netwrix

## 2025

# Netwrix Privilege Secure for Access Management v4.2

6160 Warren Parkway, Suite 100, Frisco, TX 75034 | (949) 407-5125

## Legal Notice

The information in this publication is furnished for information use only, and does not constitute a commitment from Netwrix Corporation of any features or functions, as this publication may describe features or functionality not applicable to the product release or version you are using. Netwrix makes no representations or warranties about the Software beyond what is provided in the License Agreement. Netwrix Corporation assumes no responsibility or liability for the accuracy of the information presented, which is subject to change without notice. If you believe there is an error in this publication, please report it to us in writing.

Netwrix is a registered trademark of Netwrix Corporation. The Netwrix logo and all other Netwrix product or service names and slogans are registered trademarks or trademarks of Netwrix Corporation. Microsoft, Active Directory, Exchange, Exchange Online, Office 365, SharePoint, SQL Server, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

## Disclaimers

This document may contain information regarding the use and installation of non-Netwrix products. Please note that this information is provided as a courtesy to assist you. While Netwrix tries to ensure that this information accurately reflects the information provided by the supplier, please refer to the materials provided with any non-Netwrix product and contact the supplier for confirmation. Netwrix Corporation assumes no responsibility or liability for incorrect or incomplete information provided about non-Netwrix products.

# Table of contents

# Requirements

This document describes the recommended configuration of the servers needed to install this product in a production environment. Depending on the size of the organization, it is recommended to review your environment and requirements with a support engineer prior to deployment to ensure all exceptions are covered.

## Architecture Overview

The following servers are required for installation of the product:

- Netwrix Privilege Secure Application Server – This is where the Netwrix Privilege Secure (v4.2) application is installed.
- Netwrix Privilege Secure Client – Privilege Secure is a web service that can be accessed locally or remotely through a supported browser.
- Netwrix Privilege Secure Proxy Server – This is for the supported RDP / SSH Client.
- Target Environment – The target environment includes platforms with privileged access to be managed by the application.

See the following sections for additional information:

- Application Server
- Client
- Remote Service Node
- Target Environments

# Application Server

The requirements for the (Privilege Secure) application server are:

- Windows Server 2016 R2 through Windows Server 2022

  ***RECOMMENDED:*** Windows Server 2022, non-domain-joined for security

- US English language installation

- Hardened / dedicated to Netwrix Privilege Secure (recommended)
- Controlled administrative access (recommended)
- 2.0 GHz or faster dual core 64-bit (x64) processor
- .NET Framework 4.7.2 installed (required for Windows Server 2012 R2 and Windows Server 2016 only)
    - .NET Framework 4.7.2+ is included in the “Pre-Reqs” folder of the product zip file. Alternatively, download from the following link:

      https://dotnet.microsoft.com/download/thank-you/net472
- Windows Management Framework 5.1 installed (required for Window Server 2012 R2 only)
    - Windows Management Framework is included in the “Extras” folder of the product zip file. Alternatively, download from the following link:

      https://www.microsoft.com/en-us/download/details.aspx?id=54616
- Properly functional domain-integrated DNS with ability to resolve all managed components both forwards and backwards
- Multi-Factor Authentication (MFA) token (Authenticator, DUO, Symantec VIP, etc.)

### RAM, CPU and Disk Space

These are dependent upon the total number of administrators using Privilege Secure.

| Environment | Extra Large | Large | Medium | Small |
|---|---|---|---|---|
| **Number of Admins** | 500-1000 | 100-500 | 50-100 | 50 or less |
| **RAM** | 64 GB | 32 GB | 16 GB | 16 GB |
| **Cores** | 8-16 | 6-8 | 4-6 | 4 |

| Environment | Extra Large | Large | Medium | Small |
|---|---|---|---|---|
| **C: drive** | 80 GB | 80 GB | 80 GB | 80 GB |
| **Application drive** | 300 GB | 200 GB | 100 GB | 100 GB |
| **Recording drive** | 500 GB | 300 GB | 200 GB | 150 GB |

### Permissions

The following permission is required to install the application:

- Membership in the local Administrators group on the Privilege Secure server
- Active Directory Synchronization for Vault Connectors – The account used must have Domain Admin privileges

# Virtual Environment Recommendations

While physical machines are always preferred, we fully support the use of virtual machines. This section contains special considerations when leveraging virtualization.

- VMWare® ESX® – If using ESX, the following specifications are recommended:
  - ESX 4.0 / ESXi™ 4.1 or higher
  - Virtual Hardware 7 or higher
  - All Virtual Machines installed on the same datacenter / rack
- Virtual Storage Consideration
  - In the server requirements, when separate disks are required for the servers, that should translate to separate data stores on the VM host machine.

# Client

Privilege Secure is a web service which can be accessed locally or remotely if the server's firewall permits it. The supported browsers for Privilege Secure are:

- Microsoft® Edge® Chromium

- Google® Chrome® 54.0 or later (Recommended)

- Apple® Safari®
- Mozilla® Firefox®

**NOTE:** The browser compatibility mode must be turned off to access the Privilege Secure web service.

# Remote Service Node

Privilege Secure supports a variety of RDP/SSH clients, including:

- PuTTY
- MobaXterm
- MS Remote Desktop Connection Manager
- MS Terminal Services Client (Remote Desktop)

On all Privilege Secure servers, it is recommended to exclude the following directories from antivirus and endpoint protection software. Please note a drive letter is not specified in each path, as that can be customized during each Privilege Secure and service installation.

- \Program Files\Stealthbits\PAM\ActionService
- \Program Files\Stealthbits\PAM\ActionServiceWorker
- \Program Files\Stealthbits\PAM\DatabaseTools\Data
- \Program Files\Stealthbits\Postgres12\bin
- \ProgramData\Stealthbits\Postgres12

Exclusions for Remote Services:

- Action Service:
  - \Program Files\Stealthbits\PAM\ActionService
  - \Program Files\Stealthbits\PAM\ActionServiceWorker
  - \Stealthbits\PAM\ProxyService\
- Proxy Service:
  - \Stealthbits\PAM\ProxyService\
- Scheduler Service:

  - \Stealthbits\PAM\SbPAM.SchedulerService\
  - \Stealthbits\PAM\ProxyService\

See the following topics for specific installation instructions for remote services:

- Proxy Service Install
- Action Service Install
- Scheduler Service Install

# Target Environments

Netwrix Privilege Secure supports management of the following target environments:

- Microsoft® Active Directory®
- Window Server 2008 R2 or later – Requires PowerShell v5.1
- Windows Desktop – Requires the winrm service to be running
- Cisco IOS
- Websites
- Microsoft SQL Server databases
- Oracle databases (container instances)
- Microsoft Entra ID (formerly Azure AD)
- Linux distributions with SSHv2 or higher that are under LTS
  - Debian
  - CentOS
  - Red Hat Enterprise Linux (RHEL)
  - openSUSE

**Additional Supported Platforms (no local account management or pre-configured activity steps)**

- Any device that supports a SSH Connection

- Any device / platform / web site that is AD / Microsoft Entra ID Authenticated

# Permissions

The following permissions are required for the service accounts:

- For Active Directory and Windows member server/desktop management:
    - Membership in the Domain Administrators group in the target domain(s)
- For Linux server management:
    - Service account on each server to be managed or a central domain account in the case of AD-bridged hosts
    - Permissions may either be root or delegated via sudo or other commercial least privilege solutions
- For standalone Windows Servers/desktops:
    - Membership in the local Administrator group on each server/desktop to be managed
- For Cisco
    - Level 15 Privileged EXEC — Full access to the device for configuration and management
- For Microsoft Entra ID management:
    - Microsoft Graph API
        - Application Permissions:
            - Directory.ReadWrite.All
            - Group.ReadWrite.All
            - User.ReadWrite.All
            - RoleManagement.ReadWrite.Directory
        - Delegated Permissions:
            - User.Read
    - App Registration added to the User Administrators directory role

- For Oracle database management:
  - SYSDBA privileges
- For Microsoft SQL Server database management:
  - sysadmin privileges

# Ports

Configure appropriate firewall rules to allow these connections to Privilege Secure.

## Dynamic Port Range

In Windows Server 2008 and later versions, and in Windows Vista and later versions, the default dynamic port range changed to the following range:

- Start port: 49152
- End port: 65535

Windows 2000, Windows XP, and Windows Server 2003 use the following dynamic port range:

- Start port: 1025
- End port: 5000

See Microsoft's article Service overview and network port requirements for Windows for additional information.

## Application Server Firewall Rules

The requirements for the (Privilege Secure) application server are:

- Make sure that you have configured the Antivirus exclusions according to the following Netwrix knowledge base article: SbPAM: Exclusions for Antivirus (AV) & Endpoint Software
- The following ports must be open for communication between Privilege Secure and Active Directory domain controllers:

| Port | Protocol | Source | Direction | Target | Purpose |
|---|---|---|---|---|---|
| **135** | TCP | Privilege Secure server | ↔ | Domain Controller | MS-RPC |
| **389**<br>**636** | TCP<br>UDP | Privilege Secure server | ↔ | Domain Controller | LDAP/LDAPS |
| **53** | TCP<br>UDP | Privilege Secure server | ↔ | DNS Service | DNS |
| **137**<br>**138** | UDP | Privilege Secure server | ↔ | Domain Controller | Net BIOS related |
| **9389** | TCP | Privilege Secure server | → | Domain Controller | Active Directory Web Services<br>Make sure that you have configured the Antivirus exclusions according to the following Netwrix knowledge base article: SbPAM: Exclusions for Antivirus (AV) & Endpoint Software |
| **88** | UDP | Privilege Secure server | ↔ | Domain Controller | Kerberos |

**NOTE:** Privilege Secure must be able to reach the following URLs via HTTPS (port 443)

- https://login.microsoftonline.com
- https://graph.microsoft.com

# Proxy Firewall Rules

The following ports must be open for communication between the proxy and Privilege Secure.

**Proxy Server Sizing for Windows/Linux/Docker**

| Administrators | Concurrent Sessions | Memory | CPU Cores | Disk (max) |
|---|---|---|---|---|
| **450** | 150 | 16 GB | 4 cores | 21 GB per day |
| **900** | 300 | 32 GB | 8 cores | 42 GB per day |
| **1800** | 600 | 64 GB | 16 cores | 84 G per day |

**Additional Considerations for SSH and RDP Clients**

The following ports must be open for communication between the Client and Privilege Secure:

| Port | Protocol | Source | Direction | Target | Purpose |
|---|---|---|---|---|---|
| **4422** | TCP | SSH Client | ↔ | SbPAM server | SSH Proxy |

| Port | Protocol | Source | Direction | Target | Purpose |
|---|---|---|---|---|---|
| **4489** | TCP | RDP Client | ↔ | SbPAM server | RDP Proxy |

# Target Environment Firewall Rules

The following ports must be open for communication between Privilege Secure and the platform:

| Port | Protocol | Source | Direction | Target | Purpose |
|---|---|---|---|---|---|
| **3389** | TCP | Privilege Secure server | ↔ | Windows Hosts | RDP Proxy |
| **5985**<br>**5986** | TCP | Privilege Secure server | ↔ | Windows Hosts | PowerShell Remoting |
| **5985**<br>**5986** | TCP | Privilege Secure server | ↔ | Windows Hosts | Password Change via Powershell Remoting |
| **22** | TCP | Privilege Secure server | → | Linux Hosts | SSH Proxy / Password change |
| **6520** | TCP | Privilege Secure server | ↔ | Remote Proxy | Register Proxy Service |

| Port | Protocol | Source | Direction | Target | Purpose |
|---|---|---|---|---|---|
| **6500** | TCP | Privilege Secure server | ↔ | Remote Action Service | Register Action Service |
| **443** | HTTPS (TCP) | Privilege Secure Server | ↔ | Azure | Azure Graph API Access |
| **6523** | TCP | Privilege Secure Server | ↔ | Remote Proxy | Leaf Nodes |
| **6524** | TCP | Privilege Secure Server | ↔ | Remote Proxy | Cluster Nodes |

# AWS Key Management Service

AWS Key Management Service (AWS KMS) is a managed service that makes it easy for you to create and control the cryptographic keys that are used to protect your data. Organizations using AWS Key Management Service (AWS KMS) can configure Netwrix Privilege Secure to rotate security Keys. The KMS key is not used to encrypt the secret key, but will be used to encrypt the key that is used to encrypt the secret key.

See the AWS Key Management Service article for additional information.

When creating an AWS KMS protection key for Netwrix Privilege Secure, start by creating a policy in AWS. There will be multiple configuration steps needed within AWS.

- Create an AWS Policy
- Create a User
- Create a Managed Key
- Least Privilege Policy

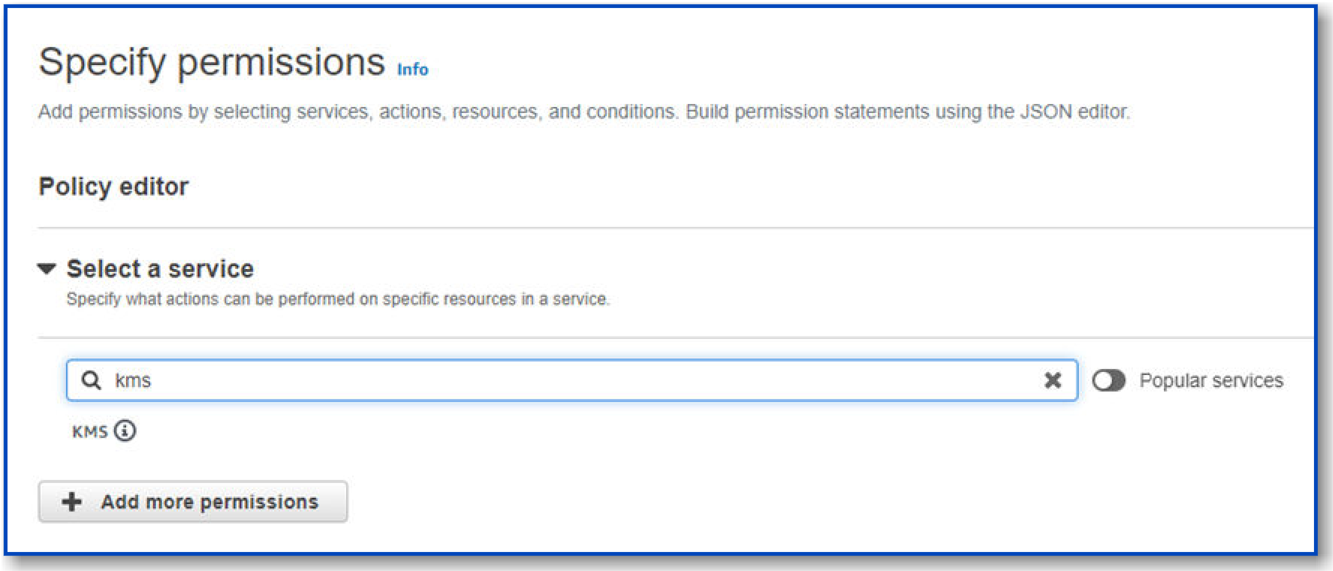
# Create an AWS Policy

Follow the steps to create a policy in AWS.

**Step 1 –** Log into AWS.

**Step 2 –** Navigate to the **IAM** page, and then the **Policies** page.

**Step 3 –** Select **Create Policy**.



Specify permissions Info

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

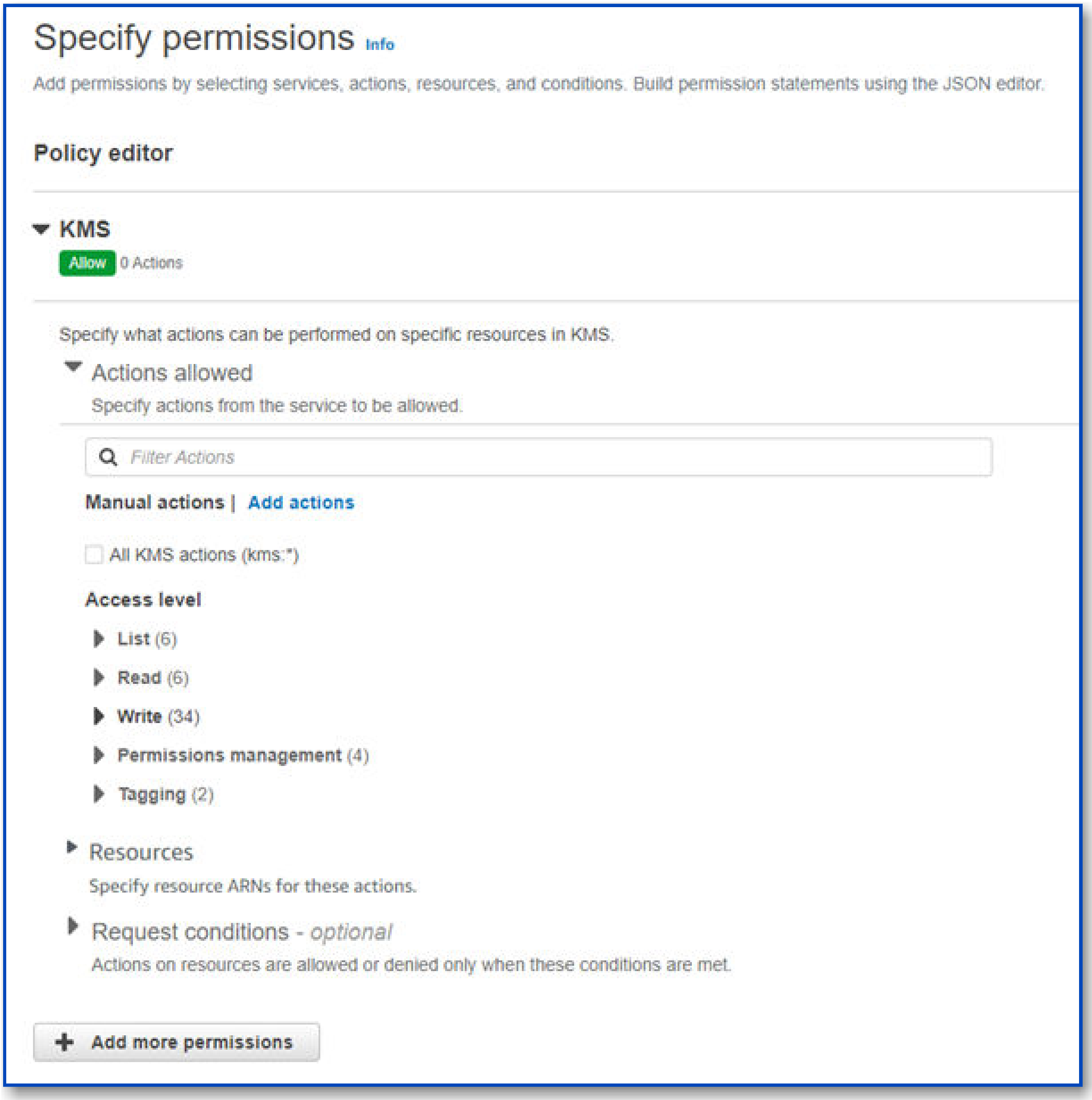
Policy editor

Select a service

Specify what actions can be performed on specific resources in a service.

kms

**Step 4 –** On the Specify permissions page, navigate to the Select a service box and search for the ‘KMS’ service.



Specify permissions Info

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Policy editor

KMS

Allow 0 Actions

Specify what actions can be performed on specific resources in KMS.

Actions allowed

Specify actions from the service to be allowed.

Filter Actions

Manual actions | Add actions

□ All KMS actions (kms:*)

Access level

- List (6)
- Read (6)
- Write (34)
- Permissions management (4)
- Tagging (2)

Resources

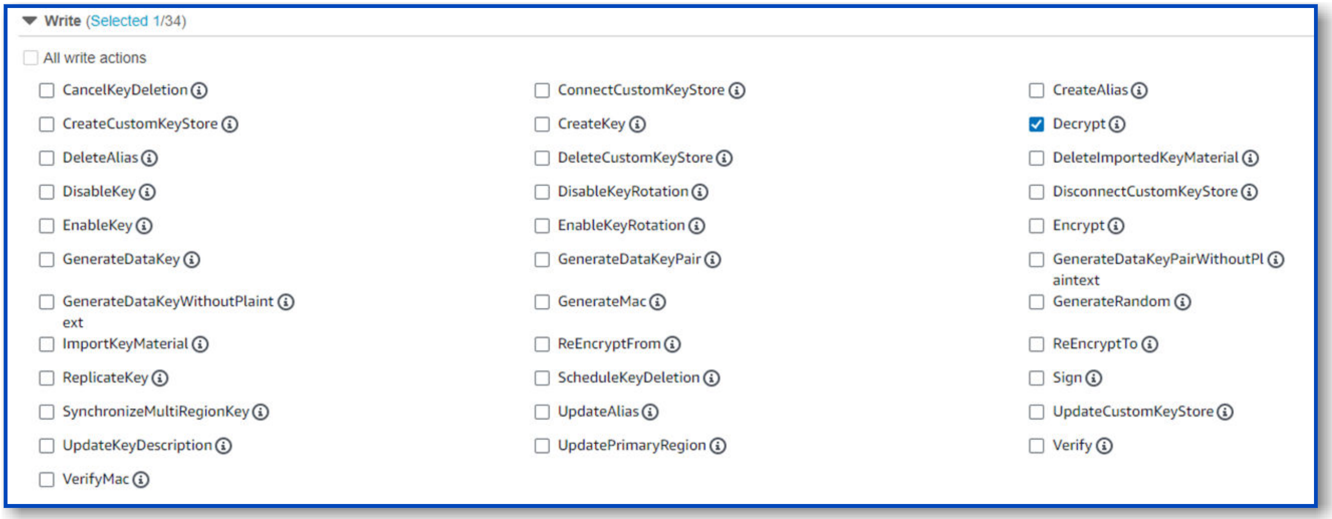
Specify resource ARNs for these actions.

Request conditions - *optional*

Actions on resources are allowed or denied only when these conditions are met.

+ Add more permissions

**Step 5 –** Select the **KMS** option.

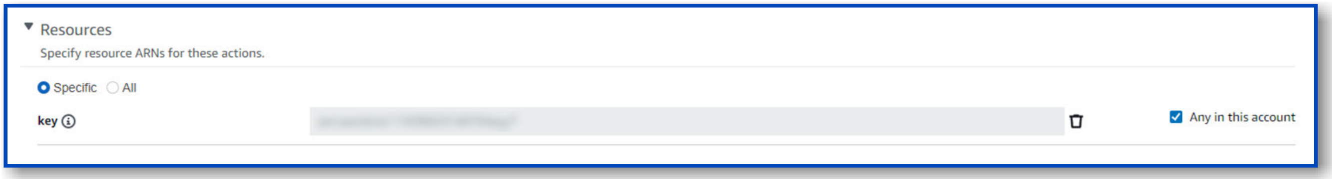


▾ Write (Selected 1/34)

□ All write actions

□ CancelKeyDeletion ⓘ
□ ConnectCustomKeyStore ⓘ
□ CreateAlias ⓘ
□ CreateCustomKeyStore ⓘ
□ CreateKey ⓘ
☑ Decrypt ⓘ
□ DeleteAlias ⓘ
□ DeleteCustomKeyStore ⓘ
□ DeleteImportedKeyMaterial ⓘ
□ DisableKey ⓘ
□ DisableKeyRotation ⓘ
□ DisconnectCustomKeyStore ⓘ
□ EnableKey ⓘ
□ EnableKeyRotation ⓘ
□ Encrypt ⓘ
□ GenerateDataKey ⓘ
□ GenerateDataKeyPair ⓘ
□ GenerateDataKeyPairWithoutPlaintext ⓘ
□ GenerateDataKeyWithoutPlaintext ⓘ
□ GenerateMac ⓘ
□ GenerateRandom ⓘ
□ ImportKeyMaterial ⓘ
□ ReEncryptFrom ⓘ
□ ReEncryptTo ⓘ
□ ReplicateKey ⓘ
□ ScheduleKeyDeletion ⓘ
□ Sign ⓘ
□ SynchronizeMultiRegionKey ⓘ
□ UpdateAlias ⓘ
□ UpdateCustomKeyStore ⓘ
□ UpdateKeyDescription ⓘ
□ UpdatePrimaryRegion ⓘ
□ Verify ⓘ
□ VerifyMac ⓘ

**Step 6 –** Under the Write dropdown menu, locate and select the **Decrypt permission** checkbox.



▾ Resources

Specify resource ARNs for these actions.

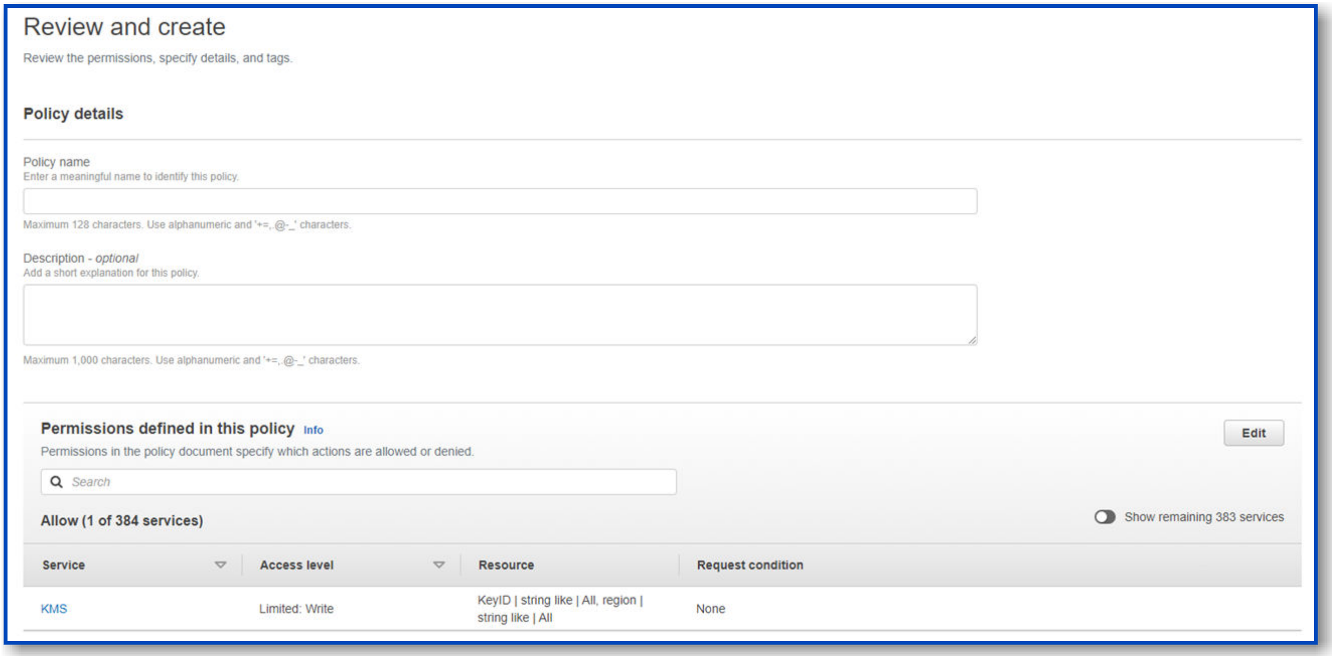
● Specific ○ All

key ⓘ [redacted]

☑ Any in this account

**Step 7 –** Under the Resources dropdown menu, select the **Any in this account** checkbox.

**NOTE:** This can be limited to a specific key when the key has been created.



Review and create

Review the permissions, specify details, and tags.

**Policy details**

Policy name
Enter a meaningful name to identify this policy.

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

Description - *optional*
Add a short explanation for this policy.

Maximum 1,000 characters. Use alphanumeric and '+=,.@-_' characters.

**Permissions defined in this policy** Info

Permissions in the policy document specify which actions are allowed or denied.

Allow (1 of 384 services)

| Service | Access level | Resource | Request condition |
|---|---|---|---|
| KMS | Limited: Write | KeyID \| string like \| All, region \| string like \| All | None |

**Step 8 –** Enter a name for the policy and a description (optional).

**Step 9 –** Save the policy.

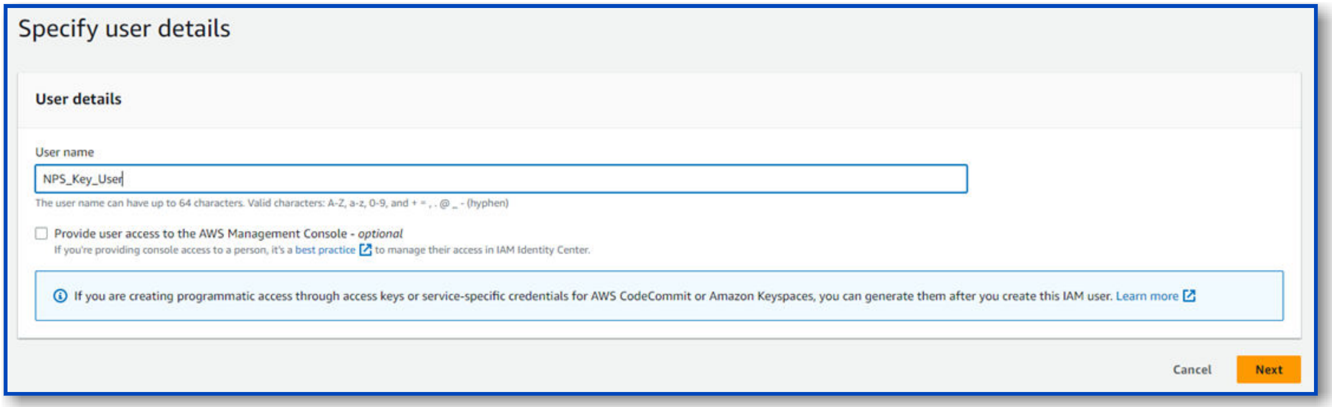
The policy is created.

# Create a User

Follow the steps to create a user in AWS.

**Step 1 –** Navigate to the **IAM** page, and then the **User** page.

**Step 2 –** Select **Create User**.



Specify user details

User details

User name

NPS_Key_User

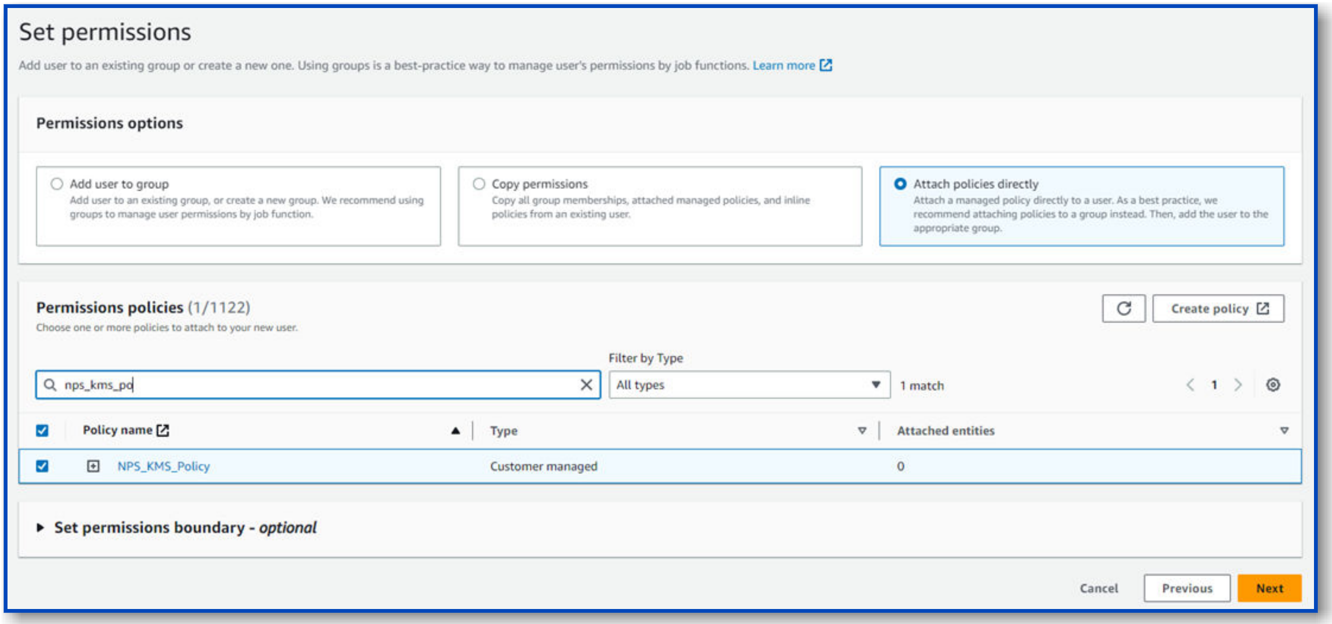
The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

□ Provide user access to the AWS Management Console - *optional*

If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.

If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. Learn more

**Step 3 –** On the Specify user details page, enter a user name. Optionally, select the **Provide user access to the AWS Management Console** checkbox.



Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more

Permissions options

○ Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

○ Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.

● Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

Permissions policies (1/1122)
Choose one or more policies to attach to your new user.

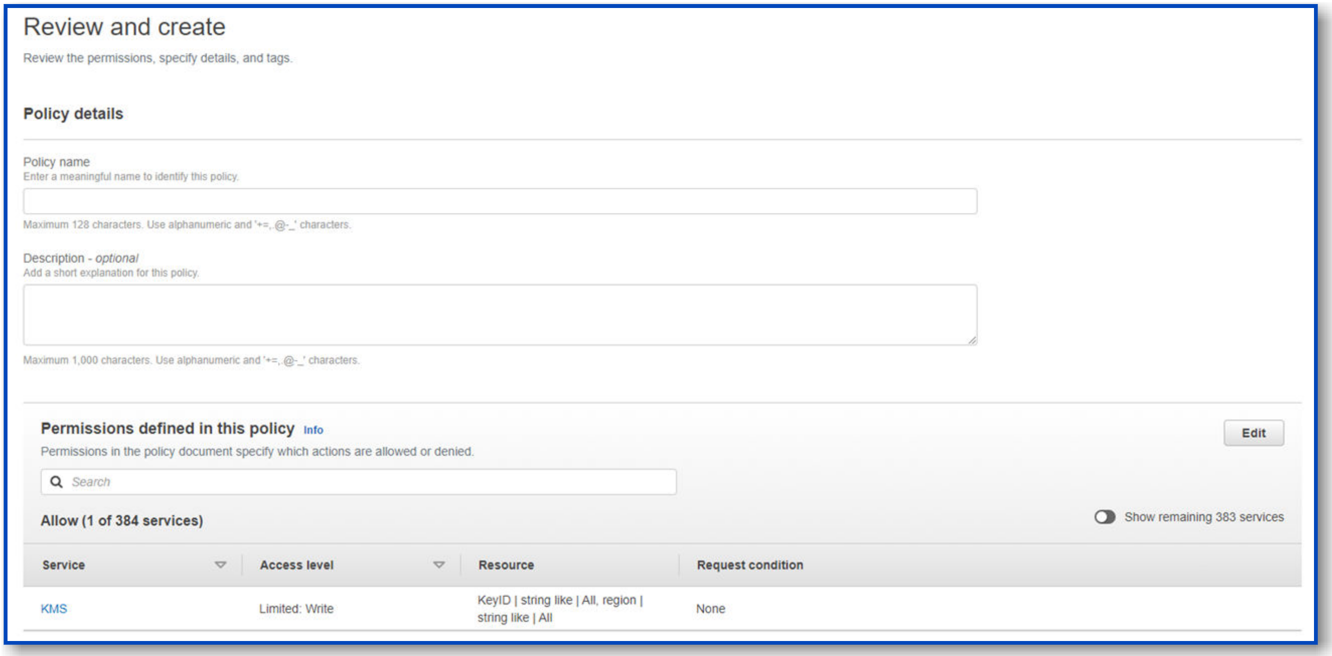
Search: nps_kms_po
Filter by Type: All types
1 match

| ☑ | Policy name | Type | Attached entities |
|---|---|---|---|
| ☑ | NPS_KMS_Policy | Customer managed | 0 |

Set permissions boundary - *optional*

**Step 4 –** In the Permissions options section, select **Attach policies directly** in the Permission options.

**Step 5 –** In the Permissions policies section, search for the NPS key policy you previously created and select the checkbox to the left of the policy. Click **Next**.



Review and create

Review the permissions, specify details, and tags.

Policy details

Policy name
Enter a meaningful name to identify this policy.

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

Description - *optional*
Add a short explanation for this policy.

Maximum 1,000 characters. Use alphanumeric and '+=,.@-_' characters.

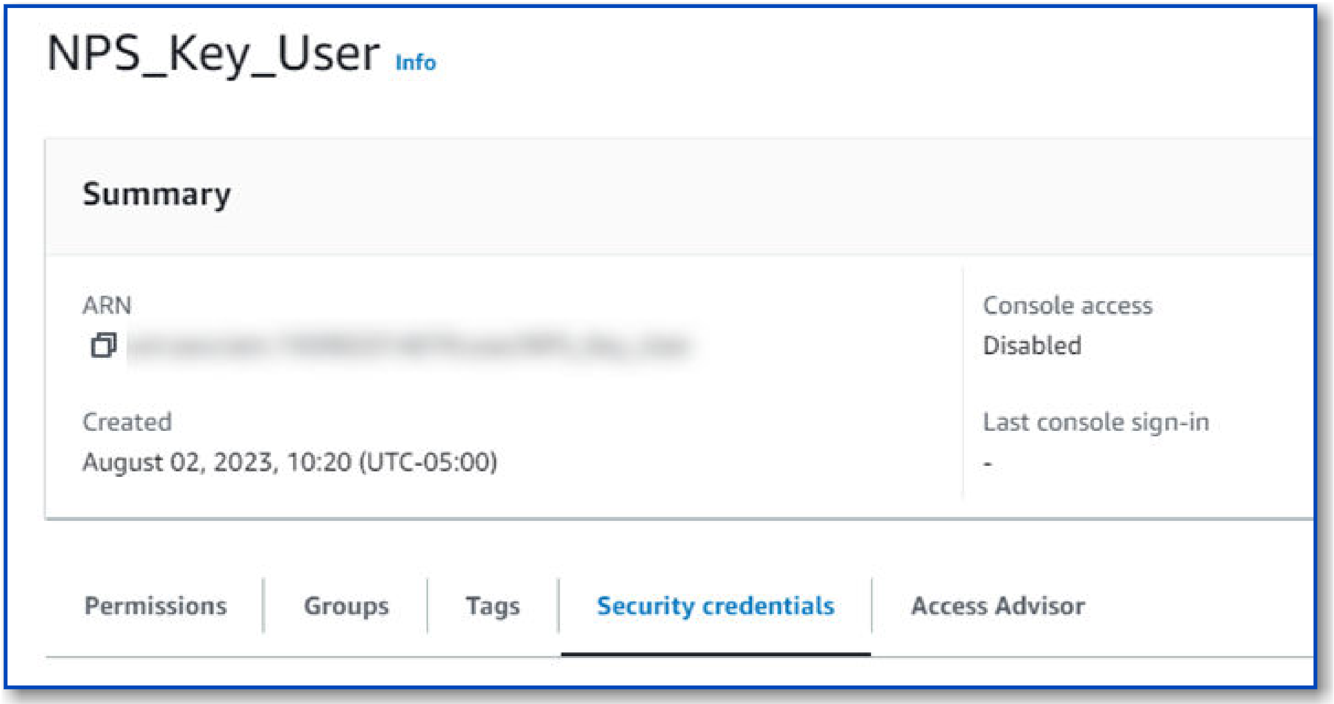
Permissions defined in this policy Info
Permissions in the policy document specify which actions are allowed or denied.

Allow (1 of 384 services)

Show remaining 383 services

| Service | Access level | Resource | Request condition |
|---|---|---|---|
| KMS | Limited: Write | KeyID \| string like \| All, region \| string like \| All | None |

**Step 6 –** On the Review and create window, review the policy configuration and click **Create now**.



NPS_Key_User Info

Summary

ARN
[redacted]

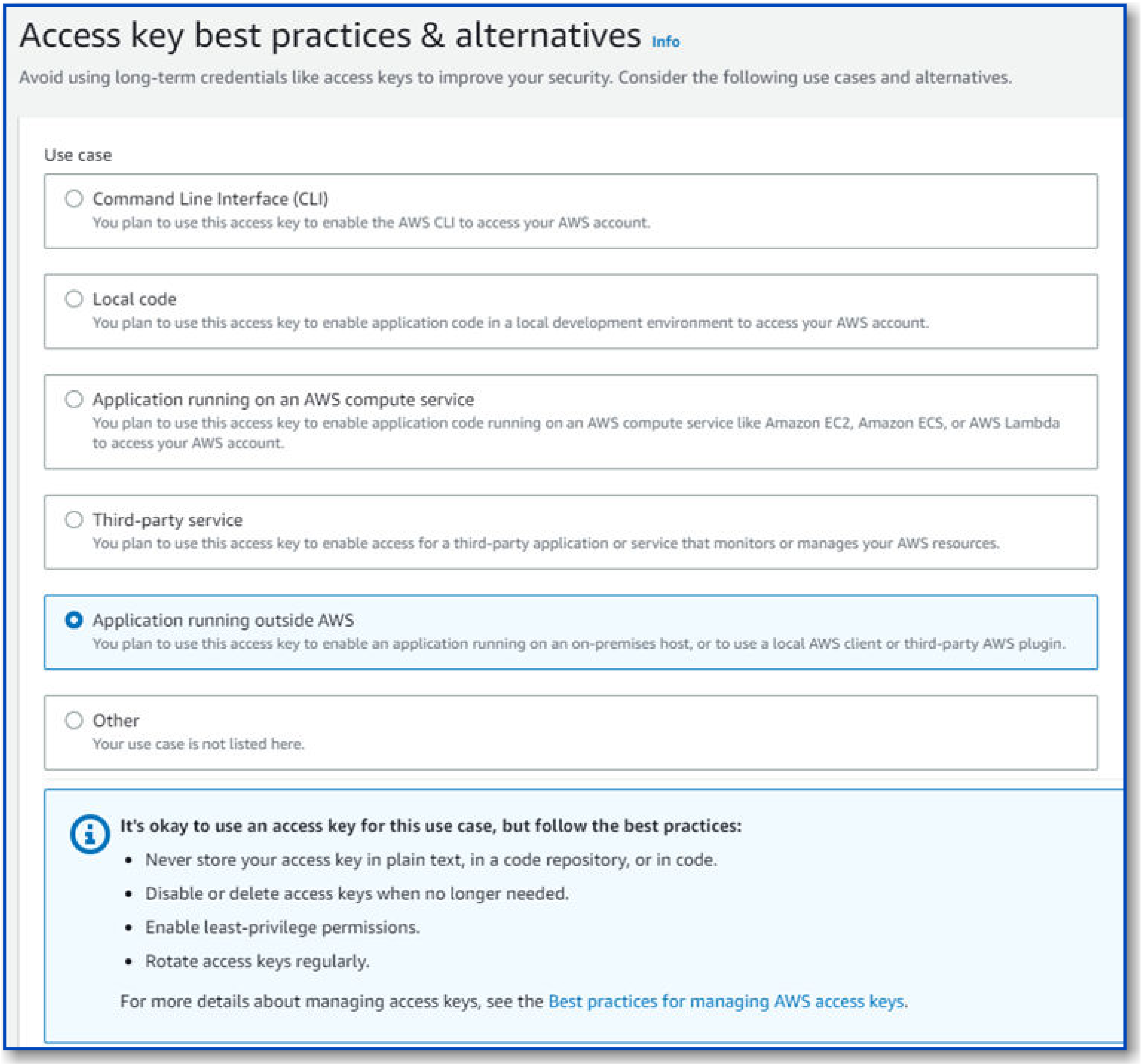
Console access
Disabled

Created
August 02, 2023, 10:20 (UTC-05:00)

Last console sign-in
-

**Step 7 –** Once the user has been created, select the user and navigate to the **Security credentials** tab.

**Step 8 –** Select **Create access key**.



Access key best practices & alternatives Info

Avoid using long-term credentials like access keys to improve your security. Consider the following use cases and alternatives.

Use case

○ Command Line Interface (CLI)
You plan to use this access key to enable the AWS CLI to access your AWS account.

○ Local code
You plan to use this access key to enable application code in a local development environment to access your AWS account.

○ Application running on an AWS compute service
You plan to use this access key to enable application code running on an AWS compute service like Amazon EC2, Amazon ECS, or AWS Lambda to access your AWS account.

○ Third-party service
You plan to use this access key to enable access for a third-party application or service that monitors or manages your AWS resources.

● Application running outside AWS
You plan to use this access key to enable an application running on an on-premises host, or to use a local AWS client or third-party AWS plugin.

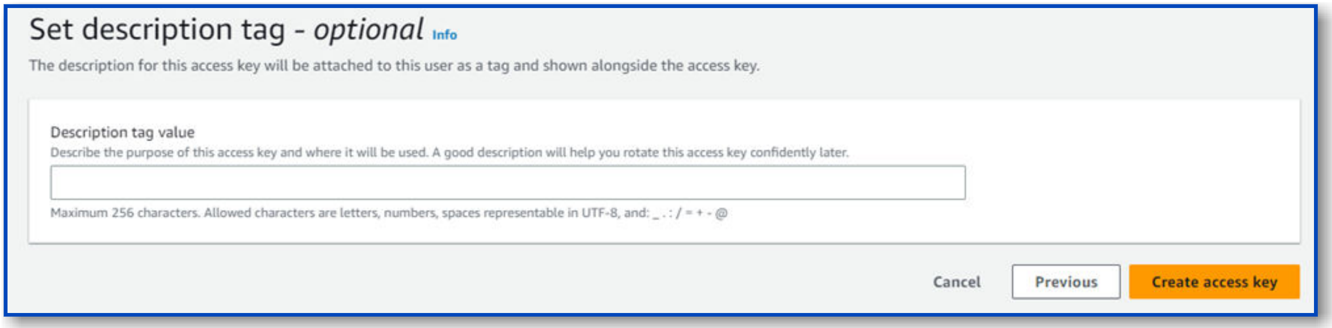
○ Other
Your use case is not listed here.

**It's okay to use an access key for this use case, but follow the best practices:**

- Never store your access key in plain text, in a code repository, or in code.
- Disable or delete access keys when no longer needed.
- Enable least-privilege permissions.
- Rotate access keys regularly.

For more details about managing access keys, see the Best practices for managing AWS access keys.

**Step 9 –** Once the creation window opens, select the **Application running outside of AWS** option.



Set description tag - *optional* Info

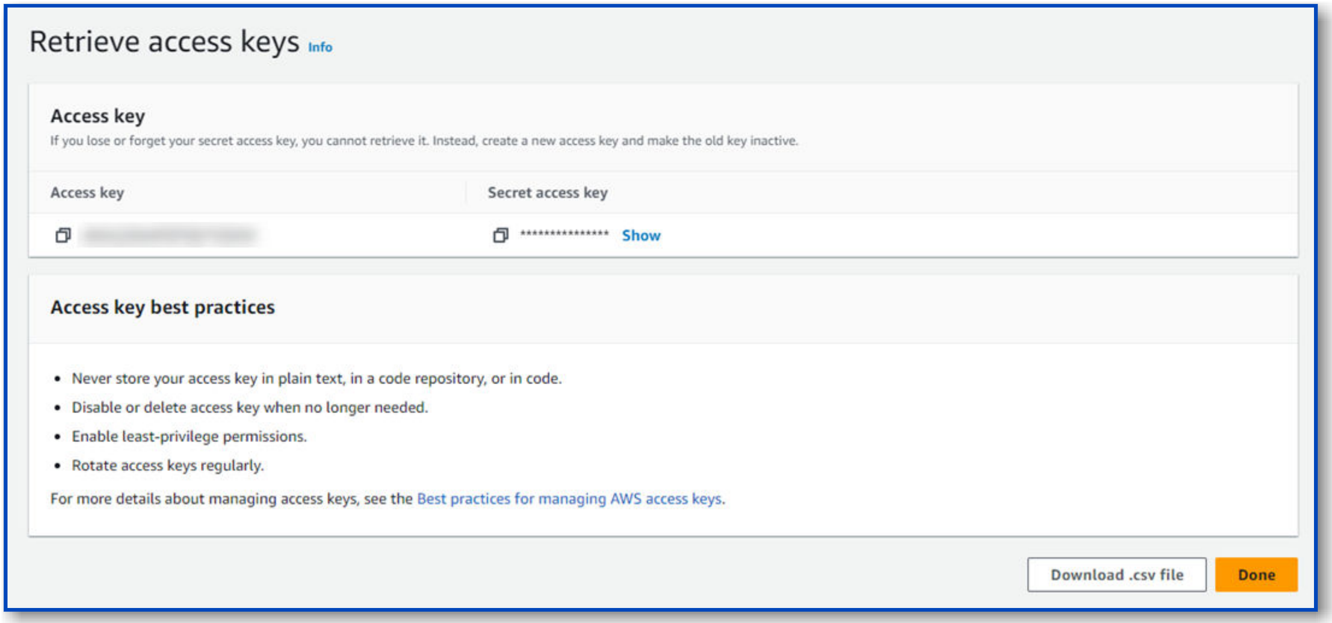
The description for this access key will be attached to this user as a tag and shown alongside the access key.

Description tag value

Describe the purpose of this access key and where it will be used. A good description will help you rotate this access key confidently later.

Maximum 256 characters. Allowed characters are letters, numbers, spaces representable in UTF-8, and: _ . : / = + - @

**Step 10 –** Set an optional description tag if required, and then select **Create access key**.



Retrieve access keys Info

Access key

If you lose or forget your secret access key, you cannot retrieve it. Instead, create a new access key and make the old key inactive.

| Access key | Secret access key |
|---|---|
| | *************** Show |

Access key best practices

- Never store your access key in plain text, in a code repository, or in code.
- Disable or delete access key when no longer needed.
- Enable least-privilege permissions.
- Rotate access keys regularly.

For more details about managing access keys, see the Best practices for managing AWS access keys.

**Step 11 –** Once the Key has been created, copy or download the Access key and Secret access key. These keys will be used by Privilege Secure to access the AWS KMS key encryption and decryption functionality.

**Step 12 –** Click **Done** when finished.

**CAUTION:** Do not delete the AWS user Access Key without rotating the NPS key first.

The best practice for use of access keys is to rotate them regularly. Follow these steps when rotating access keys.

**Step 1 –** Create a new access key.

**Step 2 –** Rotate the NPS protect key to use the new access key.

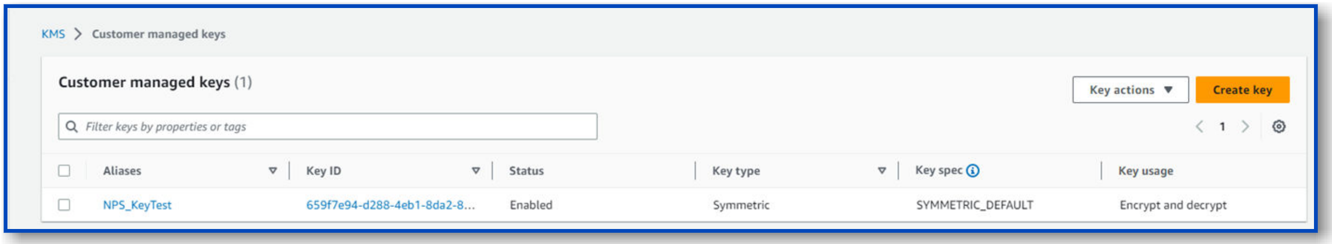
**Step 3 –** Delete old access key.

# Create a Managed Key

Follow the steps to create a managed key in AWS.

**Step 1 –** Navigate to the **Key Management Service** page.

**Step 2 –** Select **Customer Managed Keys**.

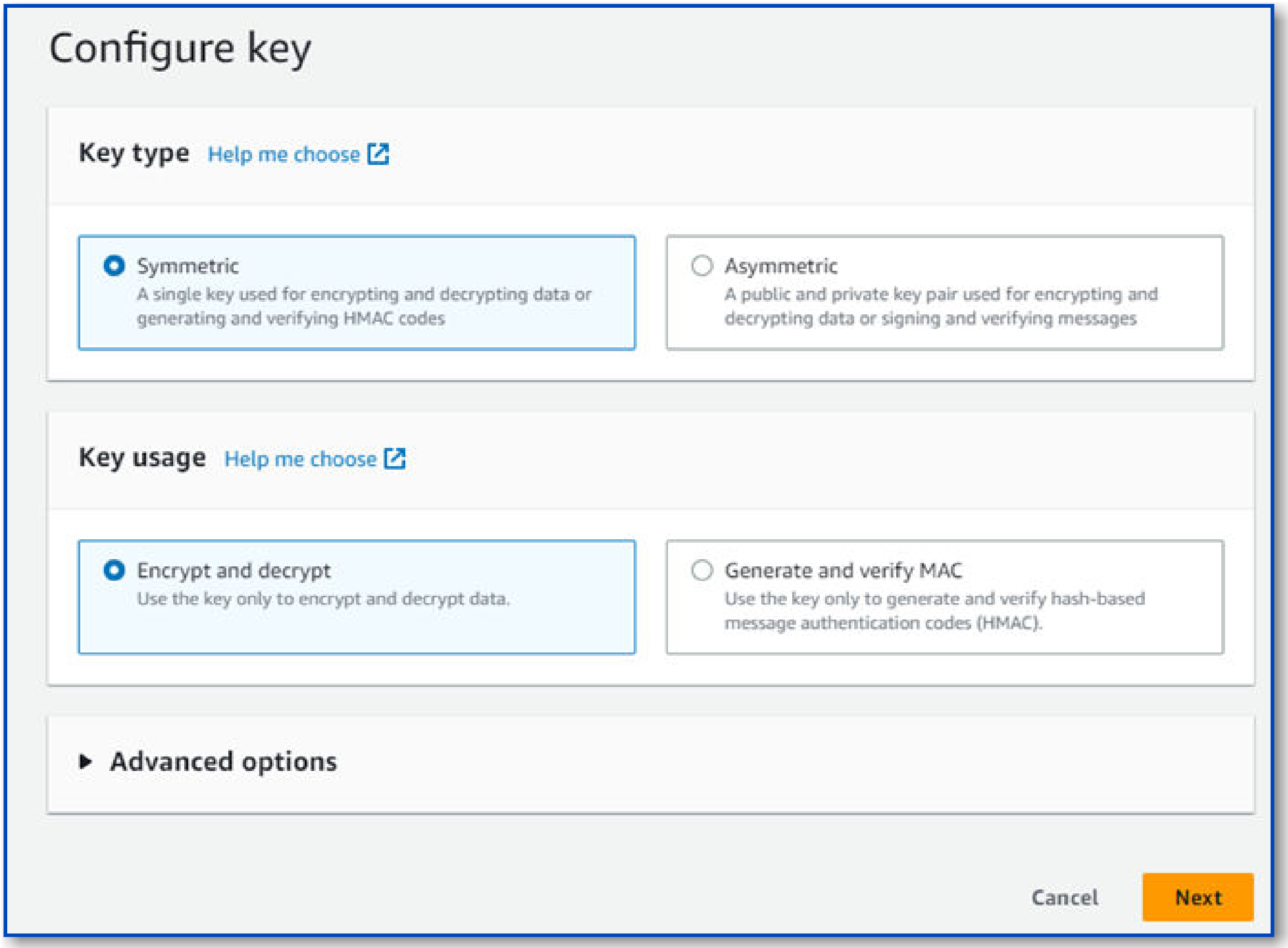


KMS > Customer managed keys

Customer managed keys (1)

| □ | Aliases | Key ID | Status | Key type | Key spec | Key usage |
|---|---|---|---|---|---|---|
| □ | NPS_KeyTest | 659f7e94-d288-4eb1-8da2-8... | Enabled | Symmetric | SYMMETRIC_DEFAULT | Encrypt and decrypt |

**Step 3 –** Select **Create Key**.



Configure key

Key type Help me choose

● Symmetric
A single key used for encrypting and decrypting data or generating and verifying HMAC codes

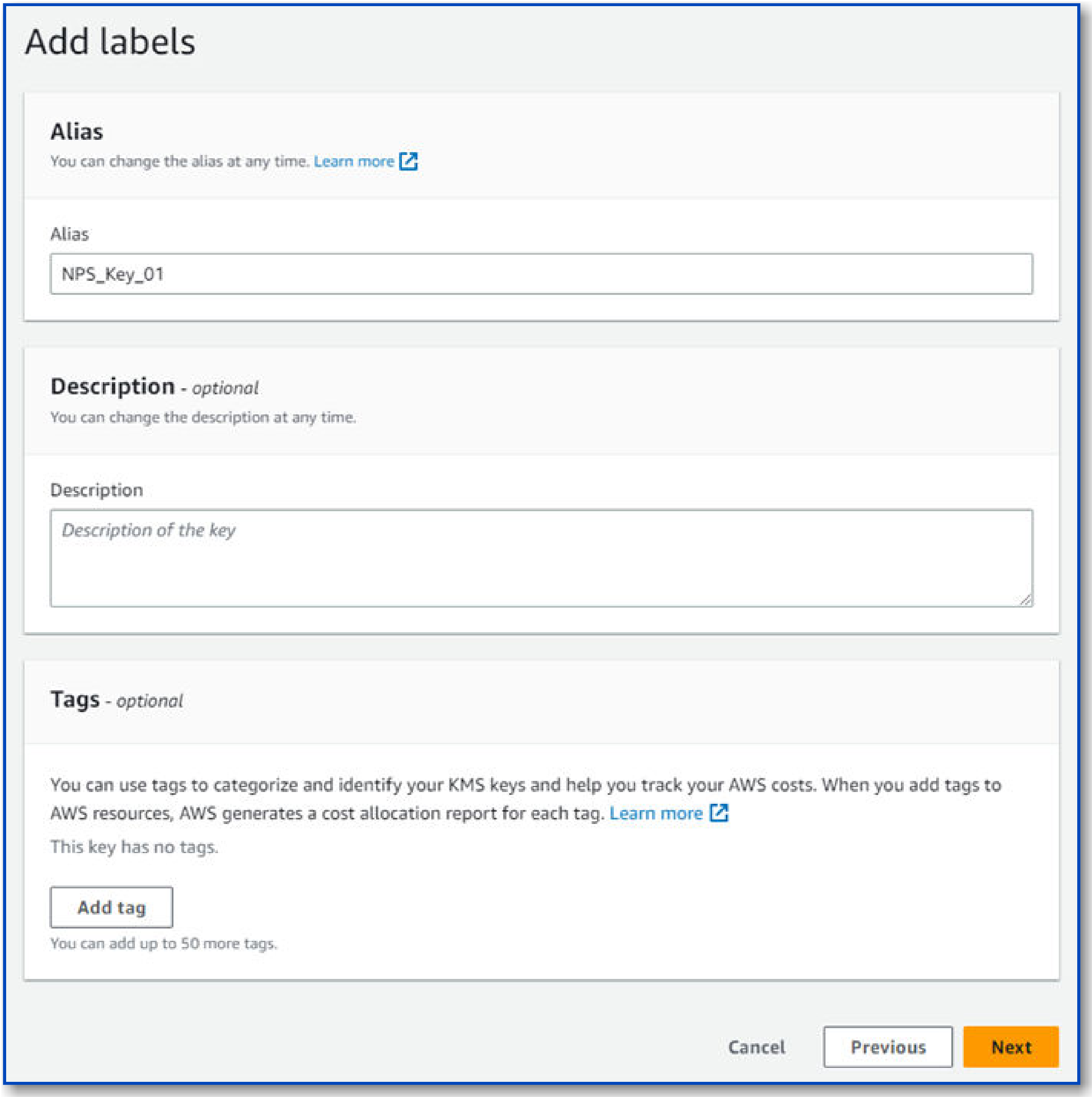
○ Asymmetric
A public and private key pair used for encrypting and decrypting data or signing and verifying messages

Key usage Help me choose

● Encrypt and decrypt
Use the key only to encrypt and decrypt data.

○ Generate and verify MAC
Use the key only to generate and verify hash-based message authentication codes (HMAC).

**Step 4 –** For Key Type, Select **Symmetric**. For Key Usage, select **Encrypt and decrypt**. Click **Next** to continue.



Add labels

Alias

You can change the alias at any time. Learn more

Alias: NPS_Key_01

Description - optional

You can change the description at any time.

Description: Description of the key

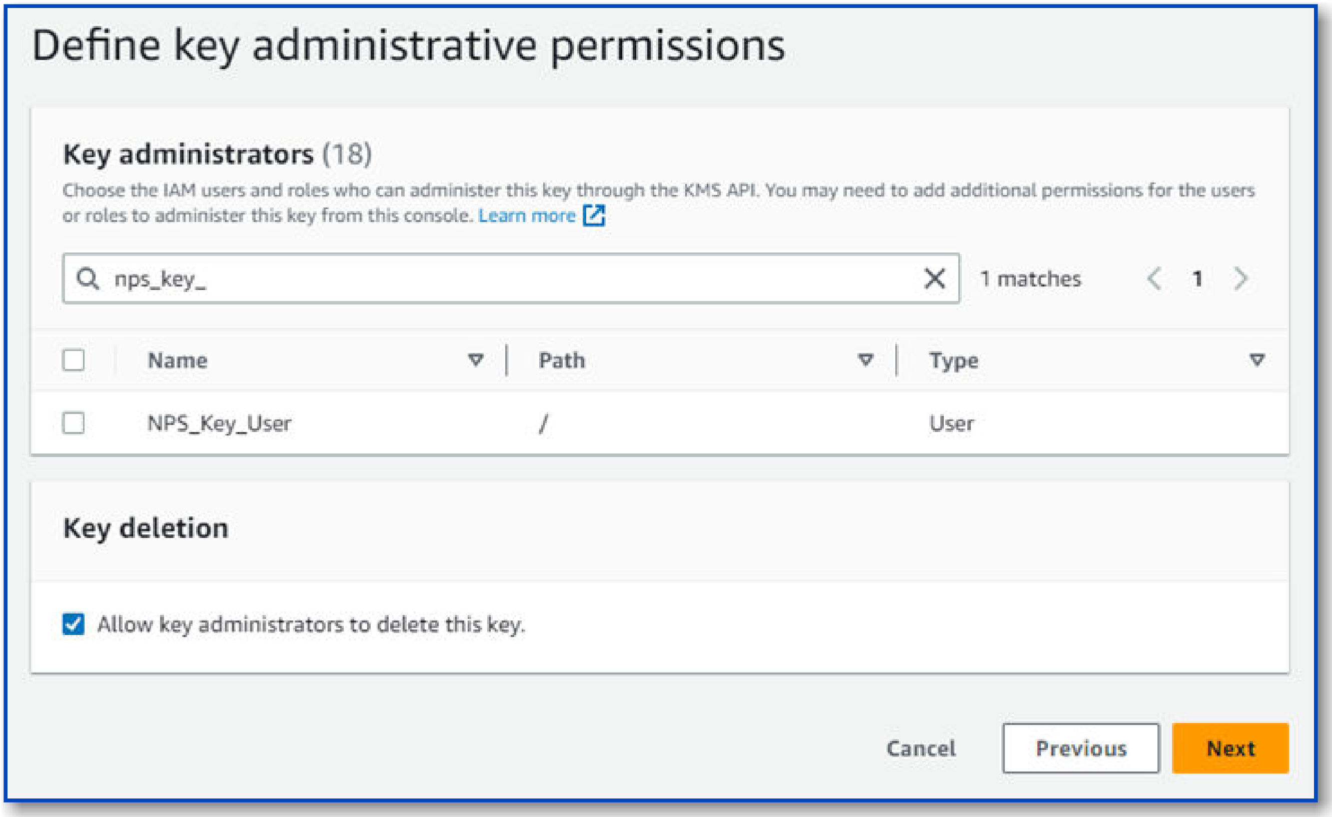
Tags - optional

You can use tags to categorize and identify your KMS keys 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

This key has no tags.

You can add up to 50 more tags.

**Step 5 –** Add an Alias for the key. The Description and Tags are optional. Click **Next** to continue.



Define key administrative permissions

**Key administrators** (18)

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

nps_key_

1 matches

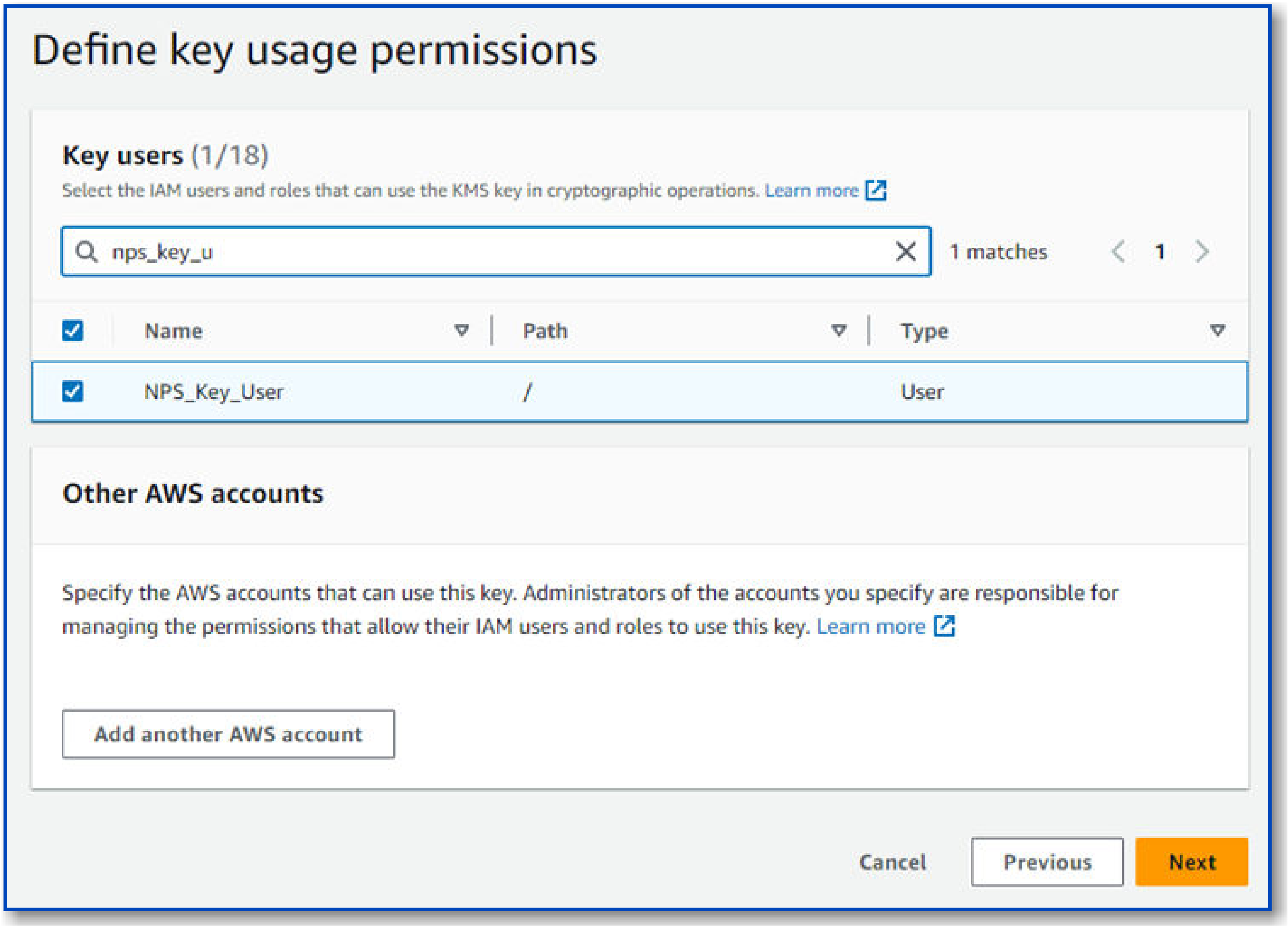
| □ | Name | Path | Type |
|---|---|---|---|
| □ | NPS_Key_User | / | User |

**Key deletion**

☑ Allow key administrators to delete this key.

**Step 6 –** Add a Key Administrator if required.

**NOTE:** The NPS Key user created earlier does not require administrative permissions at this level.



Define key usage permissions

**Key users** (1/18)

Select the IAM users and roles that can use the KMS key in cryptographic operations. Learn more

Search: nps_key_u — 1 matches

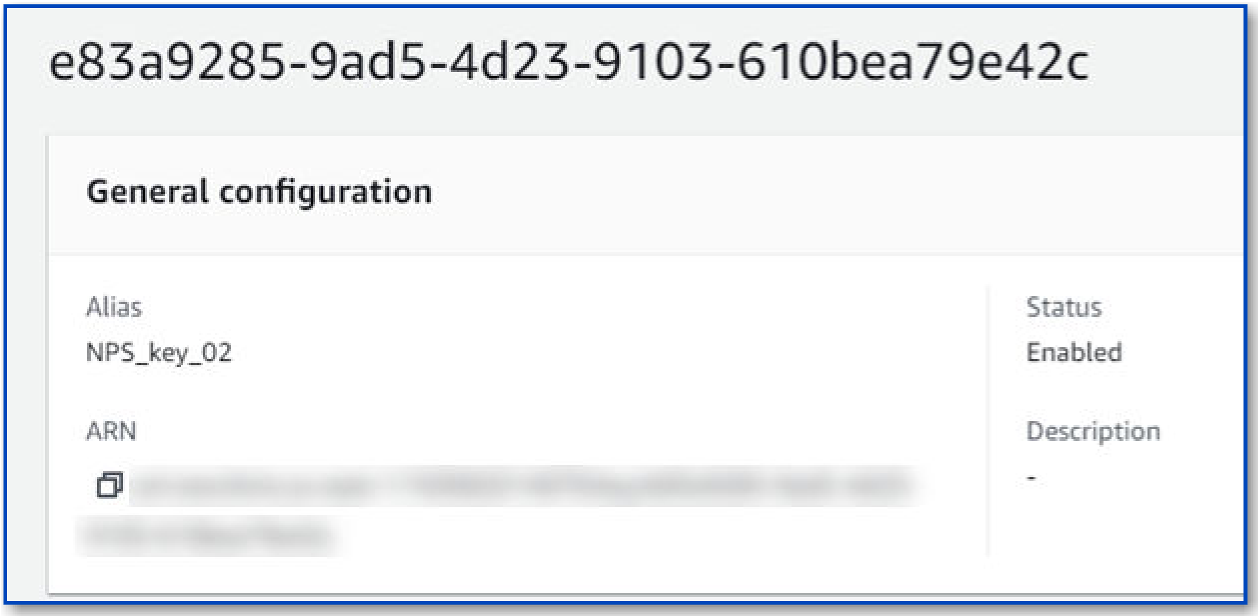
| ☑ | Name | Path | Type |
|---|---|---|---|
| ☑ | NPS_Key_User | / | User |

**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

**Step 7 –** Select the checkbox for the Privilege Secure key user created earlier as a Key user. Click **Next** to continue.

**Step 8 –** Review the key configuration and click **Create Key** to continue.



e83a9285-9ad5-4d23-9103-610bea79e42c

General configuration

Alias
NPS_key_02

ARN
[redacted]

Status
Enabled

Description
-

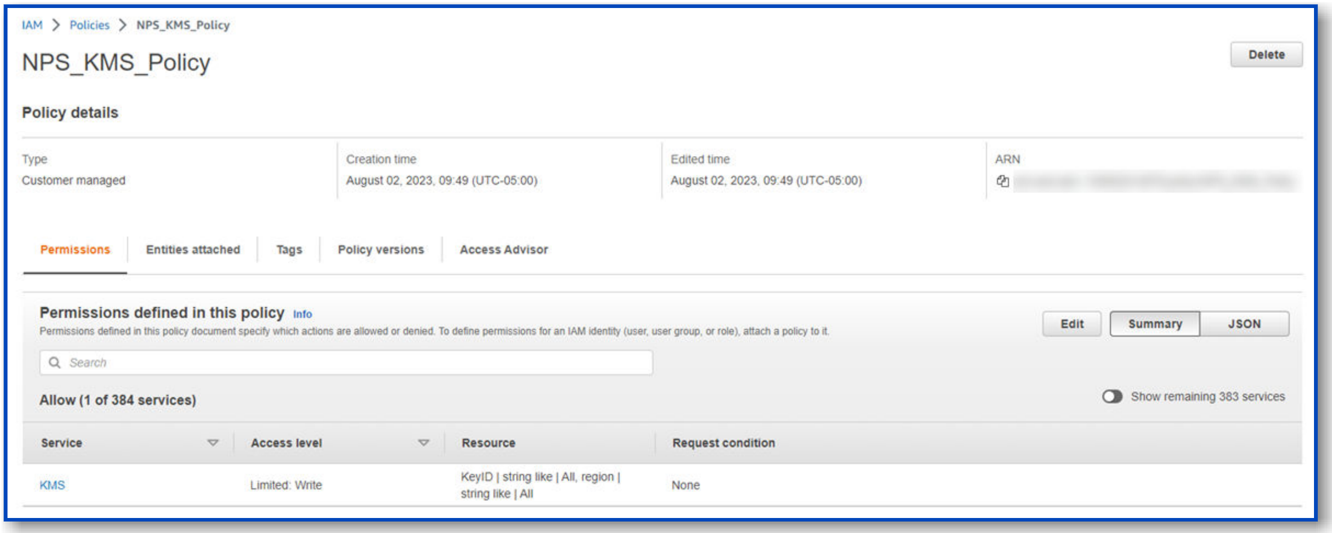
**Step 9 –** Click the **Copy** button from the newly created key, and store the ARN from the details.

The ARN will be used by Privilege Secure to identify the key used for encryption.

# Least Privilege Policy

The IAM policy created earlier can now be edited to limit to only the required key. Follow the steps to create a least privilege policy.

**Step 1 –** Navigate to the IAM Policies page and select the KMS policy created in earlier steps.



NPS_KMS_Policy

Policy details

Type: Customer managed
Creation time: August 02, 2023, 09:49 (UTC-05:00)
Edited time: August 02, 2023, 09:49 (UTC-05:00)
ARN: [redacted]

Permissions defined in this policy Info

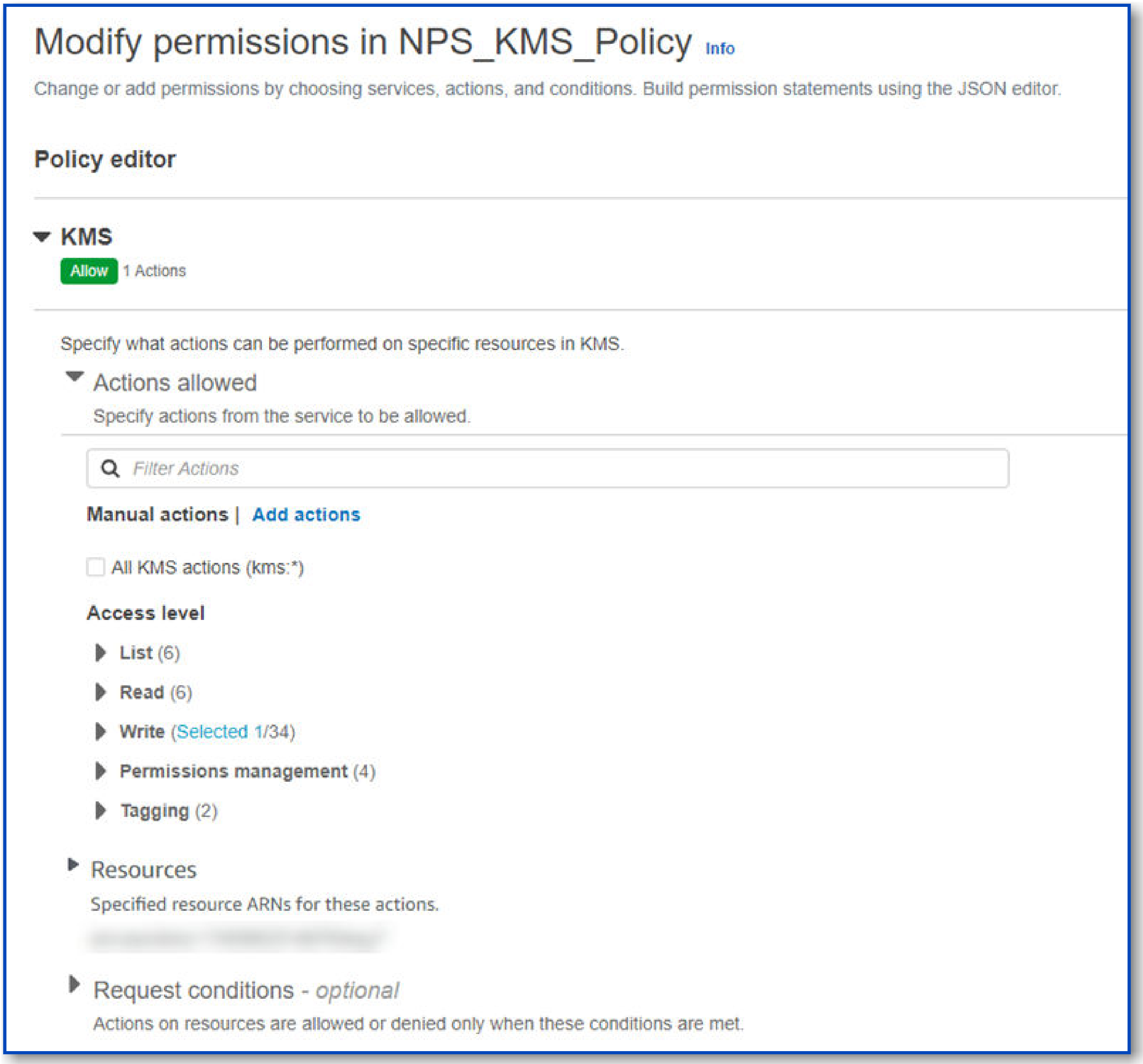
Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it.

Allow (1 of 384 services)

| Service | Access level | Resource | Request condition |
|---|---|---|---|
| KMS | Limited: Write | KeyID \| string like \| All, region \| string like \| All | None |

**Step 2 –** Select the **Permissions** tab.

**Step 3 –** Click the **Edit** button.



Modify permissions in NPS_KMS_Policy Info

Change or add permissions by choosing services, actions, and conditions. Build permission statements using the JSON editor.

Policy editor

▼ KMS

Allow 1 Actions

Specify what actions can be performed on specific resources in KMS.

▼ Actions allowed

Specify actions from the service to be allowed.

Filter Actions

Manual actions | Add actions

□ All KMS actions (kms:*)

Access level

- ▶ List (6)
- ▶ Read (6)
- ▶ Write (Selected 1/34)
- ▶ Permissions management (4)
- ▶ Tagging (2)

▶ Resources

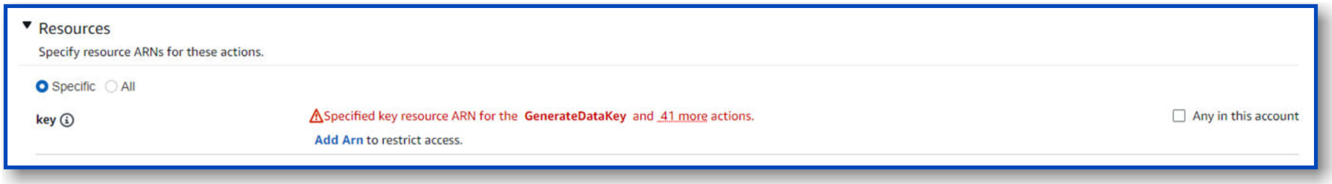
Specified resource ARNs for these actions.

[redacted]

▶ Request conditions - *optional*

Actions on resources are allowed or denied only when these conditions are met.

**Step 4 –** Once the policy editor window opens, switch to the Visual display mode and expand the KMS item dropdown.



▼ Resources

Specify resource ARNs for these actions.

● Specific ○ All

key ⓘ

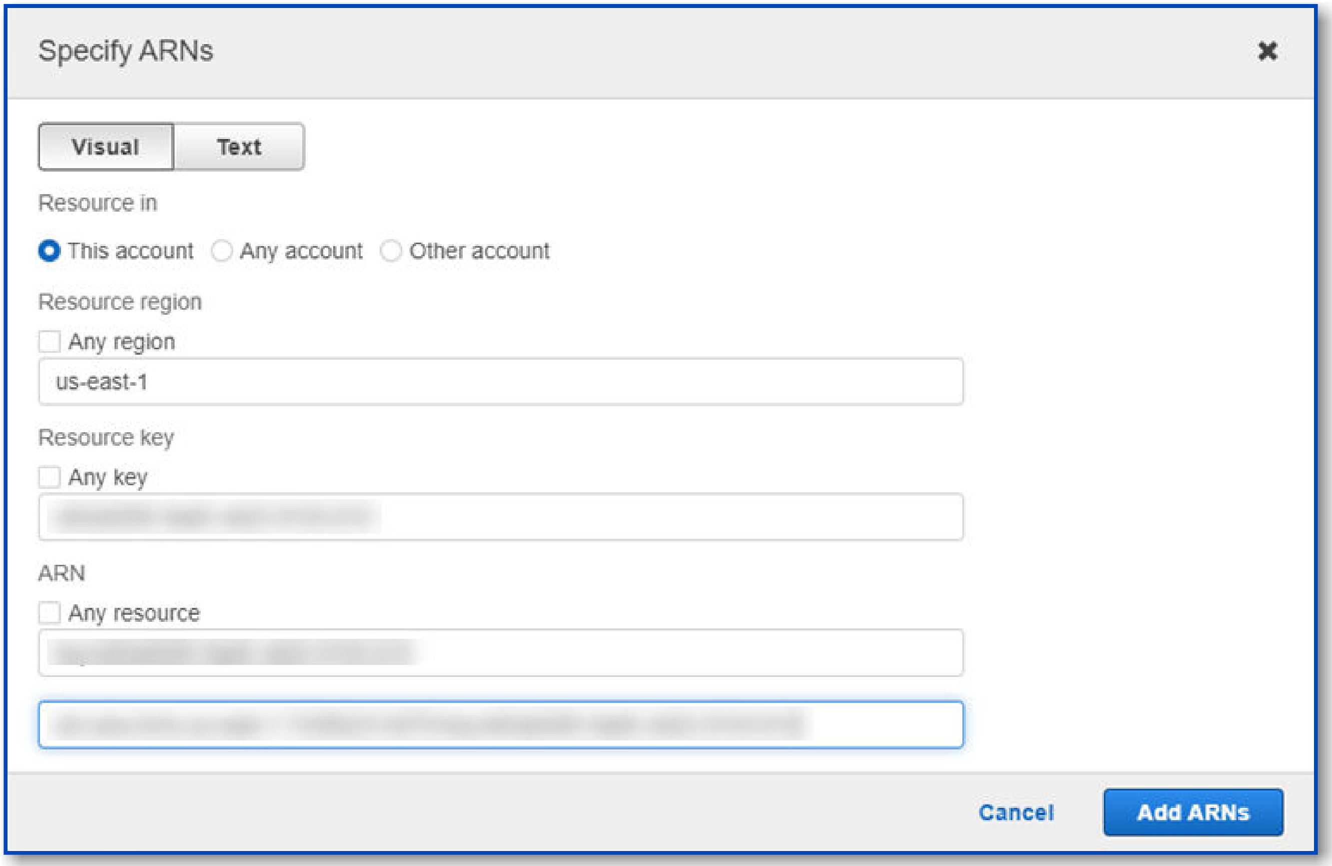
⚠Specified key resource ARN for the **GenerateDataKey** and 41 more actions.

Add Arn to restrict access.

□ Any in this account

**Step 5 –** Expand the Resources item and remove the selection from **Any in this account** checkbox.

**Step 6 –** Click **Add Arn** to restrict access.



Specify ARNs

Visual | Text

Resource in

● This account ○ Any account ○ Other account

Resource region

□ Any region

us-east-1

Resource key

□ Any key

[redacted]

ARN

□ Any resource

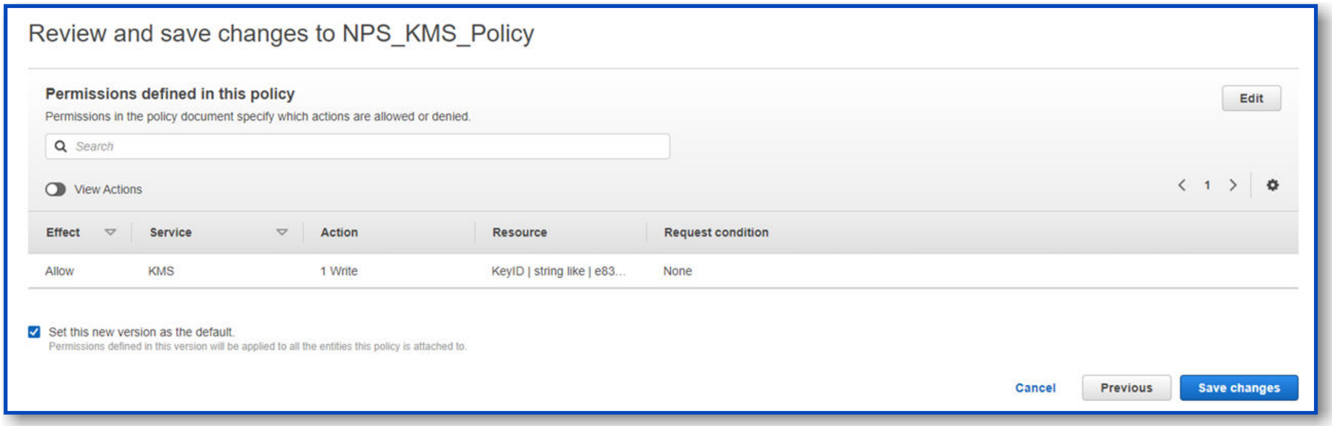
[redacted]

[redacted]

Cancel | Add ARNs

**Step 7 –** Paste the copied ARN for the NPS key into the bottom box then

**Step 8 –** Click **Add ARNs**.



Review and save changes to NPS_KMS_Policy

**Permissions defined in this policy**

Permissions in the policy document specify which actions are allowed or denied.

Edit

Search

View Actions

| Effect | Service | Action | Resource | Request condition |
|---|---|---|---|---|
| Allow | KMS | 1 Write | KeyID \| string like \| e83... | None |

☑ Set this new version as the default.
Permissions defined in this version will be applied to all the entities this policy is attached to.

Cancel | Previous | Save changes

**Step 9 –** Review configuration and click **Save changes** to the NPS_KMS_Policy.

The policy will now be limited to only the specified KMS key. The KMS is ready to be roated in Privilege Secure. See the AWS KMS Key Rotation topic for additional information.

# AWS KMS Key Rotation

Organizations using AWS Key Management Service (AWS KMS) can configure Netwrix Privilege Secure to rotate security keys. When creating an AWS KMS protection key for Privilege Secure, configuration must start by creating a policy in AWS. Once a AWS policy is created, a connection to the AWS policy can be configured using Privilege Secure Rotate AWS Key tool.

The AWS KMS key is not used to encrypt the secret key, but will be used to encrypt the key that is used to encrypt the secret key.

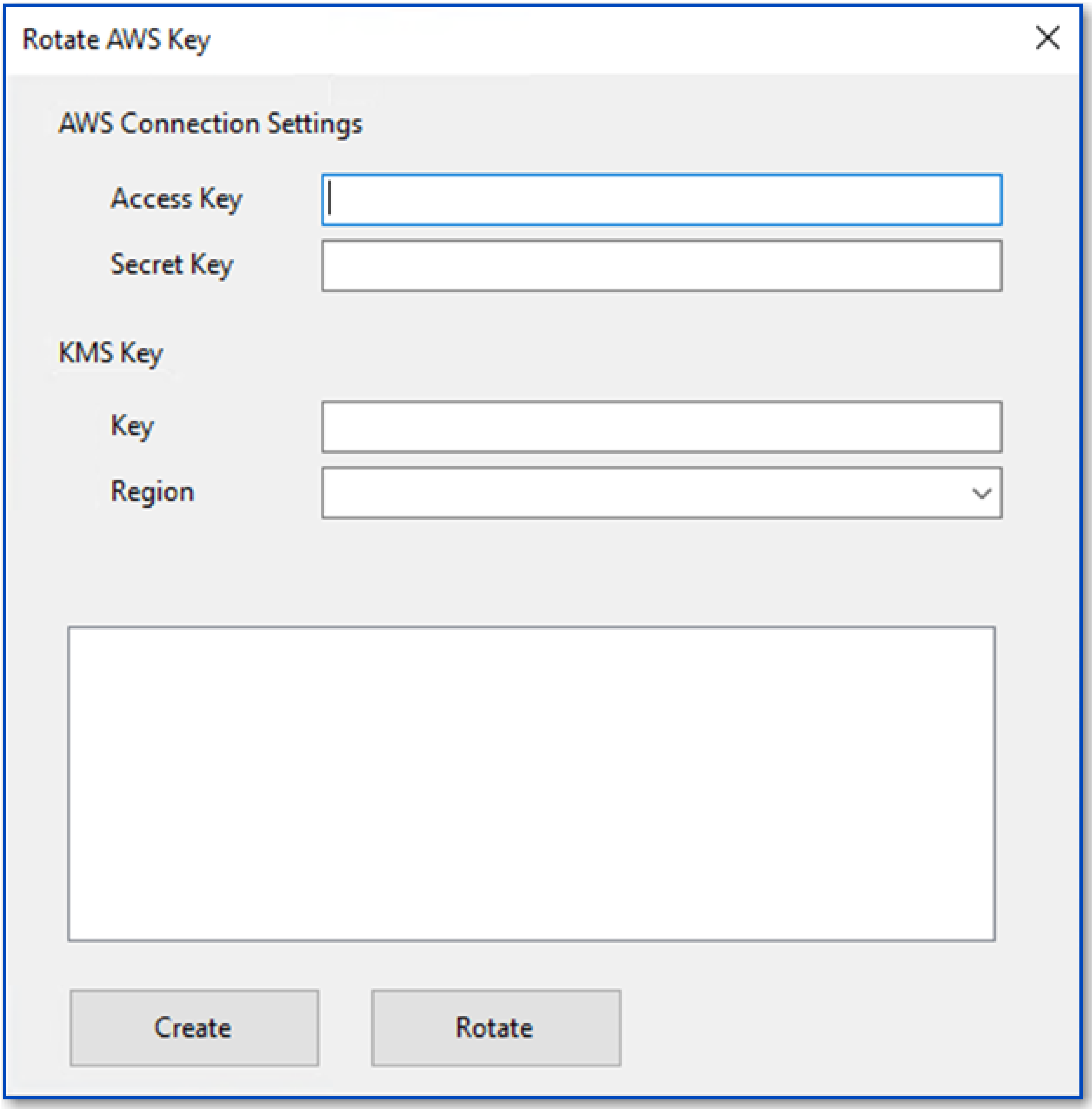
## Rotate AWS Key

Follow the steps to rotate a AWS KMS Key.

**Step 1 –** Locate the KeyTools folder in the installation directory.

```
C:\Program Files\Stealthbits\PAM\KeyTools
```

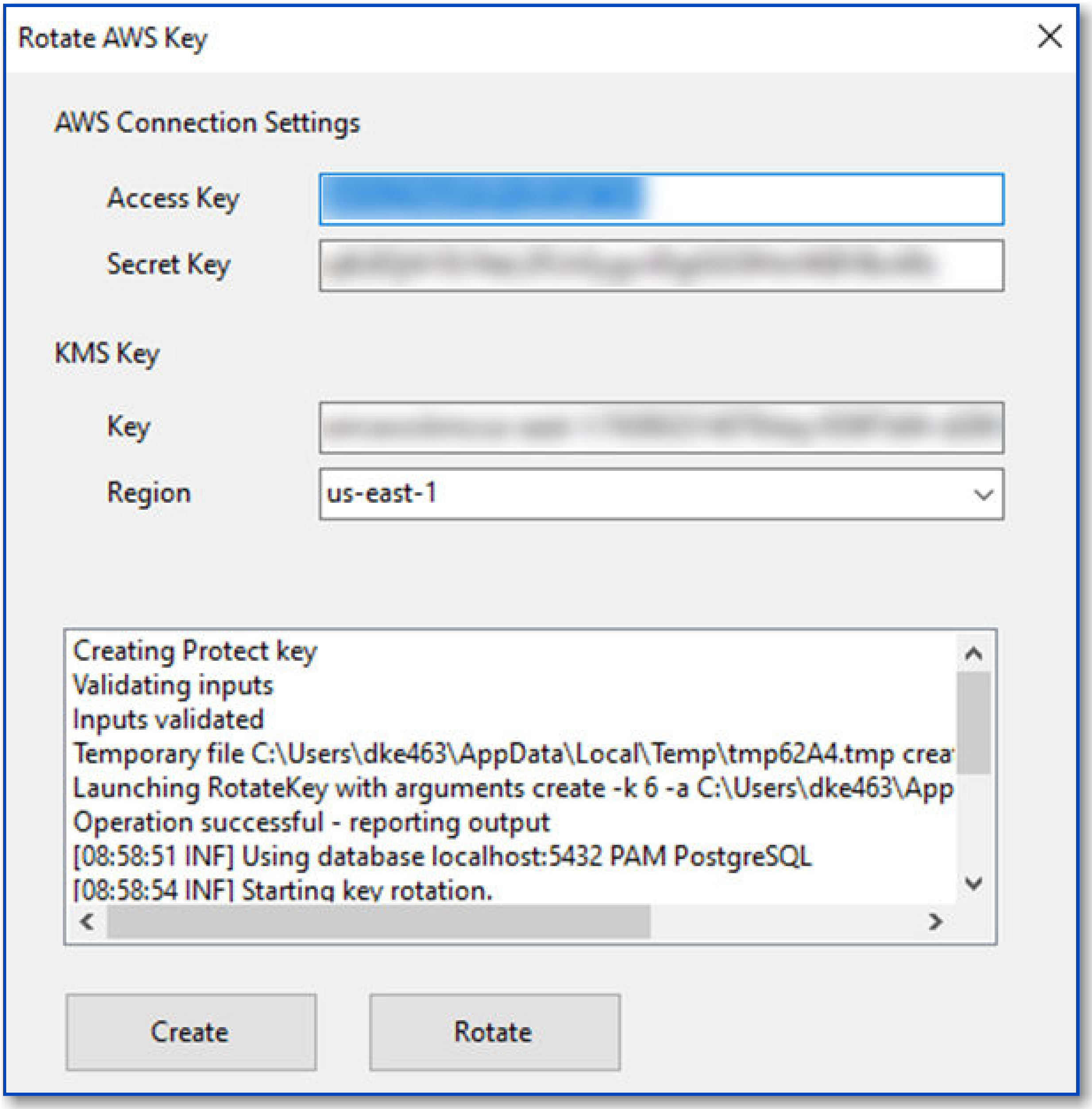
**Step 2 –** Run the `SbPAM.RotateAwsKey` executable to launch the Rotate AWS Key wizard.



**Step 3 –** Enter the **Access key** and **Secret key** created for the AWS user assigned to the AWS KMS key into the AWS Connection settings fields.

**Step 4 –** Enter the KMS key ARN into the KMS Key field.

**Step 5 –** Select the appropriate AWS region from the dropdown list.



Region: us-east-1

```
Creating Protect key
Validating inputs
Inputs validated
Temporary file C:\Users\dke463\AppData\Local\Temp\tmp62A4.tmp crea
Launching RotateKey with arguments create -k 6 -a C:\Users\dke463\App
Operation successful - reporting output
[08:58:51 INF] Using database localhost:5432 PAM PostgreSQL
[08:58:54 INF] Starting key rotation.
```

**Step 6 –** When all fields are completed, click the **Rotate** button to update all encrypted values in the Privilege Secure system.

The tool will take a few minutes to run (especially on larger systems) and the log window will show the results of the rotation.

**NOTE:** If the AWS KMS key is rotated, there is no need to rotate the NPS key. Encrypted values will continue to be decrypted and any new encryption will use the updated AWS KMS key. If the AWS user Access Key is rotated it will be necessary to rotate the NPS key to update it to use the new Ids. Best practice for use of access keys is to rotate them regularly. **Do not** delete the AWS user Access Key without rotating the NPS key first.

- **Step 1 –** Create a new access key.
- **Step 2 –** Rotate the NPS protect key to use the new access key.
- **Step 3 –** Delete old access key.

The KMS Key has been rotated.