**How to encrypt existing parameters from AWS Systems Manager Parameter Store**

Encrypting existing parameters in AWS Systems Manager Parameter Store involves using the AWS Key Management Service (KMS) to encrypt the parameter values. Here are step-by-step instructions:

**Obtain the ARN of the Default AWS Managed SSM KMS Key**

1. Log in to the AWS Management Console.
2. Navigate to the [AWS Key Management Service](https://eu-west-1.console.aws.amazon.com/kms/home) (KMS).
3. In the KMS dashboard, click on **"AWS managed keys"** from the left navigation pane.
4. Find the AWS managed key used for Systems Manager Parameter Store. It is usually named **"aws/ssm"** or similar. Click on the key to view its details.
5. Copy the Key ARN from the Key details page.

**Encrypt the Parameter Value using CloudShell**

1. Navigate to [AWS Systems Manager Parameter Store](https://eu-west-1.console.aws.amazon.com/systems-manager/parameters) service.
2. Open the AWS CloudShell by clicking on the icon in the bottom left corner of the console.
3. In the CloudShell terminal, use the following command to encrypt the existing parameter:

***aws ssm update-parameter --overwrite --name “<PARAMETER\_NAME>” --value “<PARAMETER\_VALUE>” --type SecureString --key-id “<KMS\_KEY\_ARN> “***

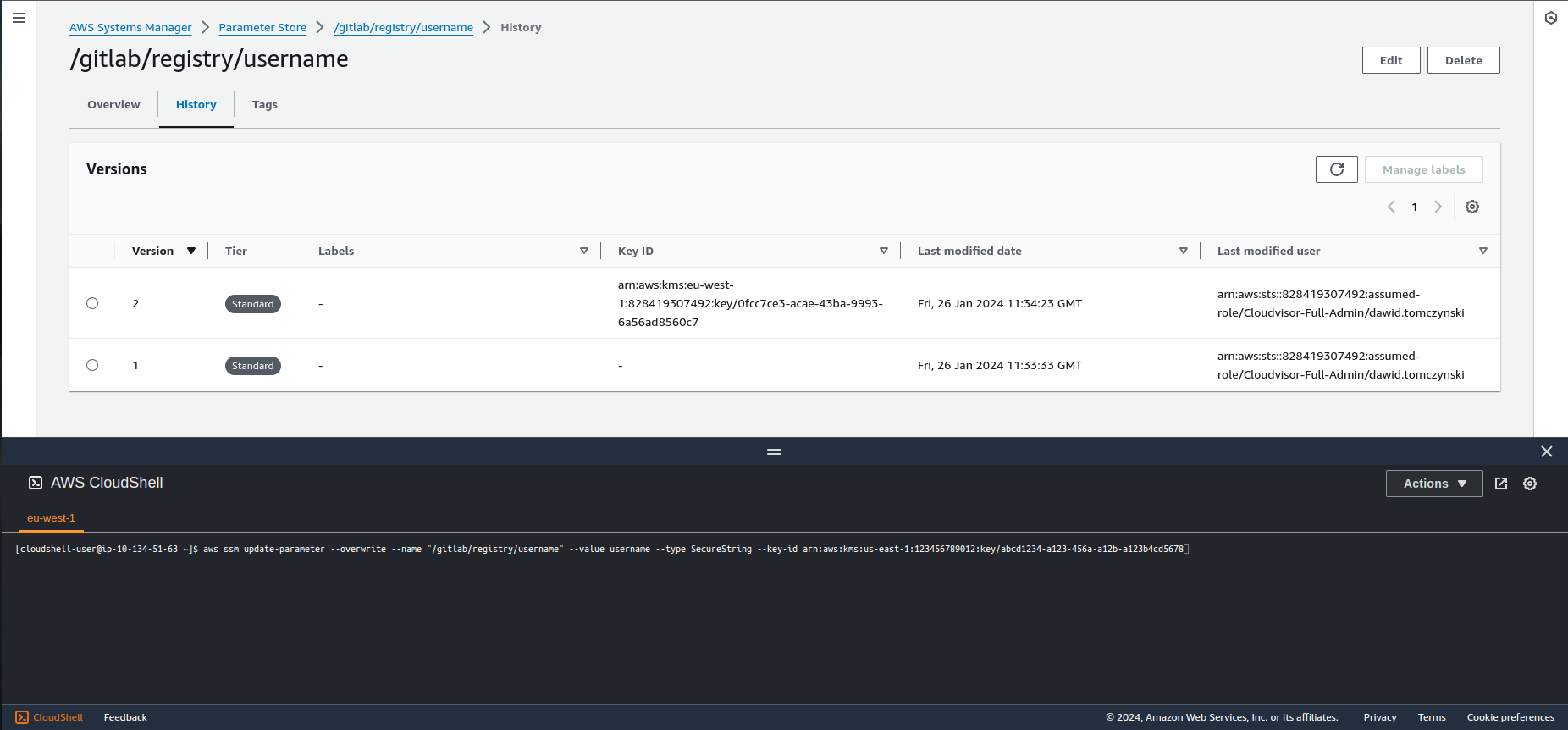
Replace the following placeholders:

* PARAMETER\_NAME: The name of the existing parameter in Systems Manager Parameter Store.
* PARAMETER\_VALUE: The value of the parameter.
* KMS\_KEY\_ARN: The ARN of the default AWS managed SSM KMS Key obtained in Step 1.

Example:

***aws ssm update-parameter --overwrite --name "/gitlab/registry/username" --value username --type SecureString --key-id arn:aws:kms:us-east-1:123456789012:key/abcd1234-a123-456a-a12b-a123b4cd5678***

A new version of the parameter will be created.



1. Verify the update by using the following command:

***aws ssm get-parameter --name “<PARAMETER\_NAME>” --with-decryption***

Replace <PARAMETER\_NAME> with the name of the parameter you just updated. The response should display the decrypted parameter value.

**Note:**

* Make sure you have the necessary IAM permissions to perform these operations.
* Replace placeholder values with your specific parameter name, value, and key ARN.
* Always be cautious while working with sensitive information, and ensure proper access controls and permissions are in place.