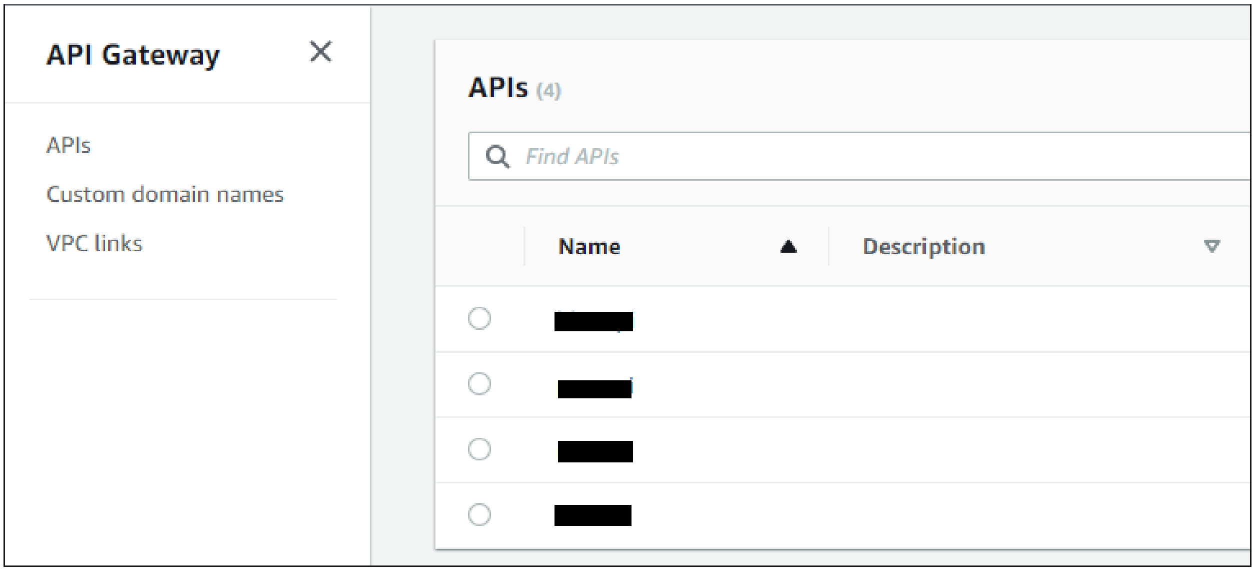
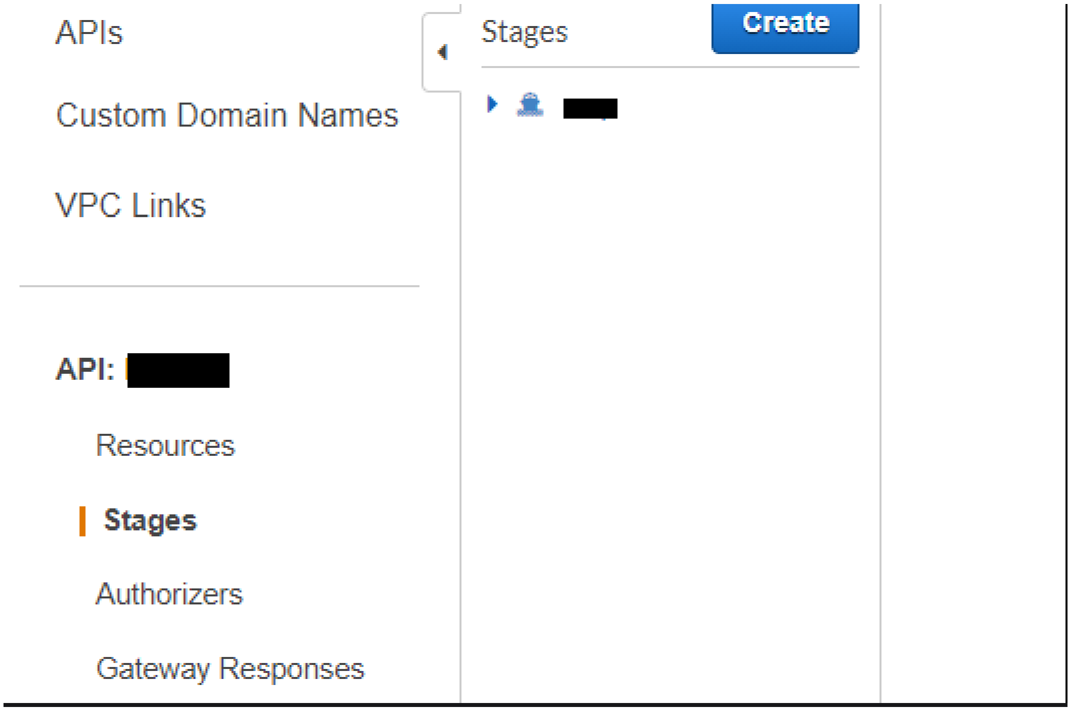
How to turn on logs for an API Gateway

If you already have logs enabled, please skip to the IAM POLICY section

1. Go into the API Gateway interface using this link.

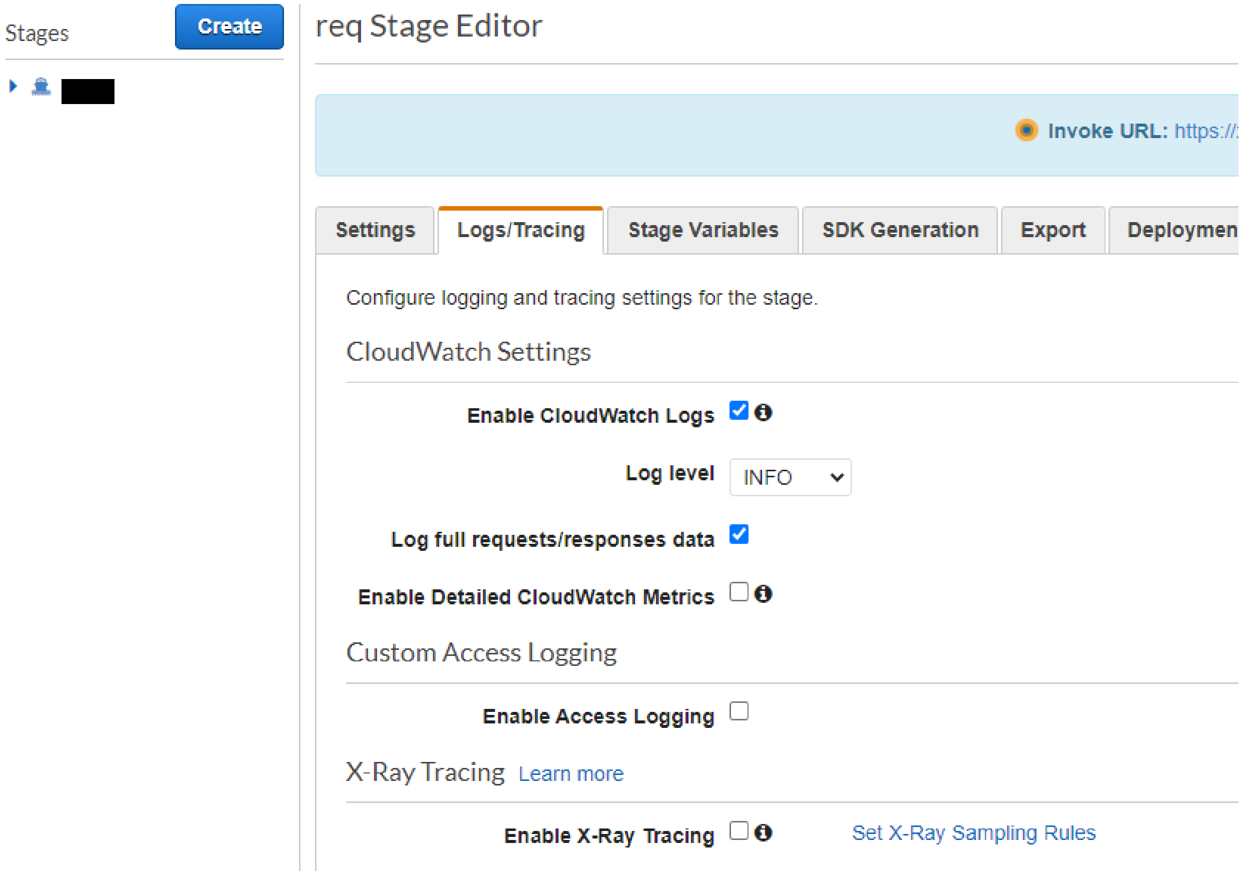


2. Click on the API you want to turn on logs for.
3. Navigate to the Stages panel.



4. Pick the stage that you want to turn on logs for and then navigate to the Logs/Tracing tab.

5. Tick the ‘Enable CloudWatch Logs’ tickbox, then pick ‘Info’ as the Log Level and also tick the ‘Log full request/response data’ checkbox.



req Stage Editor

Invoke URL: https://

Configure logging and tracing settings for the stage.

CloudWatch Settings

Enable CloudWatch Logs ☑

Log level INFO

Log full requests/responses data ☑

Enable Detailed CloudWatch Metrics □

Custom Access Logging

Enable Access Logging □

X-Ray Tracing Learn more

Enable X-Ray Tracing □ Set X-Ray Sampling Rules

6. Click on ‘Save Changes’.
7. For more information, click here or contact us.

Lambda installation

IAM policy:

1. Enter the IAM interface.
2. Enter the Policies page and click “Create Policy”.
3. In the “Create Policy” page choose the “JSON” option and copy the file named “blstsecurity-logs-policy.json” into there.
4. Click next until you reach the “Review” stage, in the policy name, write “blstsecurity-logs-policy”, and afterwards click “Create Policy”.

IAM role:

1. Enter the IAM interface.

2. Enter the Roles page and click “Create Role”.
3. In the “Create Role” page choose the “Lambda” use case and go into the next page(“permissions”).
4. In the “Permissions” page look for the policy you created in the previus section(blstsecurity-logs-policy) and activate it.
5. Click next until you reach the last page of “Create Role”, in this page give the role the name “blstsecurity-logs-role” and click “Create role”.

Lambda:

1. Enter the Lambda interface.
2. Enter the “Functions” page and click on “Create function”.
3. In the lambda name enter “blstsecurity-logs”, and in the “Runtime” choose “Python 3.8”.
4. Click on the “change default execution role” and choose the “Use an existing role” option and choose the role name you previously created(“blstsecurity-logs-role”).
5. Create the lambda by clicking on “Create function”.
6. After the lambda was created, enter the create lambda’s interface and click on “Configuration”, in the given page choose the “General configuration” option, there you should edit and change the “Timeout” to 2 minutes.
7. Afterwards return to the “Code” page and choose the option of “Upload from” and then choose “.zip file” and upload the zip file named “blstsecurity-logs”.
8. Test the lambda, wait until it’s over and open the “Execution result” tab(right next to the “Code” tab), in it, look for a “success” response, which will indicate a successful installation.