

SPANNING BACKUP for Salesforce



Customer Managed Encryption Keys

SPANNING

DASHBOARD ACTIVITY HISTORY RESTORE COMPARE METADATA SETTINGS SUPPORT

100% Complete
Tue, Feb 6, 2018 1:00 AM
The latest backup was successful.
There were **0 errors** and **0 warnings**. [Backup Details >](#)
Your next automated backup is scheduled for 1:00 AM today.

Account Contact R.
0 Updated, 0 New
0 Deleted, 0 Undeleted

Contacts
0 Updated, 0 New
0 Deleted, 0 Undeleted

Leads
0 Updated, 0 New
0 Deleted, 0 Undeleted

Opportunities
0 Updated, 0 New
0 Deleted, 0 Undeleted

[Backup Now](#) [Restore](#)

BACKUP HISTORY

API Usage

Today History

Recent Activity

Date	Status	Activity	Duration
Tue, Feb 6, 2018 03:17 PM	✓	Metadata Compare	5 m
Tue, Feb 6, 2018 02:35 PM	✓	Object Restore	5 m
Tue, Feb 6, 2018 01:00 AM	✓	Scheduled Backup	9 m

RECENT ACTIVITY

Date	Status	Activity	Duration
Sat, Mar 25, 2017 at 3:13 AM	✓	Manual Backup completed	5 m
3/25	✓	Export completed	5 m
3/24	✓	Export completed	4 m
3/22	✓	Backup completed	9 m
3/21	✓	Backup completed	9 m

Table of Contents

Welcome	3
Why should you self-manage your Encryption Keys?	3
How do Customer Managed Encryption Keys work?	4
Configuring AWS - Key Management Service	4
Revoking Access	10
Disabling Key	10
Deleting Key	10
Helpful Resources	11
Knowledge Base	11
Email Support	11
Privacy	11
Security	11
About Spanning	11

Welcome

Thanks for selecting Spanning Backup for Salesforce! 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. Spanning Backup for Salesforce is the first and only AppExchange backup and restore app that supports Encryption Key Self-Management.

Some of the organizational use cases for Spanning Backup for Salesforce 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 for Salesforce's 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 for Salesforce 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 for Salesforce will now allow organizations to manage their own encryption keys using the Amazon Key Management System (KMS).

With Spanning Backup for Salesforce Encryption Key Self-Management, both new and current 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 Salesforce backup and restore solution.

How do Customer Managed Encryption Keys work?

Spanning Backup for Salesforce offers 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.

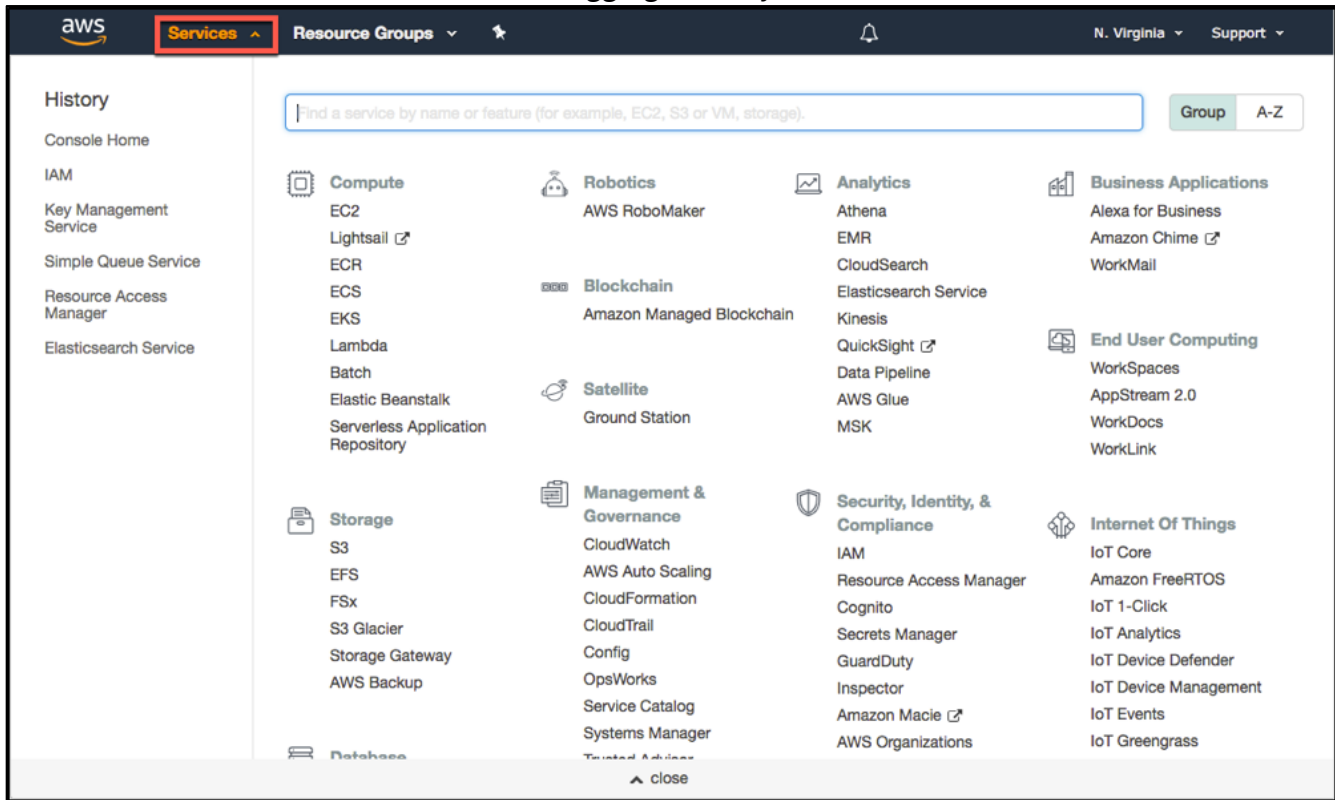
Configuring AWS Key Management Service

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 for Salesforce.

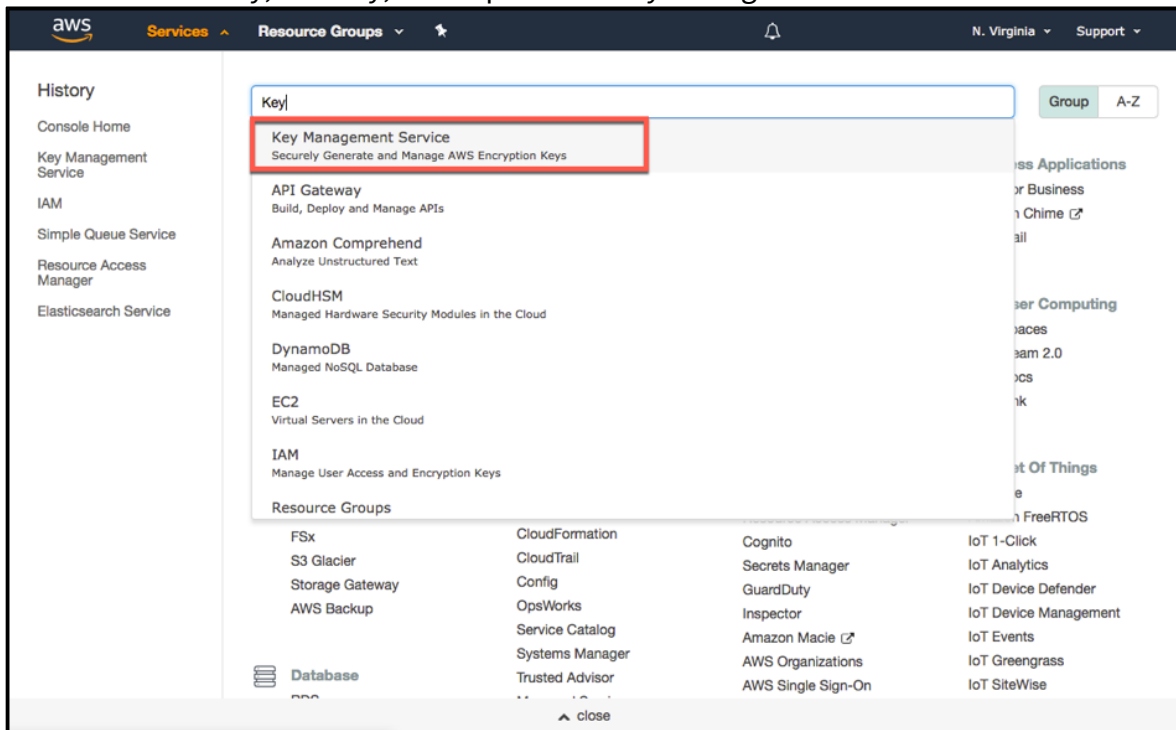
1. Login to your Amazon Web Services (AWS) account. The URL is specific to your account and should look like this: <https://yourcompany.signin.aws.amazon.com/console>

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

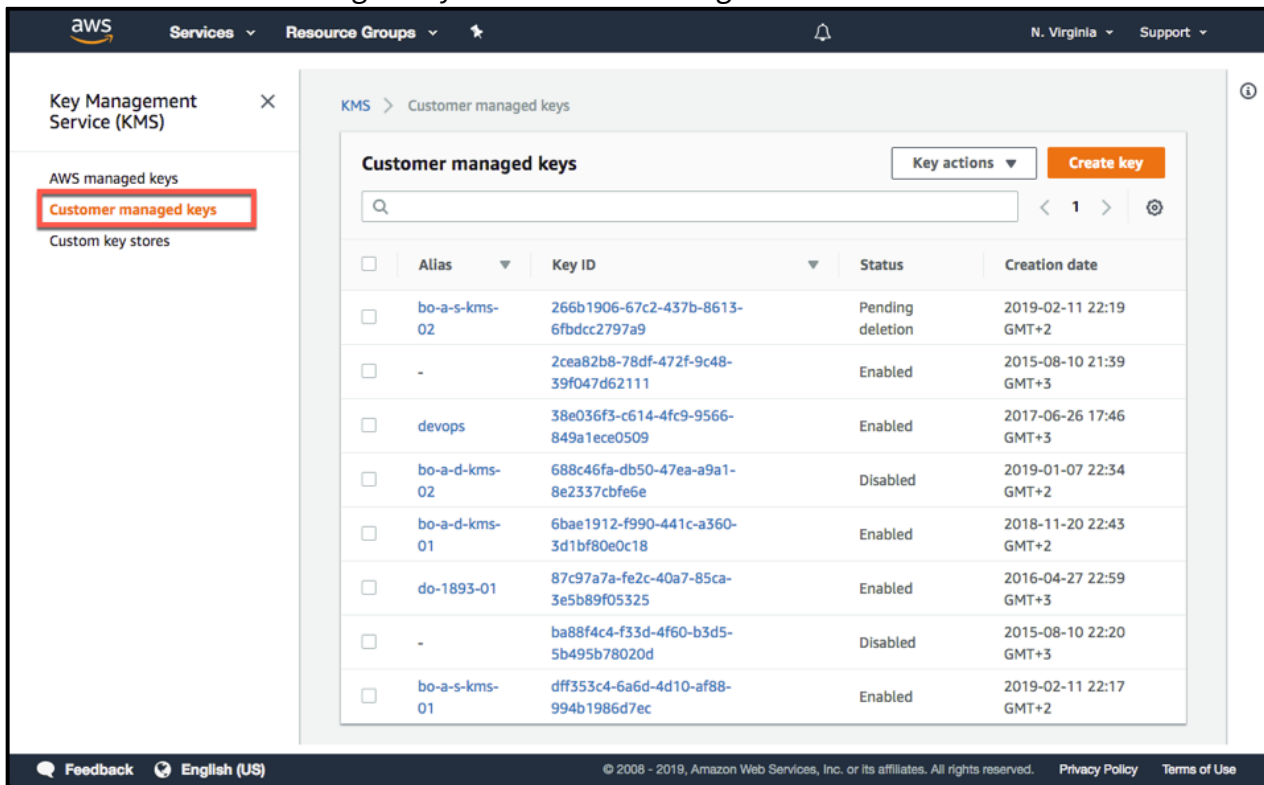
2. Select “Services” from the header after logging into to your AWS account



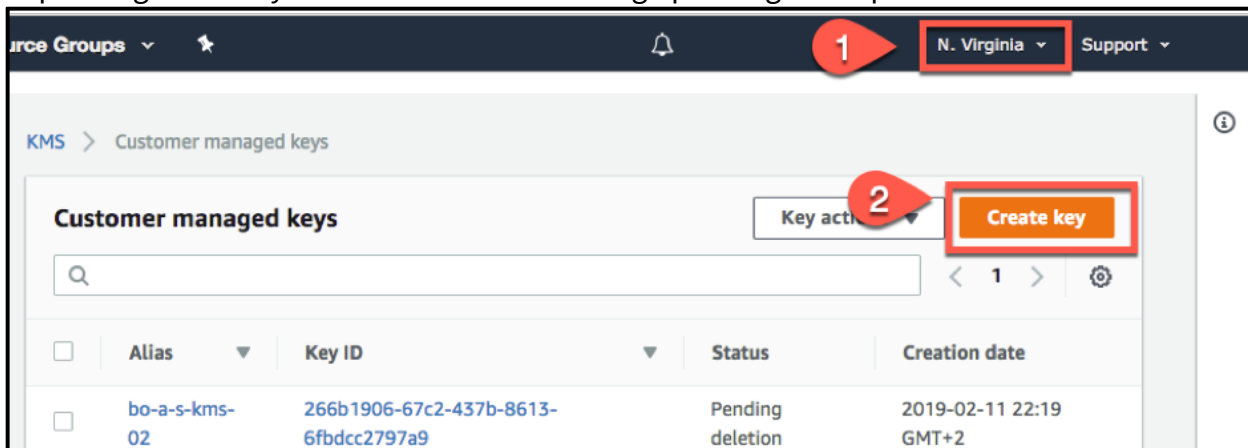
3. Choose “Security, Identity, & Compliance > Key Management Service”



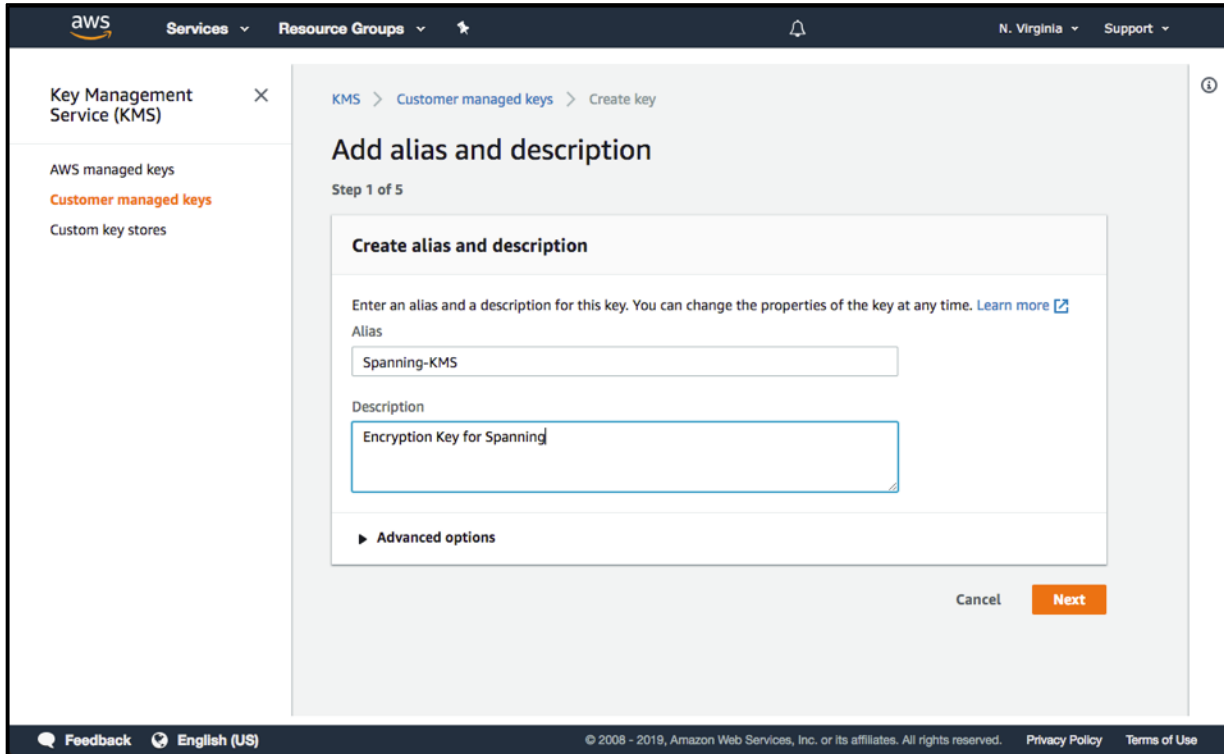
4. Select “Customer managed keys” from the left navigation



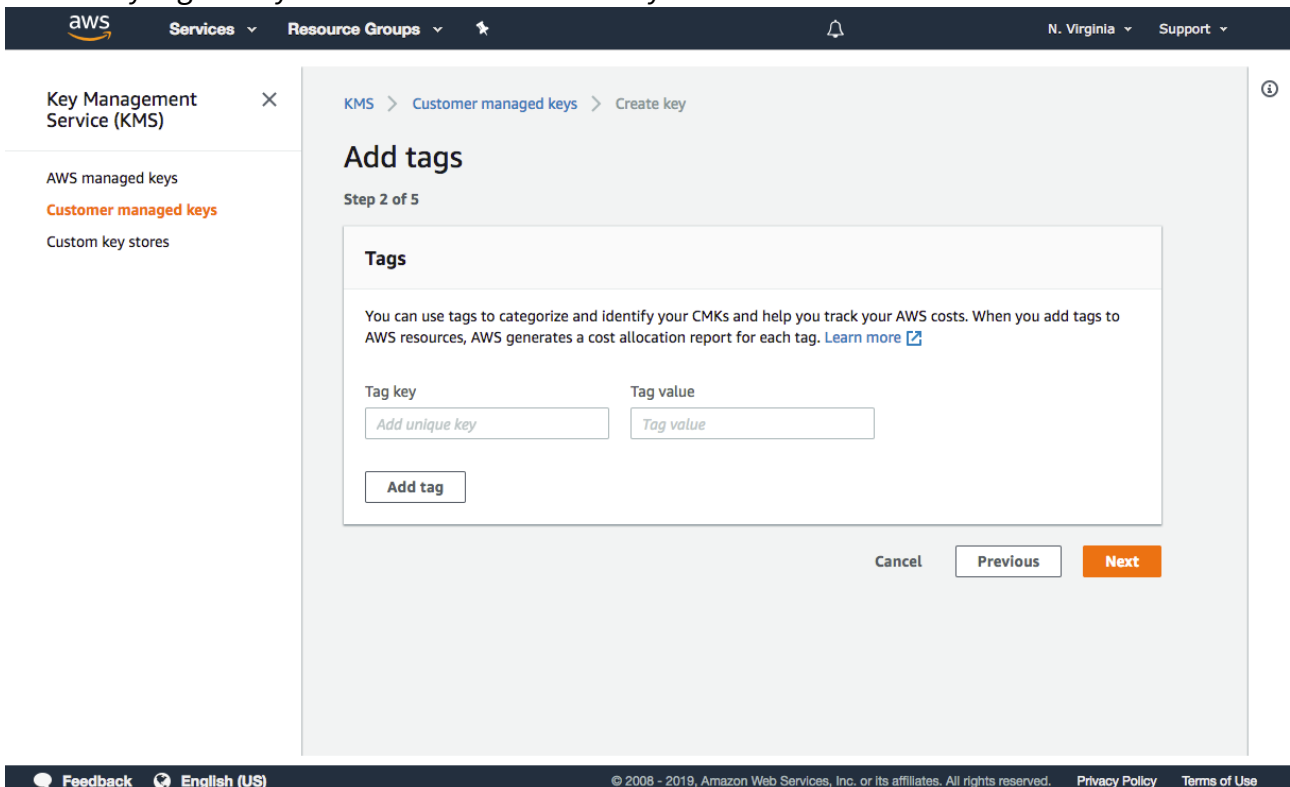
5. Ensure that you are creating the key in the same region where your Spanning Backup for Office 365 is configured. The correct option will either be US-East (N. Virginia), EU (Ireland) or ANZ (Sydney) depending on what you selected while installing Spanning Backup for Office 365. Click “Create Key”.



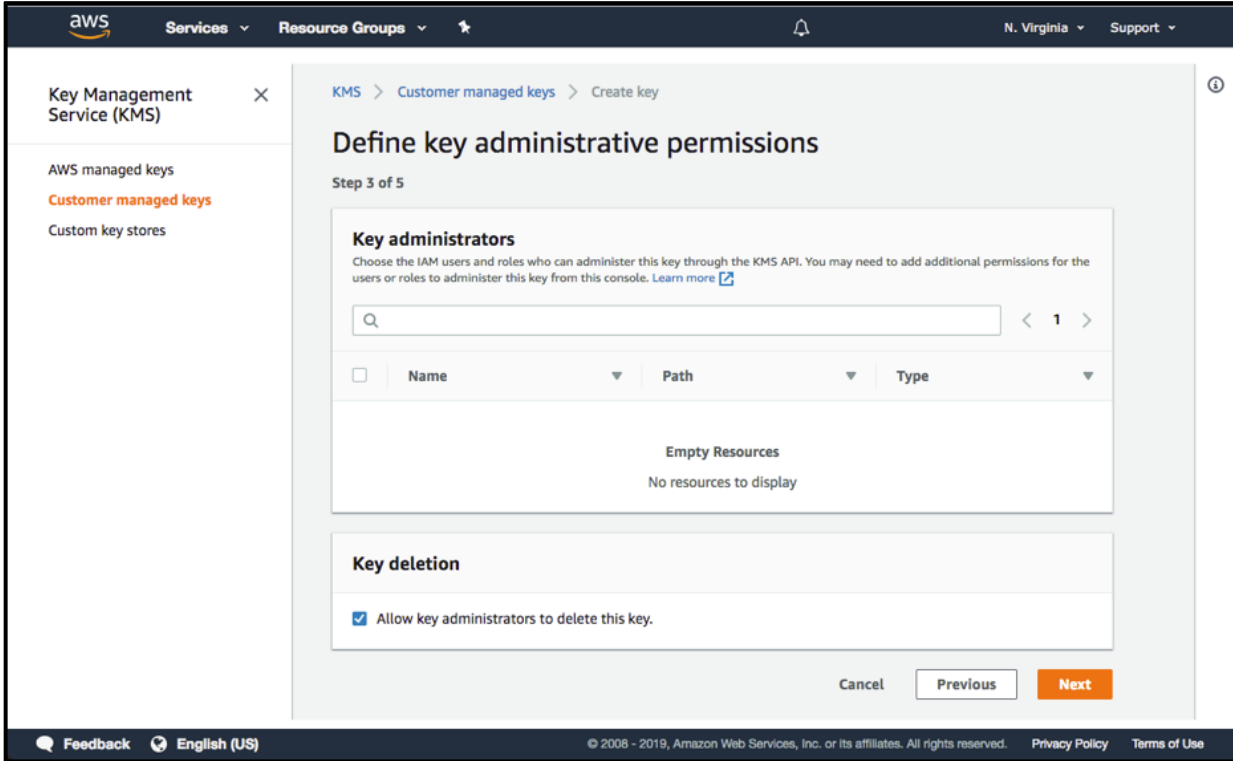
6. Give the key the alias “Spanning-KMS” and a description of “Encryption Key for Spanning Backup”. Then click “Next”.



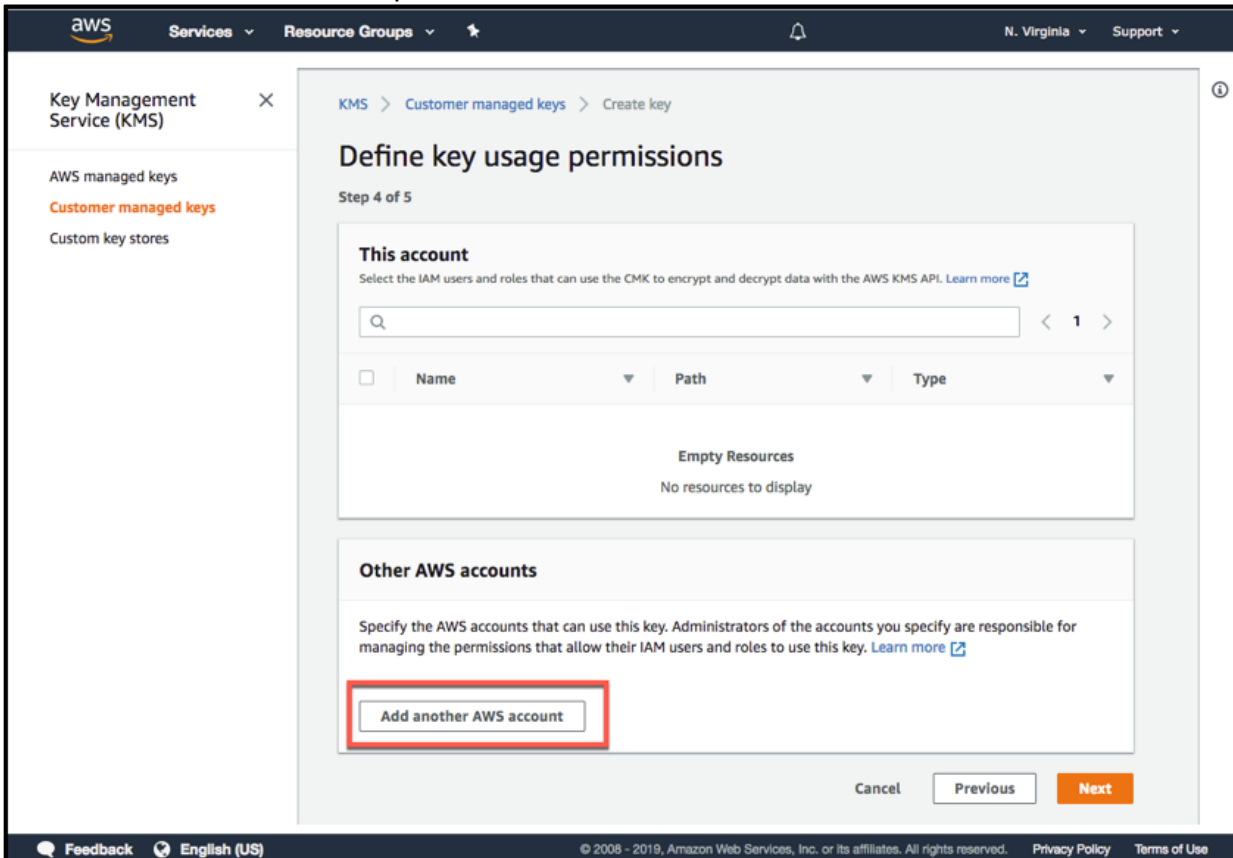
7. Add any tags that you want to describe this key. Click “Next”.

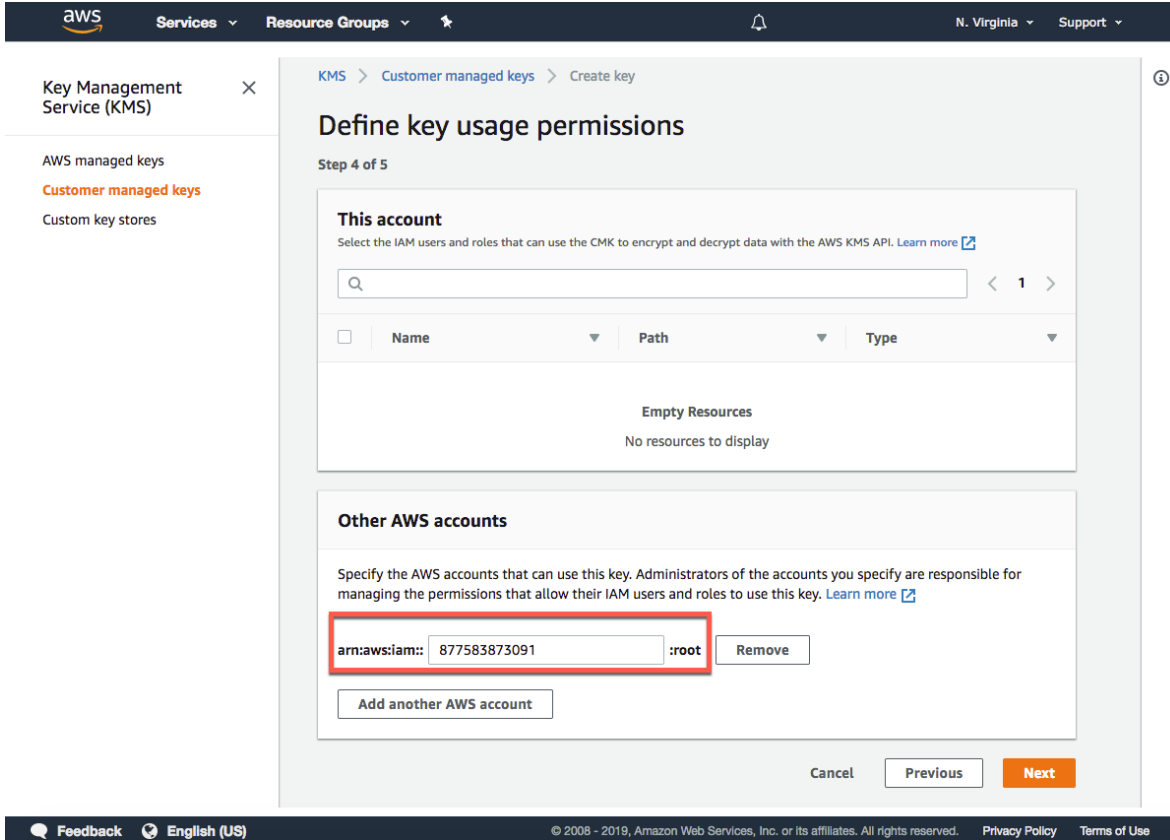


8. Define any desired key administrators, and whether or not they should be allowed to delete this key. If you have not configured any users/roles, or do not know what to put here, simply leave it blank. The values can always be modified later, after key creation. Click “Next” to continue.

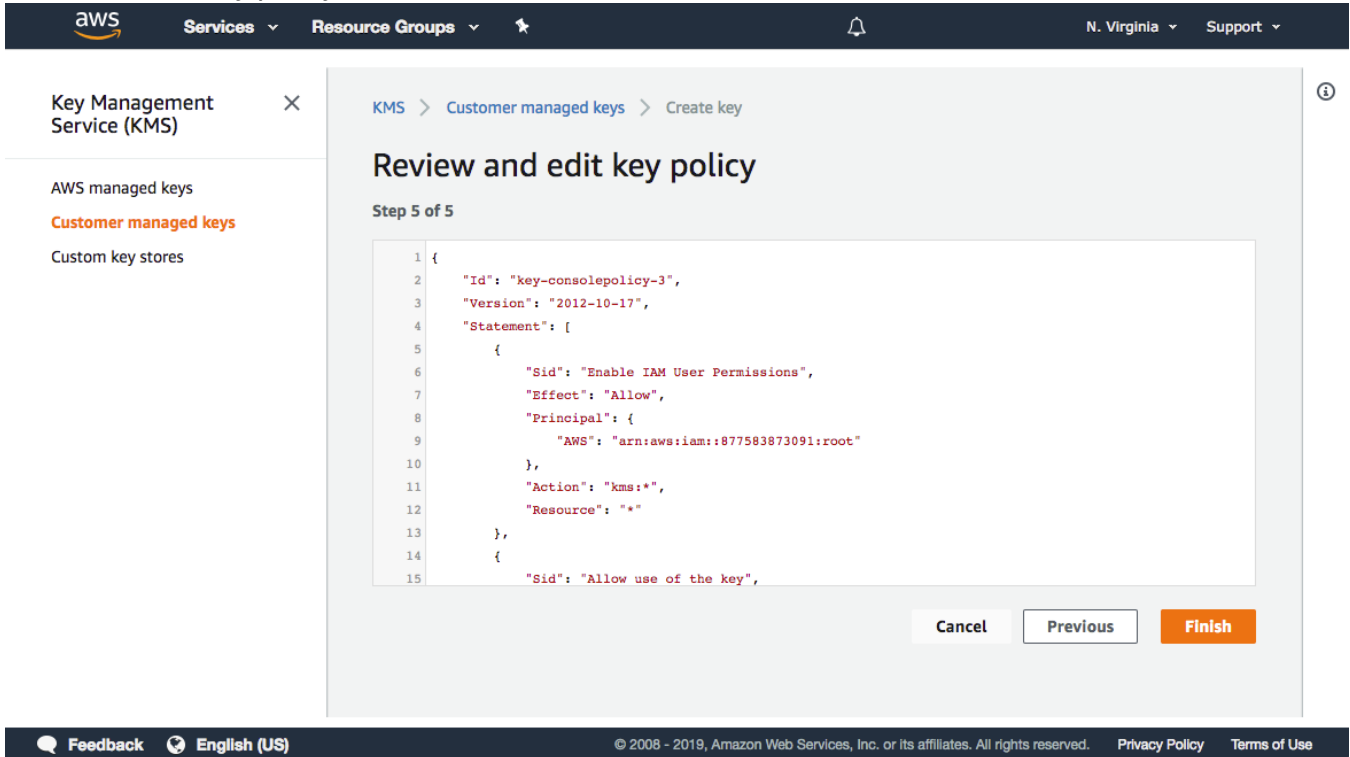


9. Click “Add an External Account” and enter the value 877583873091 which is Spanning’s Amazon account. Then click “Next Step.”





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



11. 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
CONTINUE TO SPANNING

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 the configuration steps listed [here](#) to set up an Encryption Key in your AWS account.

Enter ARN

Click “CONTINUE TO SPANNING” on the top right and then hit 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](mailto:support@spanning.com) 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](https://twitter.com/spanningbackup).