Service Level Policy Usage Scenarios for Community Manager

SOA | software™

Copyright

Copyright © 2015 SOA Software, Inc. All rights reserved.

Trademarks

SOA Software, Policy Manager, Portfolio Manager, Repository Manager, Service Manager, Community Manager, SOA Intermediary for Microsoft and SOLA are trademarks of SOA Software, Inc. All other product and company names herein may be trademarks and/or registered trademarks of their registered owners.

SOA Software, Inc.

SOA Software, Inc.
12100 Wilshire Blvd, Suite 1800
Los Angeles, CA 90025
(866) SOA-9876
www.soa.com
info@soa.com

Disclaimer

The information provided in this document is provided "AS IS" WITHOUT ANY WARRANTIES OF ANY KIND INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT OF INTELLECTUAL PROPERTY. SOA Software may make changes to this document at any time without notice. All comparisons, functionalities and measures as related to similar products and services offered by other vendors are based on SOA Software's internal assessment and/or publicly available information of SOA Software and other vendor product features, unless otherwise specifically stated. Reliance by you on these assessments / comparative assessments is to be made solely on your own discretion and at your own risk. The content of this document may be out of date, and SOA Software makes no commitment to update this content. This document may refer to products, programs or services that are not available in your country. Consult your local SOA Software business contact for information regarding the products, programs and services that may be available to you. Applicable law may not allow the exclusion of implied warranties, so the above exclusion may not apply to you.

Contents

Service Level Policy Usage Scenarios (Community Manager-specific) 4
Add / Configure Service Level Policy 4
Scenario 1: How Do I Verify Service Level Policy Alerts at the Service Level? 9
Scenario 2: How Do I Verify Service Level Policy Alerts at the Contract Level? 12
Scenario 3: How Do I Verify Service Level Policy Alerts at the License>Term Level? 15

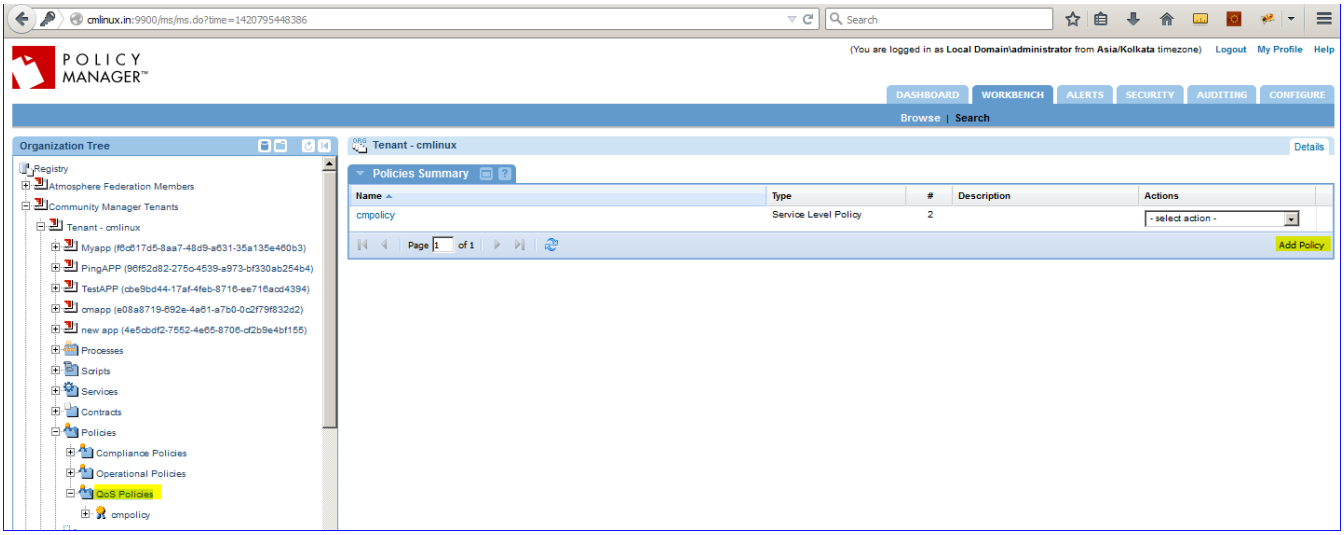
Service Level Policy Usage Scenarios (Community Manager-specific)

This document provides a list of Community Manager-specific usage scenarios for the *Service Level Policy*.

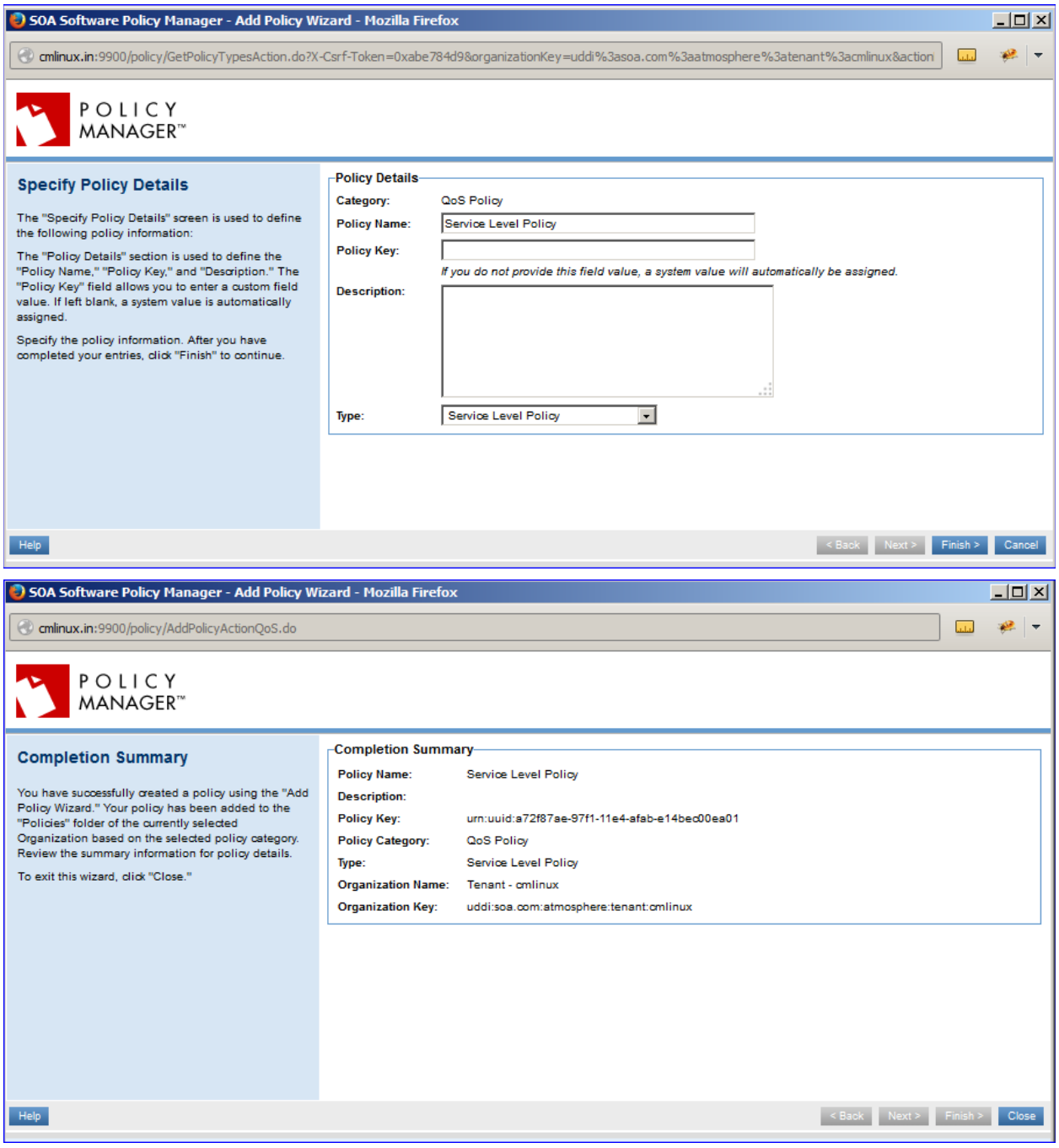
Add / Configure Service Level Policy

If you are using a *Service Level Policy* with Community Manager, the policy must be added to the Community Manager **Tenant** Organization for it to be available in the Community Manager UI.

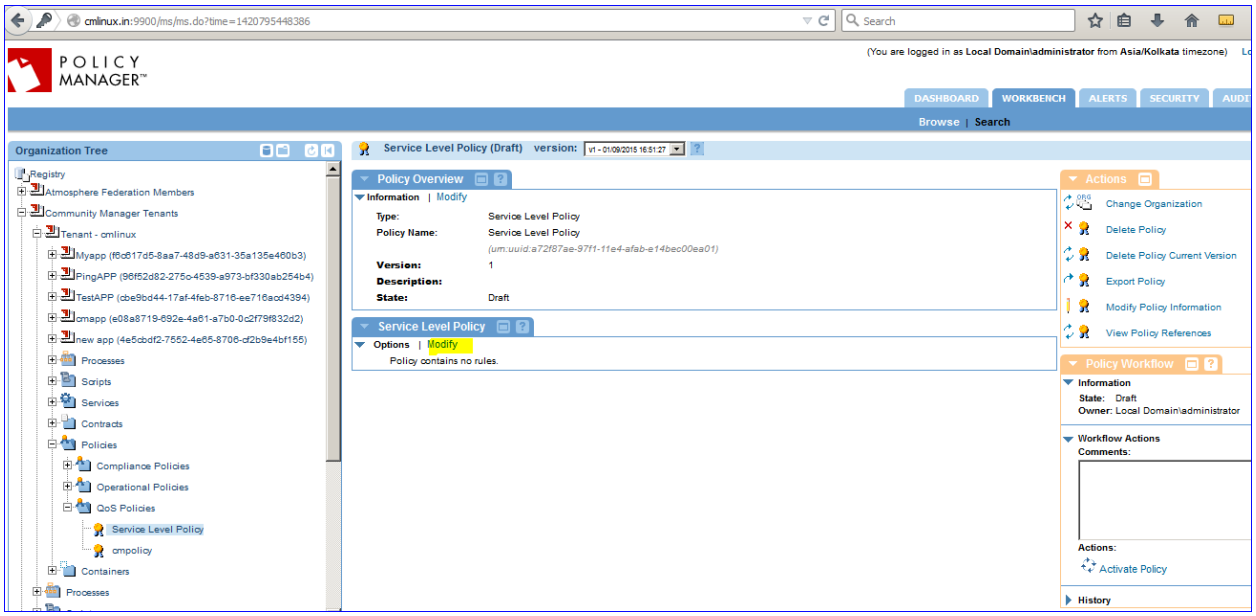
1 Go to the *Policy Manager Management Console > Tenant Organization > Policies > QoS Policies* and click **Add Policy**.



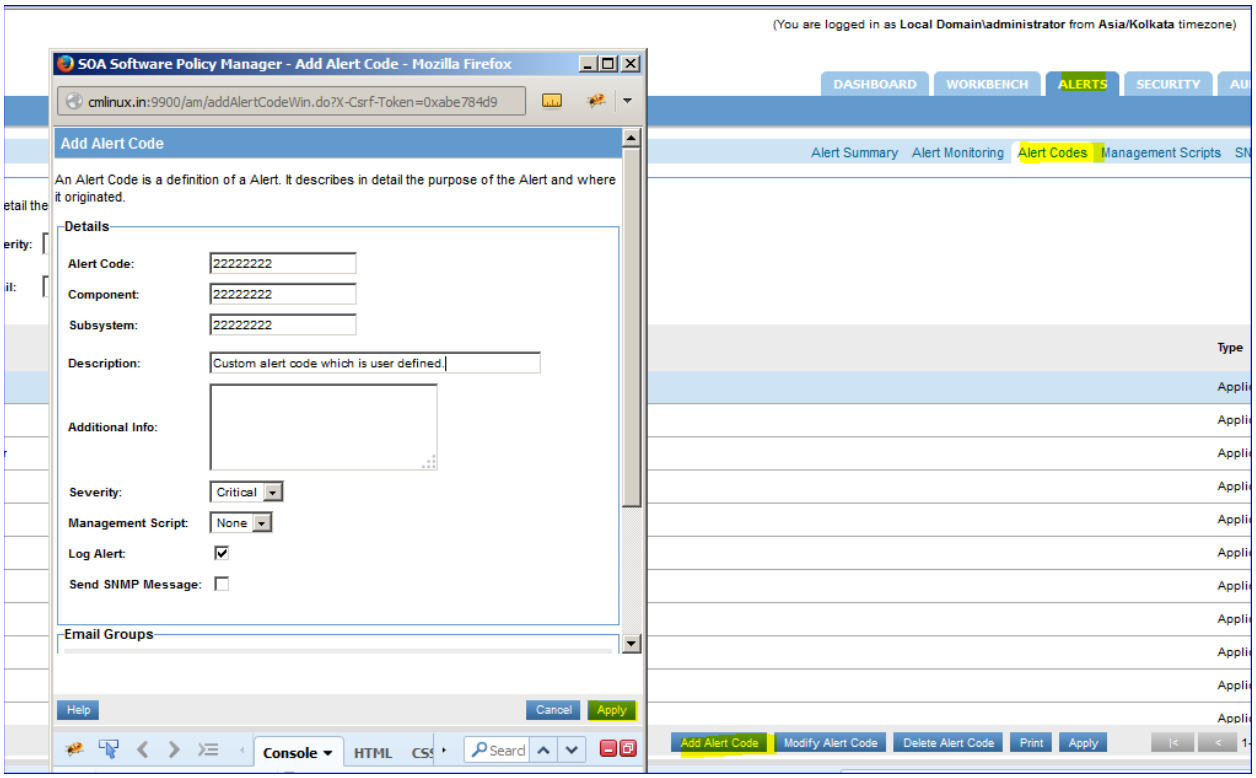
2 Specify Policy Name, Policy Type (Service Level Policy), click **Finish**, and then **Close**.



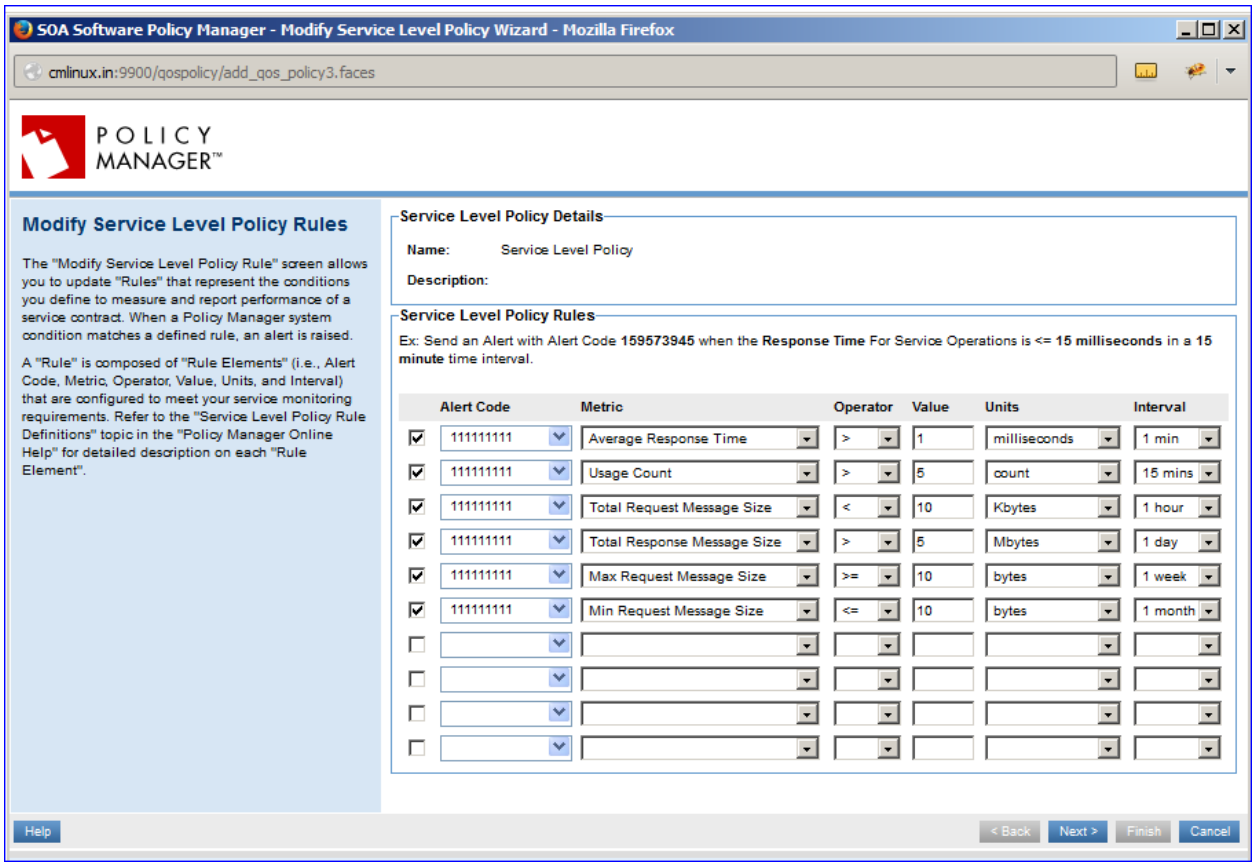
3 On the *Service Level Policy Details* screen, click **Modify**.



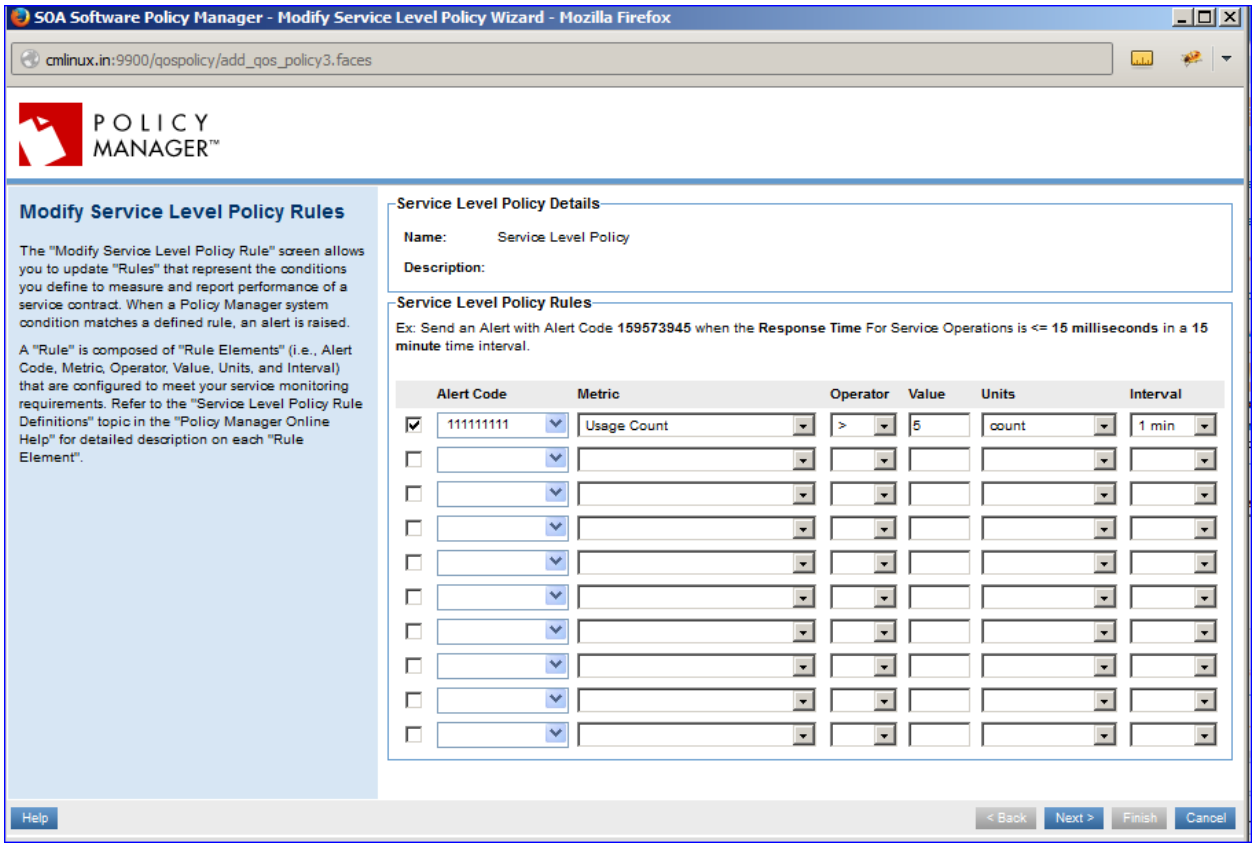
Note: You can use custom defined alert codes or predefined Policy Manager alert codes when configuring the Service Level Policy. You can add a custom alert code in the *Alerts > Alert Codes* section as illustrated below:



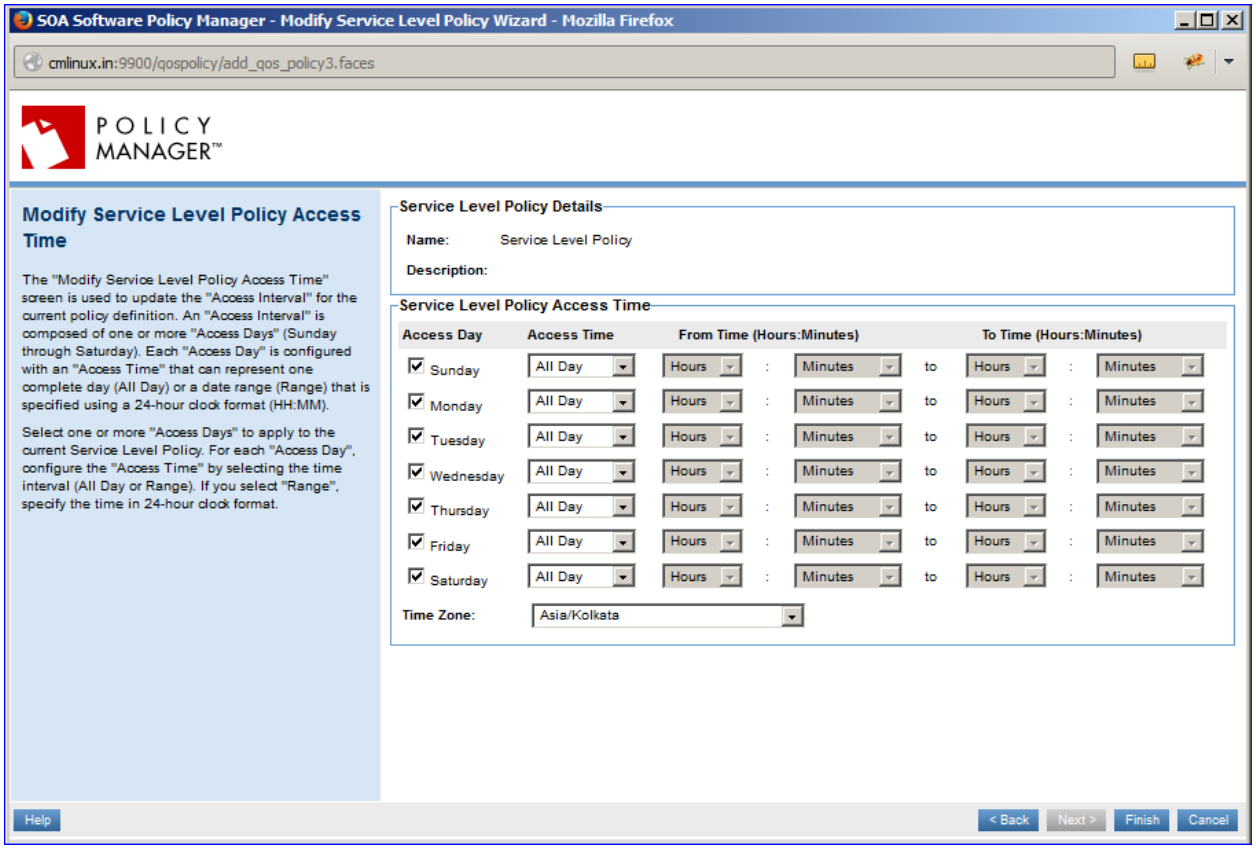
4 Below are the metrics which are available for *Service Level Policy* configuration. You can configure the metrics based on your requirement.

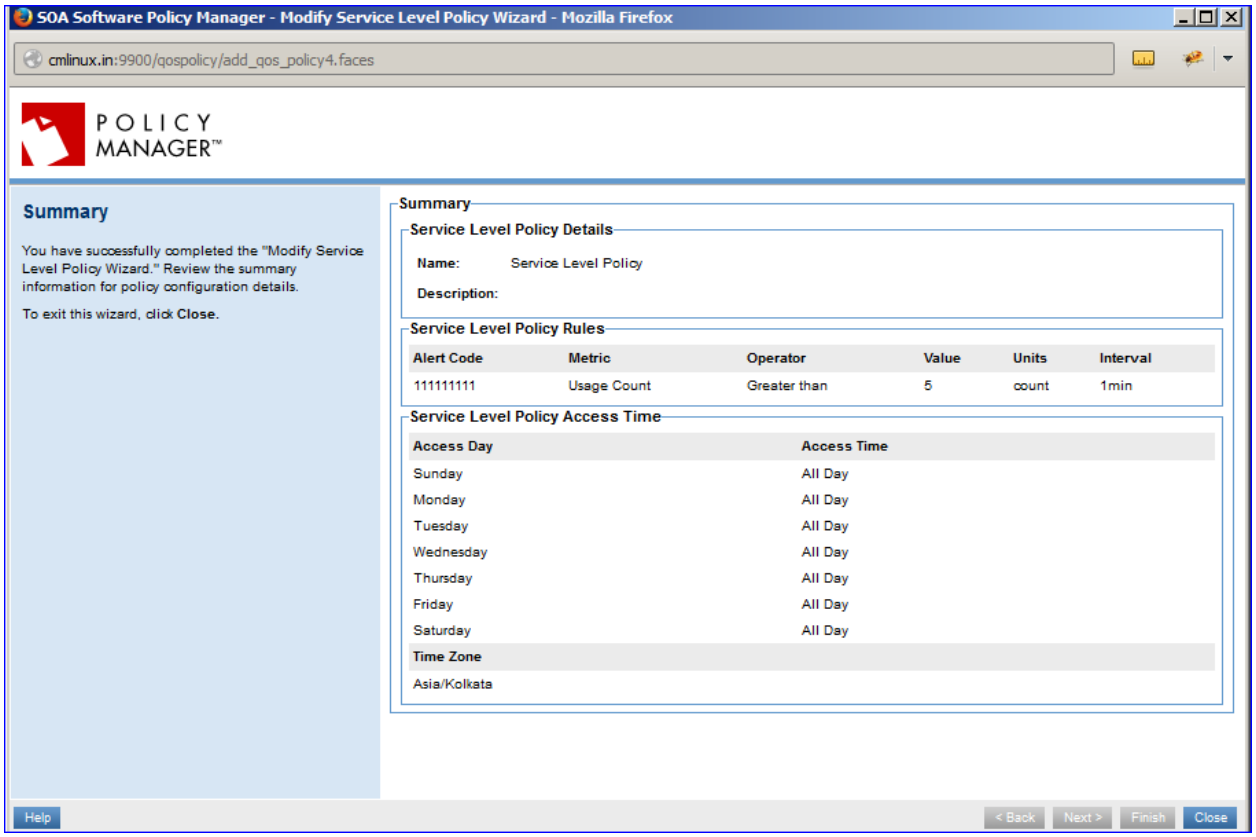


5 For example, we will use the Usage Count metric in the use case below. Click **Next** to continue.

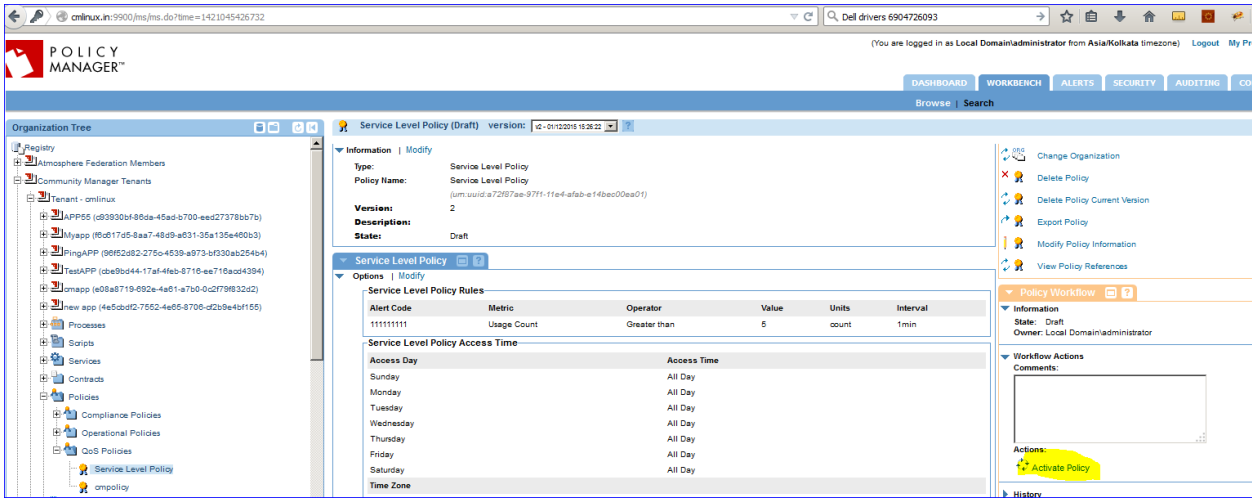


6 Configure Access Day and Access Time, click **Finish** and **Close**.





7 If you are using Policy Manager 7.2 (or above), activate the policy. Otherwise skip this step.



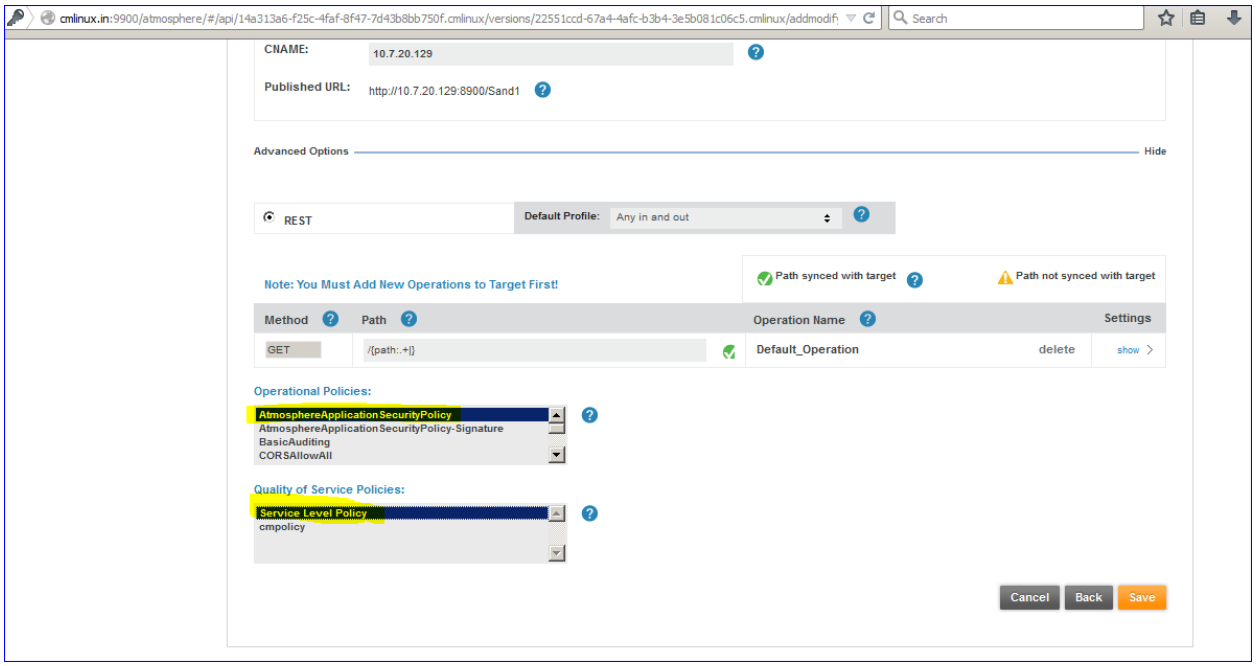
Scenario 1: How Do I Verify Service Level Policy Alerts at the Service Level?

1 Launch *Community Manager*.

2 Go to *API Details > Edit API > Proxy Section > Advanced Options* and attach the following policies:

a) In *Quality of Service Policies* section, attach *Service Level Policy*.

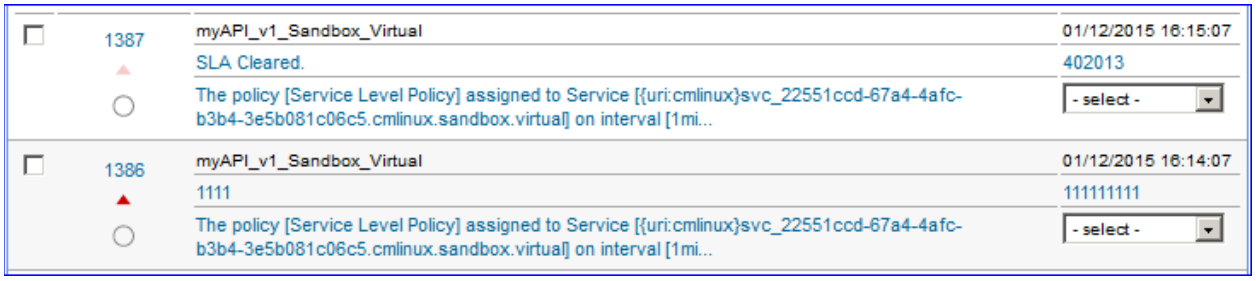
b) In *Operational Policies* section, attach *Atmosphere Application Security Policy (No Signature)* and *Detailed Auditing*.



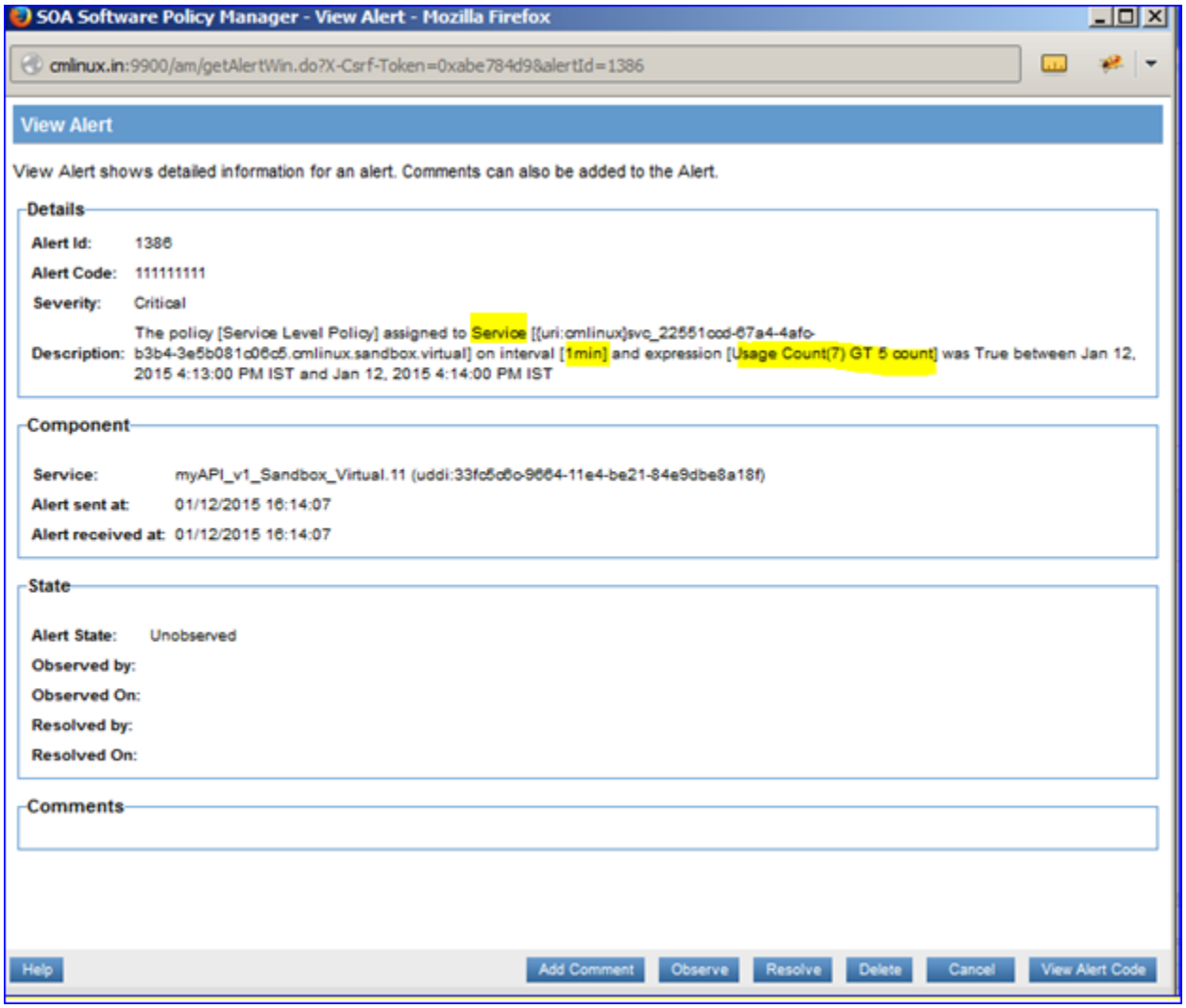
3 Go to the APP which is connected with above API (i.e., APP > DEV CONSOLE) and send more than 5 requests.

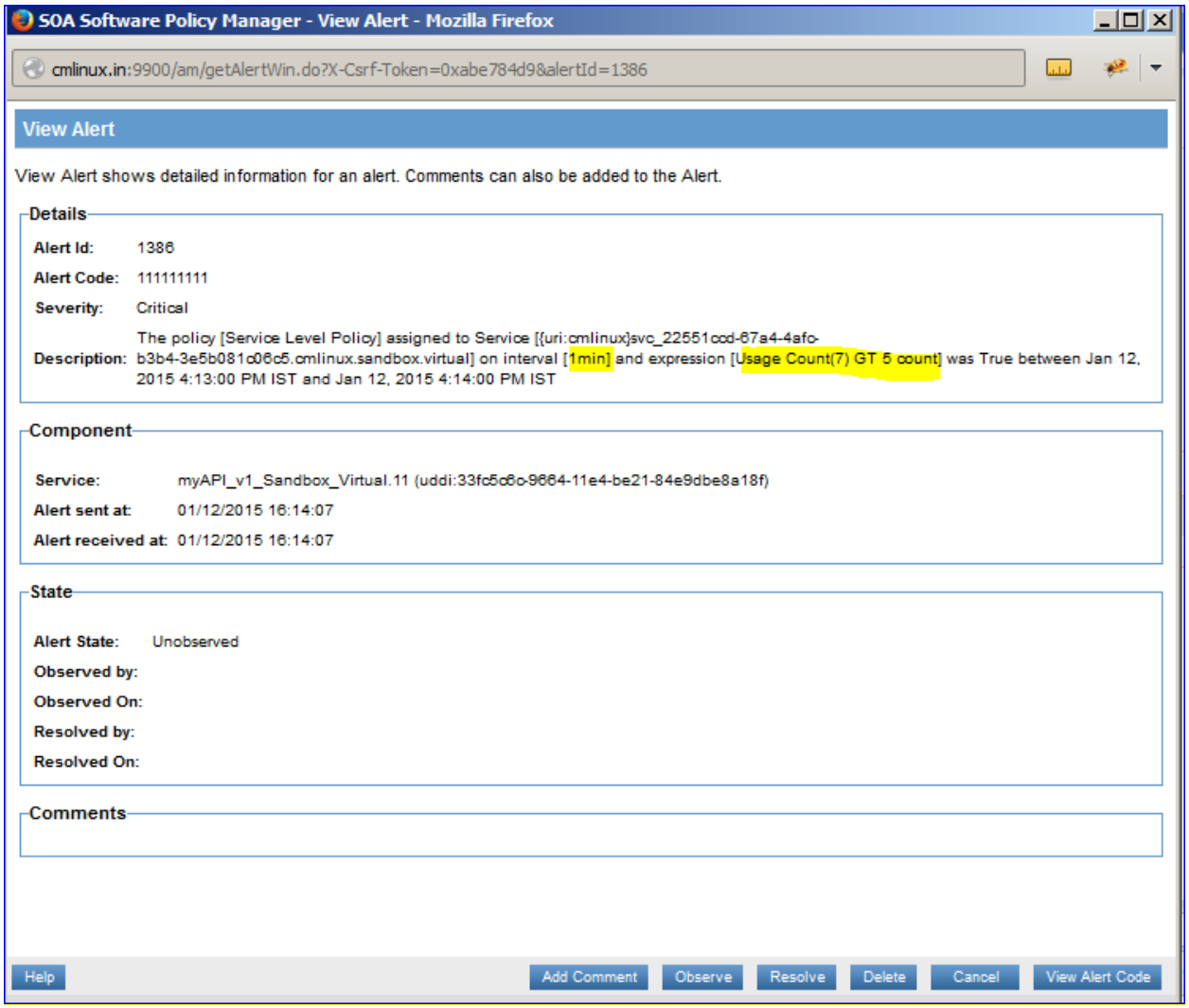
a) When a Policy condition matches a defined rule, an alert is raised as below in *Policy Manager* > *Registry* Level.

Note: These alerts are not supported in Community Manager *Dashboard*.



4 Select View Alert and review the alerts.


SOA Software Policy Manager - View Alert - Mozilla Firefox
cmlinux.in:9900/am/getAlertWin.do?X-Csrf-Token=0xabe784d9&alertId=1386
View Alert
View Alert shows detailed information for an alert. Comments can also be added to the Alert.
Details
Alert Id: 1386
Alert Code: 111111111
Severity: Critical
Description: The policy [Service Level Policy] assigned to Service [{uri:cmlinux}svc_22551ccd-67a4-4afc-b3b4-3e5b081c06c5.cmlinux.sandbox.virtual] on interval [1min] and expression [Usage Count(7) GT 5 count] was True between Jan 12, 2015 4:13:00 PM IST and Jan 12, 2015 4:14:00 PM IST
Component
Service: myAPI_v1_Sandbox_Virtual.11 (uddi:33fc5c6c-9664-11e4-be21-84e9dbe8a18f)
Alert sent at: 01/12/2015 16:14:07
Alert received at: 01/12/2015 16:14:07
State
Alert State: Unobserved
Observed by:
Observed On:
Resolved by:
Resolved On:
Comments
Help
Add Comment
Observe
Resolve
Delete
Cancel
View Alert Code



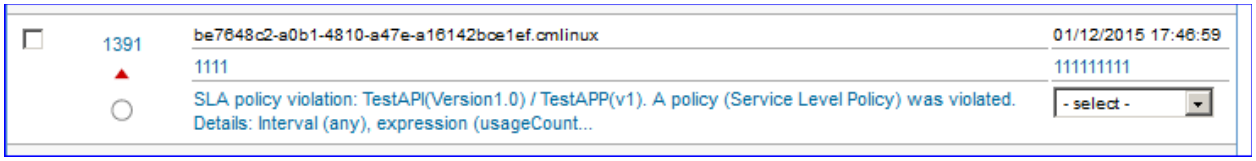
Scenario 2: How Do I Verify Service Level Policy Alerts at the Contract Level?

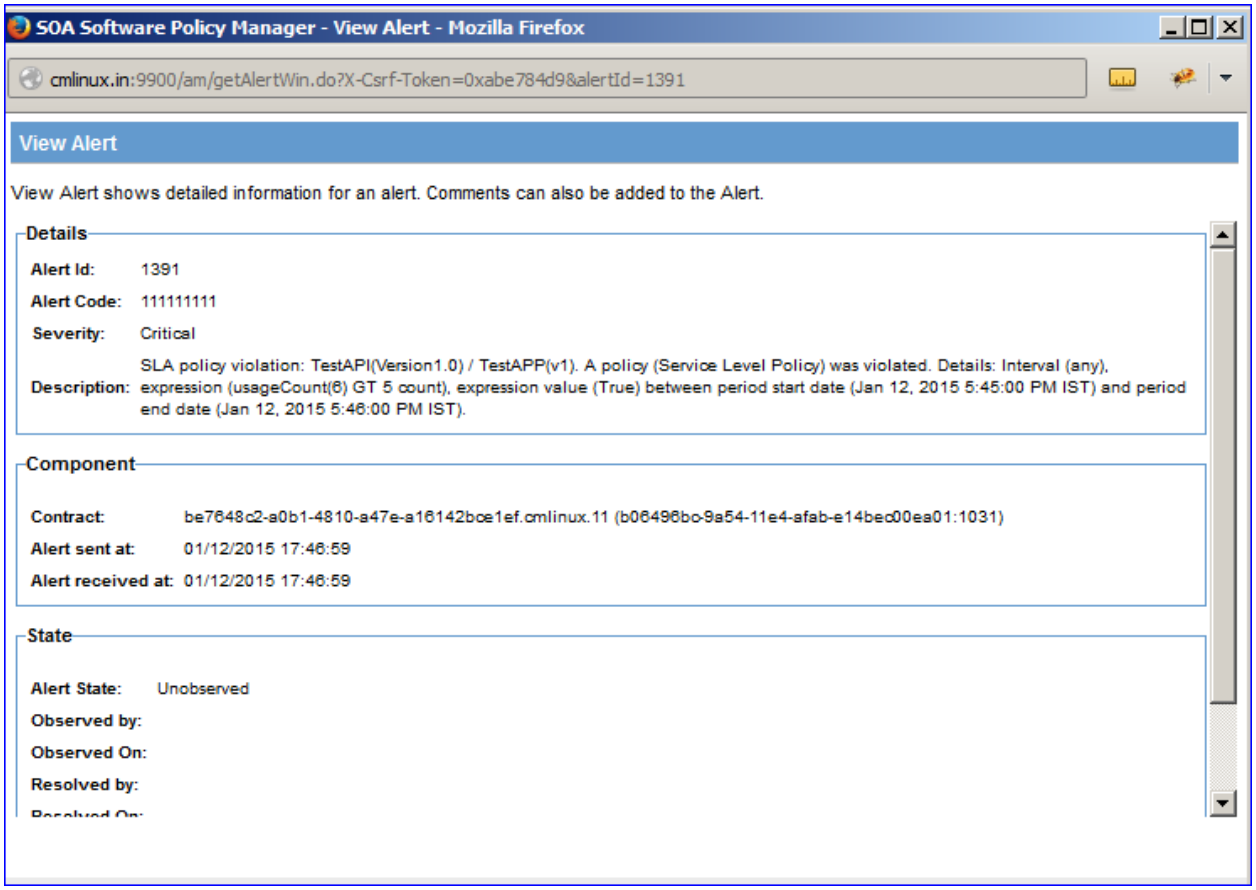
While requesting API Access, select the Service Level Policy checkbox and finish the process. Make sure the contract is activated.

Note: This scenario assumes that the *Atmosphere Application Security Policy* is attached to this API.

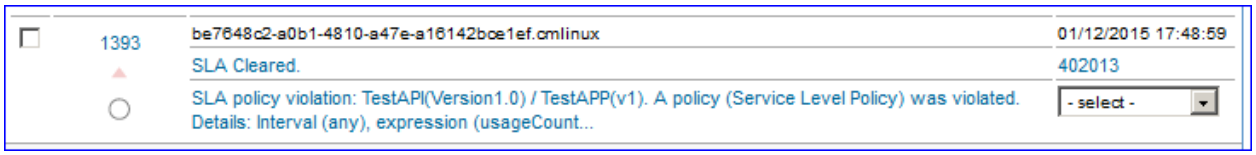
1 Go to *APP > DEV CONSOLE* and send more than 5 requests.

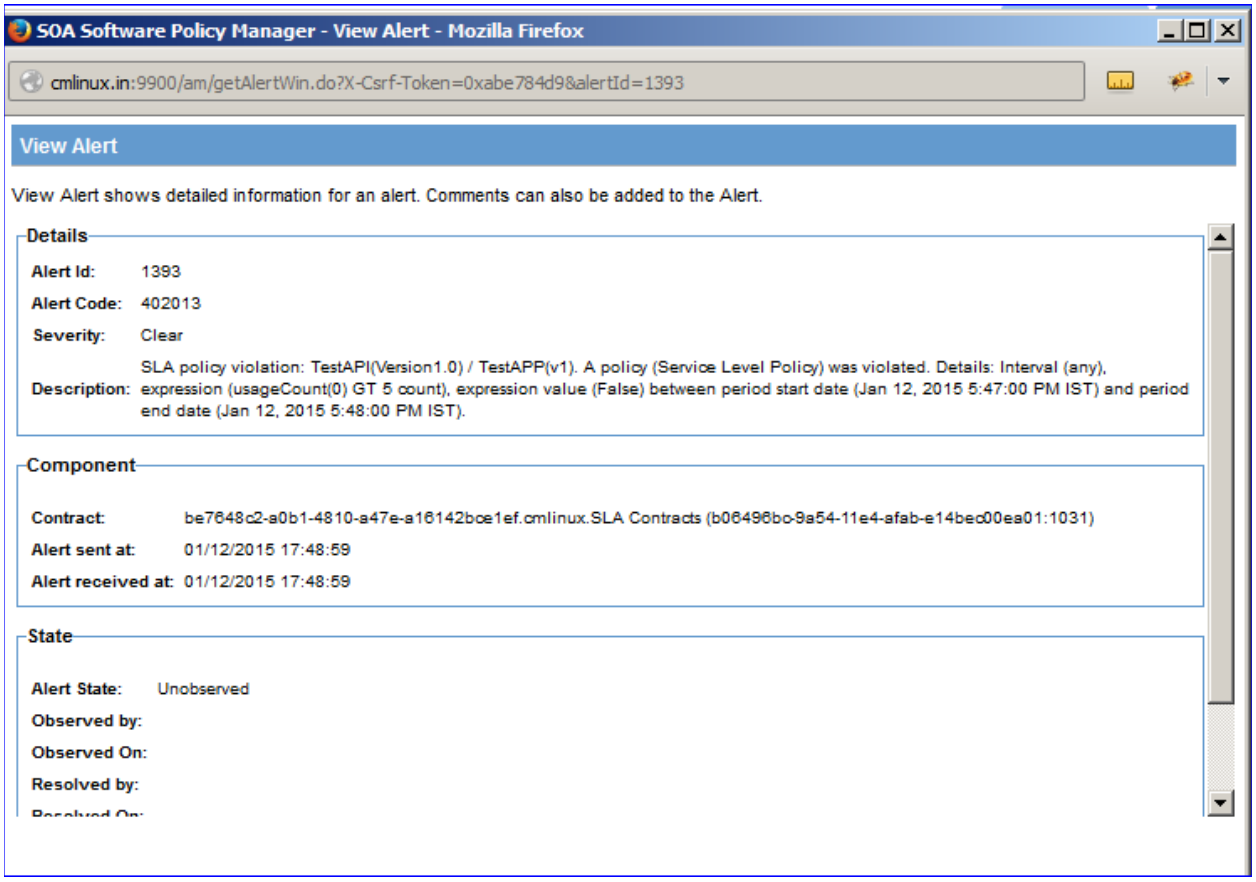
a) When a Policy condition matches a defined rule, an alert is raised in the *Policy Manager > Registry* level.





b) After a 1 min interval the SLA will be cleared.



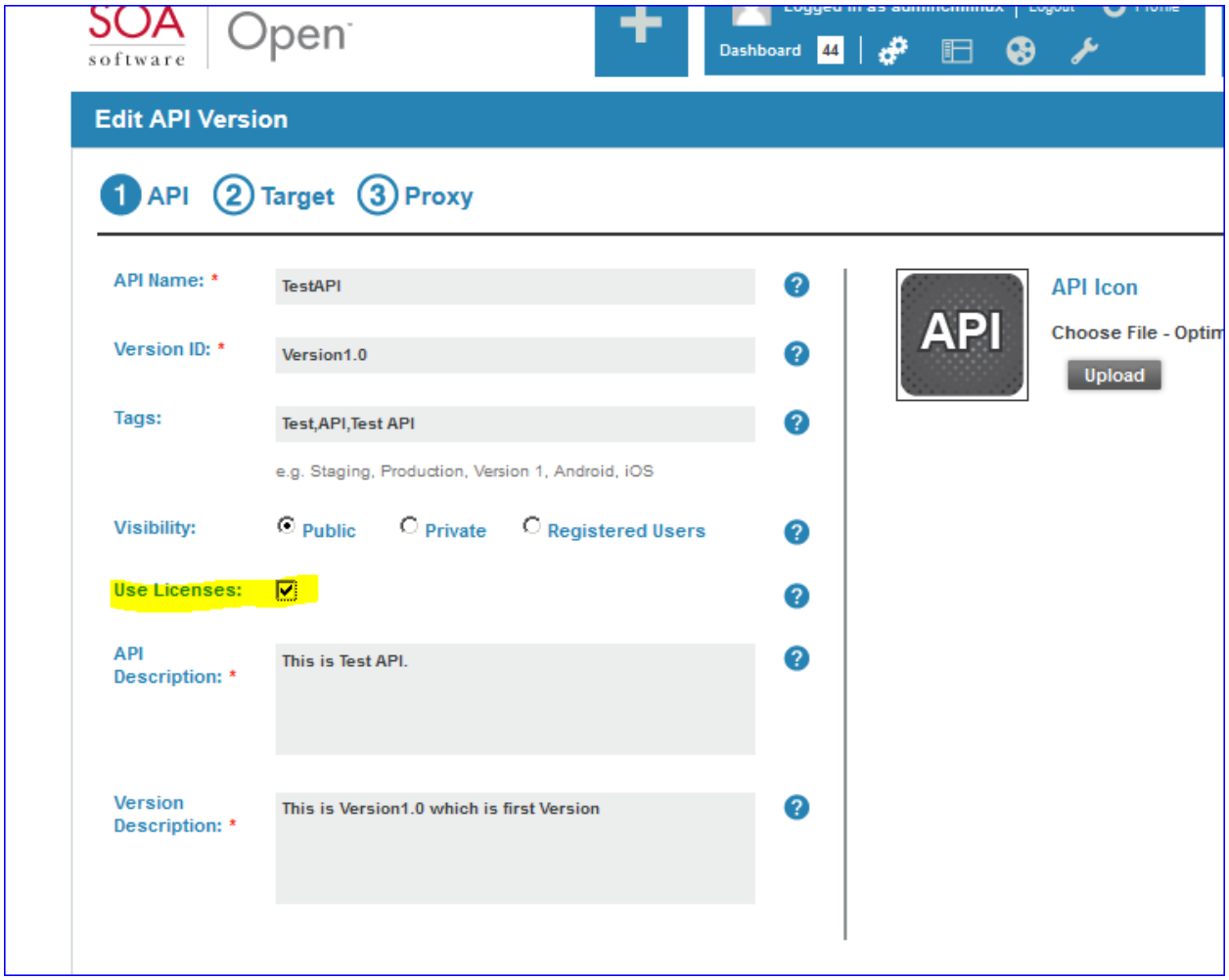


c) Alert in Community Manager *Dashboard*.

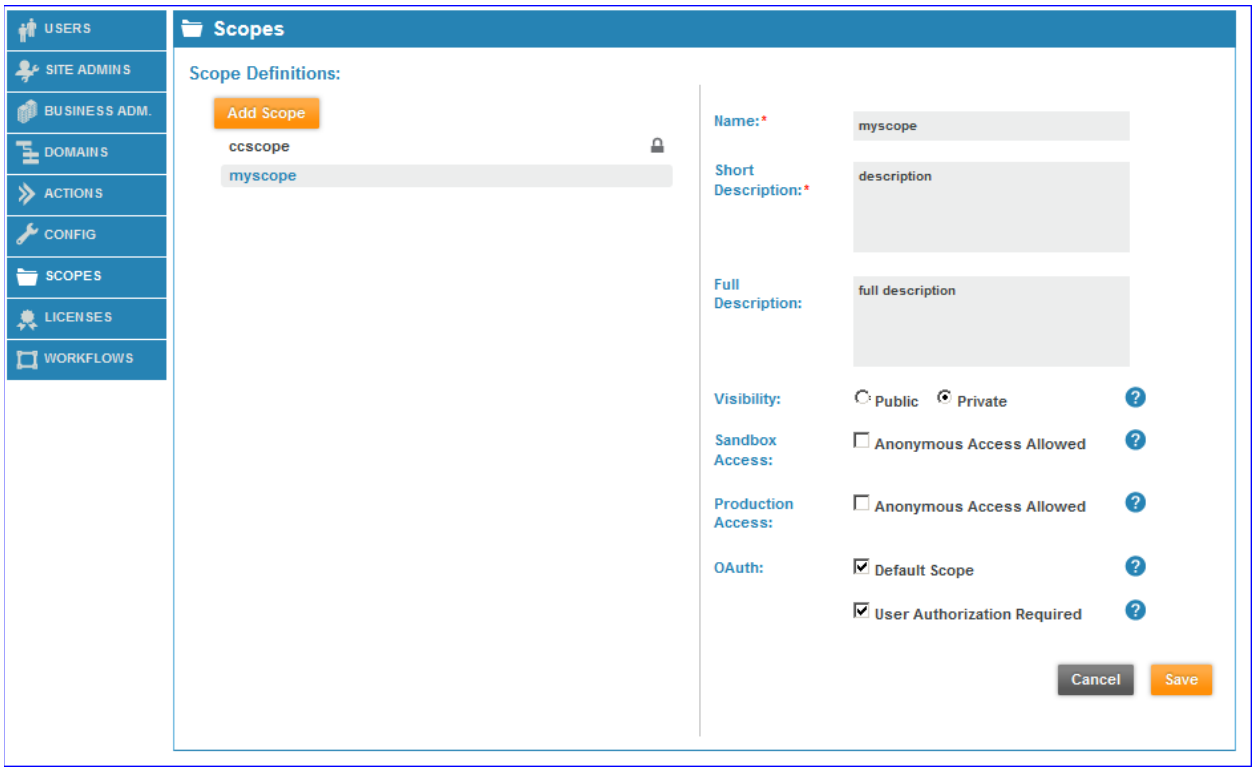
Scenario 3: How Do I Verify Service Level Policy Alerts at the License>Term Level?

1 Launch *Community Manager*.

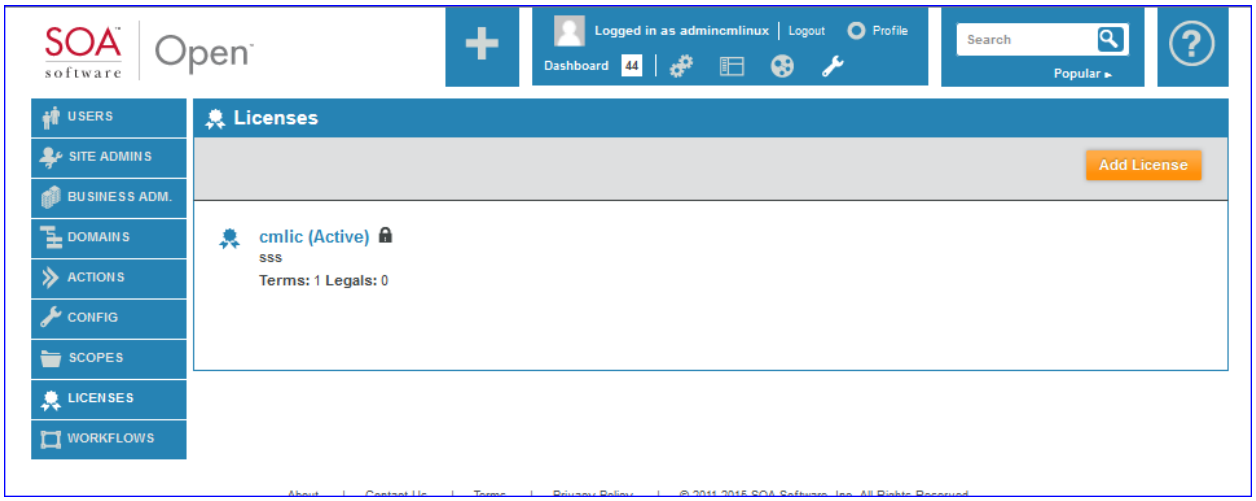
2 While adding an API, select the **Use Licenses** check box.



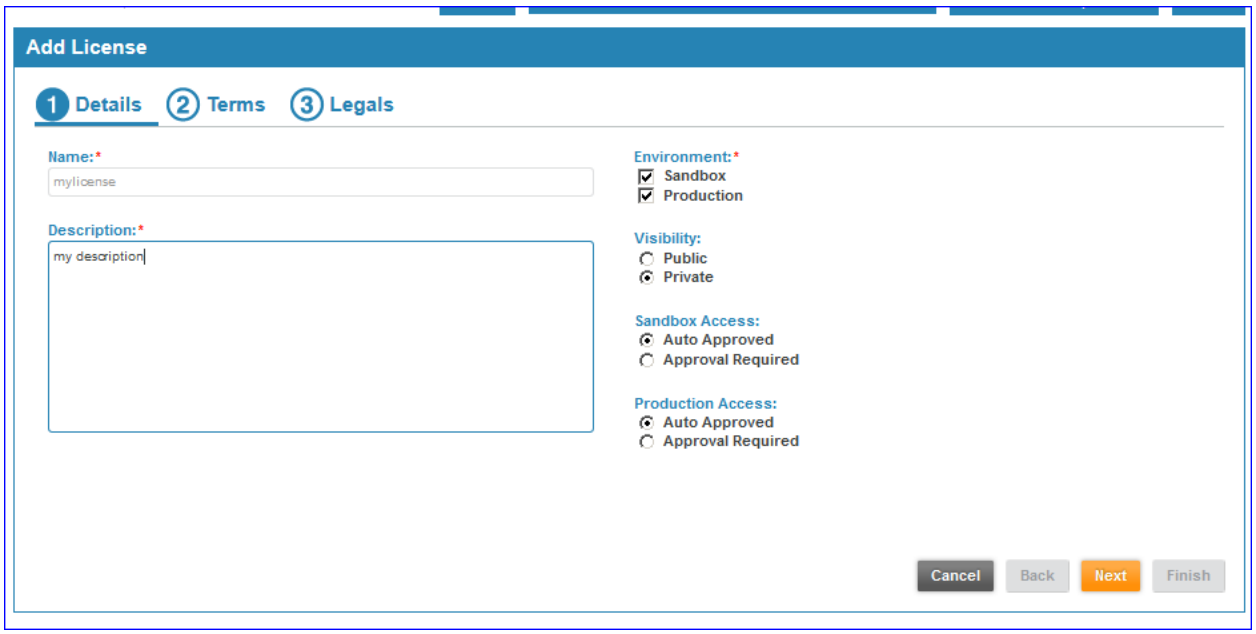
3 Go to *Site Administration* > *Scopes* and click **Add Scope**. Provide details based on your requirement and **Save**.



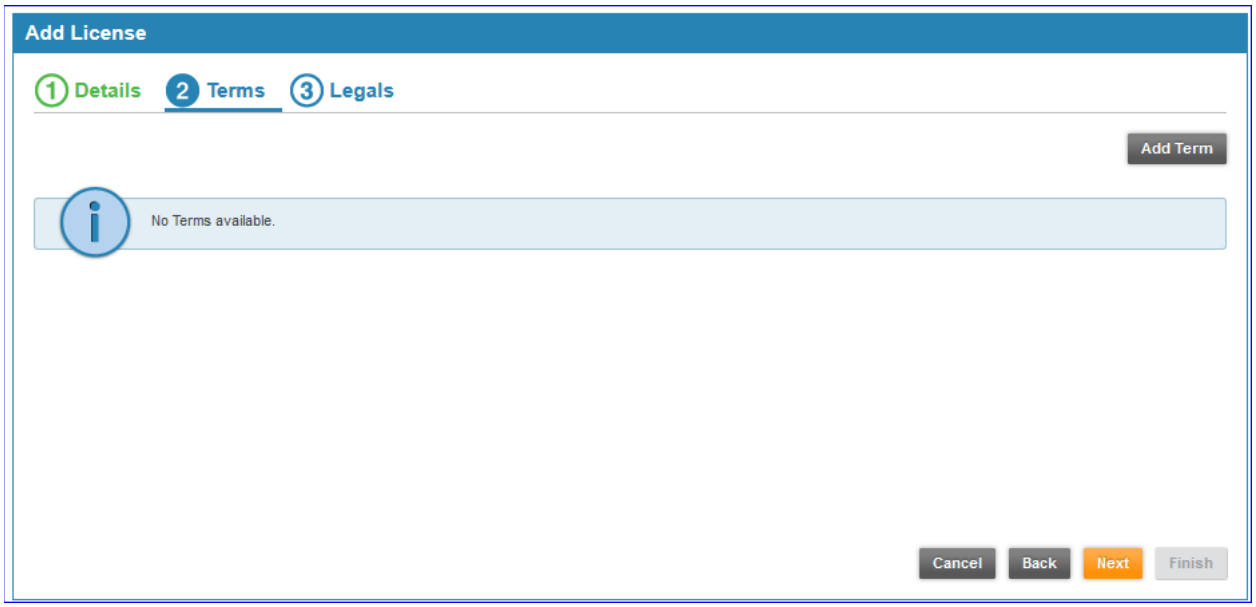
4 Go to *Licenses* and click **Add License**.



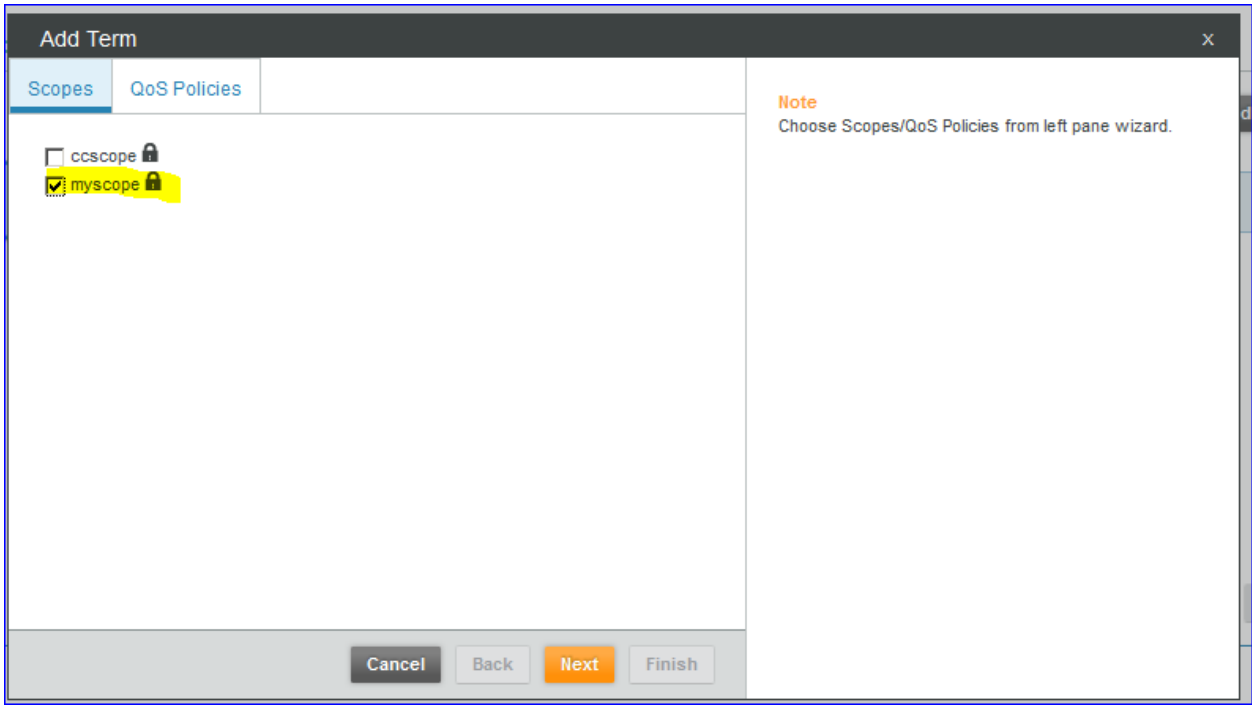
5 Provide details based on your requirements and click **Next**.



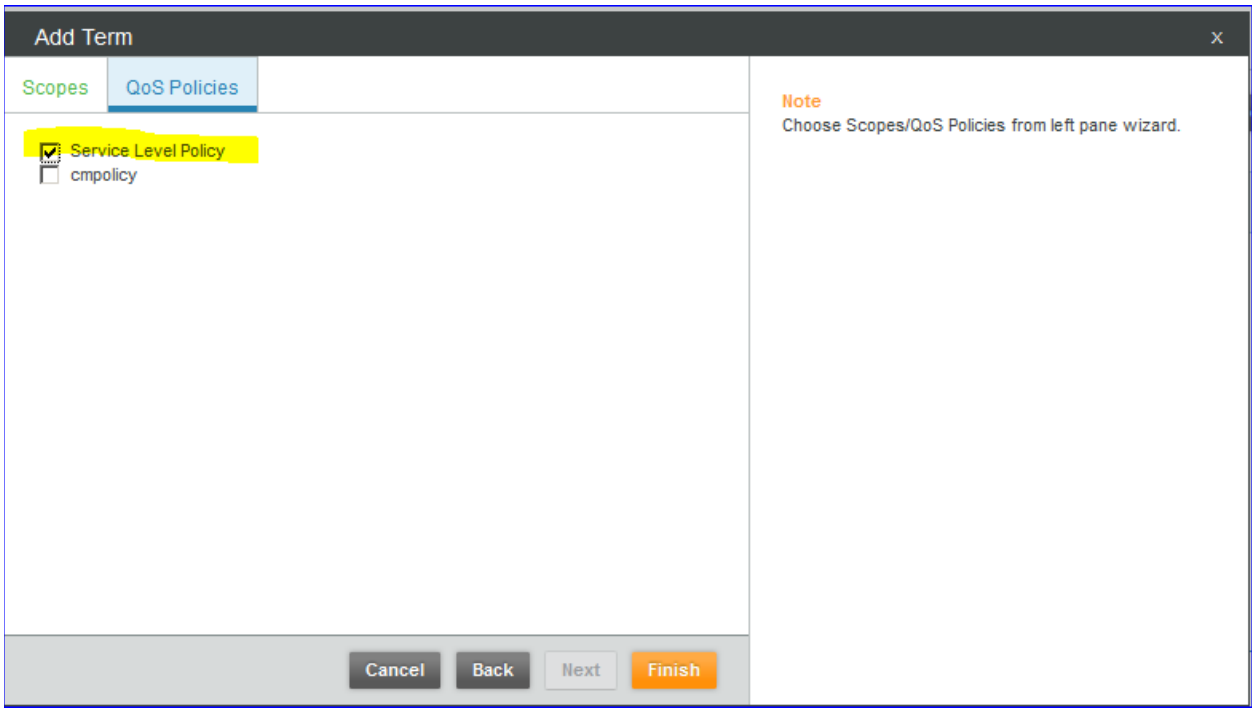
6 Click **Add Term**.



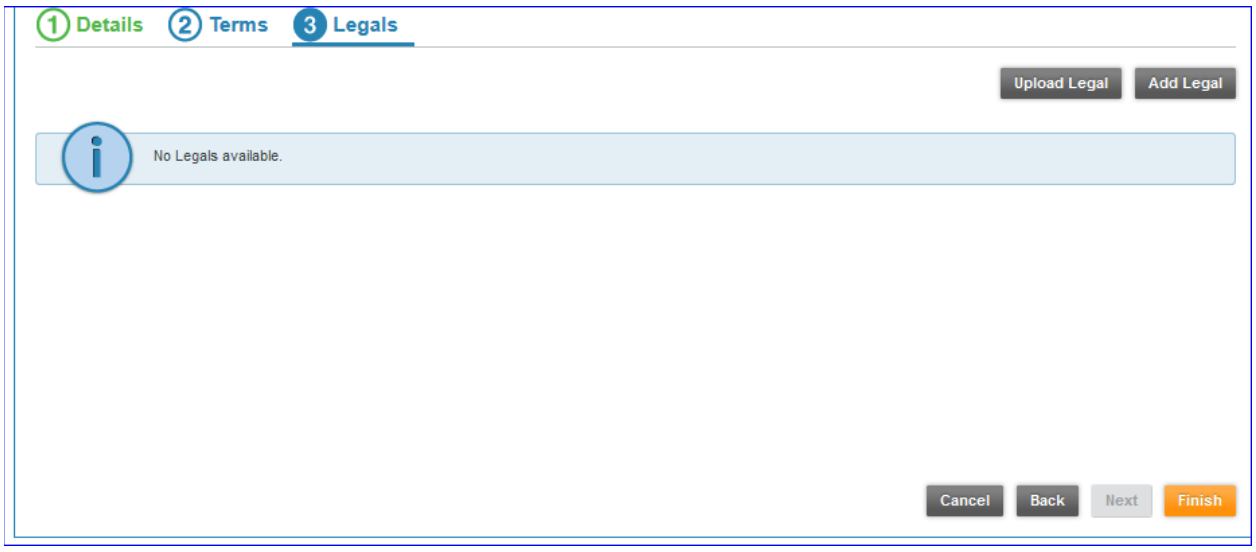
7 Select Scope and click **Next**.



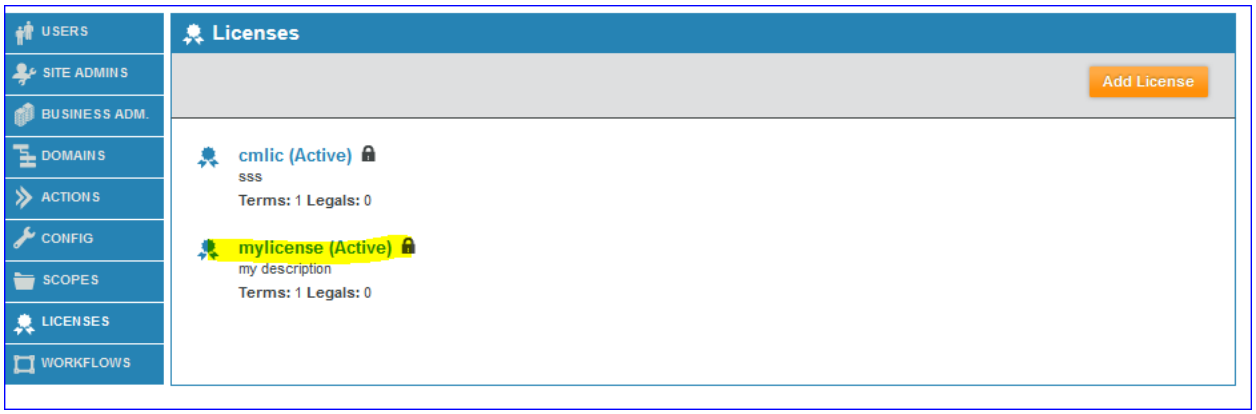
8 Attach *QoS Policies > Service Level Policy* at the *Terms* level, and click **Next**.



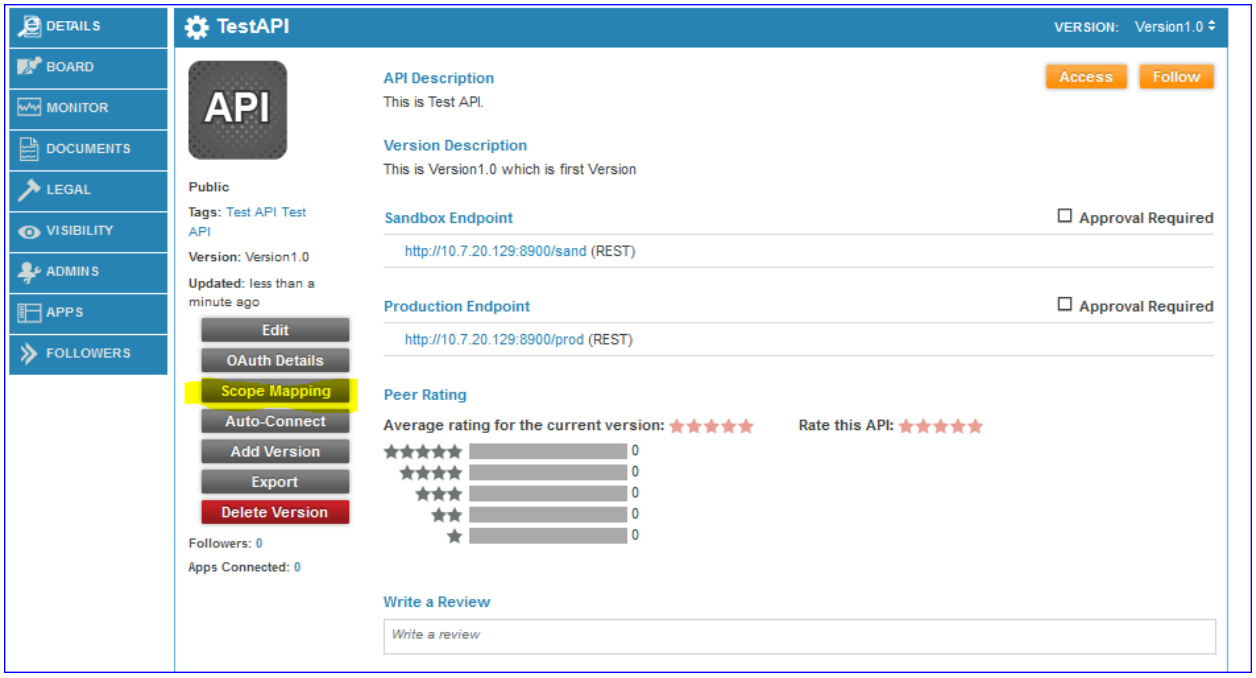
9 Upload *Legals* (if required) and click **Finish**.



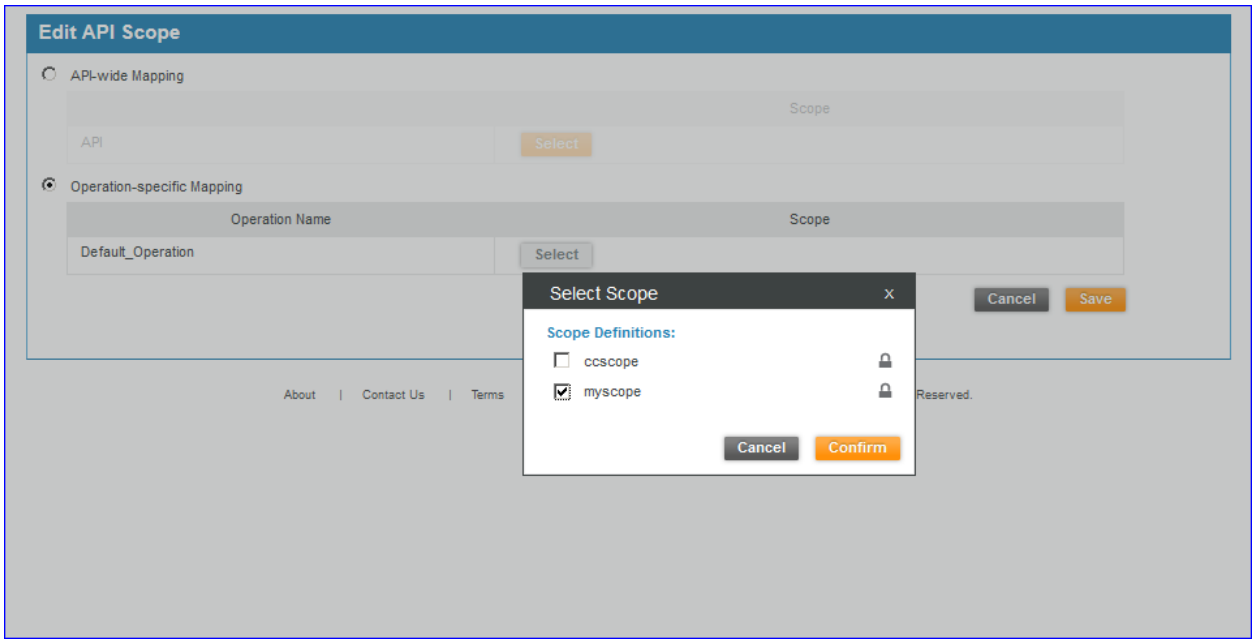
10 The license is now configured with the QoS Policy attachment at the *Terms* Level.



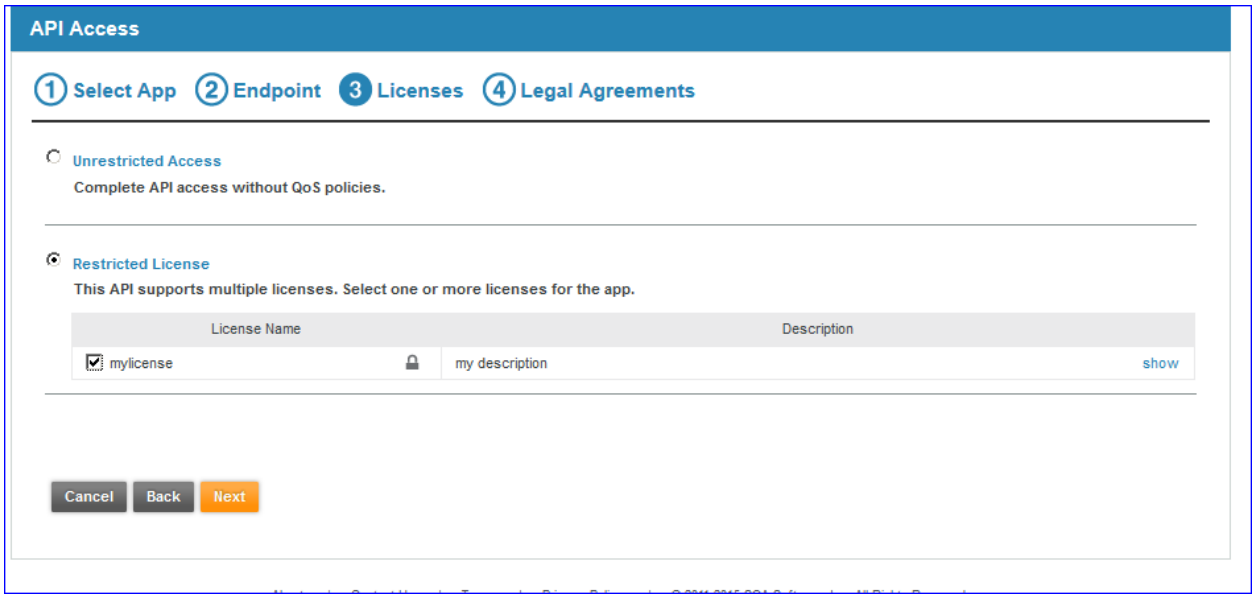
11 Next we have to use this scope in *API > Scope Mapping*. Go to *API* and click **Scope Mapping**.



12 You can map your scope at Operation level or at API level. Select **Scope**, then **Confirm** and **Save** changes.



13 Now request API Access for this API. While requesting API access, select licence that is attached to the QoS Policy at the *Terms* level.



14 Next, go to the *DEV CONSOLE* and send more that 5 requests to meet the defined *Service Level Policy* rule.

a) The following alert will display in the Community Manager *Dashboard*.

Dashboard
API
TestAPI
SLA policy (license term) violation: TestAPI(Version1.0) / TestAPP(v1)
SLA policy violation: TestAPI(Version1.0) / TestAPP(v1). A policy (Service Level Policy) was violated. Details: Interval (any), expression (usageCount(6) GT 5 count), expression value (True) between period start date (Jan 13, 2015 1:16:00 PM IST) and period end date (Jan 13, 2015 1:17:00 PM IST).
x
cmlinux
Priority: Critical
Environment: Sandbox
1/13/2015 1:19 PM
SLA policy violation cleared.
cmlinux 1/13/2015 1:19 PM
Write a comment