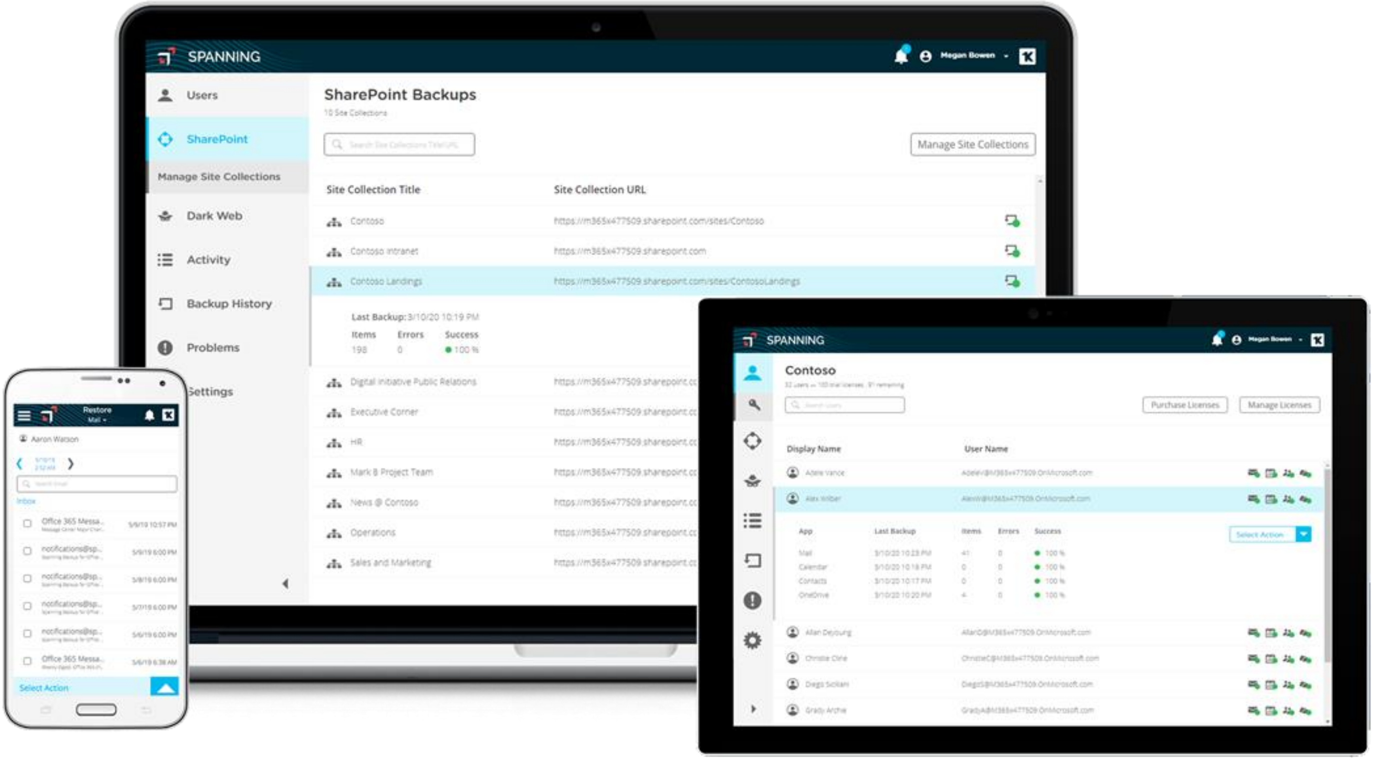
SPANNING
A Kaseya COMPANY

SPANNING BACKUP

Customer Managed Encryption Keys



SharePoint Backups
10 Site Collections

Site Collection Title	Site Collection URL
Contoso	https://m365x477509.sharepoint.com/sites/Contoso
Contoso Intranet	https://m365x477509.sharepoint.com
Contoso Landings	https://m365x477509.sharepoint.com/sites/ContosoLandings
Digital Initiative Public Relations	https://m365x477509.sharepoint.cc
Executive Corner	https://m365x477509.sharepoint.cc
HR	https://m365x477509.sharepoint.cc
Mark 8 Project Team	https://m365x477509.sharepoint.cc
News @ Contoso	https://m365x477509.sharepoint.cc
Operations	https://m365x477509.sharepoint.cc
Sales and Marketing	https://m365x477509.sharepoint.cc

Last Backup: 3/10/20 10:19 PM

Items	Errors	Success
198	0	● 100 %

Contoso

Display Name	User Name
Adele Vance	AdeleV@M365x477509.OnMicrosoft.com
Alex Wilber	AlexW@M365x477509.OnMicrosoft.com
Allan Deyoung	AllanD@M365x477509.OnMicrosoft.com
Christie Cline	ChristieC@M365x477509.OnMicrosoft.com
Diego Siciliani	DiegoS@M365x477509.OnMicrosoft.com
Grady Archie	GradyA@M365x477509.OnMicrosoft.com

App	Last Backup	Items	Errors	Success
Mail	3/10/20 10:23 PM	41	0	● 100 %
Calendar	3/10/20 10:18 PM	0	0	● 100 %
Contacts	3/10/20 10:17 PM	0	0	● 100 %
OneDrive	3/10/20 10:20 PM	4	0	● 100 %

Aaron Watson

Office 365 Messa...	5/9/19 10:57 PM
notifications@sp...	5/9/19 6:00 PM
notifications@sp...	5/8/19 6:00 PM
notifications@sp...	5/7/19 6:00 PM
notifications@sp...	5/6/19 6:00 PM
Office 365 Messa...	5/6/19 6:38 AM

Table of Contents

Welcome

Thanks for selecting Spanning Backup! Our mission is to ensure your organization's data is well protected and always available for rapid restore, keeping your business operational and your employees productive. We empower end users to correct their own mistakes, and give application administrators, IT leadership and audit teams the confidence and proof that your data is appropriately backed up, safe and ready for recovery.

Spanning strives to build real relationships with our customers and deliver exceptional service. If you ever have a question or need additional assistance please contact us at support@spanning.com or search our Knowledge Base at http://support.spanning.com/.

Why should you self-manage your Encryption Keys?

Based on recommendations by the CSA (Cloud Security Alliance) and the requirements of CJIS (Criminal Justice Information Services) Security Policy, it is a best practice for enterprise organizations to use SaaS data protection solutions that support the self-management of encryption keys.

Some of the organizational use cases for Spanning Backup Customer Managed Encryption Keys include:

- **Increased control over corporate data.** Security teams want to be able to understand and control cloud providers' level of access to their data, and they want the ability to suspend or shut off access at any time, thereby mitigating some risk related to data security. With Spanning Backup new encryption key self-management feature, organizations can revoke the encryption keys used for their data stored in Spanning, giving them the control.
- **Compliance and regulatory controls.** Many organizations must meet client contractual compliance and regulatory requirements which include encryption key self-management. This is especially true for legal, financial, and consulting firms who are required to maintain full control over client data at all times.
- **Internal policies and contracted policies.** If an organization has corporate or legal policies directing the control of access to cloud and SaaS data, or if contracted partners or customers have these policies, Spanning Backup can now support those directives.
- **Control and transparency regarding access to encrypted data.** Encryption key self-management provides data access transparency into how keys are used, as well as greater control via best practices in limiting key access.

The CSA recently wrote, "It is highly recommended that organizations maintain their own keys or use a trusted cryptographic service from a source that currently maintains such as service." In addition, CJIS (Criminal Justice Information Services) Security Policy compliance requires organizations to manage their own encryption keys when any CJI data is stored outside of an on-premises data center. In support of these recommendations, Spanning Backup will now allow organizations to manage their own encryption keys using the Amazon Key Management System (KMS).

With Spanning Backup Encryption Key Self-Management, customers can get full control over Spanning backup data. Customers can manage their own encryption keys using Amazon Web Services (AWS) Key Management Service and revoke access to their data whenever needed. And with this new feature, Spanning solidifies its leadership position as the enterprise-class backup and restore solution.

How do Customer Managed Encryption Keys work?

Spanning Backupoffers encryption key management using Amazon Web Services - Key Management Service (KMS). Once you configure AWS KMS by following the steps listed below, Spanning will use your encryption keys at the time of backup for all data stored in Amazon S3. Customers have the ability to revoke key access at any time using AWS KMS, rendering all encrypted data unreadable. Please note that if you choose to revoke access by disabling the key or deleting the key, it will severely impact or completely prevent recovery of your data.

AWS KMS also offers you the ability to rotate encryption keys and view API logs using CloudTrail. You can enable these services directly from within your AWS account. Note: your organization will be responsible for managing the AWS account and all costs associated with the services utilized on AWS.

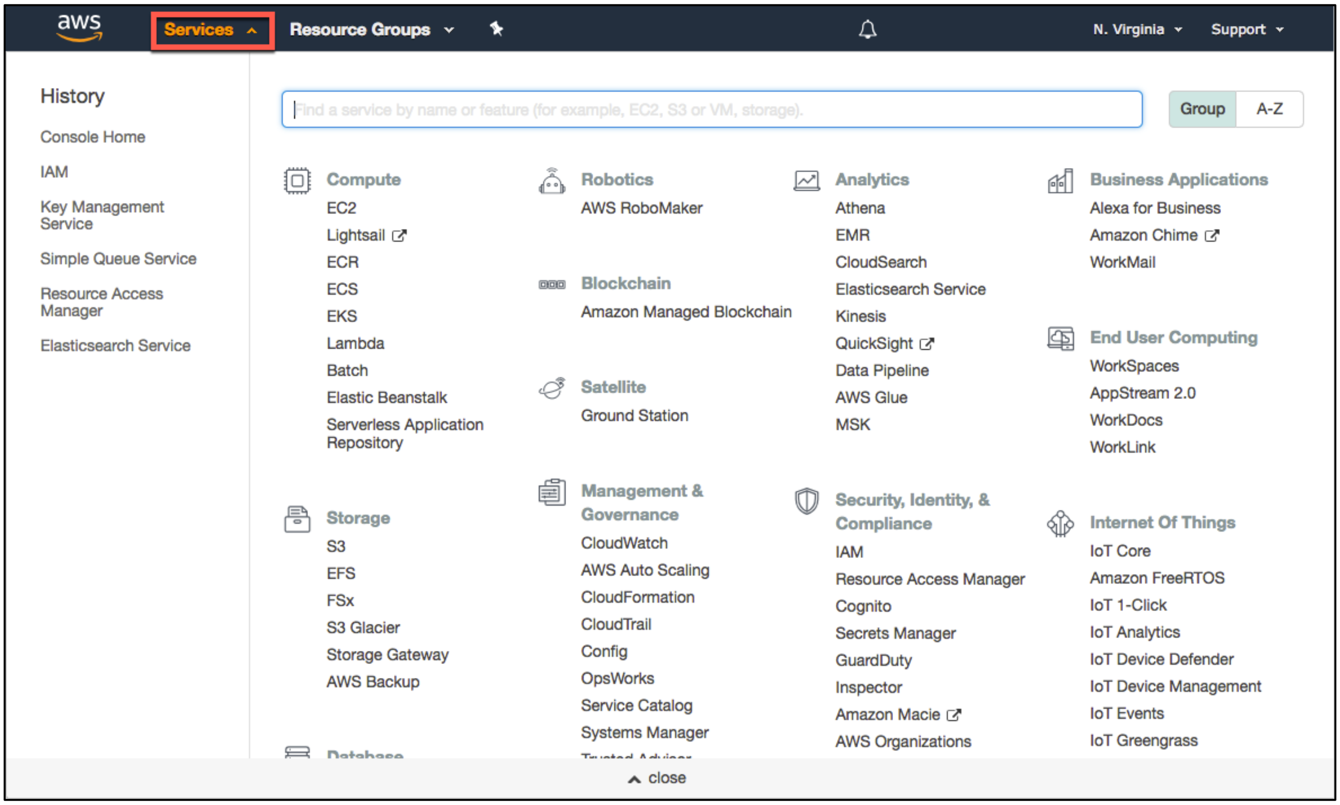
Configuring AWS Key Management Service

Please follow the steps below to configure Amazon Web Services Key Management Service to manage your encryption keys for data backed up by Spanning Backup.

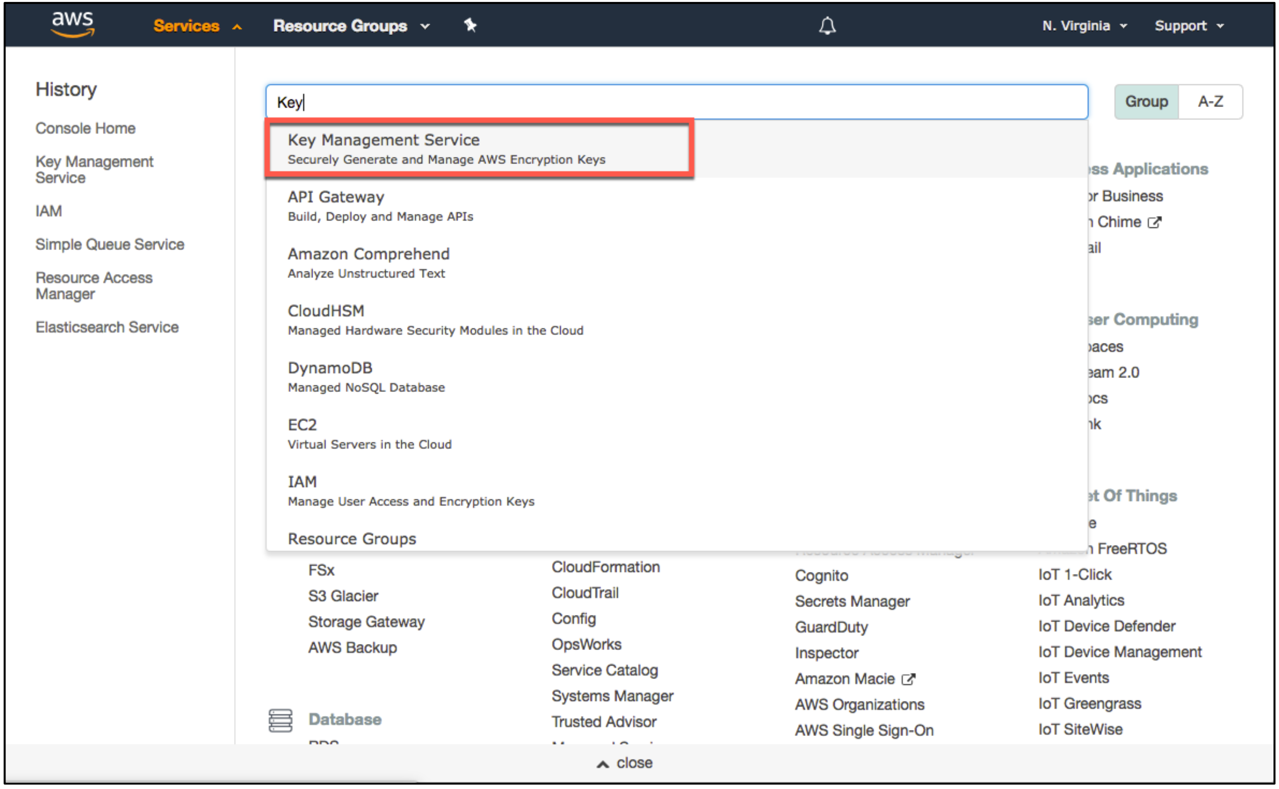
1. Login to your Amazon Web Services (AWS) account. The URL is specific to your account and should look like this: https://yourcompany.signin.aws.amazon.com/console

If you do not have an Amazon Web Services (AWS) account, create one by signing up at https://aws.amazon.com/account/

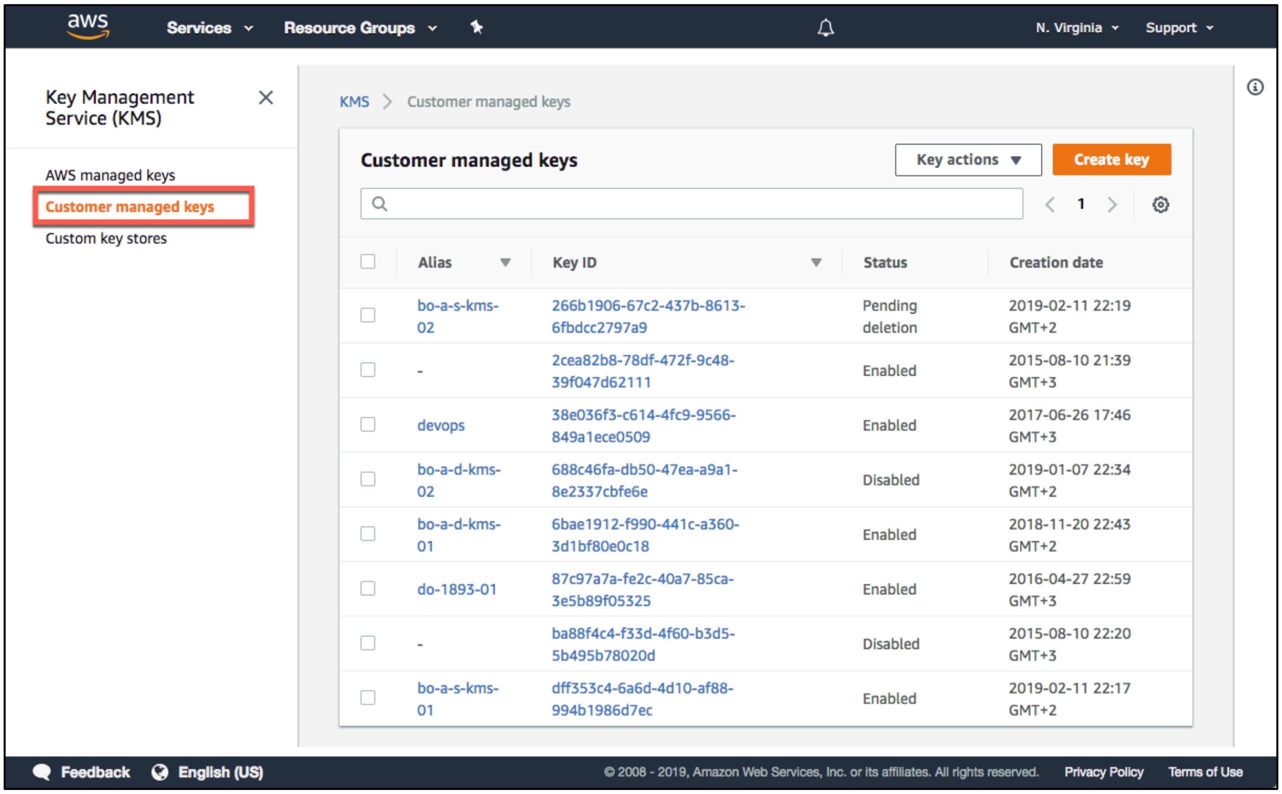
2. Select “Services” from the header after logging into to your AWS account



3. Choose “Security, Identity, & Compliance > Key Management Service”



4. Select “Customer managed keys” from the left navigation.



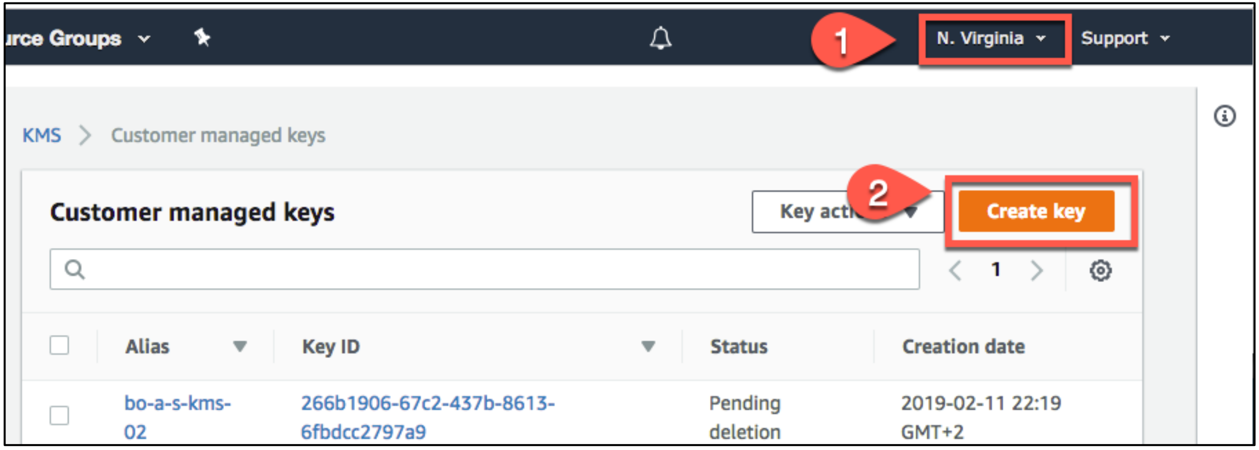
Alias	Key ID	Status	Creation date
bo-a-s-kms-02	266b1906-67c2-437b-8613-6fbdcc2797a9	Pending deletion	2019-02-11 22:19 GMT+2
-	2cea82b8-78df-472f-9c48-39f047d62111	Enabled	2015-08-10 21:39 GMT+3
devops	38e036f3-c614-4fc9-9566-849a1ece0509	Enabled	2017-06-26 17:46 GMT+3
bo-a-d-kms-02	688c46fa-db50-47ea-a9a1-8e2337cbfe6e	Disabled	2019-01-07 22:34 GMT+2
bo-a-d-kms-01	6bae1912-f990-441c-a360-3d1bf80e0c18	Enabled	2018-11-20 22:43 GMT+2
do-1893-01	87c97a7a-fe2c-40a7-85ca-3e5b89f05325	Enabled	2016-04-27 22:59 GMT+3
-	ba88f4c4-f33d-4f60-b3d5-5b495b78020d	Disabled	2015-08-10 22:20 GMT+3
bo-a-s-kms-01	dff353c4-6a6d-4d10-af88-994b1986d7ec	Enabled	2019-02-11 22:17 GMT+2

5. Ensure that you are creating the key in the same region where you plan to install Spanning Backup. Choose your region based on your Spanning data center choice:

Spanning Data Center	Data Center Name	Data Center Code
United States	US East (N. Virginia)	us-east-1
Europe	Europe (Ireland)	eu-west-1
Australia	Asia Pacific (Sydney)	ap-southeast-2
Canada	Canada (Central)	ca-central-1
United Kingdom	Europe (London)	eu-west-2

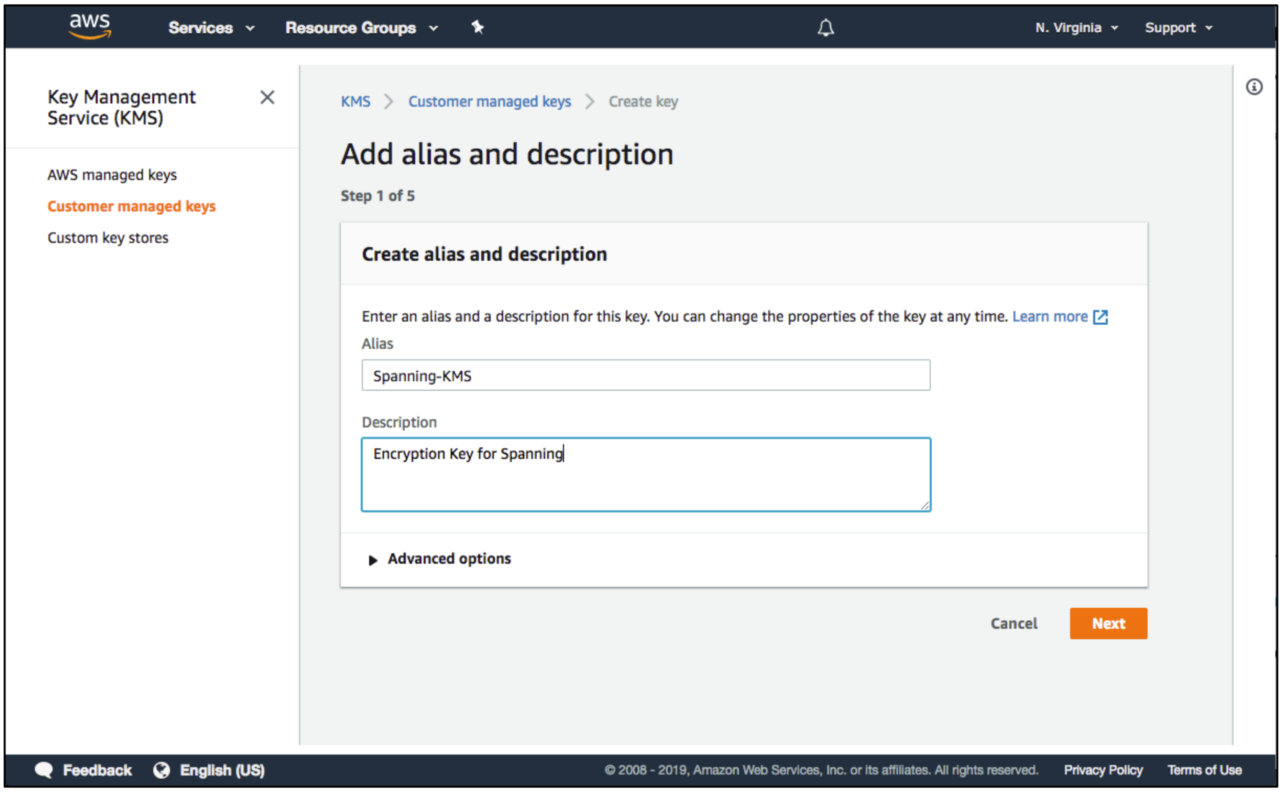
*https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html

Click "Create Key".



Alias	Key ID	Status	Creation date
bo-a-s-kms-02	266b1906-67c2-437b-8613-6fbdcc2797a9	Pending deletion	2019-02-11 22:19 GMT+2

6. Choose **Symmetric** for **Key type**. Choose “Next”.
7. Give the key the alias “Spanning-KMS” and a description of “Encryption Key for Spanning Backup”. Then click “Next”.



Add alias and description

Step 1 of 5

Create alias and description

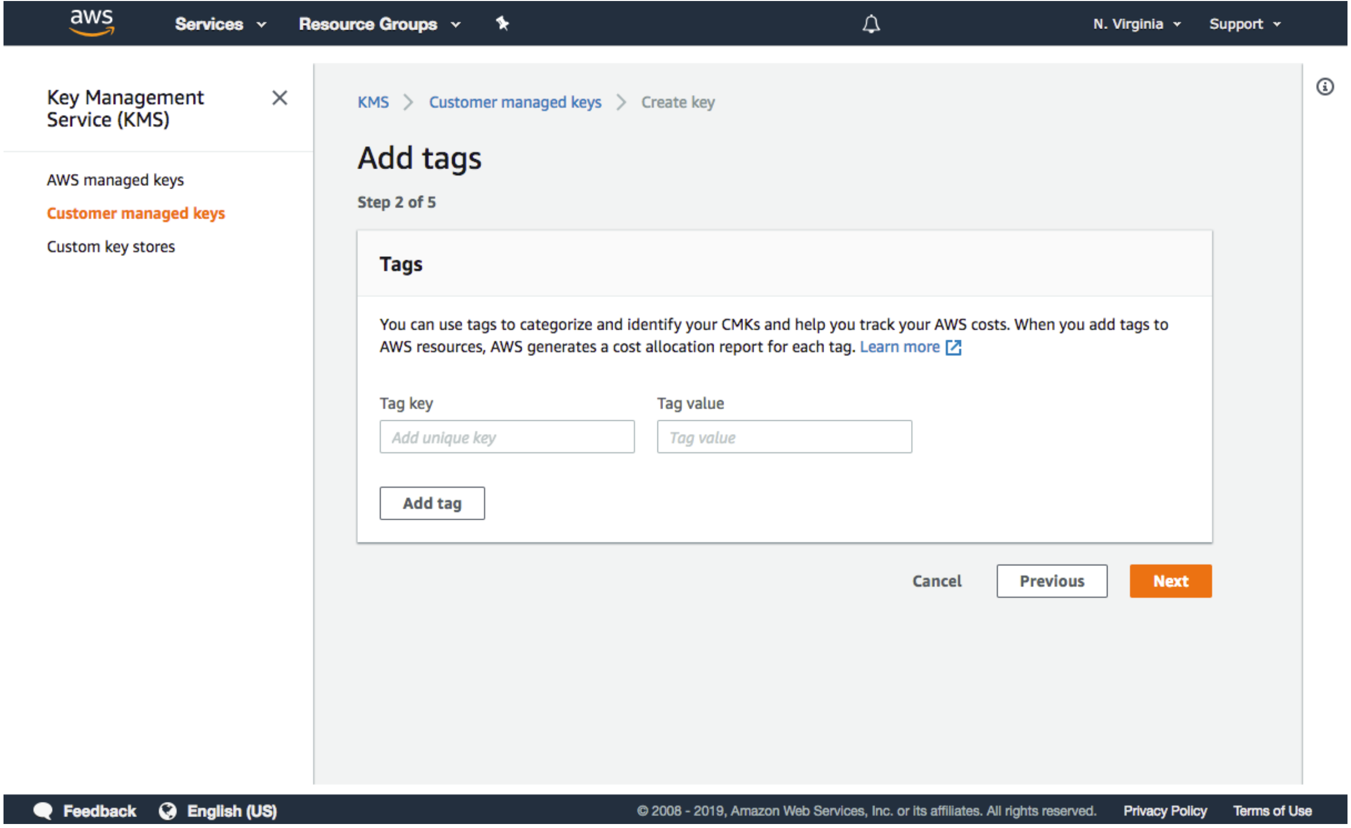
Enter an alias and a description for this key. You can change the properties of the key at any time. Learn more

Alias: Spanning-KMS

Description: Encryption Key for Spanning

Advanced options

8. Add any tags that you want to describe this key. Click “Next”.



Add tags

Step 2 of 5

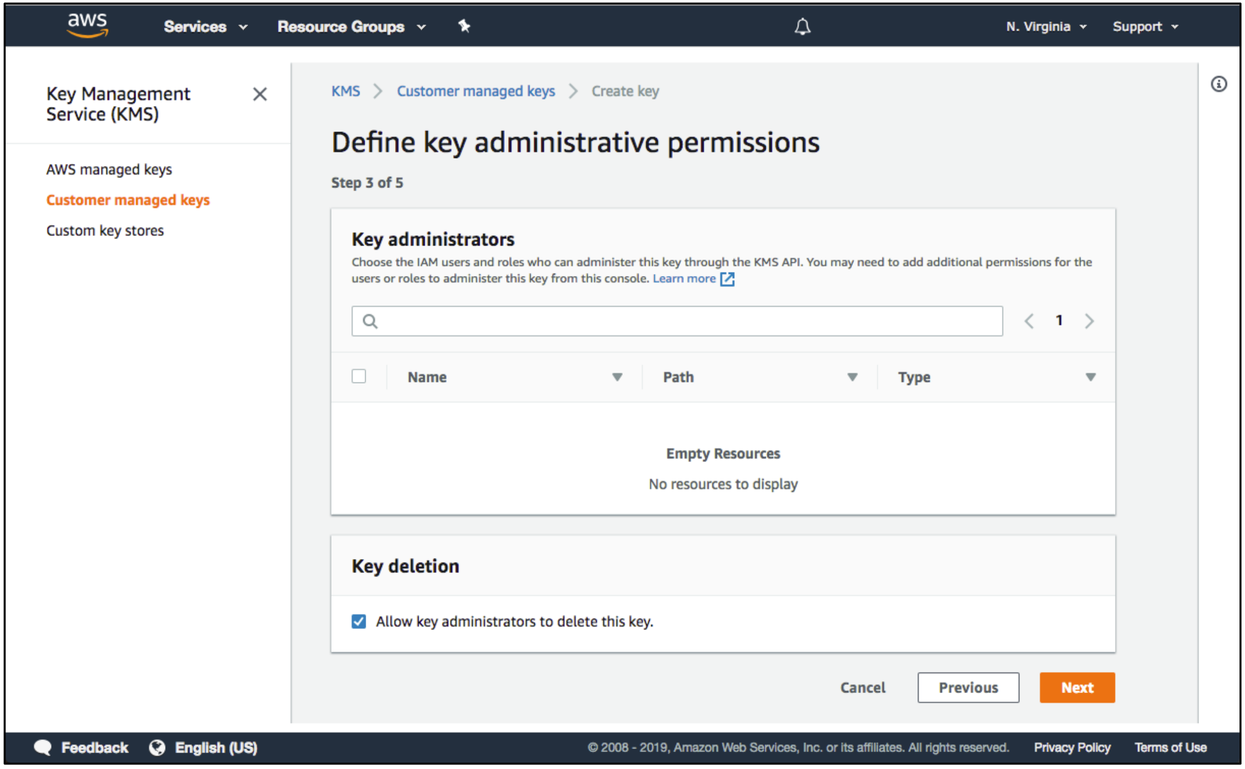
Tags

You can use tags to categorize and identify your CMKs and help you track your AWS costs. When you add tags to AWS resources, AWS generates a cost allocation report for each tag. Learn more

Tag key: Add unique key

Tag value: Tag value

9. Define any desired key administrators, and whether or not they should be allowed to delete this key. If you have not configured any users/roles, or do not know what to put here, simply leave it blank. The values can always be modified later, after key creation. Click “Next” to continue.



Define key administrative permissions

Step 3 of 5

Key administrators

Choose the IAM users and roles who can administer this key through the KMS API. You may need to add additional permissions for the users or roles to administer this key from this console. Learn more

□	Name	Path	Type

Empty Resources

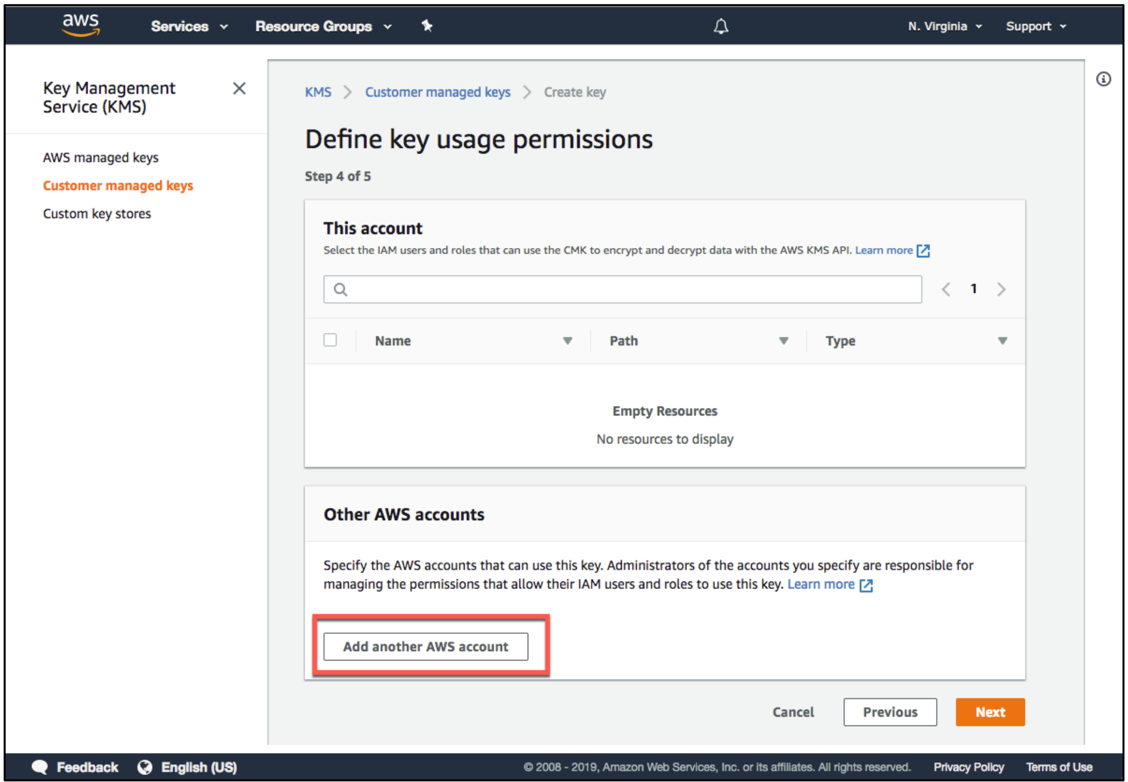
No resources to display

Key deletion

☑ Allow key administrators to delete this key.

© 2008 - 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

10. Click “Add an External Account” and enter the value 877583873091 which is Spanning’s Amazon account. Then click “Next Step.”



Define key usage permissions

Step 4 of 5

This account

Select the IAM users and roles that can use the CMK to encrypt and decrypt data with the AWS KMS API. Learn more

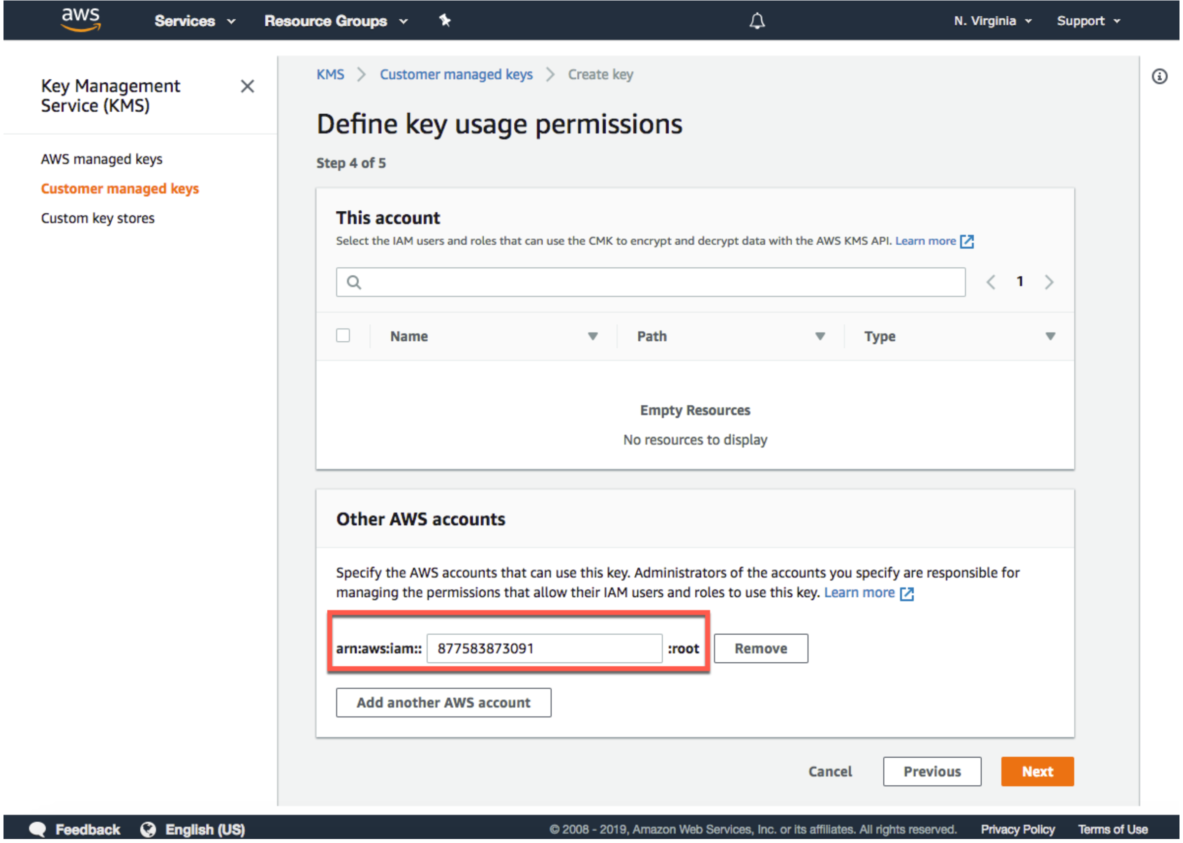
□	Name	Path	Type

Empty Resources

No resources to display

Other AWS accounts

Specify the AWS accounts that can use this key. Administrators of the accounts you specify are responsible for managing the permissions that allow their IAM users and roles to use this key. Learn more



Define key usage permissions

Step 4 of 5

This account

Select the IAM users and roles that can use the CMK to encrypt and decrypt data with the AWS KMS API. Learn more

□	Name	Path	Type

Empty Resources

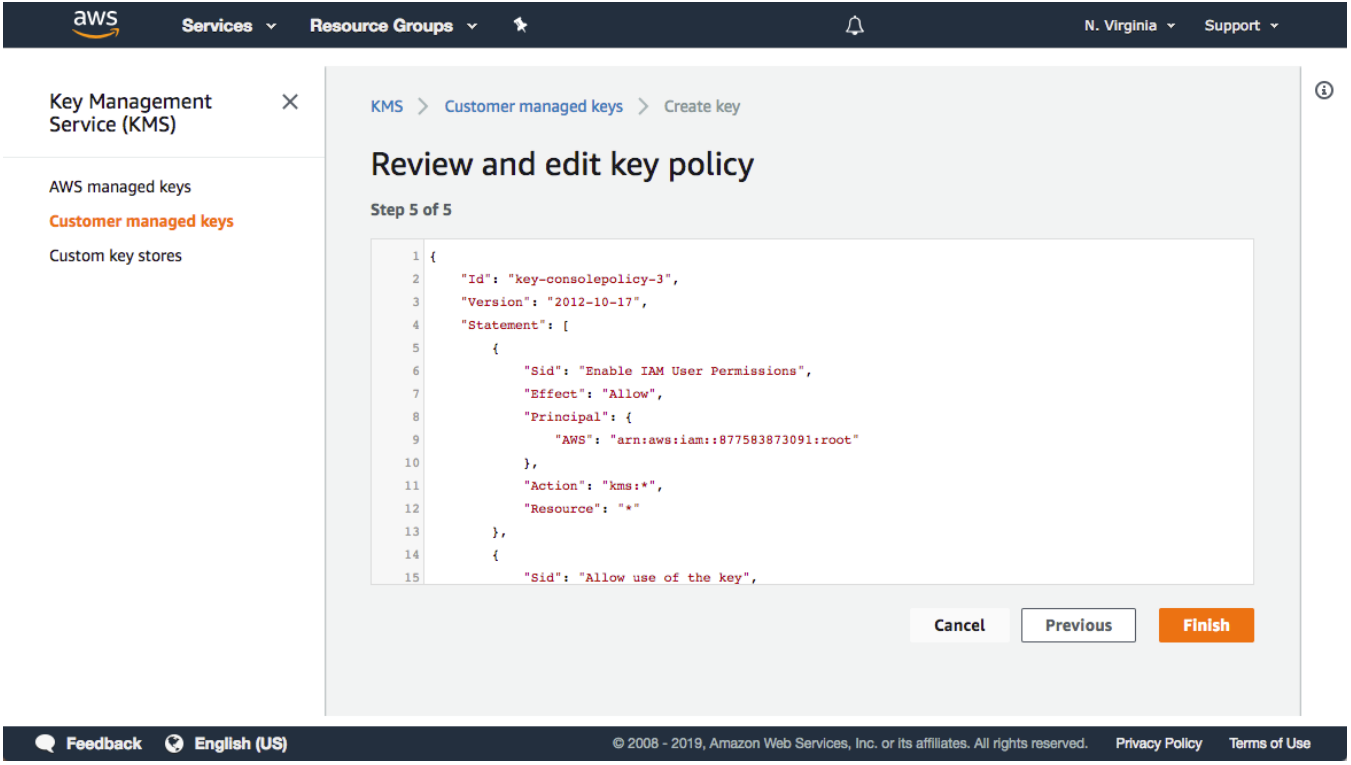
No resources to display

Other AWS accounts

Specify the AWS accounts that can use this key. Administrators of the accounts you specify are responsible for managing the permissions that allow their IAM users and roles to use this key. Learn more

arn:aws:iam:: 877583873091 :root

11. Review the key policy, then click “Finish.”

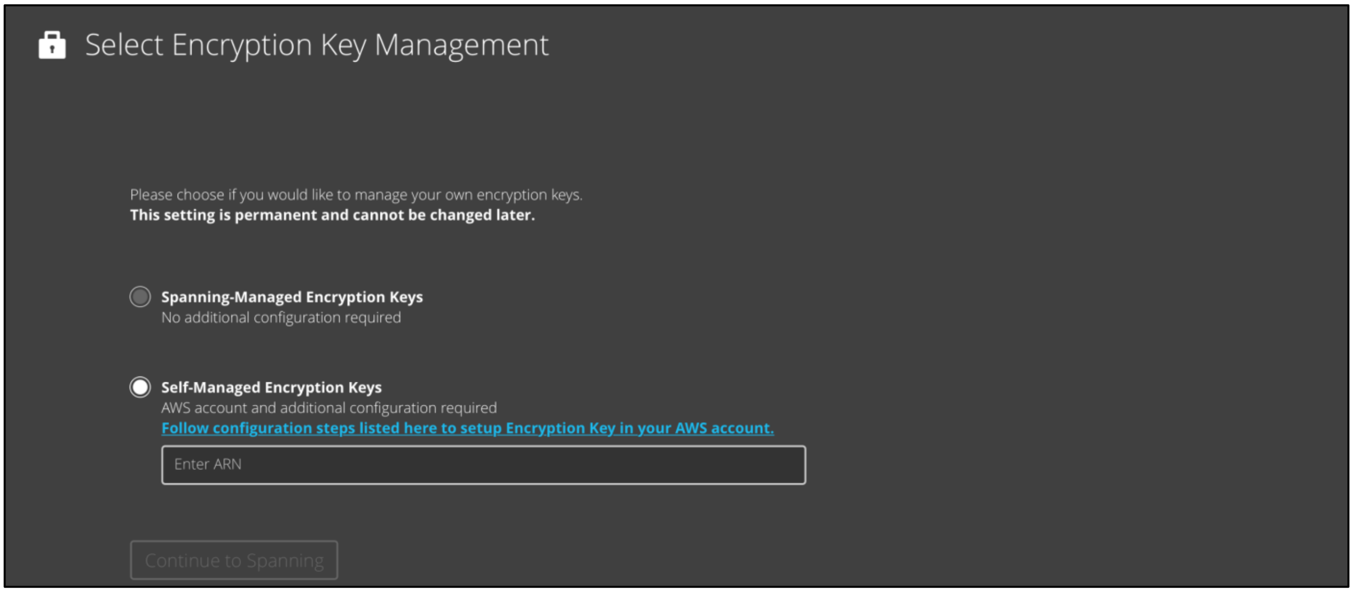


Review and edit key policy

Step 5 of 5

```
{
    "Id": "key-consolepolicy-3",
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Enable IAM User Permissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::877583873091:root"
            },
            "Action": "kms:*",
            "Resource": "*"
        },
        {
            "Sid": "Allow use of the key",
```

12. Select your newly created key from the list shown, then copy the full ARN value and paste it in the Spanning app during the installation & configuration process. The value should look something like “arn:aws:kms:us-east-1:123456789012:key/f64e93e4-3b1c-12fe-80c0-b3717fe9879c”.



Select Encryption Key Management

Please choose if you would like to manage your own encryption keys.
This setting is permanent and cannot be changed later.

○ **Spanning-Managed Encryption Keys**
No additional configuration required

○ **Self-Managed Encryption Keys**
AWS account and additional configuration required
Follow configuration steps listed here to setup Encryption Key in your AWS account.

Click “Continue to Spanning” and then click OK on the confirmation prompt.

Revoking Access

You can revoke Spanning's access to the backed up data whenever needed using AWS KMS. You can choose to disable access temporarily or permanently.

Disabling a Key

If you would like to temporarily disable access to your data, you can disable a key by logging into your AWS account and navigating to Encryption Keys as mentioned in steps 1-4 above. **Once you disable a key, backups, exports and restore operations will fail. You can enable the key to resume backups, exports and restores.**

Please note: you will not lose your backed up data if you disable the key.

Deleting a Key

If you want to permanently disable access to your data, you can delete the key by logging into your AWS account and navigating to Encryption Keys as mentioned in steps 1-4 above.

Once you delete a key, the data will become inaccessible and you will NOT be able to recover that data. We highly recommend that you use this option with caution as there will be no way to get the data back after you delete the key. Spanning will not be able to back up any data once the key is deleted.

Please note: you will lose all your backed up data if you delete the key.

Helpful Resources

Knowledge Base

Easily search through a number of articles in our Knowledge Base to find information on the most common user questions.

Email Support

If you can't find the answer to your question or need further assistance, please don't hesitate to contact us via email at support@spanning.com.

Privacy

Spanning takes privacy seriously. Read our Privacy Policy.

Security

Spanning Backup employs multiple layers of operation and physical security to ensure the integrity and safety of your data. Read how we protect your data.

About Spanning

Spanning Cloud Apps, a Kaseya company, is the leading provider of backup and recovery for SaaS applications, helping organizations around the globe protect their information in the cloud. The company provides powerful, enterprise-class data protection for Microsoft Office 365, G Suite, and Salesforce. With data centers located in North America, the EU, and Australia, Spanning Backup is the most trusted cloud-to-cloud backup solution for thousands of companies and millions of users around the world. Learn more at www.spanning.com. Follow Spanning on Twitter @spanningbackup.