# 

**CSWG- Policy As Code Documentation**

Kubernetes Sentinel Policies

4.1.5 Ensure that default service accounts are not actively used.

***Sentinel Policy Name:***

* 4.1.5 Ensure that default service accounts are not actively used

***Category:***

* Kubernetes

***Description of Policy:***

* The default Kubernetes service account should not be used to ensure that rights granted to applications can be more easily audited and reviewed.

***Sentinel Policy Restriction:***

* The default Kubernetes service account should be configured such that it does not provide a service account token and does not have any explicit rights assignments.

***Terraform attributes:***

* + Provider Ref: [kubernetes\_default\_service\_account | Resources | hashicorp/kubernetes | Terraform Registry](https://registry.terraform.io/providers/hashicorp/kubernetes/latest/docs/resources/default_service_account)

***Test cases:***

**Pass cases**

1. For 'google\_compute\_network' ensure that 'automount\_service\_account\_token = false'

"after" : 
"automunt service account token": 
false, 
"metadata" : 
" secret" : 
"timeouts" 
"annotations": null, 
"labels": 
"nane": 
"nanespace": 
[1, 
: null, 
null, 
"default" , 
"terraform -example" , 

**Fail case:**

1. For 'google\_compute\_network' the 'automount\_service\_account\_token' is set to something other than 'false'

"after" : 
"automount serwice account token": true 
n, 
"metadata" : 
"annotations" : 
"labels": 
"name" : 
"namespace" : 
null, 
null, 
"default", 
"terraform•example" , 