



FORUM SENTRY™ VERSION 9

OAUTH CLIENT CONFIGURATION GUIDE

Legal Marks

No portion of this document may be reproduced or copied in any form, or by any means – graphic, electronic, or mechanical, including photocopying, taping, recording, or information retrieval system – without expressed permission from Forum Systems, Inc.

FORUMOS™ Firmware, Forum Systems XMLSec™ WebAdmin, Forum Systems XML Security Appliance™, Forum Sentry™, Forum Presidio™, Forum XWall™, Forum Sentry™ Web Services Gateway, Forum Presidio™ OpenPGP Gateway, Forum FIA Gateway™, Forum XWall Type-PCI™, Forum XWall® Web Services Firewall and Forum XRay™ are trademarks and registered trademarks of Forum Systems, Inc.

All other products are trademarks or registered trademarks of their respective companies.

Copyright © 2002-2024 Forum Systems, Inc. – All Rights Reserved.

Forum Sentry™ Version 9 OAuth Client Configuration Guide, published May 2024.

D-ASF-SE-017828

Table of Contents

INTRODUCTION TO THE OAUTH CLIENT CONFIGURATION GUIDE	1
Audience for the OAuth Client Configuration Guide	1
1.0 OAuth Overview	2
2.0 A Simple Example of OAuth	2
3.0 Forum Sentry as an OAuth client in a OAuth with Single-Sign On use case	4
3.1 Use case without a Forum Sentry API Security Gateway	4
3.2 Use case with a Forum Sentry API Security Gateway	5
3.3 Configuring Forum Sentry as an OAuth Client with Grant Type: Auth Code	6
3.3.1 Registering Forum Sentry with an OAuth Service Provider	7
3.3.2 Configuring Forum Sentry Policies as an OAuth client	16
3.3.3 Testing Forum Sentry OAuth client	35
4.0 Forum Sentry as an OAuth Server with LDAP use case	38
4.1 Use case without a Forum Sentry OAuth Server.....	38
4.2 Use case with a Forum Sentry OAuth Server.....	40
4.3 Configuring Forum Sentry as an OAuth Server with Grant Type: Auth Code	42
4.3.2 Configuring Forum Sentry Policies as an OAuth client	59
4.3.3 Testing Forum Sentry OAuth server.....	75

INTRODUCTION TO THE OAUTH CLIENT CONFIGURATION GUIDE

Audience for the OAuth Client Configuration Guide

The *Forum Systems Sentry™ OAuth Client Configuration Guide* is for System Administrators who will manage access control and:

- Use Protocol or message Tokens
- Use SOAP WS-Security headers.
- Use SAML Assertions.
- Integration with IdP (Identity Providers)
- Provide SSO using OAuth
- Generate OAuth Tokens
- Consume OAuth Tokens
- Federate OAuth Tokens

Conventions Used in the OAuth Client Configuration Guide

A red asterisk (*) aligned with a field term means that this field is required. In this and other documentation, the Web Administration Interface is referred to as the WebAdmin and the Forum XML Security Appliance™ is referred to as the 'device', 'product' or 'system'.

In this document, all data or commands that must be entered or selected are displayed in boldface. Example:

User name: **johnsmith**
Password: *********

UI screens which display a STATUS column represent the following states:

- Green status light = enabled policy.
- Yellow status light = a required functional element of this policy is disabled.
- Red status light = disabled policy.

Throughout this and other documents in the Documentation Set, repetitive actions such as:

- View / edit a policy.
- Enable / disable a policy.
- Delete a policy.
- Rename a policy.
- Limit display of policies with Search or Max Results fields.

are not shown. For more information, refer to the Common Operations section of the *Forum Systems Sentry™ Version 9 Web-based Administration Guide*.

Any specifications and constraints referenced in this volume appear in the Appendices of this volume.

1.0 OAuth Overview

The basic model of authentication and authorization over the internet is based on the traditional client-server model. In this model, at a minimum, there are two entities involved: the client and the application running on the server. A client with valid credentials is granted access to a particular resource controlled by the application. The client credentials may be in the form of a username/password that the application validates before granting access to the resource.

This basic model of authentication has evolved overtime as a result of the need for the client to provide its credentials (e.g. username/password) only once in order to be granted access to resources that are controlled by multiple applications in a distributed environment. This model is often referred to as Single Sign-On (SSO). In this model, the client “logs in” only once by providing its credentials to a single application. Upon validation by the application, the client receives a ticket (cookie) that enables it to seamlessly access resources of other applications. An example of SSO is a user logging into Amazon.com only once and accessing resources on multiple third-party applications without having to login to each individual application.

The increased popularity of social media apps, mobile apps and cloud services has led to another authentication and authorization model. The new model is based on the OAuth standard. In this model, at least three entities are involved: the user, the client application/service and the service provider. This is referred to as the three-legged OAuth model. The user is the owner of the resource and it grants client application access to its resources that are controlled by the service provider. OAuth standard enables the user to grant client application access to its resources without ever sharing its username/password with the client application.

2.0 A Simple Example of OAuth

Traditionally, social media applications have been the main drivers behind OAuth deployment. In the past, web applications such as news media sites would maintain their own user profile data by providing the option to each of its users to create custom profile on the site for better user experience. This approach had many shortcomings for both users and media sites:

- Users had to provide email or username and password for each site during the initial creation of a profile.
- Users would often forget their passwords during the login process since they had created multiple profiles at different sites.
- Media sites were now responsible for securing their users' emails and passwords from hackers.
- Users would often create fake profiles that would provide inaccurate tracking data to media sites.

Over time, social media sites such as Facebook, Twitter, LinkedIn, and Google have become the defacto repositories of a user's social identity or profile. The availability of existing social identities with rich profile data provided an opportunity for news media sites to access user data outside their domain of control. OAuth is the standard that enables websites to access user profile data outside their domain of control without requiring users to give their username and password to the site.

Figure 1 illustrates a simple example that leverages OAuth. To create a better user experience for their visitors, websites (client application) provide the ability for users (resource owner) to post comments on articles with their Facebook account. This ability allows Facebook profile attributes such as: name, photo, and location to be displayed when they post a comment.

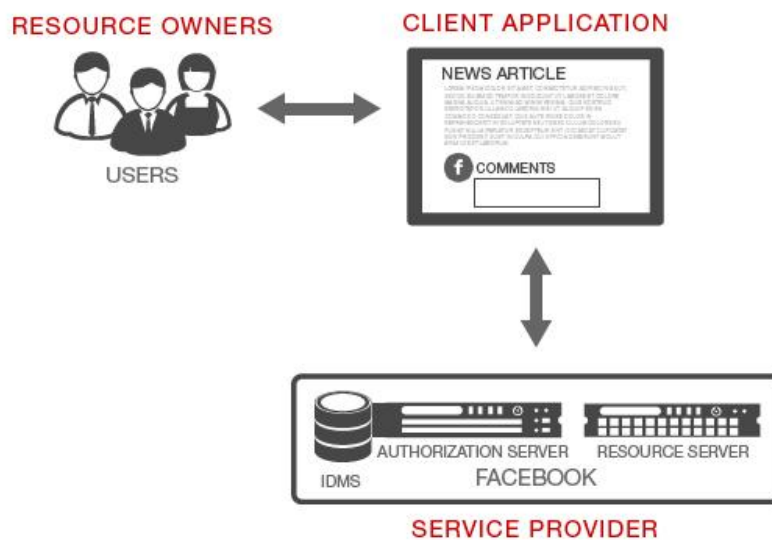


Figure 1.0 shows a common use case where a user (resource owner) is attempting to post a comment on a new media site (client application) with his/her Facebook account. Before the comment can be posted, the news media site fetches the user's Facebook profile attributes (user owned resources) from Facebook (service provider). This is made possible by the OAuth standard.

In order for this function to work, the user must give permission to the news media site to fetch his/her Facebook profile information from Facebook (service provider) without ever revealing his/her Facebook credentials (email and password) to the news media site.

This popular example of OAuth creates a better user experience for website visitors of news and media websites and it reduces risk for the website owner. By using the visitors' Facebook account, the website doesn't have to worry about storing account information of their website visitors/subscribers.

3.0 Forum Sentry as an OAuth client in a OAuth with Single-Sign On use case

3.1 Use case without a Forum Sentry API Security Gateway

The power and flexibility of OAuth in the social media sector has given enterprise companies an impetus to start adopting the OAuth standard for their cloud-based enterprise identity management. A prime example of this adoption is based on a use case where a company's email system is hosted in the Google cloud. Google cloud is the identity repository for the company's users. The company does not want to take the responsibility of hosting a user identity repository on its premise.

The company has the following goals for its access control strategy:

- Requiring a user to authenticate with Google cloud with his/her Google email and password.
- Upon successful validation with Google, a user will then grant company's applications the right to retrieve the user's profile from Google cloud. This task will be achieved using the OAuth standard.
- Once the company application retrieves the user's profile, the user can access applications multiple times without ever providing any password credentials to the company. This task will be achieved through the Single-Sign On.

Figure 2 illustrates an architecture deployment of a company leveraging a cloud based identity management system to control access to its company applications.

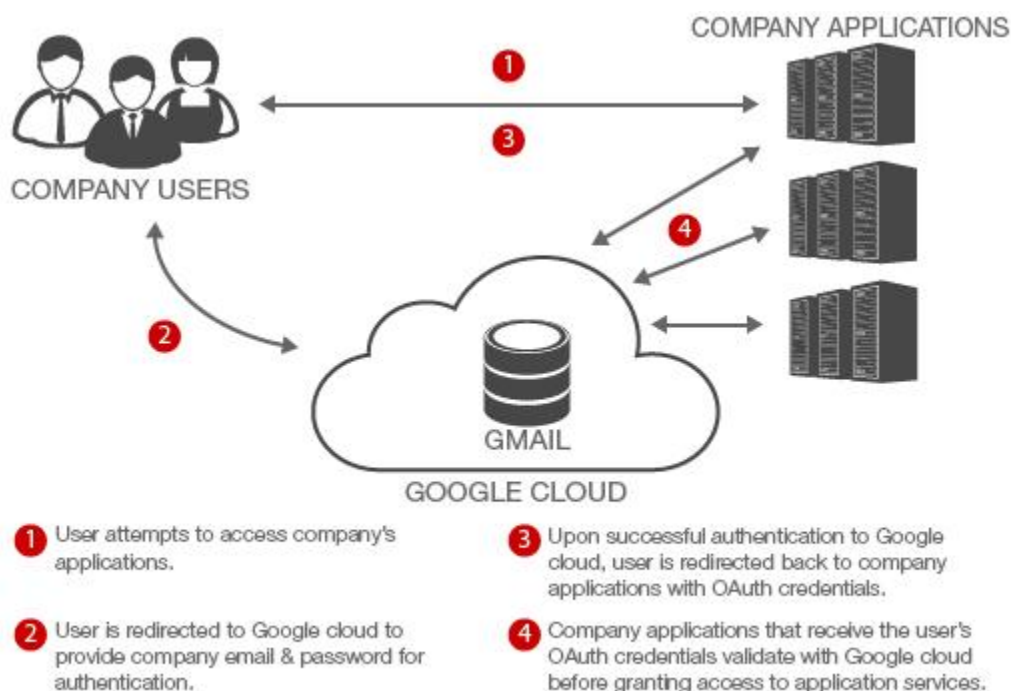


Figure 2: Enterprise applications (OAuth Clients) process flow with OAuth enabled cloud-based Identity Management System.

It should be noted that Figure 2 is a high level architecture. To keep the example simple, some details have been left out and will be discussed later in the document.

Although, a cloud-based access control architecture may appear to be straightforward and simple, it can certainly pose several challenges for an organization:

- Company applications require modification to be OAuth enabled.
- Over time, scalability becomes an issue. As new applications are deployed, they must be integrated and tested for OAuth, which requires time and resources.
- This deployment doesn't offer any centralized monitoring and enforcement.
- Performance becomes an issue when SSL is used by applications to exchange OAuth credentials with Google cloud.

3.2 Use case with a Forum Sentry API Security Gateway

When you add an API Security Gateway to the architecture as an OAuth client with Single Sign On capabilities, it alleviates many of the challenges we discussed in the example where an API

Security Gateway is not deployed:

- No modifications are required to company applications. Applications are OAuth agnostic. The gateway takes on the role of an OAuth client.
- Scalability is no longer an issue when new applications are deployed. Integration and testing of OAuth is no longer required with applications.
- Centralized monitoring and enforcement is easier with an API Gateway. API Gateway provides full visibility to who is accessing what resource.
- Performance is no longer an issue since an API Security Gateway accelerates SSL traffic that contains OAuth credentials.

Figure 4 below shows how the deployment of an API Security Gateway (OAuth client with Single-Sign On) changes the process of accessing the cloud-based identity management system.

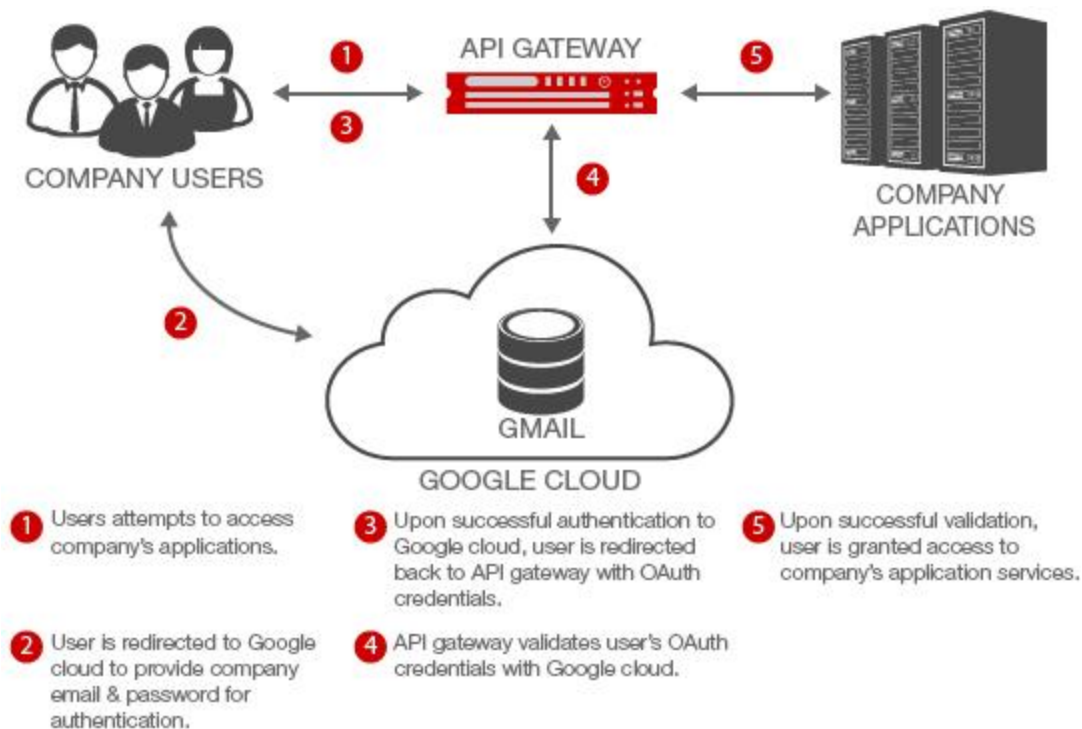


Figure 3: API Security Gateway (OAuth Client) process flow with OAuth enabled Cloud-Based Identity Management System.

3.3 Configuring Forum Sentry as an OAuth Client with Grant Type: Auth Code

We will walk you step by step on how to configure Forum Sentry to achieve the scenario described in Figure 3. Forum Sentry supports OAuth Version 2.0 as an OAuth client (for single

sign on (SSO)).

We will need the following entities to accomplish our task of configuring the use case described in Figure 3.

- Forum API Security Gateway (OAuth Client) - Identified by a DNS name forum-oauth.com
- User - A standard web browser
- Accessible back-end website - www.forumsys.com
- Access to <https://cloud.google.com>. Your valid google credentials are required.

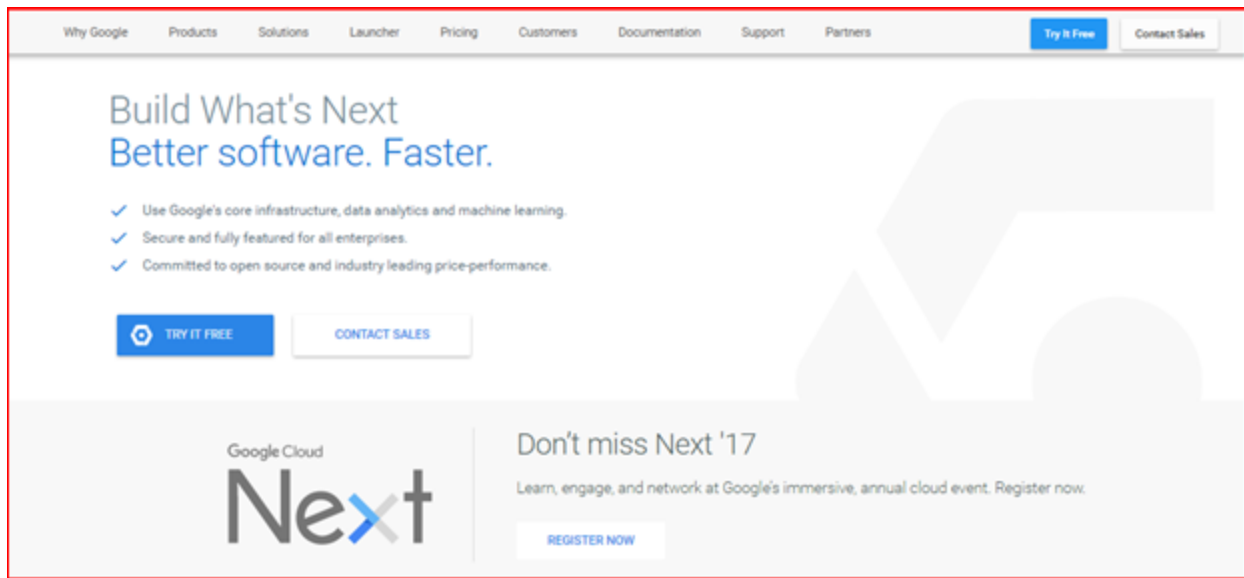
3.3.1 Registering Forum Sentry with an OAuth Service Provider

Before we proceed with configuring Sentry, we need to register Forum Sentry as a client application with OAuth Service Provider such as Google Cloud.

As indicated in Figure 3, Forum Sentry is the API Security Gateway that will take on the role of an OAuth client so company applications do not have to interact with Google Cloud. The registration of Sentry with Google Cloud enables Sentry to establish trust with Google Cloud. The trust confirms to Google Cloud that Sentry is a legit application (app) that is allowed to access user resources (e.g. user profile) on behalf of the user if and when the user grants control to Sentry. In Figure 3, run-time flow 4 would not be possible without this design time registration process.

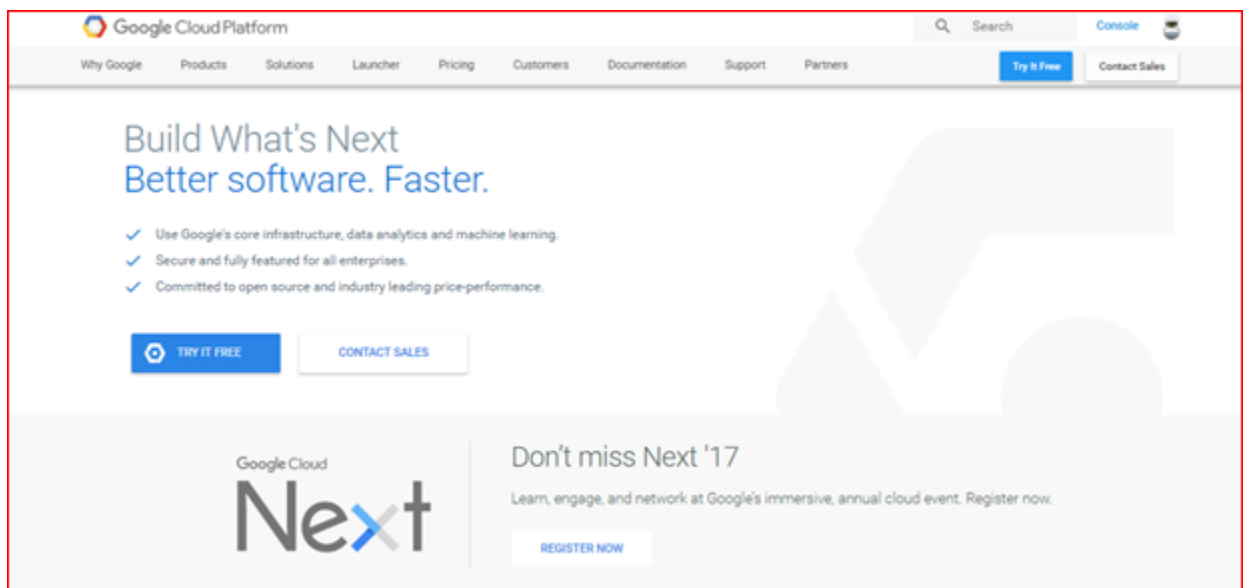
Step 1: You will need to have a valid email and password registered with Google.

Step 2: You will need to access <https://cloud.google.com>. Please hit on “sign-in” on the web page and login with your Google credentials.

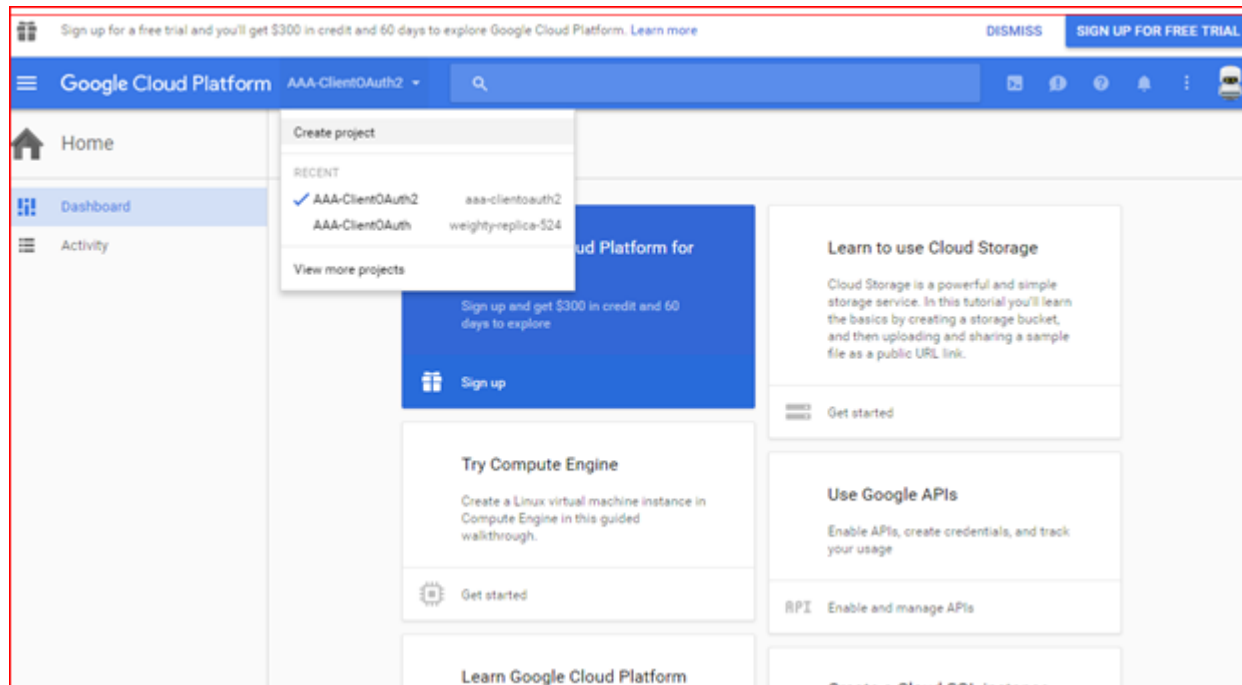


Please make sure that you are not using the old Google Cloud console interface. If you see online Google screens that look different than the screenshots in this document then you are using the old Google Cloud console.

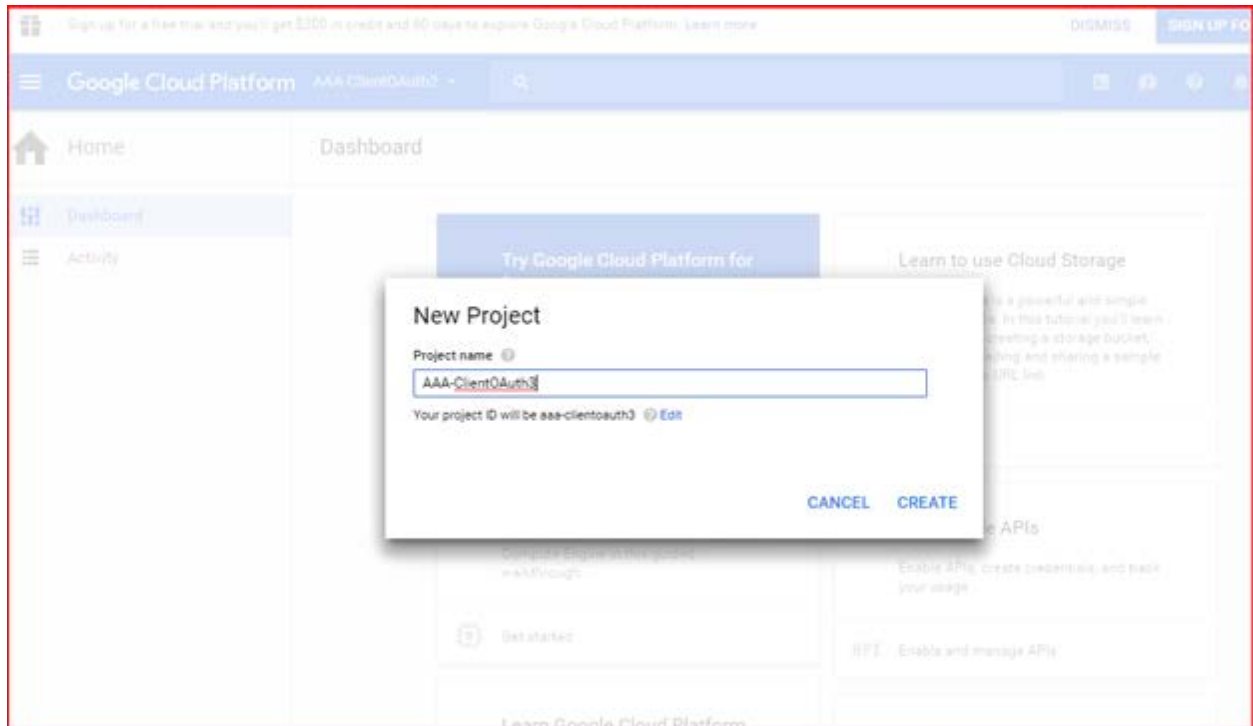
Step 3: After successfully logging in, a page below may appear. Click on the “Console” link in the upper corner.



Step 4: Open the Project dropdown menu from the top-left and select “Create Project”

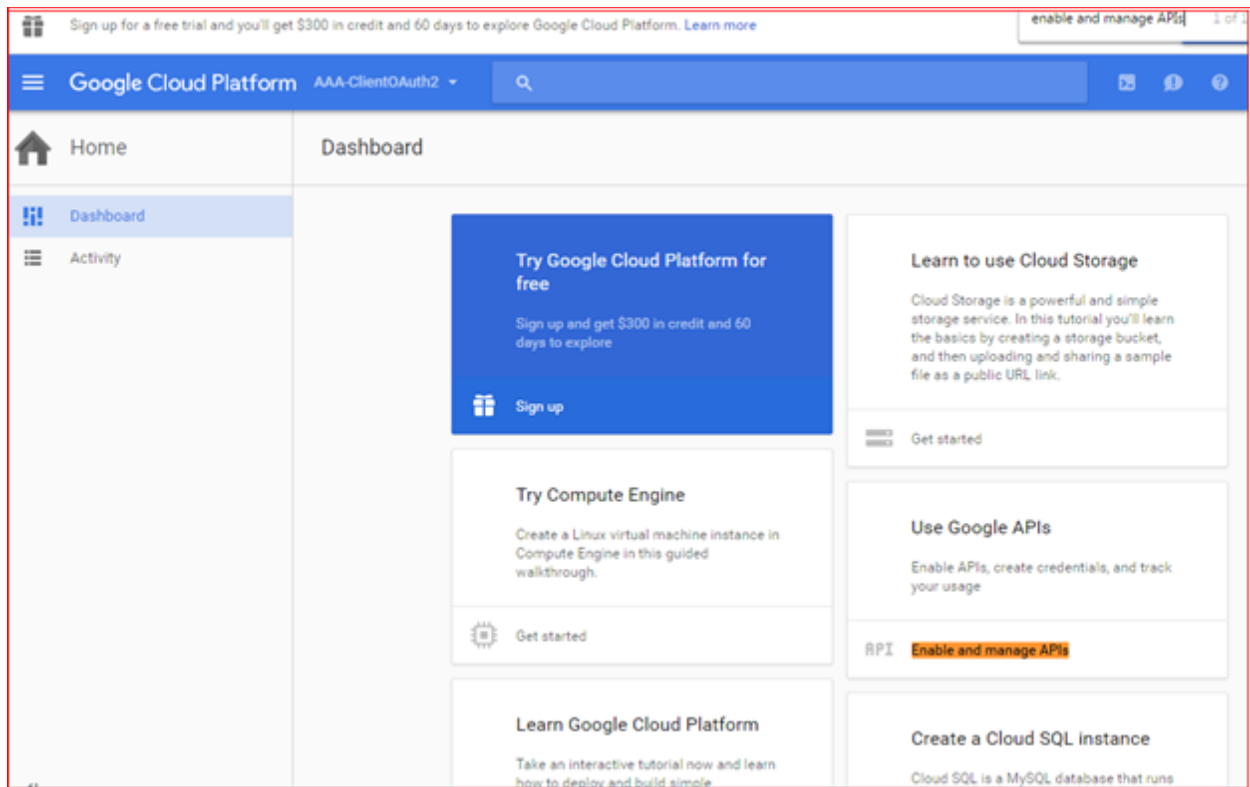


Step 5: A page leads you to a pop up. You will enter the “Project name”. The “Project ID” is pre-assigned by Google. And hit the “Create” button.



If doing this for the first time you might see a “Terms of Service” agreement check box that you will need to check before clicking Create.

Step 6: From the Dashboard display select the link to “Enable and manage APIs”



Step 7: Under the API Manager heading click on the “Credentials” link and then select the “OAuth consent screen” tab. At a minimum you will need to add a Product Name. Then click the “Save” button.

Sign up for a free trial and you'll get \$300 in credit and 60 days to explore Google Cloud Platform. [Learn more](#)

Google Cloud Platform AAA-ClientOAuth2

API Manager


Dashboard

Library

Credentials

Credentials

Credentials OAuth consent screen Domain verification

Email address 


mboukantar@forumsys.com

Product name shown to users


Forum Systems

Homepage URL (Optional)

https:// or http://

Product logo URL (Optional) 

http://www.example.com/logo.png


 This is how your logo will look to end users
Max size: 120x120 px

Privacy policy URL
Optional until you deploy your app

https:// or http://

Terms of service URL (Optional)

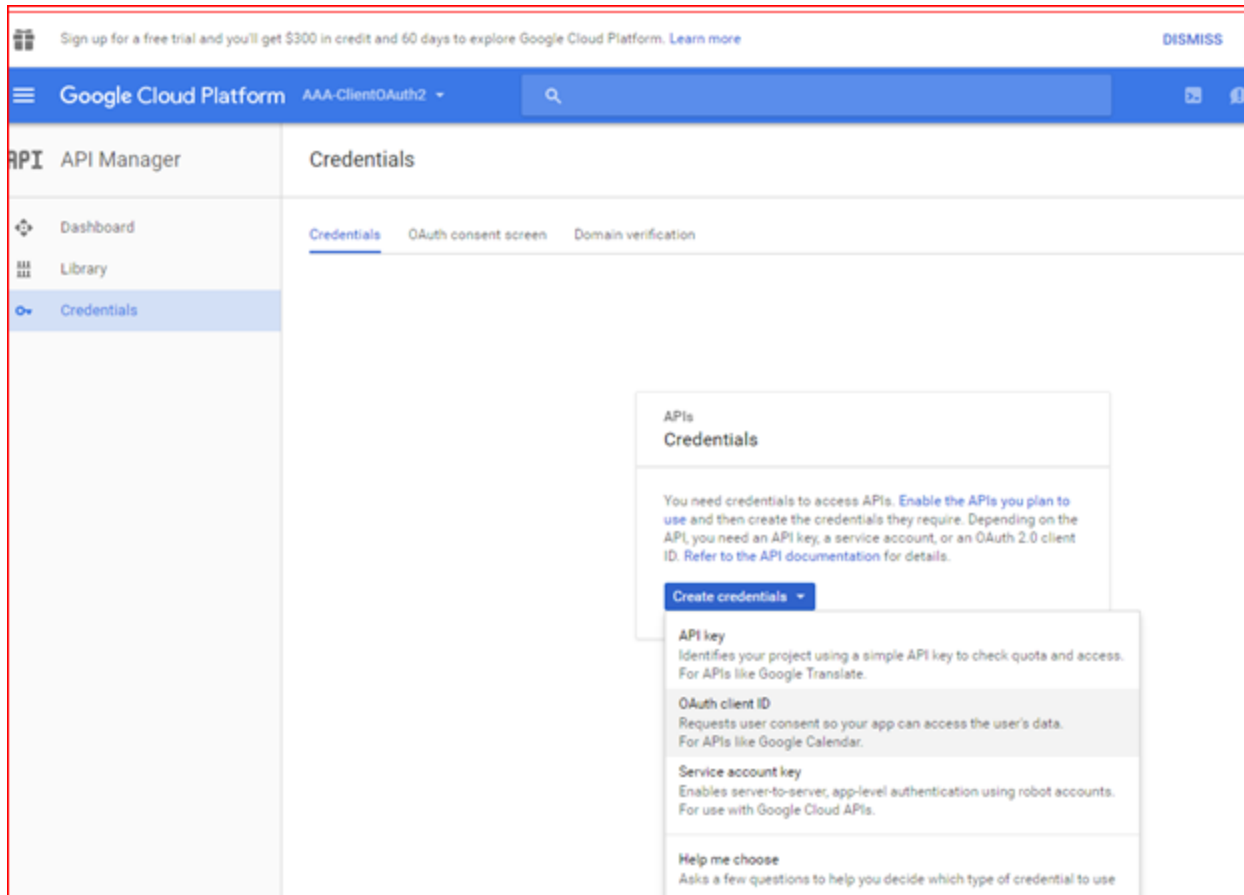
https:// or http://



The consent screen will be shown to users whenever you request access to their private data using your client ID. It will be shown for all applications registered in this project.

You must provide an email address and product name for OAuth to work.

Step 8: Click on the “Credentials” tab under the “Credentials” heading in the right pane as shown below. Click the option to “Create credentials” and select the “OAuth client ID” option.

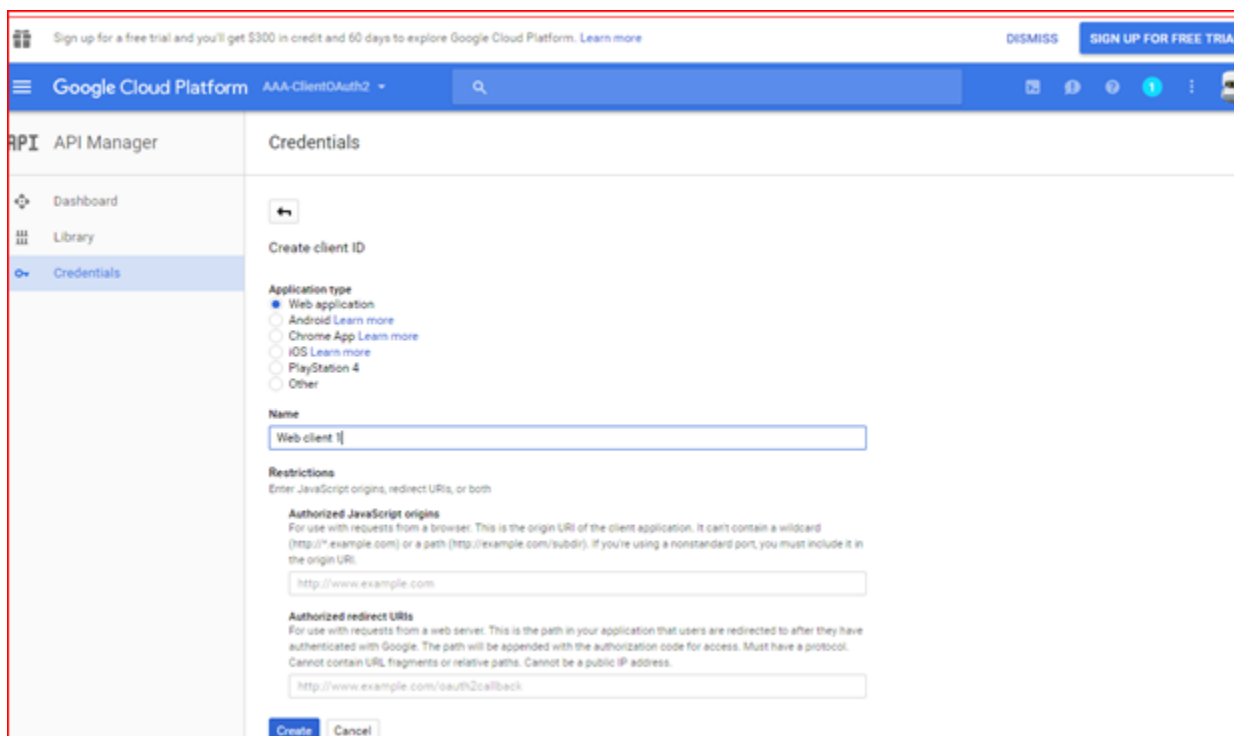


Step 9: This is the page where you enter your application attributes. In our use case, Forum Sentry is the web application. You will select the “Web application” radio button.

In the “Authorized redirect URI” section, you will enter a URI that represents Forum Sentry's location and resource. For example, in Figure 3, a user in flow 1 and 3 is connecting to Forum Sentry's service based on a URI.

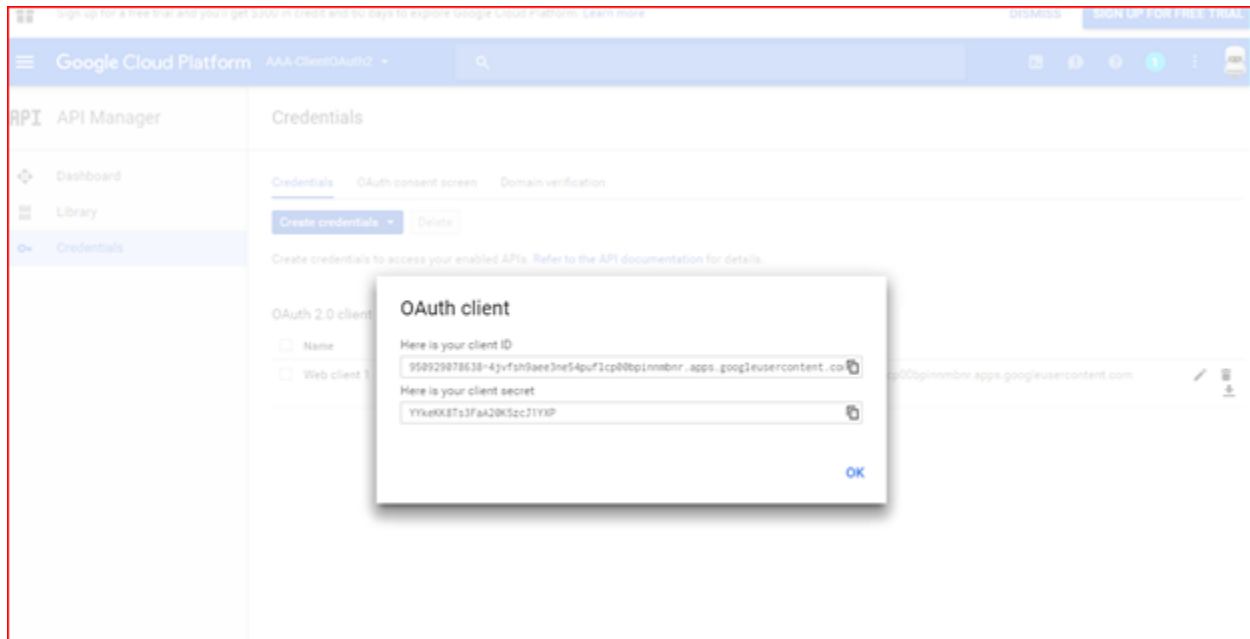
When you enter a URI, its value signals to Google OAuth Server that the OAuth code or token is to be returned to Forum Sentry identified by URI's attributes such as hostname and virtual directory. In our case, we will enter <http://forum-oauth.com/login>. Again, you can enter any hostname in the URI as long as it has a valid DNS mapping to a listener IP address of your Forum Sentry instance. The usage of the URI will become a lot clearer when we configure Sentry policies later in the document.

Note: In the URI, the hostname cannot be a IP address. Also, the virtual directory should still be named “/login”. In this configuration example, we will stick with “/login”. Click on “Create”



The screenshot displays the Google Cloud Platform API Manager interface for creating a new client ID. The left sidebar shows the navigation menu with 'API Manager' selected. The main content area is titled 'Credentials' and contains the 'Create client ID' form. The 'Application type' section has 'Web application' selected. The 'Name' field is filled with 'Web-client 1'. The 'Restrictions' section includes two text input fields: 'Authorized JavaScript origins' with the value 'http://www.example.com' and 'Authorized redirect URIs' with the value 'http://www.example.com/oauth2/callback'. At the bottom of the form are 'Create' and 'Cancel' buttons.

Step 10: Finally, a pop-up window displays two fields for the new OAuth client. The “Client ID” and “Client secret”. These need to be copied and pasted into your notepad. You will need to enter the “Client ID” and “Client secret” later into Forum Sentry once we start configuring its OAuth policy.



3.3.2 Configuring Forum Sentry Policies as an OAuth client

We will be using figure 3 as a frame of reference when configuring Forum Sentry.

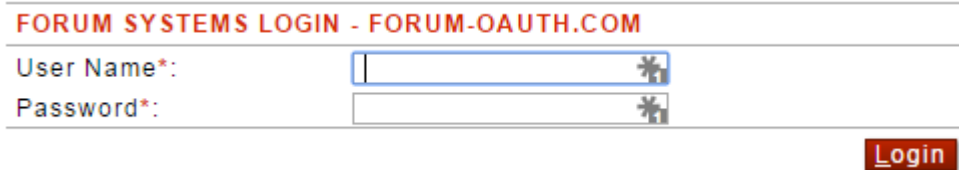
Forum Sentry is an API Security Gateway that will be configured to simulate the behavior of an OAuth client as shown in figure 3. For this configuration exercise, we will pick a website such as www.forumsys.com as the company application that will be sitting behind Sentry. You are free to select any website of your own choosing. The only condition is that the name of the website has a valid DNS mapping in your infrastructure.

In this configuration example, we will be creating the following policies to accomplish our task.

- Listener Policy - This policy defines the IP address and TCP port that Sentry listens on for connections.
- Remote Policy - This policy defines the remote service defined by an IP address and TCP port that Sentry will be connecting to after it has processed incoming messages.
- HTML Policy - This is the master policy that defines the set of services (tasks) that will be performed on incoming and outgoing messages. The HTML policy's services are triggered based on which set of URIs are being accessed by remote users or applications. These URIs are defined in the HTML policy.
- Redirect Policy - This policy contains specific URIs which helps HTML policy service determine where to redirect a user or application in case certain conditions are not met. For example, a user accesses a site defined by URI www.mybank.com. If the user does not carry any authentication credentials, the HTML policy will decide to redirect the user to URI www.mybank.com/login. www.bank.com/login will be defined in Redirect Policy and consumed by the HTML policy.
- Task List and Task Group Policy - This is the policy that actually defines a set of tasks to be performed on incoming and outgoing messages. This policy is consumed by the HTML policy. In our use case, we will define only one task

which is to obtain an OAuth credentials from Google AUTH Server.

Step 1: Enter <https://forum-oauth.com:5050> into your browser. The login page will appear. Enter your username and password and click “Login”.



FORUM SYSTEMS LOGIN - FORUM-OAUTH.COM

User Name*:

Password*:

Login

Step 2: After successful login, the general admin page will appear. Click on “Gateway”, then click on Network Policies

Step 3: Follow the steps shown to create a local listener policy. This is the Sentry network service that will accept connections over an application protocol such as http. The Sentry listener will be bound to the IP of the machine that Sentry is running on. Start by clicking on the “New” button.



NETWORK POLICIES

No items to display

GDM Transfer GDM Export Delete Enable Disable New

Step 4: Select HTTP as the application protocol for the incoming connection.



NETWORK POLICIES > NEW NETWORK POLICY

NETWORK POLICY PROTOCOL

☐ Advanced Message Queuing Protocol (AMQP)

☐ FTP

☒ HTTP

☐ SFTP

☐ SMTP

☐ Amazon S3

Step 5: Select Listener as the option since Sentry will be receiving connections from users.

NETWORK POLICIES > NEW NETWORK POLICY

NETWORK POLICY TYPE

☒ Listener
☐ Remote

Next

Step 6: Specify a Policy Name, or use the default provided, i.e. “HTTPListenerPolicy”. Click Next. At the IP ACL Policy Screen, click next.

NETWORK POLICIES > HTTP LISTENER POLICY

IP ACL

IP ACL Policy: Unrestricted [Edit](#)

Next

POLICY SELECTIONS

Policy Name: HttpListenerPolicy

Step 7: Select HTTP and HTTP Chunking as options and click Next.

NETWORK POLICIES > HTTP LISTENER POLICY

INBOUND PROTOCOL

☒ HTTP
☐ HTTPS
☒ Use HTTP Chunking (recommended)

Next

POLICY SELECTIONS

Policy Name: HttpListenerPolicy
IP ACL Policy: Unrestricted

Step 8: Select Device IP and click Next.

NETWORK POLICIES > HTTP LISTENER POLICY

LISTENER

Use Device IP: ☒
 Listener Host*: 0.0.0.0
 Listener Port*: 80

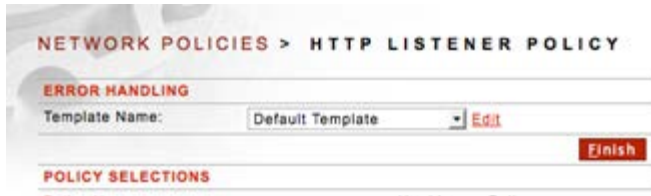
Next

POLICY SELECTIONS

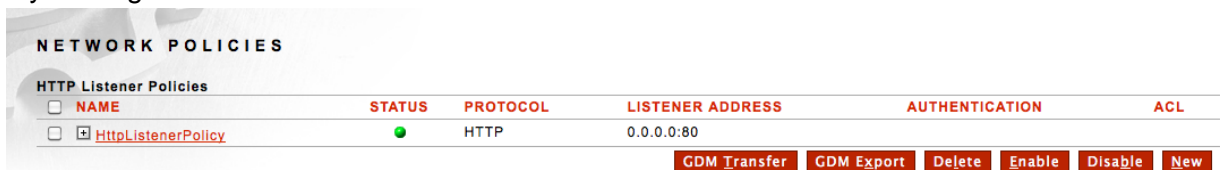
Policy Name: HttpListenerPolicy
IP ACL Policy: Unrestricted
Inbound Protocol: HTTP (chunked)

Step 9: Do not make any changes to the Password Authentication, click Next.

Step 10: Click on Finish.



You have successfully created a listener on TCP port 80. The green light indicates that it is actively waiting for connections.

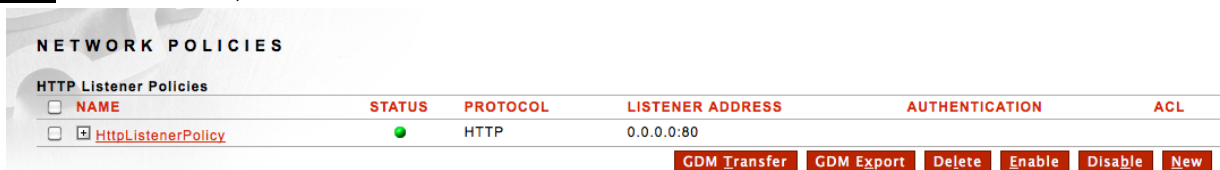


NETWORK POLICIES					
HTTP Listener Policies					
<input type="checkbox"/> NAME	STATUS	PROTOCOL	LISTENER ADDRESS	AUTHENTICATION	ACL
<input type="checkbox"/> HttpListenerPolicy	●	HTTP	0.0.0.0:80		

GDM Transfer GDM Export Delete Enable Disable New

Step 11: Now you are ready to create a remote policy in Sentry. This remote policy contains the location of the application or website that Sentry is protecting. The location is identified by the URI or an IP address of the remote application. For example, in Figure 3, the company application would be configured as part of Sentry's network remote policy. In this configuration, our application is "www.forumsys.com" and we will make it part of our network remote policy.

Step 12: Click on New, Select HTTP and click Next.



NETWORK POLICIES					
HTTP Listener Policies					
<input type="checkbox"/> NAME	STATUS	PROTOCOL	LISTENER ADDRESS	AUTHENTICATION	ACL
<input type="checkbox"/> HttpListenerPolicy	●	HTTP	0.0.0.0:80		

GDM Transfer GDM Export Delete Enable Disable New

Step 13: Select Remote and click Next. This the application Sentry will be connecting to. Click Next.



NETWORK POLICIES > NEW NETWORK POLICY

NETWORK POLICY TYPE

☐ Listener

☒ Remote

Next

Step 14: Enter the Policy Name. You can select the default “HttpRemotePolicy” and click Next.

Step 15: Select HTTP as the application protocol for the back-end application. Click Next.

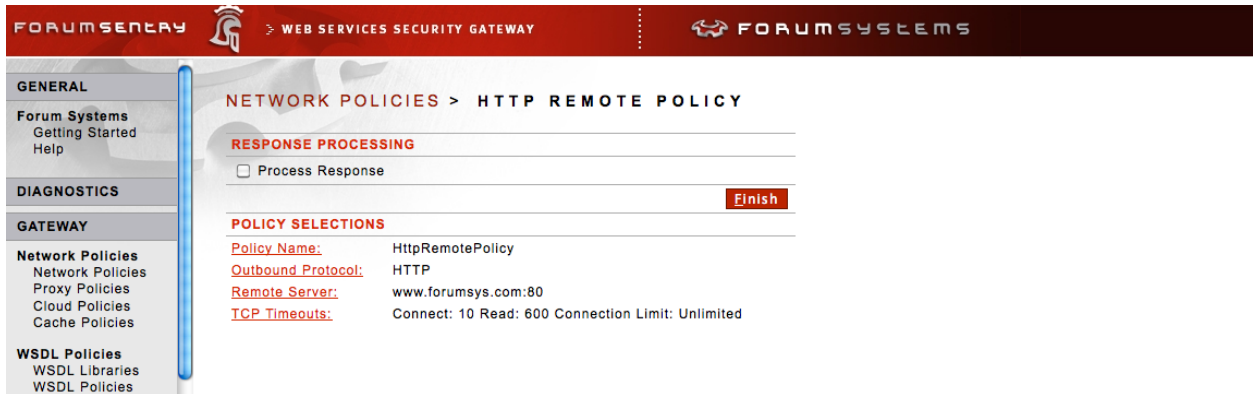
Step 16: Enter www.forumsys.com (or your favorite website) as Remote Server. Default port is 80. Click Next.

The screenshot shows the 'API SECURITY GATEWAY' configuration page for 'HTTP REMOTE POLICY'. The left sidebar contains a navigation menu with sections: GENERAL (Forum Systems, Getting Started, Help), DIAGNOSTICS, and GATEWAY (Network Policies, WSDL Policies, Content Policies). The main content area is titled 'NETWORK POLICIES > HTTP REMOTE POLICY'. Under the 'REMOTE SERVER' section, the 'Remote Server*' field is set to 'www.forumsys.com', 'Remote Port*' is '80', and 'Proxy Settings Policy' is 'No Proxy'. There are checkboxes for 'Provide Basic Authentication Credentials', 'Provide Digest Authentication Credentials', and 'Dynamic EndPoint Routing', all of which are unchecked. Below these, there are radio buttons for 'Use Inbound HTTP Host header' (selected) and 'Use Attribute*'. The 'Proxy Client's User Agent' is set to '[From System Policy]'. A 'Next' button is located at the bottom right of this section. The 'POLICY SELECTIONS' section shows 'Policy Name' as 'HttpRemotePolicy' and 'Outbound Protocol' as 'HTTP'.

Step 17: Keep the default settings for the timeout and click Next.

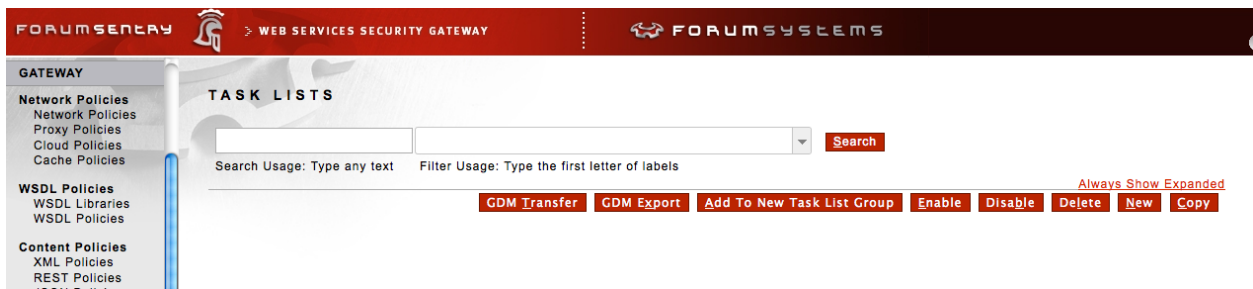
The screenshot shows the 'WEB SERVICES SECURITY GATEWAY' configuration page for 'HTTP REMOTE POLICY'. The left sidebar is similar to the previous screenshot. The main content area is titled 'NETWORK POLICIES > HTTP REMOTE POLICY'. Under the 'TCP TIMEOUTS' section, 'Custom connect timeout' is set to '10' seconds and 'Custom read timeout' is set to '600' seconds. The 'Limit Connections' checkbox is unchecked, and the value is '0'. A 'Next' button is located at the bottom right of this section. The 'POLICY SELECTIONS' section shows 'Policy Name' as 'HttpRemotePolicy', 'Outbound Protocol' as 'HTTP', and 'Remote Server' as 'www.forumsys.com:80'.

Step 18: Leave Process Response unchecked. Click Finish.



Now we are ready to create a policy in Forum Sentry which will enable it to be an OAuth client. It is a Task Policy that contains OAuth attributes. The following steps are needed to enable this policy.

Step 1: Click on Task Lists in the lower left panel and the following screen will appear. Click on New.



Step 2: Enter the name of the Task List as "Task_OAuth_Google_GrantType_OAuth_Code". Click Apply.



Step 3: Now you ready to pick a specific task that will be associated with this Task List. Click on New.

FORUMSENTRY > WEB SERVICES SECURITY GATEWAY **FORUMSYSTEMS**

GATEWAY

- Network Policies
 - Network Policies
 - Proxy Policies
 - Cloud Policies
 - Cache Policies
- WSDL Policies
 - WSDL Libraries
 - WSDL Policies
- Content Policies
 - XML Policies
 - REST Policies
 - JSON Policies
 - HTML Policies
 - STS Policies
 - OAuth Policies
 - Tests
- Task Policies
 - Task List Groups
 - Task Lists

TASK LISTS > TASK LIST

Task List added

TASK LIST

Name*: Task_OAuth_Google_GrantType_OAuth_Code

Description:

Labels:

Sample Document: SoapDocument.xml [Edit](#)

[Apply](#) [Save](#)

Tasks

<input type="checkbox"/>	#	TASK NAME	TASK TYPE	STATUS
No items to display				

[Run](#) [Settings](#) [Enable](#) [Disable](#) [Delete](#) [New](#)

Step 4: Under User Identity and Access Control select the radio button “User identity & Access Control”. Click Next.

FORUMSENTRY > API SECURITY GATEWAY **FORUMSYSTEMS** System N IP Address

GENERAL

- Forum Systems
 - Getting Started
 - Help

DIAGNOSTICS

GATEWAY

- Network Policies
 - Network Policies
 - Proxy Policies
 - Cloud Policies
 - Cache Policies

TASK LISTS > TASK LIST: TASK_OAUTH_GOOGLE_GRANTTYPE_OAUTH_CODE

TASK TYPE

Conditional Identification	User Identity and Access Control	Credential Generation
<input type="radio"/> Identify Document	<input checked="" type="radio"/> IP ACL <input type="radio"/> Logout <input checked="" type="radio"/> User Identity & Access Control	<input type="radio"/> Generate Password <input type="radio"/> SAML Assertion <input type="radio"/> WS-Security Header
Mediation and Transformation <input type="radio"/> Add XML Node <input type="radio"/> AS2 <input type="radio"/> Convert CSV	Flow Control <input type="radio"/> Abort Processing <input type="radio"/> Cache Response <input type="radio"/> Delay Processing	Security Processing <input type="radio"/> Decrypt Elements <input type="radio"/> Encrypt Elements <input type="radio"/> OpenPGP

Step 5: The default task name will appear as “User Identity & Access Control”. Click Next.

FORUMSENTRY > WEB SERVICES SECURITY GATEWAY **FORUMSYSTEMS**

GATEWAY

- Network Policies
 - Network Policies
 - Proxy Policies
 - Cloud Policies
 - Cache Policies
- WSDL Policies
 - WSDL Libraries
 - WSDL Policies
- Content Policies
 - XML Policies
 - REST Policies
 - JSON Policies
 - HTML Policies

TASK LISTS > TASK LIST: TASK_OAUTH_GOOGLE_GRANTTYPE_OAUTH_CODE > TASK: USER IDENTITY & ACCESS CONTROL

TASK NAME

Task Name*: User Identity & Access Control [Next](#)

USER IDENTITY & ACCESS CONTROL

Task Type: User Identity & Access Control

Step 6: Uncheck the check box on “Map identified user to a known user”. Click Next.

FORUMSENTRY

WEB SERVICES SECURITY GATEWAY

FORUMSYSTEMS

GATEWAY

Network Policies

- Network Policies
- Proxy Policies
- Cloud Policies
- Cache Policies

WSDL Policies

- WSDL Libraries
- WSDL Policies

Content Policies

- XML Policies
- REST Policies
- JSON Policies
- HTML Policies
- STS Policies
- OAuth Policies

TASK LISTS > TASK LIST: TASK_OAUTH_GOOGLE_GRANTTYPE_OAUTH_CODE > TASK: USER IDENTITY & ACCESS CONTROL

ACCESS CONTROL

Map identified user to a known user: ☐

ACL Policy:

[Allow All]

Next

USER IDENTITY & ACCESS CONTROL

Task Type:

User Identity & Access Control

Task Name:

User Identity & Access Control

Step 7: Select the radio button “Validate OAuth SSO token & establish identity”. Click Next

The screenshot shows the ForumSentry Web Services Security Gateway configuration interface. The left sidebar contains a navigation menu with categories: GATEWAY, Network Policies, WSDL Policies, Content Policies, Task Policies, Redirect Policies, and RESOURCES. The main content area displays the breadcrumb path: TASK LISTS > TASK LIST: TASK_OAUTH_GOOGLE_GRANTTYPE_OAUTH_CODE > TASK: USER IDENTITY & ACCESS CONTROL. Below this, the 'USER IDENTITY MECHANISM' section lists several options with radio buttons. The option 'Validate OAuth SSO token & establish identity' is selected. A 'Next' button is located at the bottom right of this section. The 'USER IDENTITY & ACCESS CONTROL' section shows 'Task Type' as 'User Identity & Access Control', 'Task Name' as 'User Identity & Access Control', and 'ACL Policy' as 'No user mapping'.

FORUMSENTRY > WEB SERVICES SECURITY GATEWAY **FORUMSYSTEMS**

GATEWAY

Network Policies
Network Policies
Proxy Policies
Cloud Policies
Cache Policies

WSDL Policies
WSDL Libraries
WSDL Policies

Content Policies
XML Policies
REST Policies
JSON Policies
HTML Policies
STS Policies
OAuth Policies
Tests

Task Policies
Task List Groups
Task Lists

Redirect Policies
Redirect Policies

RESOURCES

TASK LISTS > TASK LIST: TASK_OAUTH_GOOGLE_GRANTTYPE_OAUTH_CODE > TASK: USER IDENTITY & ACCESS CONTROL

USER IDENTITY MECHANISM

☐ Identity established in network policy (basic auth or client cert)

☐ Identity established by validating cookies

☐ Validate WS-Security & establish identity

☐ Validate SAML assertion & establish identity

☐ Validate SAML SSO assertion & establish identity

☐ Validate OAuth token & establish identity

☒ Validate OAuth SSO token & establish identity

☐ Identity established by attribute mapping

☐ Identity established by digital signature

☐ Identity established by Sentry REST authentication

Next

USER IDENTITY & ACCESS CONTROL

Task Type: User Identity & Access Control

Task Name: User Identity & Access Control

ACL Policy: No user mapping

Step 8: Select Google as your OAuth Service provider. Click Next.

The screenshot shows the ForumSentry API Security Gateway configuration interface. The left sidebar contains a navigation menu with categories: GENERAL, Forum Systems, DIAGNOSTICS, GATEWAY, Network Policies, WSDL Policies, Content Policies, and OAuth Policies. The main content area displays the breadcrumb path: TASK LISTS > TASK LIST: TASK_OAUTH_GOOGLE_GRA CONTROL. Below this, the 'IDENTITY PROVIDER' section lists several options with radio buttons. The option 'Google' is selected. The 'USER IDENTITY & ACCESS CONTROL' section shows 'Task Type' as 'User Identity & Access Control', 'Task Name' as 'User Identity & Access Control', 'ACL Policy' as 'Allow All', and 'User Identity Mechanism' as 'Validate OAuth SSO token & establish identity'.

FORUMSENTRY > API SECURITY GATEWAY **FORUMSYSTEMS**

GENERAL
Forum Systems
Getting Started
Help

DIAGNOSTICS

GATEWAY

Network Policies
Network Policies
Proxy Policies
Cloud Policies
Cache Policies

WSDL Policies
WSDL Libraries
WSDL Policies

Content Policies
XML Policies
REST Policies
JSON Policies
HTML Policies
STS Policies
OAuth Policies

TASK LISTS > TASK LIST: TASK_OAUTH_GOOGLE_GRA CONTROL

IDENTITY PROVIDER

☐ Salesforce.com

☐ Microsoft

☒ Google

☐ Facebook

☐ LinkedIn

☐ Ping Identity

☐ Other

USER IDENTITY & ACCESS CONTROL

Task Type: User Identity & Access Control

Task Name: User Identity & Access Control

ACL Policy: Allow All

User Identity Mechanism: Validate OAuth SSO token & establish identity

Remember you had saved Client Id and Client Secret from earlier steps in Section 3.3.1. You copied these from Google Cloud service. You will need to paste these each in its appropriate field on this screen. Click Next.

FORUMSENTRY > WEB SERVICES SECURITY GATEWAY **FORUMSYSTEMS**

GATEWAY

- Network Policies
 - Network Policies
 - Proxy Policies
 - Cloud Policies
 - Cache Policies
- WSDL Policies
 - WSDL Libraries
 - WSDL Policies
- Content Policies
 - XML Policies
 - REST Policies
 - JSON Policies
 - HTML Policies
 - STS Policies
 - OAuth Policies
 - Tests
- Task Policies
 - Task List Groups
 - Task Lists

TASK LISTS > TASK LIST: TASK_OAUTH_GOOGLE_GRANTTYPE_OAUTH_CODE > TASK: USER IDENTITY & ACCESS CONTROL

CLIENT CREDENTIALS

Client Id*: 77hdaic9d8nhq3bf9vd3c.apps.googleusercontent.com

Client Secret*: [Masked]

Authentication: ☒ Form (not recommended) ☐ HTTP Basic ☐ SSL **Next**

USER IDENTITY & ACCESS CONTROL

Task Type: User Identity & Access Control

Task Name: User Identity & Access Control

ACL Policy: No user mapping

User Identity Mechanism: Validate OAuth SSO token & establish identity

Identity Provider: Google

Step 9: In the Redirect Parameter, enter “origUri”. You can pick any string besides “origUri” in the Redirect Parameter field as long it is consistently used across other policies within Sentry. origUri is a placeholder for the original URI that a user enters to connect to Sentry’s listener. In our example configuration, that URI is “forum-oauth.com”. Once OAuth processing is successfully completed by Sentry’s OAuth engine, it will redirect the user browser to connect to forum-oauth.com with valid credentials (cookie).

FORUMSENTRY > WEB SERVICES SECURITY GATEWAY **FORUMSYSTEMS**

GATEWAY

- Network Policies
 - Network Policies
 - Proxy Policies
 - Cloud Policies
 - Cache Policies
- WSDL Policies
 - WSDL Libraries
 - WSDL Policies
- Content Policies
 - XML Policies
 - REST Policies
 - JSON Policies
 - HTML Policies
 - STS Policies
 - OAuth Policies
 - Tests
- Task Policies
 - Task List Groups
 - Task Lists
- Redirect Policies
 - Redirect Policies

TASK LISTS > TASK LIST: TASK_OAUTH_GOOGLE_GRANTTYPE_OAUTH_CODE > TASK: USER IDENTITY & ACCESS CONTROL

REDIRECT PARAMETER

Redirect Parameter*: origUri **Next**

USER IDENTITY & ACCESS CONTROL

Task Type: User Identity & Access Control

Task Name: User Identity & Access Control

ACL Policy: No user mapping

User Identity Mechanism: Validate OAuth SSO token & establish identity

Identity Provider: Google

Client Credentials: 717677268983-ujp6aeeek6hg77hdaic9d8nhq3bf9vd3c.apps.googleusercontent.com (Form)

Redirect Parameter: origUri

Error Template: [From Policy]

Step 10: Click on Finish.

The screen will indicate that Task List “Task_OAuth_Google_GrantType_OAuth_Code” is associated with Task “User_identity_&_Access_Control”. Click Save.

Step 11: The task list that was created in the previous step will be consumed by the Task List Group. Click on “Task List Groups” button to create a Task List Group policy. Click New. Enter the Task List Group Name as “Task_Group_GrantType_OAuth_Code”. Click Create.

Step 12: Now you can add the Task List “Task_OAuth_Google_GrantType_OAuth_Code” to the group and Click Save.

Step 13: We will now create the Redirect Policy. This is the policy that will be consumed by the HTML policy, providing information of where a user’s initial connection would be redirected to in case the initial connection to Sentry does not contain any credentials (in the form of a cookie) or the credentials may have expired. Under the Gateway menu click Redirect Policies. Click New.

Step 14: Enter the name “NoAccess_Redirect_Policy”. Check two fields, Authentication Fails and No Credentials. Fill both fields with <http://forum-oauth.com/login> as shown below. Then check Include Origin URI field with the URI Parameter Name “origUri”. What you are configuring is a sub-policy which will be eventually consumed by the HTML policy which you will create

later. This sub-policy tells Sentry that when the user first connects to <http://forum-oauth.com/> and the user carries no credentials then the user will be redirected to a new location such as <http://forum-oauth.com/login>. Click Save.

REDIRECT POLICIES > REDIRECT POLICY

REDIRECT POLICY

Name*: NoAccess_Redirect_Polic

Description:

Labels:

Include Original URI: ☒

URI Parameter Name*: origUri

REDIRECT POLICY EVENTS

Authentication Success

Enabled: ☐

URL*:

Use Host Header: ☐

Processing: Task List Groups Type or select label (None)

Authentication Failure

Enabled: ☒

URL*: http://forum-oauth.com/login

Use Host Header: ☐

Processing: Task List Groups Type or select label (None)

No Credentials

Enabled: ☒

URL*: http://forum-oauth.com/login

Use Host Header: ☐

Processing: Task List Groups Type or select label (None)

On Error

Enabled: ☐

URL*:

Use Host Header: ☐

Processing: Task List Groups Type or select label (None)

Apply Save

Step 15: Click on HTML Policy in the left panel. You are now ready to create the master HTML policy. This is the policy that contains the URIs such as forum-oauth.com and forum-oauth.com/login and defines the authentication policies and various tasks. Click New.

Step 16: Enter the Name as "Browser_to_Sentry_OAuth_Policy". Click Next.

FORUMSENTRY > API SECURITY GATEWAY

HTML POLICIES > NEW HTML POLICY

NEW HTML POLICY

Name*: Browser_to_Sentry_OAuth_Policy

Next

Step 17: Select the existing listener policy from the default setting. Select the remote existing remote policies. Remember both the listener and remote network policies were created by you earlier. Click Finish.

WEB SERVICES SECURITY GATEWAY FORUMSYSTEMS

Please specify a listener policy for virtual directory: New Virtual Directory

☒ Select from existing listener policies
 HttpListenerPolicy (0.0.0.0:80) [Edit](#)

☐ Create a new HTTP listener policy
 Listener Policy Name*:
 Use Device IP: ☐
 Listener IP*:
 Listener Port*:

SET VIRTUAL DIRECTORY PATH
 Virtual Directory Path:

SET REMOTE POLICY
 Please specify a remote network policy

☐ Do not send to remote server
☒ Select from existing remote policies
 HttpRemotePolicy (www.forumsys.com:80) [Edit](#)

☐ Create a new HTTP remote policy for this remote server
 Remote Policy Name*:
 Remote Policy Host*:
 Remote Policy Port*:

[Finish](#)

Step 18: Upon success you will see the following the screen. Now you will enter more details. Click on New Virtual Directory shown.

HTML POLICIES > HTML POLICY

HTML POLICY
 Policy Name:

Virtual Directories | Task Lists | Settings | IDP Rules | Logging

VIRTUAL DIRECTORY	STATUS	VIRTUAL URI	REMOTE URI
<input type="checkbox"/> New Virtual Directory	●	http://10.5.1.101:80	http://www.forumsys.com:80

[Enable](#) [Disable](#) [Delete](#) [New](#)

Step 19: You are in the virtual directory screen. This is the screen where you will setup the policy of the first virtual directory that a user accesses from his/her browser. You will need change the following:

- Change the Name to “Initial_Contact”.
- Add Virtual Path /. So the user will be coming on URI http://forum-oauth.com/
- Filter Expression (.*)

Step 20: Scroll down further. You will need to select the following:

- Password Authentication: Specify
- Use Cookie Authentication must be checked.
- Require password authentication (any type) must be checked.
- Redirect Policy is associated with “NoAccess_Redirect_Policy”.

What this configuration is telling Sentry is that any user who comes in virtual / must come in with a cookie. If the user does not come with a cookie then he/she will be redirected to another URI that is described in “NoAccess_Redirect_Policy”. Remember, we had defined http://forum-oauth.com/login as the location in “NoAccess_Redirect_Policy”. It is the location where the user will be redirected to if he/she does not carry a cookie. Click Save.

FORUMSENTRY

API SECURITY GATEWAY

FORUMSYSTEMS

GENERAL

Forum Systems

Getting Started

Help

DIAGNOSTICS

GATEWAY

Network Policies

Network Policies

Proxy Policies

Cloud Policies

Cache Policies

WSDL Policies

WSDL Libraries

WSDL Policies

Content Policies

XML Policies

REST Policies

JSON Policies

HTML Policies

STS Policies

OAuth Policies

Tests

Task Policies

Task List Groups

Task Lists

Redirect Policies

Redirect Policies

Request Filters

Request Filters

RESOURCES

IDP

ACCESS

SYSTEM

PARTNERS

HTML POLICIES > HTML POLICY

HTML POLICY

Policy Name: Browser_to_Sentry_OAuth_Policy

Virtual Directories

Task Lists

Settings

IDP Rules

Logging

Virtual Directories > Virtual Directory: New Virtual Directory

VIRTUAL DIRECTORY

Name*: Initial_Contact

Description:

Virtual URI: http://127.0.0.1:80(/.*)?

Remote URI: http://www.forumsys.com:80\$0

VIRTUAL URI SETTINGS

Listener Policy: HttpListenerPolicy

Virtual Host:

Virtual Path:

Filter Expression: (/.*)?

Replace Expression: \$0

Request Filter Policy: Default_HTML

Error Template: [From Listener Policy]

ACCESS CONTROL

IP ACL Policy: Unrestricted

ACL Policy: [Allow All]

XACML Policy: [None]

Password Authentication: [Specify]

Use basic authentication:

Use digest authentication:

Use kerberos authentication:

Use cookie authentication:

Use form post authentication:

Username Parameter:

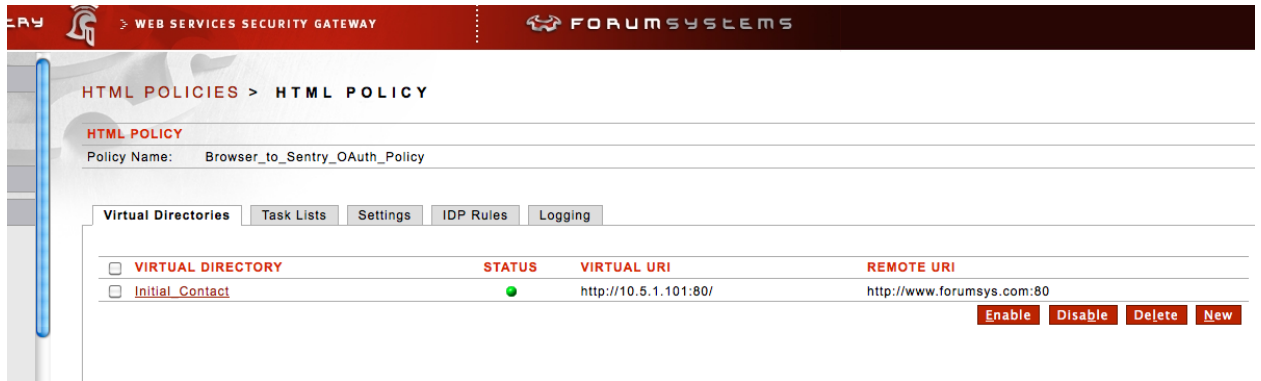
Password Parameter:

Require password authentication (any type):

Password Authentication Realm:

Redirect Policy: NoAccess_Redirect_Policy

Step 21: Upon success you will see the following screen. You are now ready to create a virtual directory policy for “/login”. Click New.



Enter the attributes as shown in the following screen:

- Name: Login
- Virtual Path: /login
- Filter Expression: (.*)
- Make sure that Send to remote server option is unchecked.

FORUMSENTRY

API SECURITY GATEWAY

FORUMSYSTEMS

GENERAL

Forum Systems
Getting Started
Help

DIAGNOSTICS

GATEWAY

Network Policies
Network Policies
Proxy Policies
Cloud Policies
Cache Policies

WSDL Policies
WSDL Libraries
WSDL Policies

Content Policies
XML Policies
REST Policies
JSON Policies
HTML Policies
STS Policies
OAuth Policies
Tests

Task Policies
Task List Groups
Task Lists

Redirect Policies
Redirect Policies

Request Filters
Request Filters

RESOURCES

IDP

ACCESS

SYSTEM

PARTNERS

HTML POLICIES > HTML POLICY

HTML POLICY

Policy Name: Browser_to_Sentry_OAuth_Policy

Virtual Directories
Task Lists
Settings
IDP Rules
Logging

Virtual Directories > Virtual Directory: New Virtual Directory

VIRTUAL DIRECTORY

Name*: Login
Description:
Virtual URI: http://127.0.0.1:80/login(.)
Remote URI:

VIRTUAL URI SETTINGS

Listener Policy: HttpListenerPolicy
Virtual Host:
Use virtual host as a regular expression
Virtual Path: /login
Enable Virtual Path Case Insensitivity
Filter Expression: (.)
Replace Expression: \$0
Request Filter Policy: Default_HTML
Error Template: [From Listener Policy]

ACCESS CONTROL

IP ACL Policy: Unrestricted
ACL Policy: [Allow All]
XACML Policy: [None]
Password Authentication: [From Listener Policy]
Redirect Policy: [None]

VIRTUAL DIRECTORY TASKS

Request Task List Group: Task List Groups
Response Task List Group: Task List Groups

REMOTE SETTINGS

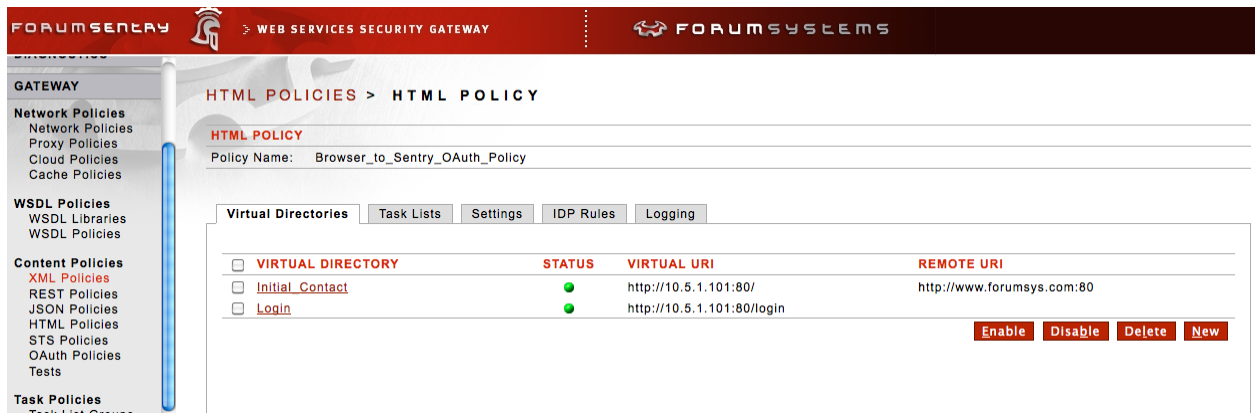
Send to remote server
Remote Policy: FIR_DSIT_RemotePolicy
Remote Path:
Host Header:
Process Response:
Discard response from server

Step 22: Under the Virtual Directory Tasks associate Request Task List Group to “Task_Group_Google_GrantType_OAuth_Code”. This is telling Sentry that when the user is redirected to /login virtual directory, Sentry will be processing the task in Task_Group_Google_GrantType_OAuth_Code. Click Save.

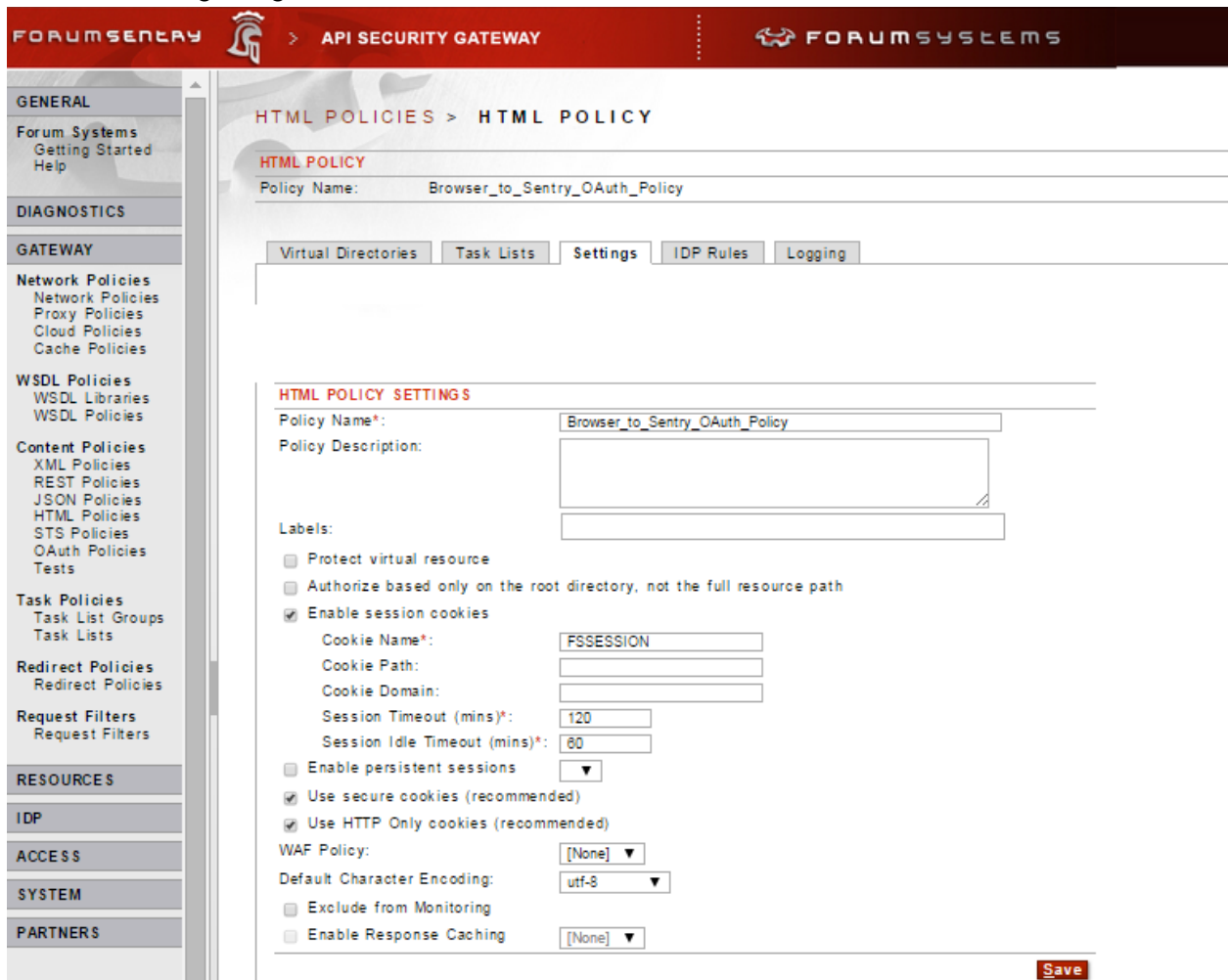
VIRTUAL DIRECTORY TASKS

Request Task List Group: Task List Groups No Labels Task_Group_GrantType_OA
Response Task List Group: Task List Groups Type or select label --NONE--

Step 23: Upon success, you will see the following screen. Click Settings.



Step 24: In the Settings screen, you want to check “Enable session cookies” and “Use secure cookies” options. This is the configuration which is telling Sentry to generate cookies for the user. This enables Single-Sign On for the user. Click Save.

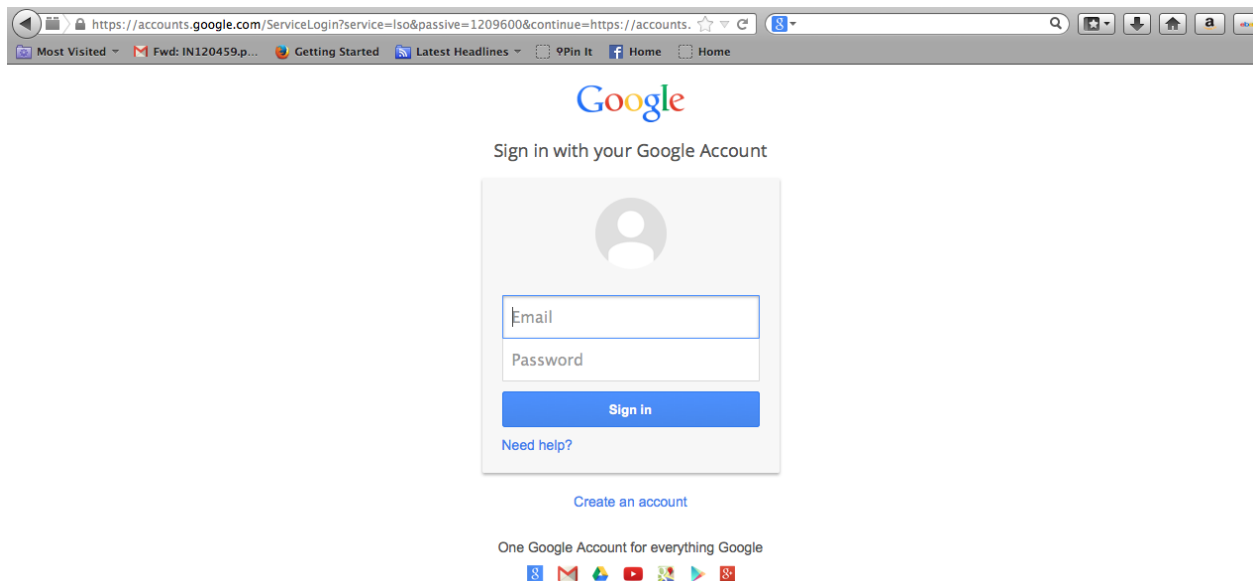


3.3.3 Testing Forum Sentry OAuth client

Step 1: Pick your favorite browser and enter <http://forum-oauth.com/>

Please make sure that your system that is running the browser can resolve the DNS name forum-oauth.com or any name that you are using to access Sentry.

Since you do not carry any credentials, your browser will be redirected to Google Authentication Server and page below will appear. Enter your Google credentials and sign in.



After successful login, the following screen will appear. It will be asking you to allow the app to fetch your profile information. Basically, at this step Google auth server is asking you that will it be okay with you if the app (Sentry in our case) will be allowed to access your email address and other profile data associated with your Google account. If you accept then you are allowing Sentry to make subsequent calls to fetch your email and profile data. Click Accept.



Project Default Service Account ▾

This app would like to:



View your email address



View basic information about your account



Project Default Service Account and Google will use this information in accordance with their respective terms of service and privacy policies.

Cancel

Accept

Once you click Accept, Google AUTH server will perform the following steps:

- Return your browser to Sentry.
- Sentry will fetch your Google profile data.
- Generate cookies.
- Send the cookies back to your browser with the instruction that your browser needs to access <http://forum-oauth.com>
- Your browser will connect to <http://forum-oauth.com> again with the cookies. This time it will be allowed to access www.forumsys.com. If it all goes well, you will see the Forum Systems page.



4.0 Forum Sentry as an OAuth Server with LDAP use case

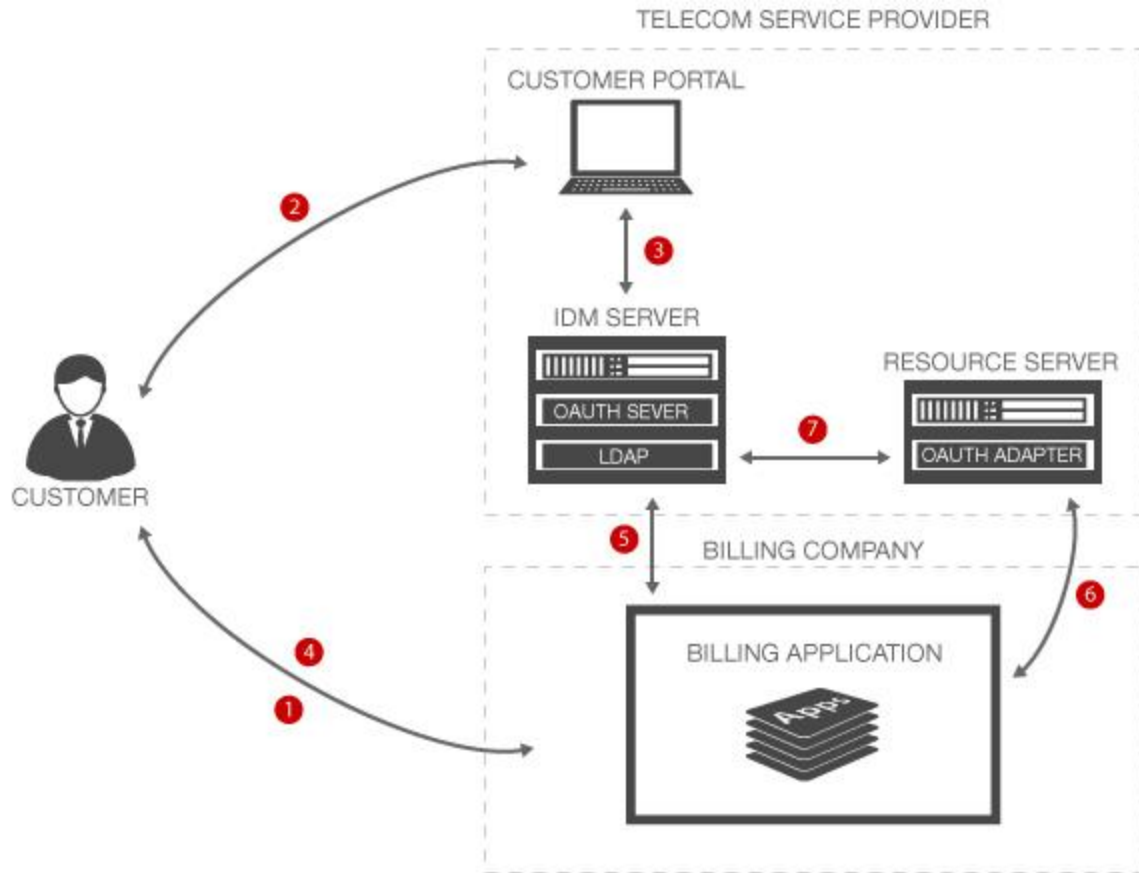
4.1 Use case without a Forum Sentry OAuth Server

An enterprise's identity management system is a critical component of its IT infrastructure. It is the primary service that is responsible for authenticating and authorizing an enterprise's users and applications as it contains a rich repository of users' identities and their profile data. For example, identity management for user-to-application interaction is a well-known domain that has been successfully addressed in the industry through standards such as LDAP. An LDAP enabled identity management system (IdM) is tightly-coupled with its enterprise applications. As enterprises continue to evolve, there is a constant demand to integrate with not only applications within its domain but applications outside its domain. The applications outside its domain are often referred to as partner applications or third-party applications.

An enterprise company may outsource some of its business services that are not core to its corporate strategy. For example, a telecom service provider may outsource customer billing to a third party. When a telecom customer needs to obtain his/her telecom bill, the request will be serviced by the third-party billing company's application (billing application). In order to fulfill this request, the partner application (billing application) is granted access to customer's call records, that is stored in a resource server controlled by the telecom service provider.

Access control mechanisms must be put in place to enable the telecom service provider to grant the billing application access to its call record in order to complete the billing process. The OAuth standard provides such mechanism for the customer to delegate access to the billing application and for the telecom service provider to leverage its existing IdM to validate the partner application's access request before giving access to customer's call record data. The IdM is OAuth enabled, and is often referred to as the OAuth server.

Figure 4 illustrates the deployment architecture for this type of scenario.



- 1 Customer attempts to connect to the billing application without username/password credentials.
- 2 Customer is redirected to the Telecom Service Provider's portal and asked to enter his/her username/password credentials.
- 3 Customer portal validates customer's credentials with the IdM. Upon successful validation, IdM generates OAuth credentials for the customer.
- 4 Customer is now redirected back to the billing application with OAuth credentials.
- 5 Billing application obtains an OAuth token on behalf of the customer.
- 6 Billing application uses OAuth token to retrieve customer records from the resource server.
- 7 The resource server validates the OAuth token with IdM server and then sends the customer records back to the billing application.

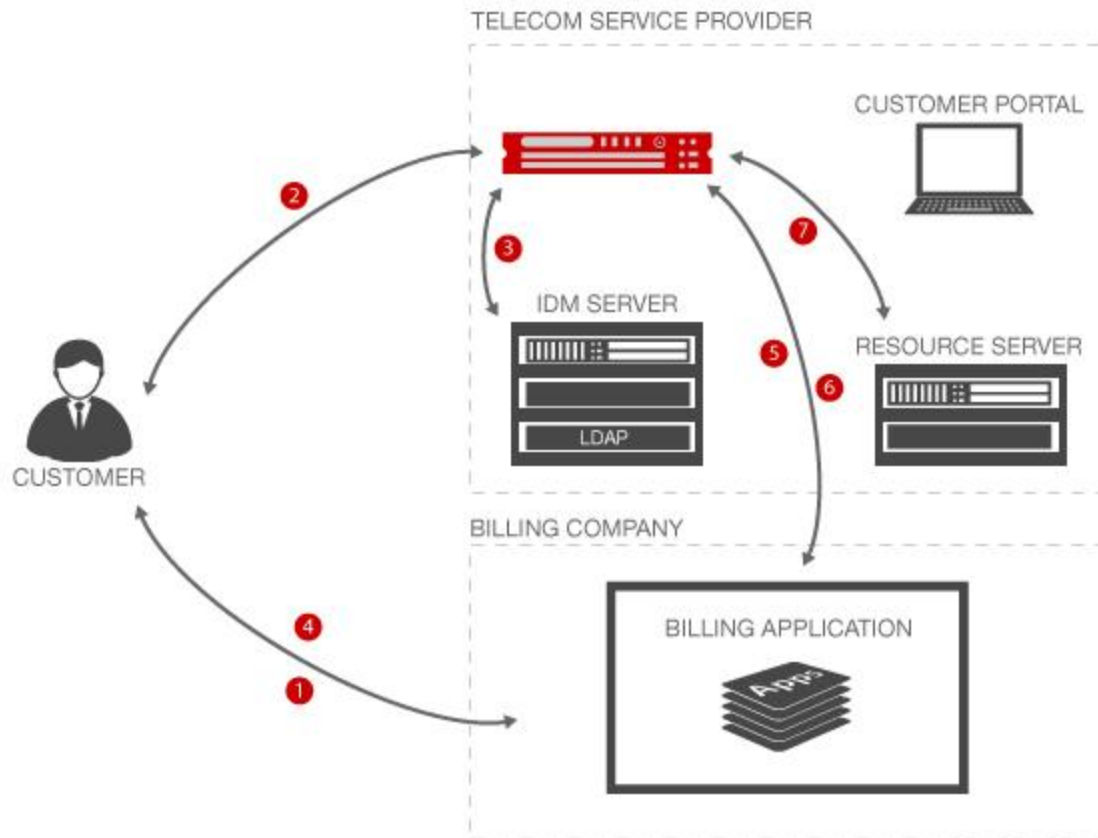
Figure 4: Enterprise OAuth enabled IdM Server generating, validating and consuming OAuth tokens

Although, an OAuth server enhances an enterprise's access control capabilities by authenticating and authorizing third party applications access to its resources, there are several challenges that arise:

- Existing enterprise IdM needs to be modified to be OAuth enabled or it needs to be replaced by a new OAuth enabled IdM.
- The resource server needs to be modified to be OAuth enabled. It needs to OAuth integration with the enterprise IdM.
- Managing and troubleshooting enterprise LDAP policies is a complex task. Adding OAuth management policies that need to be tightly-coupled with LDAP policies within an IdM further complicates the task.
- Over time, scalability becomes an issue as new resource servers are deployed. They must be integrated and tested for OAuth, which requires time and resources.
- Performance becomes an issue when SSL traffic is sent to an IdM containing OAuth requests.

4.2 Use case with a Forum Sentry OAuth Server

Figure 5 illustrates an architecture deployment with a dedicated API Security Gateway that performs the tasks of an OAuth server.



- 1 Customer attempts to connect to the billing application without username/password credentials.
- 2 Customer is redirected to the Telecom Service Provider's API Gateway (OAuth Server) and asked to enter his/her username/password credentials.
- 3 API Gateway validates customer's credentials with the IdM. Upon successful validation, IdM generates OAuth credentials for the customer.
- 4 Customer is now redirected back to the billing application with OAuth credentials.
- 5 Billing application obtains an OAuth token on behalf of the customer.
- 6 Billing application sends a request via the API Gateway, with customer's OAuth token, to retrieve customer records from the resource server.
- 7 After successful gateway validation of OAuth token, API Gateway passes customer record retrieval to the resource server.

Figure 5: Forum API Security Gateway as an OAuth Server generating, validating and consuming OAuth tokens

When an API Security gateway is added to the architecture deployment as an OAuth server, it addresses many of the challenges we discussed in the previous scenario:

- No modifications are required to the enterprise IdM.
- No modifications are required to the resource server.
- Diagnosing an access control issue becomes easier since OAuth policies are now loosely coupled with IdM LDAP policies.
- A dedicated API Security Gateway deployed as an OAuth server is a single point of enforcement that provides enterprise applications and users access control to their profile data.
- Scalability is no longer an issue as new resource servers can be deployed without any integration to an enterprise IdM.
- Centralized monitoring and enforcement is easier with an API Security Gateway. It provides full visibility to which application is accessing what service.
- Performance is no longer an issue since the API Security Gateway accelerates SSL traffic that communicates with cloud providers.

Using an API Security Gateway as part of your OAuth architecture becomes a minimally invasive IT operation. If your company is enabling more and more third-party applications, an API Security Gateway should be a key fabric of your enterprise's identity management strategy.

4.3 Configuring Forum Sentry as an OAuth Server with Grant Type: Auth Code

We will walk you step by step on how to configure Forum Sentry to achieve the scenario described in Figure 5. Forum Sentry supports OAuth Version 2.0 as an OAuth server.

Note: we recommend that you configure OAuth server policies on a brand-new instance of Forum Sentry. Avoid configuring policies on the same Forum Sentry instance that was configured in Section 3.3.2.

4.3.1 Configuring Forum Sentry Policies as an OAuth Server

We will be using Figure 6 as a frame of reference when configuring Forum Sentry.

We will need the following entities to accomplish our task of configuring the use case described in Figure 6.

- Forum API Security Gateway (OAuth Server) - Identified by a DNS name forumoauthserver.com
- User - A standard web browser
- Accessible back-end website - www.forumsys.com
- Accessible LDAP server: ldap.forumsys.com
- A second Forum API Security Gateway (OAuth Client) - Identified by a DNS name forum-oauth.com

Forum Sentry is an OAuth Server that will be configured to be an authentication and authorization service. For this configuration exercise, we will name the Forum Sentry OAuth server as forumoauthserver.com. You are free to select any name you like for the service. The only requirement is that the name of the OAuth server has a valid DNS mapping in your infrastructure. This Forum Sentry OAuth Server will treat the IdM (LDAP) and the resource server as one component. If you note in Figure 5, they are treated as two different components of the infrastructure. In our configuration example, they are treated as one. This is done for simplicity.

Figure 6 shows the various paths of access to forumoauthserver.com that need to be configured in order for the Forum OAuth server to provide an LDAP enabled OAuth service.

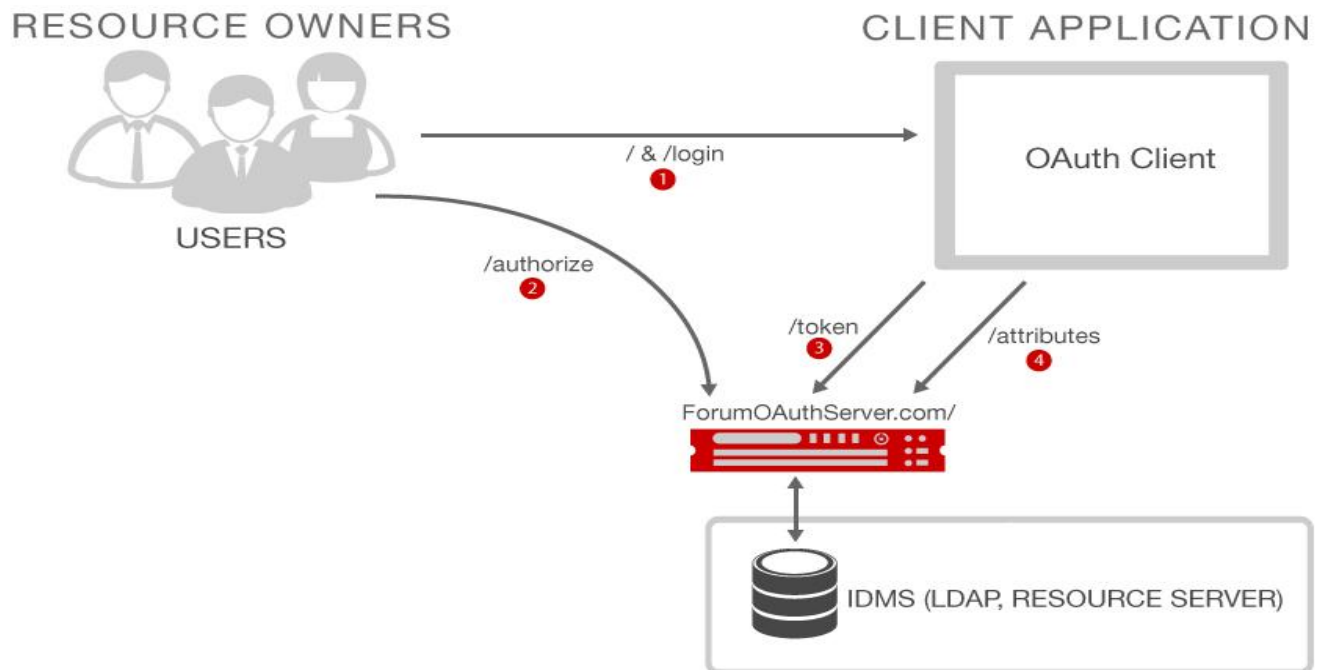


Figure 6: An OAuth Server through its OAuth policy can expose three main services via access paths defined by label 2, label 3 and label 4. Path <https://forumoauthserver.com/authorize>, identified by label 2, gives a requestor access to an OAuth code. Path <https://forumoauthserver.com/token>, identified by label 3, gives a requestor access to an OAuth token. Path <https://forumoauthserver.com/userinfo>, identified by label 4, gives a requestor access to user attributes or user profile data.

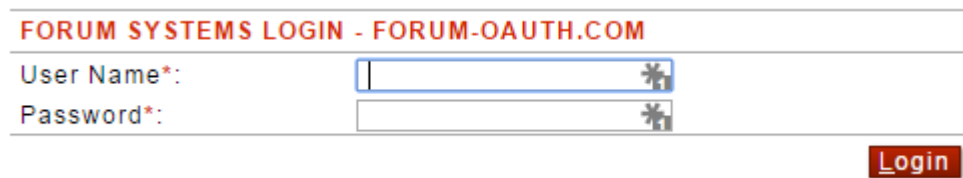
Based on Figure 6, we will be creating the following policies to accomplish our task.

- Listener Policy - This policy defines the IP address and TCP port that the Forum OAuth Server listens on for connections. For example, in figure 6, this listener could be listening on ip address identified with forumoauthserver.com.
- OAuth Policy - This is the master policy that defines authentication, authorization and resource services offered to users (resource owners) and client applications. For example, based on figure 6, the OAuth policy will enable three paths for access. <https://forumoauthserver.com/authorize>, <https://forumoauthserver.com/token>, and <https://forumoauthserver.com/userinfo>. The configuration and usage of each of these paths is further explained in section 4.3.2 Step 7.
- ACL Policy - This policy consumes the LDAP policy
- LDAP Policy - This is the policy that ties Forum OAuth Server to an LDAP Server.

We will be using ldap.forumsys.com which is an LDAP test server hosted in the Amazon cloud by Forum Systems. It is publicly available so users can easily test their authentication use cases against an LDAP server without going through the arduous task of installing and configuring an LDAP server. More information on this LDAP server can be found via this link:
<http://www.forumsys.com/tutorials/integration-how-to/ldap/api-identity-management-ldap-server/>

The identities configured on this server can be found via this link:
<http://www.forumsys.com/tutorials/integration-how-to/ldap/online-ldap-test-server/>

Step 1: Enter <https://forumoauthserver.com:5050> into your browser. The login page will appear. Enter your username and password and click “Login”.



FORUM SYSTEMS LOGIN - FORUM-OAUTH.COM

User Name*:

Password*:

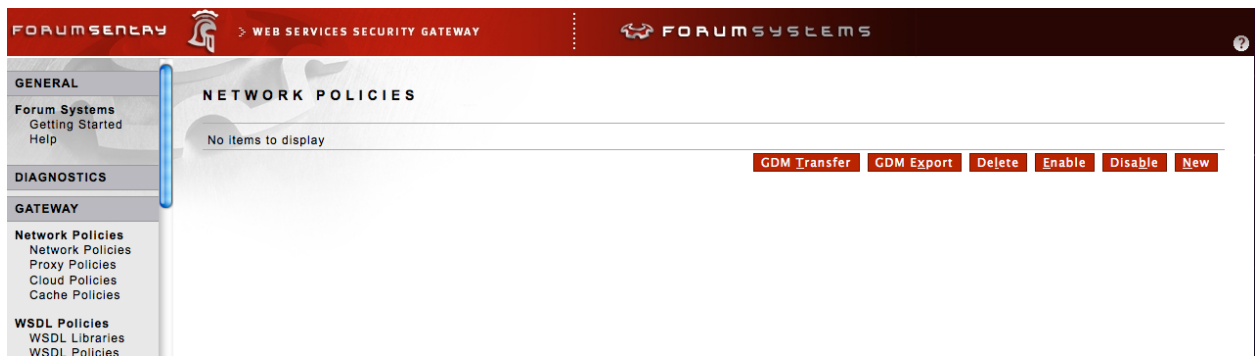
Login

Step 2: After successful login, the general admin page will appear. Click on “Gateway”

Step 3: The Gateway menu expands. Click on “Network Policies”



Step 4: Follow the steps shown in the following screen shots to create a local listener policy. This is the Sentry network service that will accept connections over an application protocol such as http. The Sentry listener will be bound to the IP of the machine that Sentry is running on. Start by clicking on the “New” button.



Select HTTP as the application protocol for the incoming connection. Click Next.



Select Listener as the option since Sentry will be receiving connections from users. Click Next.



Enter ForumOAuthListener then click Next

FORUMSENTRY



> API SECURITY GATEWAY

 FORUMSYSTEMS

GENERAL

Forum Systems
Getting Started
Help

DIAGNOSTICS

GATEWAY

NETWORK POLICIES > HTTP LISTENER POLICY

POLICY NAME

Policy Name*:

Labels:

Next

Select HTTP and HTTP Chunking as options and click Next.

FORUMSENTRY > API SECURITY GATEWAY FORUMSYSTEMS System Name: IP Address: 10

GATEWAY

- Network Policies
 - Network Policies
 - Proxy Policies
 - Cloud Policies
 - Cache Policies
- WSDL Policies
 - WSDL Libraries
 - WSDL Policies
- Content Policies
 - XML Policies
 - REST Policies
 - JSON Policies
 - HTML Policies
 - STS Policies
 - OAuth Policies

NETWORK POLICIES > HTTP LISTENER POLICY

INBOUND PROTOCOL

☐ HTTP

☒ HTTPS

☒ Use HTTP Chunking (recommended)

POLICY SELECTIONS

Policy Name: ForumOAuthListener

IP ACL Policy: Unrestricted

[Next](#)

Select Device IP and click Next.

FORUMSENTRY > API SECURITY GATEWAY FORUMSYSTEMS System Name: IP Address: 10

GATEWAY

- Network Policies
 - Network Policies
 - Proxy Policies
 - Cloud Policies
 - Cache Policies
- WSDL Policies
 - WSDL Libraries
 - WSDL Policies
- Content Policies
 - XML Policies
 - REST Policies
 - JSON Policies
 - HTML Policies
 - STS Policies
 - OAuth Policies

NETWORK POLICIES > HTTP LISTENER POLICY

LISTENER

☒ Use Device IP:

Listener Host*: 192.168.1.170

Listener Port*: 443

POLICY SELECTIONS

Policy Name: ForumOAuthListener

IP ACL Policy: Unrestricted

Inbound Protocol: HTTPS (chunked)

[Next](#)

No selection here. Click Next.

FORUMSENTRY > API SECURITY GATEWAY FORUMSYSTEMS System Name: IP Address: 1

GATEWAY

- Network Policies
 - Network Policies
 - Proxy Policies
 - Cloud Policies
 - Cache Policies
- WSDL Policies
 - WSDL Libraries
 - WSDL Policies
- Content Policies
 - XML Policies
 - REST Policies
 - JSON Policies
 - HTML Policies
 - STS Policies
 - OAuth Policies
 - Tests
- Task Policies
 - Task List Groups
 - Task Lists
- Redirect Policies
 - Redirect Policies

NETWORK POLICIES > HTTP LISTENER POLICY

PASSWORD AUTHENTICATION

☐ Use basic authentication:

☐ Use digest authentication:

☐ Use kerberos authentication:

☐ Use cookie authentication:

☐ Use form based authentication:

☐ Require password authentication (any type):

Password Authentication Realm:

POLICY SELECTIONS

Policy Name: ForumOAuthListener

IP ACL Policy: Unrestricted

Inbound Protocol: HTTPS (chunked)


Listener: 192.168.1.170:443

Timeout:

[Next](#)

Click Next to select the SSL Termination policy to use

FORUMSENTRY



> API SECURITY GATEWAY

FORUMSYSTEMS

System Name: A
IP Address: 10.5

GATEWAY

Network Policies

Network Policies

Proxy Policies

Cloud Policies

Cache Policies

WSDL Policies

WSDL Libraries

WSDL Policies

Content Policies

XML Policies

REST Policies

JSON Policies

HTML Policies

STS Policies

OAuth Policies

Tests

NETWORK POLICIES > HTTP LISTENER POLICY

SSL TERMINATION

SSL Termination Policy:

SSL_Termination_Policy

Edit

Next

POLICY SELECTIONS

Policy Name:

ForumOAuthListener

IP ACL Policy:

Unrestricted

Inbound Protocol:

HTTPS (chunked)

Listener:

192.168.1.170:443

Timeout:

Password Authentication:

Click on Finish.

You have successfully created a listener on TCP port 443. The green light indicates that it is actively waiting for connections.

NAME	STATUS	PROTOCOL	LISTENER ADDRESS	OTHER	DATE MODIFIED
ForumOAuthListener	●	HTTPS	0.0.0.0	Authentication: SSL Client Auth ACL: [Allow All]	2017/11/07 14:02

Step 5: Now you are ready to create an LDAP policy. In the left panel under “Access” menu click on LDAP. You will screen below. Click on New.

This is the main LDAP policy screen. Enter the following:

- Policy Name is Forum-LDAP-Server
- Enable Privilege Access is No
- Server is ldap.forumsys.com
- User is cn=read-only-admin, dc=example,dc=com

- Password is password

The screenshot shows the 'LDAP POLICIES > LDAP POLICY' configuration page. The left sidebar contains a tree view with categories like 'User ACLs', 'Admin Access', and 'User Policies'. The main content area is titled 'LDAP SERVER' and includes the following fields:

- Policy Name*:** Forum-LDAP-Server
- Enable privileged access:** ☐ Yes ☒ No
- Restrict Menus:** ☐
- Role policy:**
- Server*:** ldap.forumsys.com
- Port*:** 389
- Use SSL to connect:** ☐
- Authentication type:** Simple
- User*:** cn=read-only-admin,dc=example,dc=com
- Password*:** (masked with asterisks)
- Cache timeout (in minutes):** 30
- Read Timeout (in minutes):** 2

Scroll down further on the same screen. And enter the following:

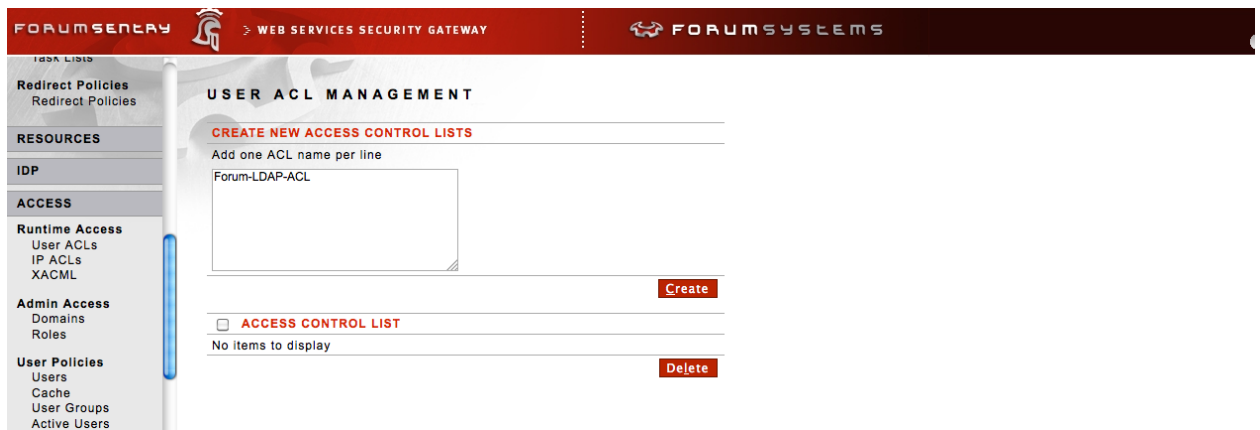
- Root DN as ou=mathematicians,dc=example,dc=com
- User/group context is Group containing users
- Click Apply
- Click Test to see if we can connect to the LDAP successfully. You will see the result at the top of the screen.
- If it is a success then click Save.

The screenshot shows the 'MAPPINGS' configuration page. It includes the following fields:

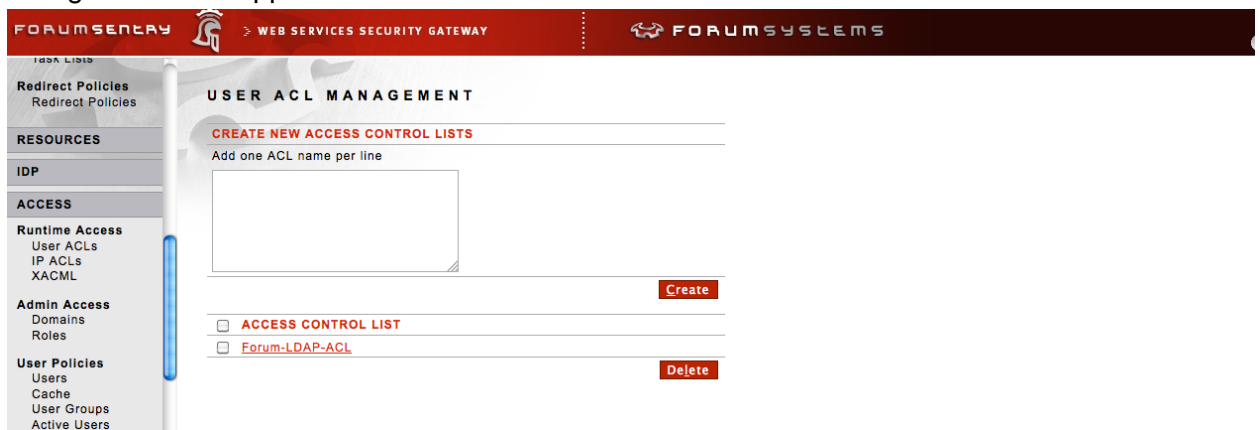
- Toggle Mappings :** LDAP v3
- Root DN*:** ou=mathematicians,dc=example,dc=com
- User/group context:** ☐ List of users ☒ Group containing users
- Optimized group search:** ☐

At the bottom, there are four buttons: Copy, Test, Apply, and Save.

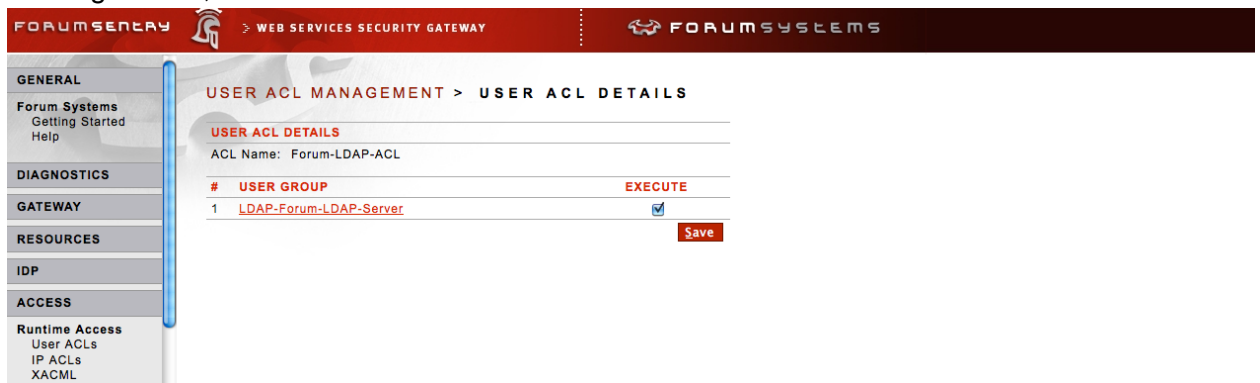
Step 6: You will create an Access Control List by first clicking on User ACLs under ACCESS menu in the left panel. In the screen below you will enter Forum-LDAP-ACL and click Create.



The following screen will appear. Now click on Forum-LDAP-ACL.



In the following screen, click on EXECUTE checkbox and click SAVE.



Step 7: In the left panel, under Content Policies click on OAuth Policies. The screen below will appear. Click on New.



The following screen is where you start entering data for parameters in the OAuth server policy. Before we provide the example data, we want to highlight some key points about the OAuth policy.

- Up to three access paths can be defined in a single OAuth server policy. These paths define various ways an OAuth server can be accessed for different tasks.
 - Listener policy with a default [/authorize](#) virtual directory is accessed by remote users or applications to provide credentials to an OAuth server and retrieve an OAuth code. This is the code which is then used by an application to retrieve an OAuth token. Figure 6 best illustrates the usage of this path.
 - Listener policy with a default [/token](#) virtual directory is accessed by remote applications to request an OAuth token. Figure 6 best illustrates the usage of this path.
 - Listener policy with a default [/userinfo](#) virtual directory is accessed by remote applications to request user attributes or profile data. For example, this could be your Facebook profile or Google profile or LinkedIn profile or an enterprise profile. Figure 6 best illustrates the usage of this path.
 - Each access path can either share the same listener policy or each one can have a unique listener policy.

Now we are ready to populate the fields in the following screen.

- Name is ForumOAuthServer_Policy
- Client Type is Confidential (Web Application).
- Client id is client1
- Client Secret is automatically generated.
- Grant Type is Authorization code.
- Redirect URI is forum-oauth.com/login. Once OAuth server authenticates the user, it redirects the user to the original target application location. In our case, it happens to be the OAuth enabled Sentry client as described in Figure 3.

Please note down the client id and client secret. You will need these to enter in the client application or another Forum Sentry that will be communicating as the client OAuth. Click Next.

The screenshot shows the 'NEW OAUTH POLICY' configuration page in the Forum Sentry API Security Gateway. The page is divided into several sections: GENERAL, DIAGNOSTICS, GATEWAY, and RESOURCES. The GATEWAY section is expanded, showing various policy categories like Network Policies, WSDL Policies, Content Policies, Task Policies, Redirect Policies, and Request Filters. The main configuration area is titled 'NEW OAUTH POLICY' and contains the following fields:

- NAME:** ForumOAuthServer_Policy
- DESCRIPTION:** (empty text area)
- Labels:** (empty text area)
- OAuth REQUEST PROCESSING:**
 - Client Authentication Mode:** ☒ Use these client credentials
 - Client Id*:** client1
 - Client Secret*:** ur_x/3eSk5sxpJkMXTCSA
 - Redirect URI*:** http://www.forumsys.com/sentry
 - ☐ Use this ACL to authenticate client
 - Client Authentication ACL:** [Allow All]
- Client Type:** ☒ Confidential (Web Application) ☐ Public (Native or JavaScript)
- Grant types*:** ☒ Authorization code ☐ Implicit ☐ Password ☐ Client credentials ☐ JWT ☐ SAML
- Scope*:** default openid
- ACL Policy (password grant):** [Allow All]
- Request Issuer:** http://www.forumsys.com/sentry
- Verification Policy:** [None]
- Request Processing:** Task List Groups, Type or select label, [None]

- OAuth RESPONSE PROCESSING:**
- Default Access Token Lifetime (secs)*:** 7200
- ☐ Default Refresh Token Lifetime (secs): 5184000
 - ☐ Reuse refresh token
- ☐ Enable persistent token storage
- OpenID Connect Issuer*:** http://www.forumsys.com/sentry
- OpenID Connect Signing Key:** [Use client secret]
- Response Processing:** Task List Groups, Type or select label, [None]

A 'Next' button is located at the bottom right of the configuration area.

Scroll down further. You bind OAuth server to a listener with virtual directory /keys. This creates a path to the OpenID Connect Signing Key. Click Next.

FORUMSENTRY > **API SECURITY GATEWAY** **FORUMSYSTEMS**

GENERAL
 Forum Systems
 Getting Started
 Help

DIAGNOSTICS

GATEWAY
Network Policies
 Network Policies
 Proxy Policies
 Cloud Policies
 Cache Policies
WSDL Policies
 WSDL Libraries
 WSDL Policies
Content Policies
 XML Policies
 REST Policies
 JSON Policies

OAUTH POLICIES > NEW OAUTH POLICY

OAuth policy settings saved

SET LISTENER POLICY
 Please specify a listener policy for virtual directory: keys

☒ Select from existing listener policies
 ForumOAuthListener (0.0.0.0) [Edit](#)

☐ Create a new HTTP listener policy
 Listener Policy Name*: OAUTH_Policy-Listener
 Use Device IP: ☐
 Listener Host*: 192.168.1.170
 Listener Port*: 80

SET VIRTUAL DIRECTORY PATH
 Virtual Directory Path: /keys

Next, you bind OAuth server to a listener with virtual directory /userinfo. This creates an entry point for remote applications that want to access resources protected by the OAuth server. Click Next.

FORUMSENTRY > **API SECURITY GATEWAY** **FORUMSYSTEMS**

GENERAL
 Forum Systems
 Getting Started
 Help

DIAGNOSTICS

GATEWAY
Network Policies
 Network Policies
 Proxy Policies
 Cloud Policies
 Cache Policies
WSDL Policies
 WSDL Libraries
 WSDL Policies
Content Policies
 XML Policies
 REST Policies

OAUTH POLICIES > NEW OAUTH POLICY

SET LISTENER POLICY
 Please specify a listener policy for virtual directory: userinfo

☒ Select from existing listener policies
 ForumOAuthListener (0.0.0.0) [Edit](#)

☐ Create a new HTTP listener policy
 Listener Policy Name*: ForumOAuthServer_Policy-Listener
 Use Device IP: ☐
 Listener Host*: 192.168.1.170
 Listener Port*: 80

SET VIRTUAL DIRECTORY PATH
 Virtual Directory Path: /userinfo

Scroll down further. You bind OAuth server to a listener with virtual directory /token This creates an entry point for remote applications that want to access OAuth token which is generated by the OAuth server. Click Next.

FORUMSENTRY **API SECURITY GATEWAY** **FORUMSYSTEMS**

GENERAL

Forum Systems
Getting Started
Help

DIAGNOSTICS

GATEWAY

Network Policies
Network Policies
Proxy Policies
Cloud Policies
Cache Policies

WSDL Policies
WSDL Libraries
WSDL Policies

Content Policies
XML Policies

OAUTH POLICIES > NEW OAUTH POLICY

SET LISTENER POLICY
Please specify a listener policy for virtual directory: token

☒ Select from existing listener policies
ForumOAuthListener (0.0.0.0) [Edit](#)

☐ Create a new HTTP listener policy

Listener Policy Name*: ForumOAuthServer_Policy-Listener

Use Device IP: ☐

Listener Host*: 192.168.1.170

Listener Port*: 80

SET VIRTUAL DIRECTORY PATH
Virtual Directory Path: /token

Scroll down further. You bind OAuth server to a listener with virtual directory /authorize. This creates an entry point for remote applications or users that request an OAuth code that is generated by the OAuth server. Before OAuth server issues an OAuth code, valid credentials need to be provided. Click Next.

FORUMSENTRY **API SECURITY GATEWAY** **FORUMSYSTEMS**

GENERAL

Forum Systems
Getting Started
Help

DIAGNOSTICS

GATEWAY

Network Policies
Network Policies
Proxy Policies
Cloud Policies
Cache Policies

WSDL Policies
WSDL Libraries
WSDL Policies

Content Policies
XML Policies

OAUTH POLICIES > NEW OAUTH POLICY

SET LISTENER POLICY
Please specify a listener policy for virtual directory: authorize

☒ Select from existing listener policies
ForumOAuthListener (0.0.0.0) [Edit](#)

☐ Create a new HTTP listener policy

Listener Policy Name*: ForumOAuthServer_Policy-Listener

Use Device IP: ☐

Listener Host*: 192.168.1.170

Listener Port*: 80

SET VIRTUAL DIRECTORY PATH
Virtual Directory Path: /authorize

The following screen appears with the three access paths to OAuth Server activated. The activation indicated by the green lights under status column. Click on “authorize” virtual directory.



This screen below details the access path which remote parties will call into to request an OAuth server to issue an OAuth authorization code. The OAuth server will have to validate the credentials of the requesting party before issuing the OAuth authorization code. The validation is achieved by tying this access path with an LDAP policy.

FORUMSENTRY

API SECURITY GATEWAY

FORUMSYSTEMS

System IP Address

GATEWAY

Network Policies

Network Policies

Proxy Policies

Cloud Policies

Cache Policies

WSDL Policies

WSDL Libraries

WSDL Policies

Content Policies

XML Policies

REST Policies

JSON Policies

HTML Policies

STS Policies

OAuth Policies

Tests

Task Policies

Task List Groups

Task Lists

Redirect Policies

Redirect Policies

Request Filters

Request Filters

RESOURCES

IDP

ACCESS

SYSTEM

PARTNERS

OAuth Policies > OAuth Policy

OAuth Policy

Policy Name: OAuth_Policy

OAuth

Virtual Directories

Settings

IDP Rules

Logging

Virtual Directories > Virtual Directory: authorize

VIRTUAL DIRECTORY

Name*: authorize

Description:

Listener Policy: ForumOAuthListener

Use virtual host as a regular expression

Virtual Host:

Enable Virtual Path Case Insensitivity

Virtual Path: /authorize

Virtual URL: https://127.0.0.1/authorize(/.*)?(\\?.*)?

Filter Expression: (/.)?(\\?.*)?

IP ACL Policy: Unrestricted

ACL Policy: [Allow All]

Password Authentication: [From Listener Policy]

Redirect Policy: [None]

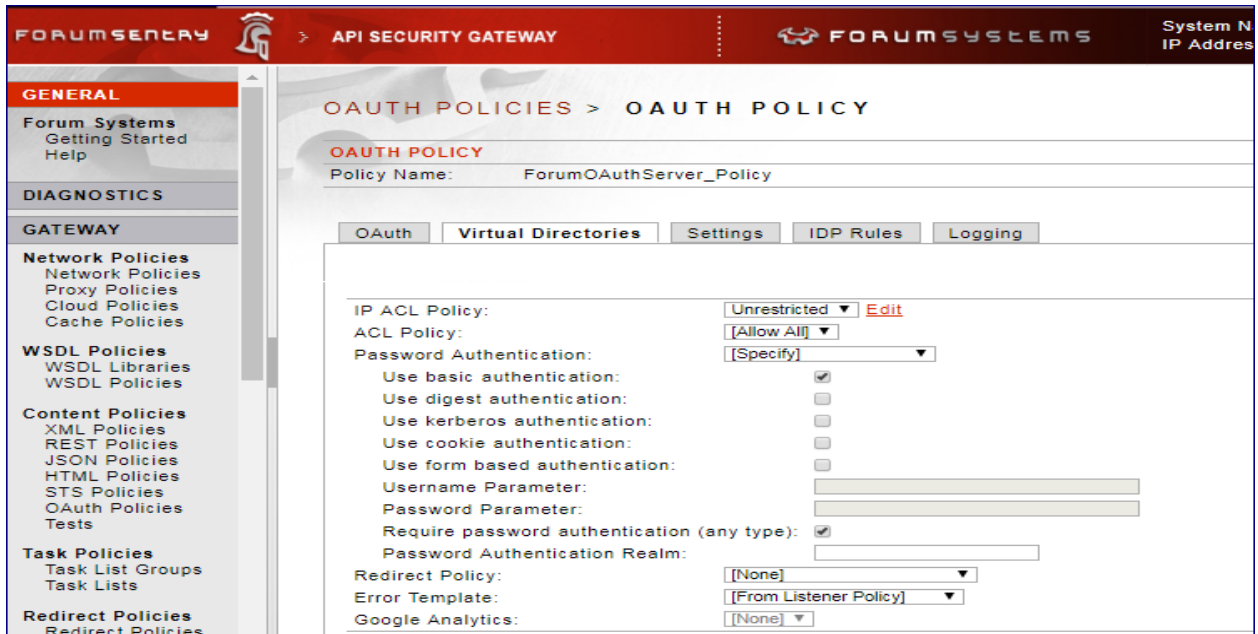
Error Template: [From Listener Policy]

Google Analytics: [None]

Scroll down the screen.

- In Password Authentication field select Specify.
- Check Basic Authentication
- Check Request password authentication
- Click Save.

Forum Sentry™ OAuth Client Configuration Guide | 58



4.3.2 Configuring Forum Sentry Policies as an OAuth client

To test the configuration in Section 4.3.1, you will need to configure an OAuth client. Please skip this whole section if you have your own custom OAuth client and are not using Forum Sentry API Security Gateway as an OAuth client described in figure 3. If you want to use a Forum Sentry API Security Gateway as an OAuth client then you need to follow the configuration steps described in Section 3.3.2 first and then follow the steps in this section. The steps described in this section are an add-on to the policies configured in section 3.3.2.

We strongly recommend that you should avoid configuring any of the OAuth client policies on Forum Sentry instance that acts as an OAuth server. The two Forum Sentry instances should be separated.

Step 1: The first step is to create a remote HTTP service policy. This remote HTTP service represents the Forum OAuth server. The Forum OAuth client through this service will know how to reach the Forum OAuth server.

- Click on Network Policies in the left panel.
- Select HTTP.
- Click Next.

FORUMSENTRY > **API SECURITY GATEWAY** **FORUMSYSTEMS**

GENERAL

Forum Systems
Getting Started
Help

DIAGNOSTICS

GATEWAY

Network Policies
Network Policies
Proxy Policies
Cloud Policies
Cache Policies

WSDL Policies
WSDL Libraries
WSDL Policies

Content Policies
XML Policies
REST Policies
JSON Policies
HTML Policies
STS Policies
OAuth Policies
Tests

Task Policies
Task List Groups
Task Lists

NETWORK POLICIES > NEW NETWORK POLICY

NETWORK POLICY PROTOCOL

☐ Advanced Message Queuing Protocol (AMQP)
☐ FTP
☒ HTTP
☐ SFTP
☐ SMTP
☐ Amazon S3

JMS PROTOCOLS

☐ ActiveMQ
☐ WebLogic
☐ IBM Websphere MQ
☐ JBoss
☐ Solace
☐ Sun Java MQ
☐ TIBCO EMS
☐ TIBCO Rendezvous

LOAD BALANCING / FAILOVER

☐ Group Remote

Next

Select Remote. Click Next.

FORUMSENTRY > **WEB SERVICES SECURITY GATEWAY** **FORUMSYSTEMS**

GENERAL

Forum Systems
Getting Started
Help

DIAGNOSTICS

GATEWAY

Network Policies
Network Policies
Proxy Policies
Cloud Policies
Cache Policies

WSDL Policies

NETWORK POLICIES > NEW NETWORK POLICY

NETWORK POLICY TYPE

☐ Listener
☒ Remote

Next

Enter the name of the Policy. We chose HttpRemote_ForumOAuthServer. Click Next.

FORUMSENTRY > **API SECURITY GATEWAY** **FORUMSYSTEMS**

GENERAL

Forum Systems
Getting Started
Help

DIAGNOSTICS

GATEWAY

Network Policies
Network Policies
Proxy Policies
Cloud Policies

NETWORK POLICIES > HTTP REMOTE POLICY

POLICY NAME

Policy Name*:
 Labels:

POLICY SELECTIONS

Next

Select HTTP. Click Next.

FORUMSENTRY > **API SECURITY GATEWAY** **FORUMSYSTEMS** System Name: API Security Gateway IP Address: 10.5.4.70

GATEWAY

- Network Policies**
 - Network Policies
 - Proxy Policies
 - Cloud Policies
 - Cache Policies
- WSDL Policies**
 - WSDL Libraries
 - WSDL Policies
- Content Policies**
 - XML Policies
 - REST Policies
 - JSON Policies
 - HTML Policies

NETWORK POLICIES > HTTP REMOTE POLICY

OUTBOUND PROTOCOL

☐ HTTP

☒ **HTTPS**

☒ Use HTTP Chunking

Next

POLICY SELECTIONS

Policy Name: HttpRemote_ForumOAuthServer

The location of the remote server

- Remote Server is forumoauthserver.com. This is the DNS name of the service.
- TCP port 443. It is the default selection.
- Basic Authentication Credentials should be checked. It should be note that the Forum OAuth Server does require authentication credentials before allowing access.
- Click Next.

FORUMSENTRY > **API SECURITY GATEWAY** **FORUMSYSTEMS** System Name: API Security Gateway IP Address: 10.5.4.70

GATEWAY

- Network Policies**
 - Network Policies
 - Proxy Policies
 - Cloud Policies
 - Cache Policies
- WSDL Policies**
 - WSDL Libraries
 - WSDL Policies
- Content Policies**
 - XML Policies
 - REST Policies
 - JSON Policies
 - HTML Policies
 - STS Policies
 - OAuth Policies
 - Tests
- Task Policies**
 - Task List Groups
 - Task Lists
- Redirect Policies**
 - Redirect Policies

NETWORK POLICIES > HTTP REMOTE POLICY

REMOTE SERVER

Remote Server*: forumoauthserver.com

Remote Port*: 443

Proxy Settings Policy: No Proxy

Provide Basic Authentication Credentials: ☒

Provide Digest Authentication Credentials: ☐

Dynamic EndPoint Routing: ☐

☒ Use Inbound HTTP Host header:

☐ Use Attribute*:

Proxy Client's User Agent: [From System Policy]

Next

POLICY SELECTIONS

Policy Name: HttpRemote_ForumOAuthServer

Outbound Protocol: HTTPS (chunked)

Select Propagate client's credentials. It means that the registered client or the app id and the secret password will be sent to Forum OAuth server.

FORUMSENTRY > API SECURITY GATEWAY FORUMSYSTEMS System Name: API IP Address: 10.5.4.7

GATEWAY

- Network Policies
 - Network Policies
 - Proxy Policies
 - Cloud Policies
 - Cache Policies
- WSDL Policies
 - WSDL Libraries
 - WSDL Policies
- Content Policies
 - XML Policies
 - REST Policies
 - JSON Policies
 - HTML Policies
 - STS Policies
 - OAuth Policies
 - Tests
- Task Policies

NETWORK POLICIES > HTTP REMOTE POLICY

REMOTE AUTHENTICATION

☐ Static credentials from User Policy
☐ Dynamic credentials from authenticated user
☒ Propagate client's credentials

[Next](#)

POLICY SELECTIONS

Policy Name: HttpRemote_ForumOAuthServer
Outbound Protocol: HTTPS (chunked)
Remote Server: forumoauthserver.com:443 (Basic Auth)

Select the SSL Initiation Policy to use. Click Next.

FORUMSENTRY > API SECURITY GATEWAY FORUMSYSTEMS System Name: API IP Address: 10.5.4.7

GATEWAY

- Network Policies
 - Network Policies
 - Proxy Policies
 - Cloud Policies
 - Cache Policies
- WSDL Policies
 - WSDL Libraries
 - WSDL Policies
- Content Policies
 - XML Policies
 - REST Policies
 - JSON Policies
 - HTML Policies
 - STS Policies
 - OAuth Policies

NETWORK POLICIES > HTTP REMOTE POLICY

SSL INITIATION

SSL Initiation Policy: [SSL_Initiation_Policy](#) [Edit](#)

[Next](#)

POLICY SELECTIONS

Policy Name: HttpRemote_ForumOAuthServer
Outbound Protocol: HTTPS (chunked)
Remote Server: forumoauthserver.com:443 (Basic Auth)
Remote Authentication: Propagate client's credentials

Select the defaults. Click Next.

FORUMSENTRY > API SECURITY GATEWAY FORUMSYSTEMS System Name: API IP Address: 10.5.4.7

GATEWAY

- Network Policies
 - Network Policies
 - Proxy Policies
 - Cloud Policies
 - Cache Policies
- WSDL Policies
 - WSDL Libraries
 - WSDL Policies
- Content Policies
 - XML Policies
 - REST Policies
 - JSON Policies
 - HTML Policies
 - STS Policies
 - OAuth Policies
 - Tests
- Task Policies

NETWORK POLICIES > HTTP REMOTE POLICY

TCP TIMEOUTS

☒ Custom connect timeout seconds
☒ Custom read timeout seconds
☐ Limit Connections

[Next](#)

POLICY SELECTIONS

Policy Name: HttpRemote_ForumOAuthServer
Outbound Protocol: HTTPS (chunked)
Remote Server: forumoauthserver.com:443 (Basic Auth)
Remote Authentication: Propagate client's credentials
SSL Initiation Policy: SSL_Initiation_Policy

Click Finish.

FORUMSENTRY > API SECURITY GATEWAY **FORUMSYSTEMS** System Name: IP Address: 10

GATEWAY

- Network Policies
 - Network Policies
 - Proxy Policies
 - Cloud Policies
 - Cache Policies
- WSDL Policies
 - WSDL Libraries
 - WSDL Policies
- Content Policies
 - XML Policies
 - REST Policies
 - JSON Policies
 - HTML Policies
 - STS Policies
 - OAuth Policies
 - Tests

NETWORK POLICIES > HTTP REMOTE POLICY

RESPONSE PROCESSING

☐ Process Response **Finish**

POLICY SELECTIONS

Policy Name: HttpRemote_ForumOAuthServer
Outbound Protocol: HTTPS (chunked)
Remote Server: forumoauthserver.com:443 (Basic Auth)
Remote Authentication: Propagate client's credentials
SSL Initiation Policy: SSL_Initiation_Policy
TCP Timeouts: Connect: 10 Read: 600 Connection Limit: Unlimited

You should land on this page. The green light indicates that the remote policy is activated.

FORUMSENTRY > API SECURITY GATEWAY **FORUMSYSTEMS** System Name: API Security Gateway A User: admin1 Version: 0.9.20
IP Address: 10.5.4.70 Date: 11/7/2017 2:12 PM Max Conns: Unlimited

GATEWAY	OAuth Listener Policies	STATUS	PROTOCOL	LISTENER ADDRESS	OTHER	DATE MODIFIED
<ul style="list-style-type: none"> Network Policies <ul style="list-style-type: none"> Network Policies Proxy Policies Cloud Policies Cache Policies WSDL Policies <ul style="list-style-type: none"> WSDL Libraries WSDL Policies Content Policies <ul style="list-style-type: none"> XML Policies 	<input type="checkbox"/> NAME <input checked="" type="checkbox"/> ForumOAuthListener	●	HTTPS	0.0.0.0	Authentication: SSL Client Auth ACL: [Allow All]	2017/11/07 14:02
	Remote Policies	STATUS	PROTOCOL	REMOTE ADDRESS	OTHER	DATE MODIFIED
	<input type="checkbox"/> NAME <input checked="" type="checkbox"/> HttpRemote_ForumOAuthServer	●	HTTPS	forumoauthserver.com	Authentication: Basic Process Response: Off	2017/11/07 14:13

Step 2: Click on Task Lists in the left panel under Task Policies. Then click on New.

FORUMSENTRY > WEB SERVICES SECURITY GATEWAY **FORUMSYSTEMS**

TASK LISTS

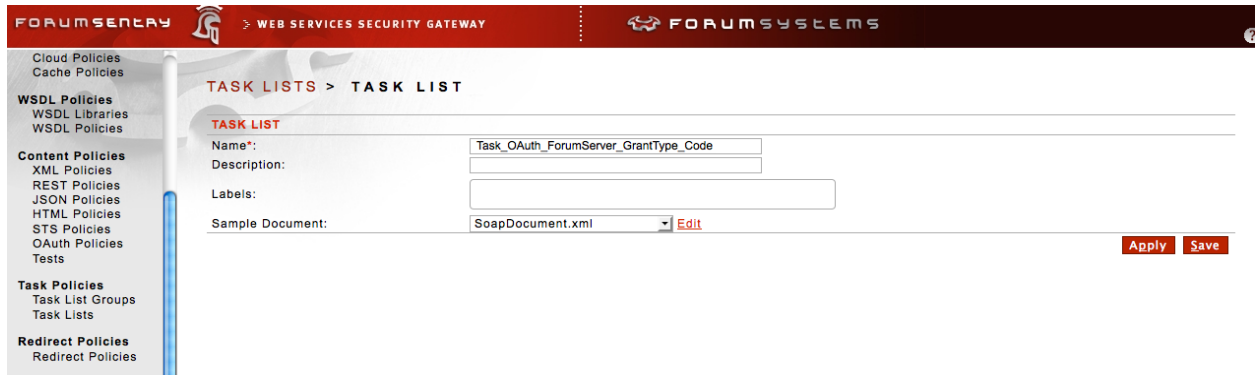
Search Usage: Type any text Filter Usage: Type the first letter of labels **Search**

No Labels [Always Show Expanded](#)

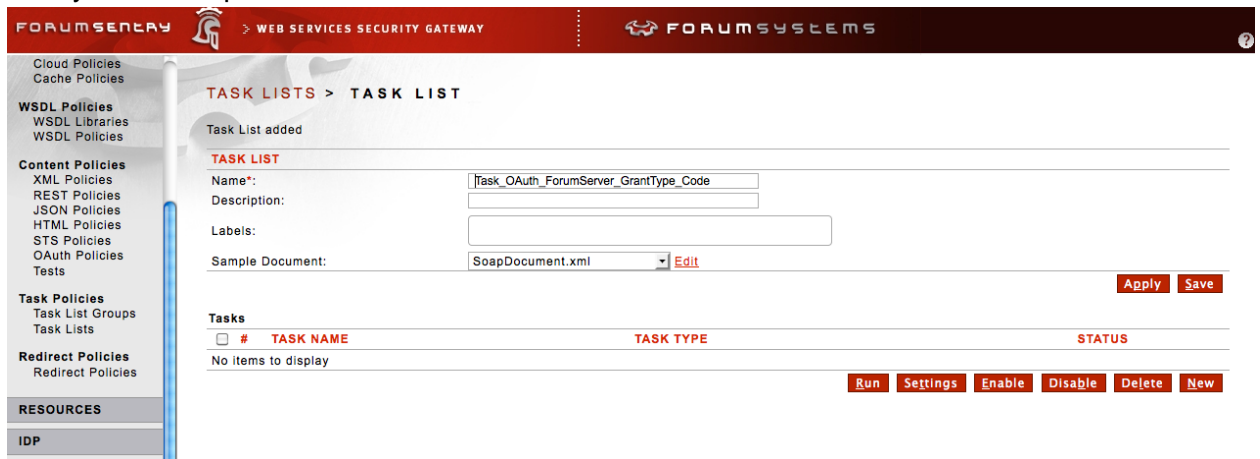
<input type="checkbox"/> NAME	STATUS
<input checked="" type="checkbox"/> Task_OAuth_Google_GrantType_OAuth_Code (1)	●

GDM Transfer GDM Export Add To New Task List Group Enable Disable Delete New Copy

The Name we enter is Task_OAuth_ForumServer_GrantType_OAuth. Then click Apply.



We are ready to add a specific task to the Task List. Select New.



Select User Identity & Access Control. Click Next.



Click Next.

FORUMSENTRY > API SECURITY GATEWAY FORUMSYSTEMS System Name: API Security Gateway A IP Address: 10.5.4.70

GENERAL
Forum Systems
Getting Started
Help

DIAGNOSTICS

GATEWAY
Network Policies
Network Policies
Proxy Policies

TASK LISTS > TASK LIST: TASK_OAUTH_FORUMSERVER_GRANTTYPE_OAUTH > CONTROL

TASK NAME

Task Name*: User Identity & Access Control

Next

USER IDENTITY & ACCESS CONTROL

Task Type: User Identity & Access Control

Uncheck “Map identified user to a known user”. Click Next.

FORUMSENTRY > API SECURITY GATEWAY FORUMSYSTEMS System Name: API Security Gateway A IP Address: 10.5.4.70

GENERAL
Forum Systems
Getting Started
Help

DIAGNOSTICS

GATEWAY
Network Policies
Network Policies
Proxy Policies
Cloud Policies
Cache Policies

TASK LISTS > TASK LIST: TASK_OAUTH_FORUMSERVER_GRANTTYPE_OAUTH > CONTROL

ACCESS CONTROL

Map identified user to a known user: ☐

ACL Policy: [Allow All] ▼

Next

USER IDENTITY & ACCESS CONTROL

Task Type: User Identity & Access Control

Task Name: User Identity & Access Control

Select Validate OAuth SSO token & establish identity.

FORUMSENTRY > API SECURITY GATEWAY FORUMSYSTEMS System Name: API Security Gateway A IP Address: 10.5.4.70

GENERAL
Forum Systems
Getting Started
Help

DIAGNOSTICS

GATEWAY
Network Policies
Network Policies
Proxy Policies
Cloud Policies
Cache Policies
WSDL Policies
WSDL Libraries
WSDL Policies
Content Policies
XML Policies
REST Policies
JSON Policies
HTML Policies
STS Policies
OAuth Policies
Tests

TASK LISTS > TASK LIST: TASK_OAUTH_FORUMSERVER_GRANTTYPE_OAUTH > TA CONTROL

USER IDENTITY MECHANISM

☐ Identity established in network policy (basic auth or client cert)
☐ Identity established by validating cookies
☐ Validate WS-Security & establish identity
☐ Validate SAML assertion & establish identity
☐ Validate SAML SSO assertion & establish identity
☐ Validate OAuth token & establish identity
☒ Validate OAuth SSO token & establish identity
☐ Identity established by attribute mapping
☐ Identity established by digital signature
☐ Identity established by Sentry REST authentication

Next

USER IDENTITY & ACCESS CONTROL

Task Type: User Identity & Access Control

Task Name: User Identity & Access Control

ACL Policy: No user mapping

Select Other.

FORUMSENTRY > API SECURITY GATEWAY FORUMSYSTEMS System Name: API Security Gateway A IP Address: 10.5.4.70

GENERAL
Forum Systems
Getting Started
Help

DIAGNOSTICS

GATEWAY
Network Policies
Network Policies
Proxy Policies
Cloud Policies
Cache Policies
WSDL Policies
WSDL Libraries
WSDL Policies
Content Policies
XML Policies
REST Policies
JSON Policies
HTML Policies

TASK LISTS > TASK LIST: TASK_OAUTH_FORUMSERVER_GRANTTYPE_OAUTH > CONTROL

IDENTITY PROVIDER

☐ Salesforce.com
☐ Microsoft
☐ Google
☐ Facebook
☐ LinkedIn
☐ Ping Identity
☒ Other

Next

USER IDENTITY & ACCESS CONTROL

Task Type: User Identity & Access Control
Task Name: User Identity & Access Control
ACL Policy: No user mapping
User Identity Mechanism: Validate OAuth SSO token & establish identity

This is the URL that contains the access location information of where one could obtain an OAuth code from. In our case it is the <http://forumoauthserver.com/authorize>. Click Next.

FORUMSENTRY > API SECURITY GATEWAY FORUMSYSTEMS System Name: API Security Gateway A IP Address: 10.5.4.70

GENERAL
Forum Systems
Getting Started
Help

DIAGNOSTICS

GATEWAY
Network Policies
Network Policies
Proxy Policies
Cloud Policies
Cache Policies
WSDL Policies
WSDL Libraries
WSDL Policies
Content Policies
XML Policies
REST Policies
JSON Policies
HTML Policies

TASK LISTS > TASK LIST: TASK_OAUTH_FORUMSERVER_GRANTTYPE_OAUTH > TASK CONTROL

SCOPE

Scope: default

Next

USER IDENTITY & ACCESS CONTROL

Task Type: User Identity & Access Control
Task Name: User Identity & Access Control
ACL Policy: No user mapping
User Identity Mechanism: Validate OAuth SSO token & establish identity
Identity Provider: Other
Authorization URL: http://forumoauthserver.com/authorize

This is where you select the remote policy. In our case it is the ForumOAuthServer that will issue the OAuth token. Click Next.

FORUMSENTRY > WEB SERVICES SECURITY GATEWAY **FORUMSYSTEMS**

TASK LISTS > TASK LIST: TASK_OAUTH_FORUMSERVER_GRANTTYPE_CODE > TASK: USER IDENTITY & ACCESS CONTROL

TOKEN ENDPOINT POLICY

Token Endpoint Policy: [Edit](#) [Next](#)

USER IDENTITY & ACCESS CONTROL

Task Type: User Identity & Access Control

Task Name: User Identity & Access Control

ACL Policy: No user mapping

User Identity Mechanism: Validate OAuth SSO token & establish identity

Identity Provider: Other

Authorization URL: http://forumoauthserver.com/authorize

Scope: default

The default end-point is /token. If this is what was configured in your Forum OAuth Server then you should leave it as is. Click Next.

FORUMSENTRY > WEB SERVICES SECURITY GATEWAY **FORUMSYSTEMS**

TASK LISTS > TASK LIST: TASK_OAUTH_FORUMSERVER_GRANTTYPE_CODE > TASK: USER IDENTITY & ACCESS CONTROL

TOKEN ENDPOINT PATH

Token Endpoint Path*: [Next](#)

USER IDENTITY & ACCESS CONTROL

Task Type: User Identity & Access Control

Task Name: User Identity & Access Control

ACL Policy: No user mapping

User Identity Mechanism: Validate OAuth SSO token & establish identity

Identity Provider: Other

Authorization URL: http://forumoauthserver.com/authorize

Scope: default

Token Endpoint Policy: HttpRemote_ForumOAuthServer

Token Endpoint Path: /token

Enter the Client Id and Client Secret. These two security attributes can be obtained from your Forum OAuth server under OAuth policy. These credentials are used to authenticate to the server. Click Next.

FORUMSENTRY > WEB SERVICES SECURITY GATEWAY **FORUMSYSTEMS**

TASK LISTS > TASK LIST: TASK_OAUTH_FORUMSERVER_GRANTTYPE_CODE > TASK: USER IDENTITY & ACCESS CONTROL

CLIENT CREDENTIALS

Client Id*:

Client Secret*:

Authentication: ☒ Form (not recommended) ☐ HTTP Basic ☐ SSL [Next](#)

USER IDENTITY & ACCESS CONTROL

Task Type: User Identity & Access Control

Task Name: User Identity & Access Control

ACL Policy: No user mapping

User Identity Mechanism: Validate OAuth SSO token & establish identity

Identity Provider: Other

Authorization URL: http://forumoauthserver.com/authorize

Scope: default

Token Endpoint Policy: HttpRemote_ForumOAuthServer

Token Endpoint Path: /token

Select the Remote policy. This Remote policy identifies the network location of the service that provides attributes of a user. Attributes such as your Facebook user profile data.

FORUMSENTRY > WEB SERVICES SECURITY GATEWAY **FORUMSYSTEMS**

TASK LISTS > TASK LIST: TASK_OAUTH_FORUMSERVER_GRANTTYPE_CODE > TASK: USER IDENTITY & ACCESS CONTROL

SERVICE ENDPOINT POLICY

Service Endpoint Policy: [Edit](#) [Next](#)

USER IDENTITY & ACCESS CONTROL

Task Type:	User Identity & Access Control
Task Name:	User Identity & Access Control
ACL Policy:	No user mapping
User Identity Mechanism:	Validate OAuth SSO token & establish identity
Identity Provider:	Other
Authorization URL:	http://forumoauthserver.com/authorize
Scope:	default
Token Endpoint Policy:	HttpRemote_ForumOAuthServer
Token Endpoint Path:	/token
Client Credentials:	client1 (Form)

The default virtual directory where the attributes of a user can be obtained. Again, this virtual directory path depends on what was configured in your OAuth server.

FORUMSENTRY > WEB SERVICES SECURITY GATEWAY **FORUMSYSTEMS**

TASK LISTS > TASK LIST: TASK_OAUTH_FORUMSERVER_GRANTTYPE_CODE > TASK: USER IDENTITY & ACCESS CONTROL

SERVICE ENDPOINT PATH

Service Endpoint Path*: [Next](#)

USER IDENTITY & ACCESS CONTROL

Task Type:	User Identity & Access Control
Task Name:	User Identity & Access Control
ACL Policy:	No user mapping
User Identity Mechanism:	Validate OAuth SSO token & establish identity
Identity Provider:	Other
Authorization URL:	http://forumoauthserver.com/authorize
Scope:	default
Token Endpoint Policy:	HttpRemote_ForumOAuthServer
Token Endpoint Path:	/token
Client Credentials:	client1 (Form)
Service Endpoint Policy:	HttpRemote_ForumOAuthServer

Click Next and then Next again

The variable “orgiUri” keeps the value of the original URI that a remote user accessed. This variable is declared in the Redirect Policy also. The OAuth engine wants to store this value so it knows which URI to redirect the user to once the OAuth token and attributes are obtained. In our example, this origUri points to http://forum-oauth.com/

Click Finish.

FORUMSENTRY > WEB SERVICES SECURITY GATEWAY **FORUMSYSTEMS**

TASK LISTS > TASK LIST

Configuration saved

TASK LIST

Name*: Task_OAuth_ForumServer_GrantType_Code

Description:

Labels:

Sample Document: SoapDocument.xml [Edit](#)

[Apply](#) [Save](#)

<input type="checkbox"/>	#	TASK NAME	TASK TYPE	STATUS
<input type="checkbox"/>	1	User Identity & Access Control	User Identity & Access Control	●

[Run](#) [Settings](#) [Enable](#) [Disable](#) [Delete](#) [New](#)

Click on Task Lists to see the activated task lists configured.

FORUMSENTRY > WEB SERVICES SECURITY GATEWAY **FORUMSYSTEMS**

TASK LISTS

Task List saved

Search Usage: Type any text Filter Usage: Type the first letter of labels [Search](#)

[Always Show Expanded](#)

<input type="checkbox"/>	NAME	STATUS
<input type="checkbox"/>	Task_OAuth_ForumServer_GrantType_Code (1)	●
<input type="checkbox"/>	Task_OAuth_Google_GrantType_OAuth_Code (1)	●

[GDM Transfer](#) [GDM Export](#) [Add To New Task List Group](#) [Enable](#) [Disable](#) [Delete](#) [New](#) [Copy](#)

Step 3: We now need to create a Task List Group. Click on Task List Groups under Task Policies. The screen below appears. Click New.

FORUMSENTRY > WEB SERVICES SECURITY GATEWAY **FORUMSYSTEMS**

TASK LIST GROUP

Search Usage: Type any text Filter Usage: Type the first letter of labels [Search](#)

[Always Show Expanded](#)

<input type="checkbox"/>	NAME	ASSOCIATIONS
<input type="checkbox"/>	System Request Group (0)	Policies(0)
<input type="checkbox"/>	System Response Group (0)	Policies(0)

<input type="checkbox"/>	NAME	ASSOCIATIONS
<input type="checkbox"/>	Task_Group_Google_GrantType_OAuth_Code (1)	Policies(1)

[GDM Transfer](#) [GDM Export](#) [Delete](#) [New](#)

Enter the Task List Group name.

FORUMSENTRY > WEB SERVICES SECURITY GATEWAY FORUMSYSTEMS

TASK LIST GROUP > TASK LIST GROUP DETAILS

NEW TASK LIST GROUP

Task List Group Name*: **Create**

Cloud Policies
Cache Policies

WSDL Policies
WSDL Libraries
WSDL Policies

Content Policies
XML Policies
REST Policies
JSON Policies
HTML Policies
STS Policies
OAuth Policies
Tests

Task Policies
Task List Groups
Task Lists

Redirect Policies
Redirect Policies

Add the Task List Task_OAuth_ForumServer_GrantType_Code. Click Add.

FORUMSENTRY > API SECURITY GATEWAY FORUMSYSTEMS

TASK LIST GROUP > TASK LIST GROUP DETAILS

TASK LIST GROUP DETAILS

Task List Group Name*:

Description:

Process Each Task List Below in Sequence: ☐

Labels:

#	TASK LIST	STATUS
No items to display		
No Labels	Task_OAuth_ForumServer_GrantType_OAuth	Add

Remove Apply Save

[Always Show Expanded](#)

After the Add the screen is updated. Click Save.

FORUMSENTRY > WEB SERVICES SECURITY GATEWAY FORUMSYSTEMS

TASK LIST GROUP > TASK LIST GROUP DETAILS

TASK LIST GROUP DETAILS

Task List Group Name: Task_Group_Forum_OAuthServer_GrantType_Code

Description:

Process Each Task List Below in Sequence: ☐

Labels:

☐ # **TASK LIST** Always Show Expanded STATUS

☐ 1 ☒ Task_OAuth_ForumServer_GrantType_Code(1)

Task_OAuth_Google_GrantType_OAuth_Code [Add](#)

[Remove](#) [Apply](#) [Save](#)

Step 4: This is the final step. Click on HTML policies under the GATEWAY menu in the left panel. The screen below shows the existing HTML policy. Click on [Browser_to_Sentry_OAuth_Policy](#) link in red.

FORUMSENTRY > WEB SERVICES SECURITY GATEWAY FORUMSYSTEMS

HTML POLICIES

Search Usage: Type any text Filter Usage: Type the first letter of labels [Search](#)

No Labels

<input type="checkbox"/>	NAME	VIRTUAL DIRECTORY	STATUS	VIRTUAL URI	REMOTE URI	LISTENER ACL	DIRECTORY
<input type="checkbox"/>	Browser_to_Sentry_OAuth_Policy	Initial_Contract	●	http://10.5.1.101:80/	http://www.forumsys.com:80	[Allow All]	[Allow All]
		Login	●	http://10.5.1.101:80/login		[Allow All]	[Allow All]

[GDM Transfer](#) [GDM Export](#) [Delete](#) [New](#) [Copy](#)

The screen with the list of two virtual directories appears below. We are interested in the Login virtual directory since that is the one that triggers the OAuth processing if access this virtual directory. Click on Login.

FORUMSENTRY > WEB SERVICES SECURITY GATEWAY **FORUMSYSTEMS**

Forum Systems
Getting Started
Help

HTML POLICIES > HTML POLICY

HTML POLICY

Policy Name: Browser_to_Sentry_OAuth_Policy

Virtual Directories Task Lists Settings IDP Rules Logging

<input type="checkbox"/> VIRTUAL DIRECTORY	STATUS	VIRTUAL URI	REMOTE URI
<input type="checkbox"/> Initial Contact	●	http://10.5.1.101:80/	http://www.forumsys.com:80
<input type="checkbox"/> Login	●	http://10.5.1.101:80/login	

[Enable](#) [Disable](#) [Delete](#) [New](#)

You will see the details of the Login virtual directory

FORUMSENTRY > WEB SERVICES SECURITY GATEWAY **FORUMSYSTEMS**

Forum Systems
Getting Started
Help

HTML POLICIES > HTML POLICY

HTML POLICY

Policy Name: Browser_to_Sentry_OAuth_Policy

Virtual Directories Task Lists Settings IDP Rules Logging

Virtual Directories > Virtual Directory: Login

VIRTUAL DIRECTORY

Name*:

Description:

Listener Policy: [Edit](#)

☐ Use virtual host as a regular expression

Virtual Host:

Virtual Path:

Virtual URI:

Filter Expression:

Replace Expression:

Scroll down the screen and in the Request Task List Group down you will select the task list Task_Group_Forum_OAuthServer_GrantType_Code. This is where you hook the virtual directory with OAuth processing. Click Save.

FORUMSENTRY > **API SECURITY GATEWAY** **FORUMSYSTEMS**

HTML POLICIES > HTML POLICY

HTML POLICY

Policy Name: Browser_to_Sentry_OAuth_Policy

Virtual Directories Task Lists Settings IDP Rules Logging

Virtual Directories > Virtual Directory: Login

VIRTUAL DIRECTORY

Name*: Login

Description:

Virtual URI: http://127.0.0.1:80/login(.*)

Remote URI:

VIRTUAL URI SETTINGS

Listener Policy: HttpListenerPolicy Edit

Virtual Host:

☐ Use virtual host as a regular expression

Virtual Path: /login

☐ Enable Virtual Path Case Insensitivity

Filter Expression: (.*)

Replace Expression: \$0

Request Filter Policy: Default_HTML Edit

Error Template: [From Listener Policy]

ACCESS CONTROL

IP ACL Policy: Unrestricted Edit

ACL Policy: [Allow All]

XACML Policy: [None]

Password Authentication: [From Listener Policy]

Redirect Policy: [None]

VIRTUAL DIRECTORY TASKS

Request Task List Group: Task List Groups Type or select label Task_Group_GrantType_OA Edit

Response Task List Group: Task List Groups Type or select label --NONE--

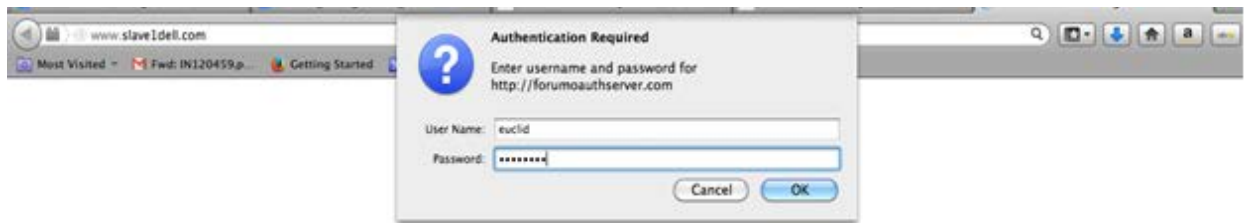
4.3.3 Testing Forum Sentry OAuth server

Please make sure that your system that is running the browser can resolve the DNS name `forum-oauth.com` or any name that you are using to access Sentry OAuth client.

You will be prompted for credentials. Enter the following if you are using Forum LDAP server.

Enter User Name: `euclid`

Password: `password`



Once you click Accept, Forum Systems OAuth server will perform the following steps:

- Return your browser to OAuth client (your application or Forum Sentry OAuth client).
- Application will fetch your LDAP profile data via Forum Sentry OAuth server.
- Generate cookies.
- Send the cookies back to your browser with the instruction that your browser needs to access `http://forum-oauth.com`
- Your browser will connect to <http://forum-oauth.com> again with the cookies. This time it will be allowed to access www.forumsys.com. If it all goes well, you will see the Forum Systems page.

