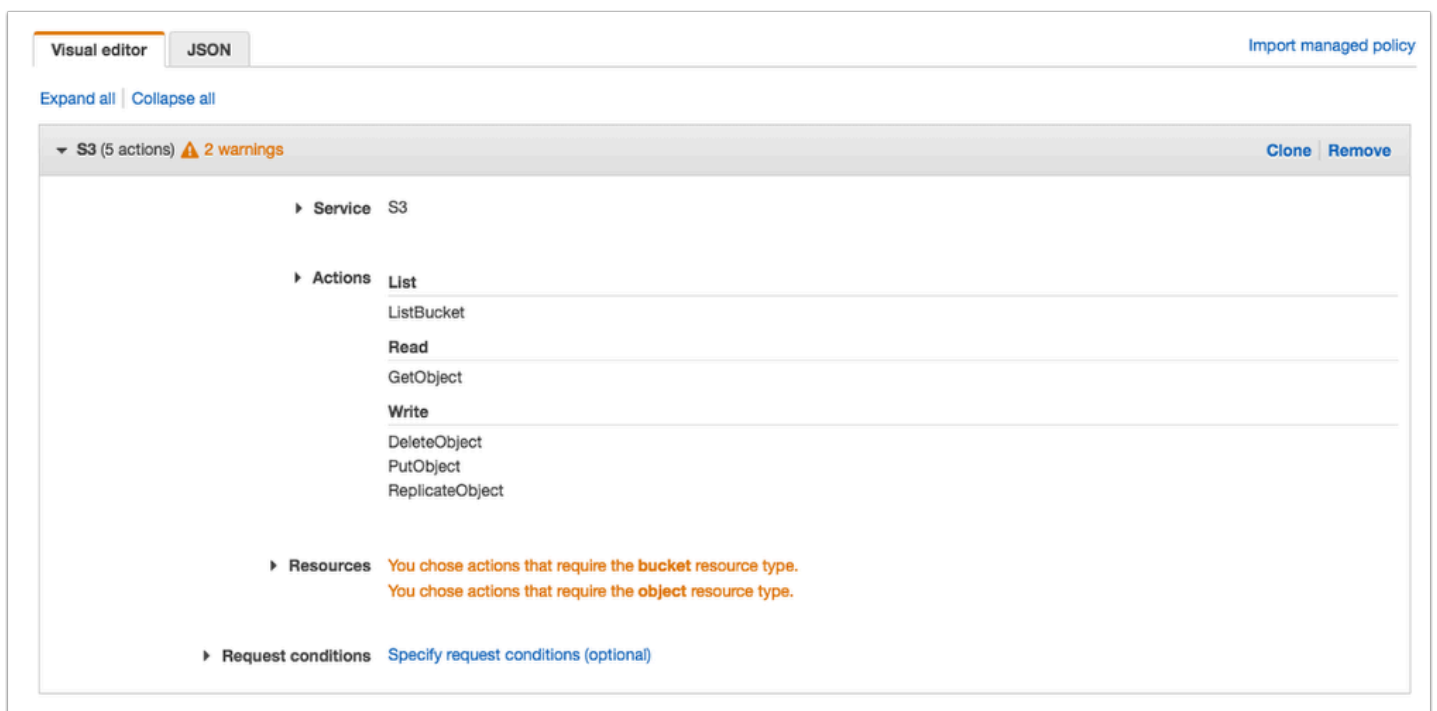
14. Click **Create policy**. The visual policy editor will load.



15. Select **S3** for **Service**.

16. Select all of the following S3-related permissions:

- *ListBucket*
- *GetObject*
- *PutObject*
- *ReplicateObject*
- *DeleteObject*



17. Under **Resources**, select *Specific*.

18. Click **Add ARN** under **bucket**.

▼ **Resources** [close](#) ☒ Specific **17** ☐ All resources

bucket [?](#) **18** You chose actions that require the **bucket** resource type.
[Add ARN](#) to restrict access

object [?](#) You chose actions that require the **object** resource type.
[Add ARN](#) to restrict access

19. Enter the name of the bucket that you created earlier.

20. Click **Add**.

21. Click **Add ARN** under **object**.

▼ **Resources** ☒ Specific [close](#) ☐ All resources

bucket ?

[Add ARN](#) to restrict access

object ? You chose actions that require the **object** resource type.

[Add ARN](#) to restrict access

22. Enter the name of the bucket that you created earlier for **Bucket name**.

23. Check **Any**.

24. Click **Add**.

Add ARN(s) ×

Amazon Resource Names (ARNs) uniquely identify AWS resources. Resources are unique to each service. [Learn more](#)

Specify ARN for object [List ARNs manually](#)

Bucket name ☐ Any

Object name ☒ Any

[Cancel](#) [Add](#)

25. Click **Review Policy**.

Visual editor JSON [Import managed policy](#)

Expand all Collapse all

▼ S3 (5 actions) [Clone](#) [Remove](#)

► Service S3

► Actions

- List
- ListBucket
- Read
- GetObject
- Write
- DeleteObject
- PutObject
- ReplicateObject

► Resources ☒ Specific [close](#) ☐ All resources

bucket [?](#) [EDIT](#) [+](#) ☐ Any

[Add ARN to restrict access](#)

object [?](#) [EDIT](#) [+](#) ☐ Any

[Add ARN to restrict access](#)

► Request conditions [Specify request conditions \(optional\)](#)

[Add additional permissions](#)

[Cancel](#) [Review policy](#)

26. Enter a name for the new policy and, optionally, a description to help you identify it later.

27. Click **Create Policy**.

Name*

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

Description

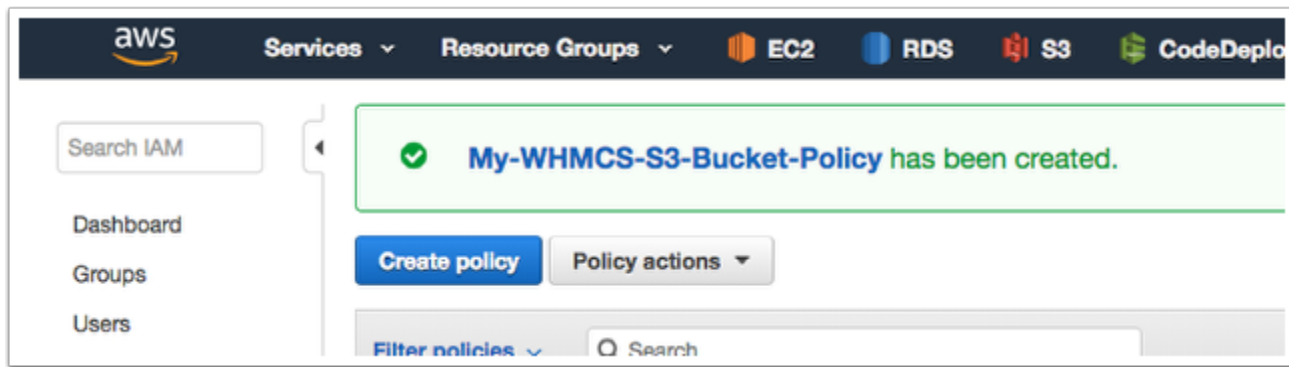
Maximum 1000 characters. Use alphanumeric and '+=, @ _' characters.

Summary

Service ▼	Access level	Resource	Request condition
Allow (1 of 167 services) Show remaining 166			
S3	Limited: List, Read, Write	Multiple	None

[Cancel](#) [Previous](#) [27 Create policy](#)

A success message will appear:

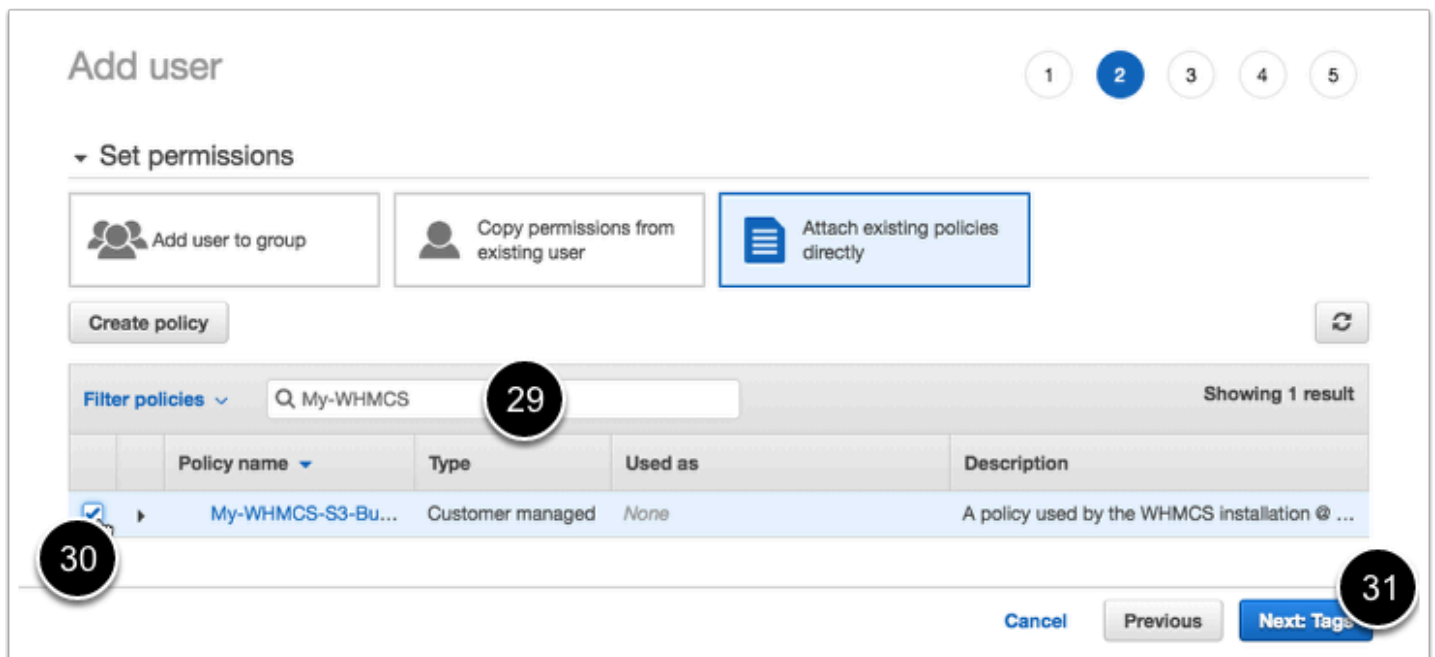


28. Return to the previous tab and refresh the list of policies.

29. Search for the name of the policy that you created.

30. Select the policy in the search results.

31. Click **Next: Tags**.



32. Optionally, assign tags to the policy.

33. Click **Next: Review** and review the details.

34. Click **Create user**. A programmatic access key ID and secret will display.

35. Copy and store the displayed ID and secret. You will need them in order to configure the bucket in WHMCS.

Add user

1 2 3 4 5



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://yourcompanyname.signin.aws.amazon.com/console>

Download .csv

	User	Access key ID	Secret access key
▶	✓ whmcs-s3-demo	AKIAJW2Y76GBLOLCT3A	***** Show

Close