Zscaler Deployment Guide

Nov 2021

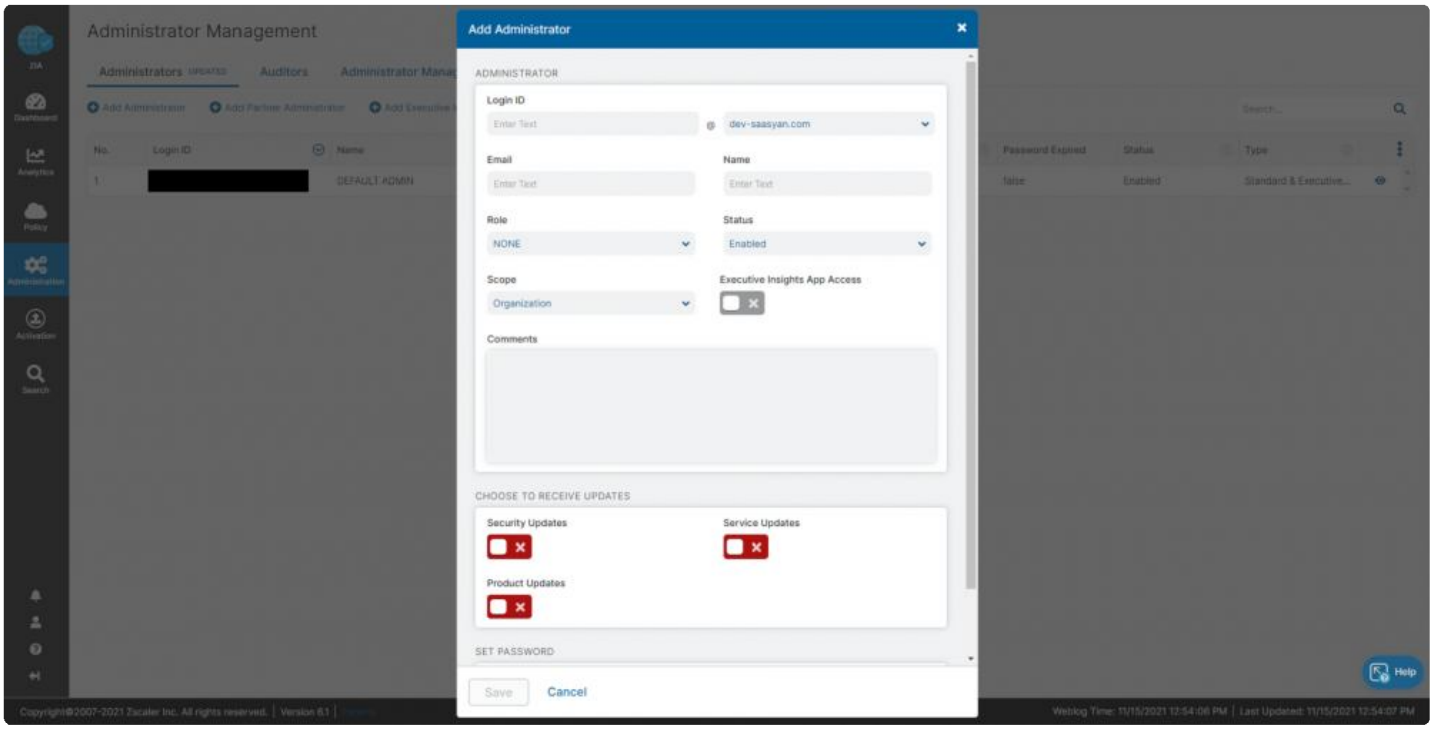
For the latest documentation, please go to https://docs.saasyan.com.au/manuals/assure-deployment-guide/1/en/topic/zscaler-specific-configuration-steps

Zscaler Specific Configuration Steps

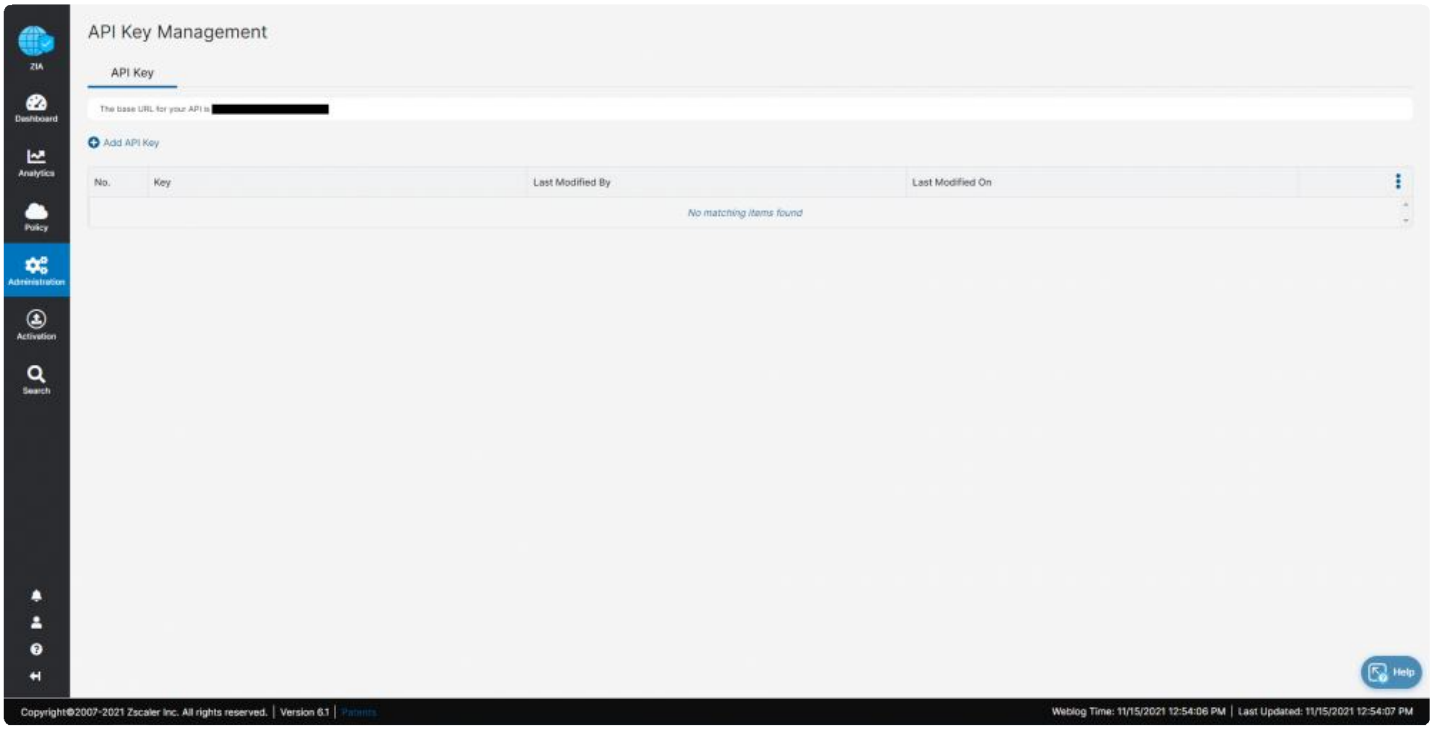
The below steps need to be performed in the **Zscaler Cloud Portal.**

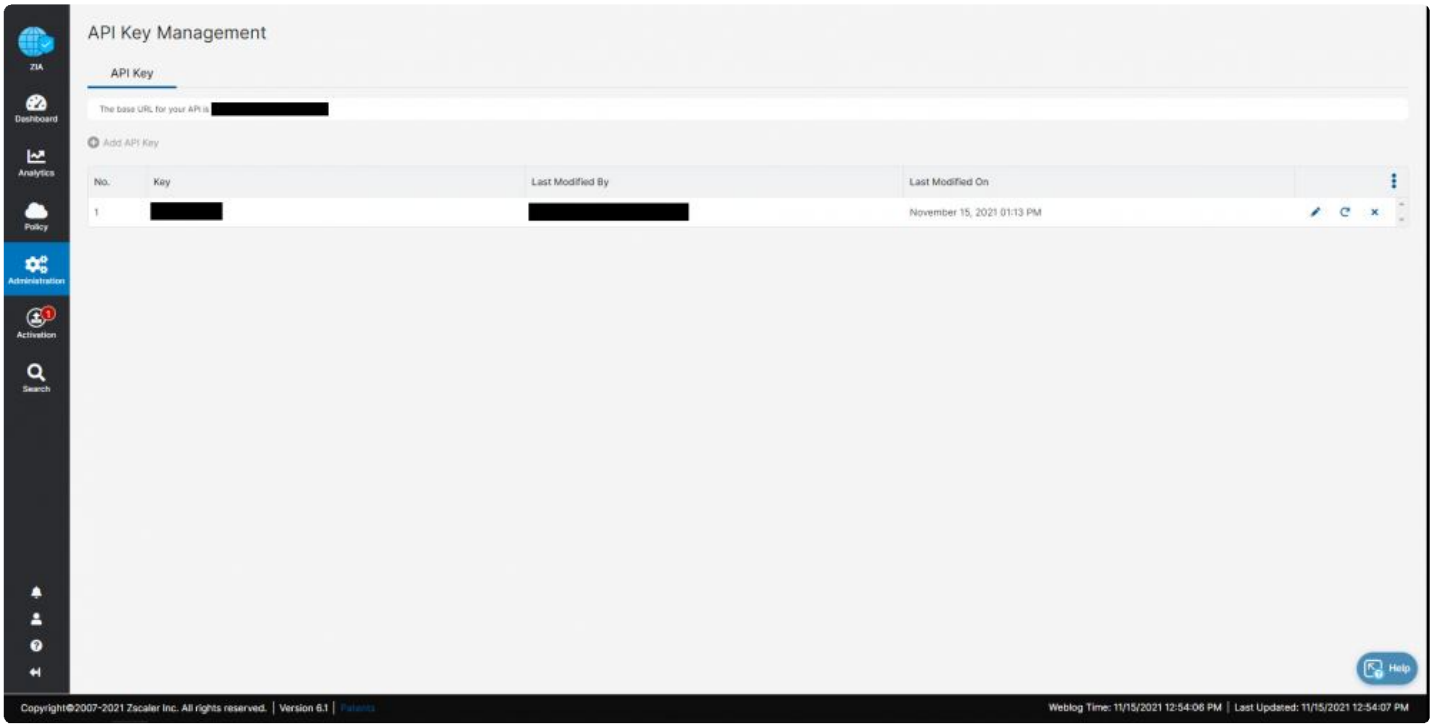
Create Admin account and generate API Key

- Navigate to Administration -> Authentication -> Administrator Management and click on Add Administrator. Make sure you select Super Admin for the role.



- Navigate to Administration -> Authentication -> API Key Management and click on Add API Key.



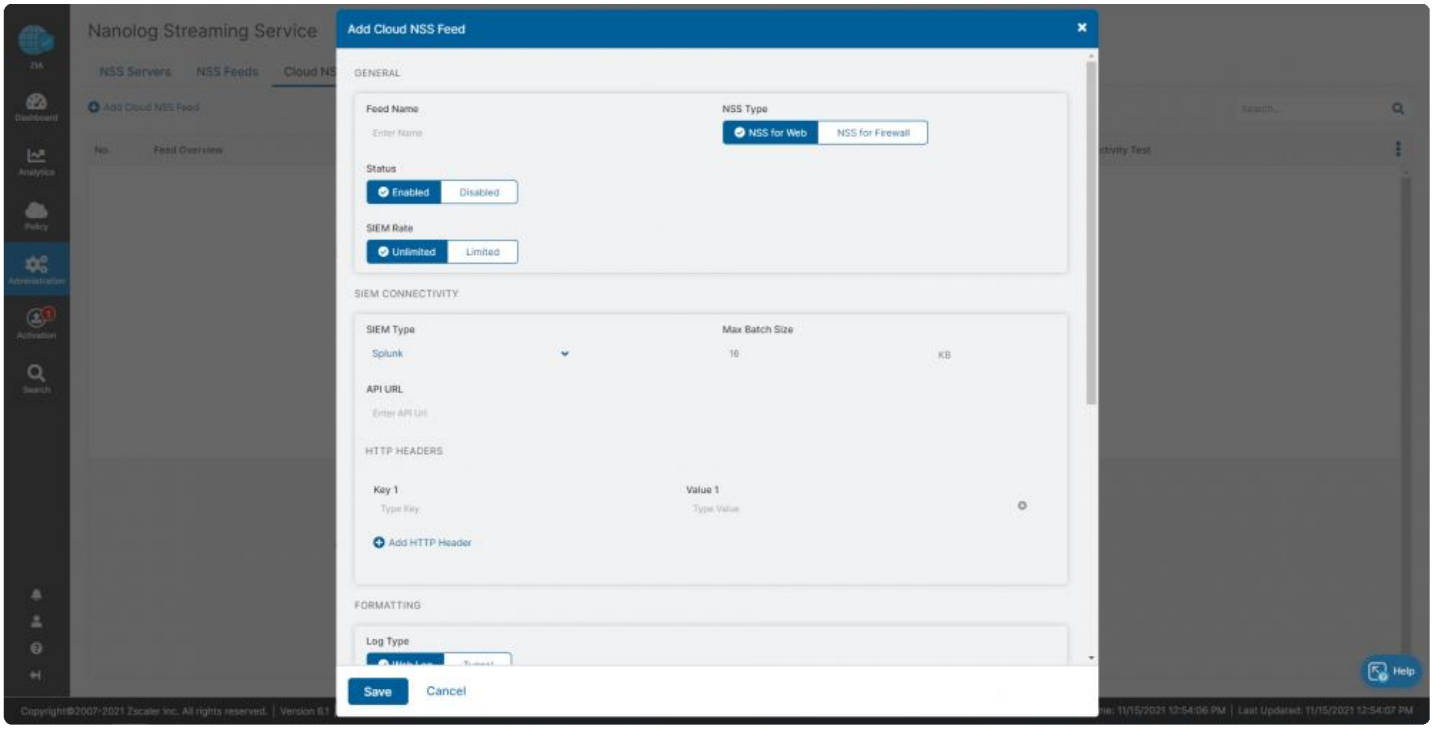


- Send Saasyan the admin credentials, the API key and the base URL for the API. These will be used by Assure to interact with the ZIA.

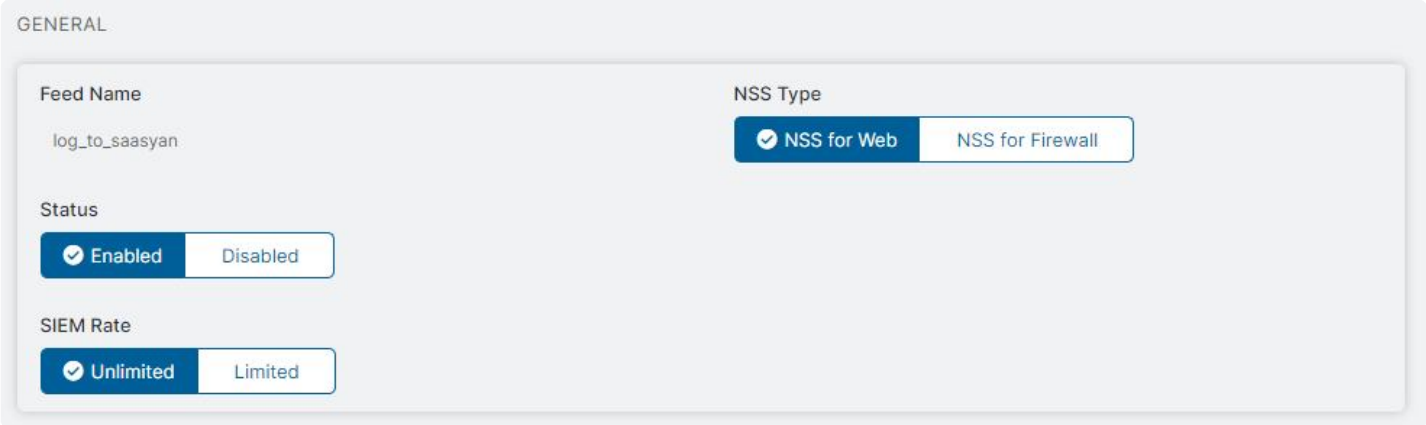
Log Forwarding

- This is for ZIA to forward logs to the Assure log receivers.
- Navigate to Administration -> Settings -> Nanolog Streaming Service, select the Cloud NSS Feeds tab and click on Add Cloud NSS Feed.

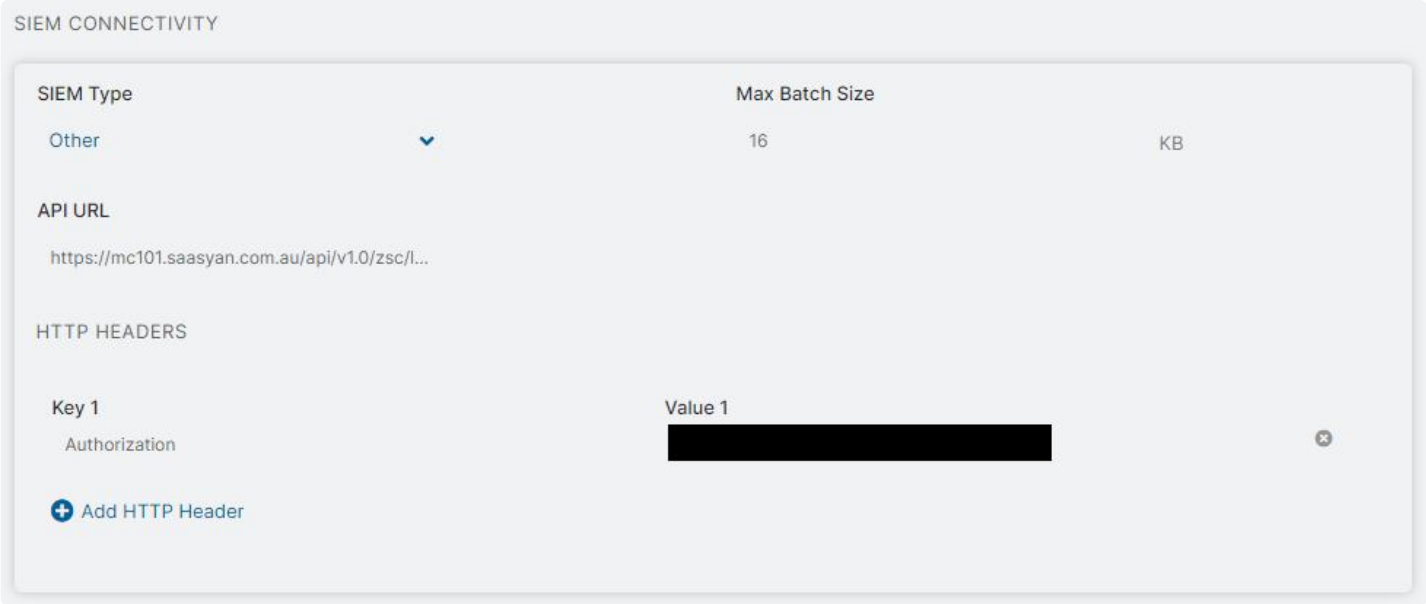
NOTE: If the Cloud NSS Feeds tab is not visible, please contact the Zscaler Support Team to enable this.



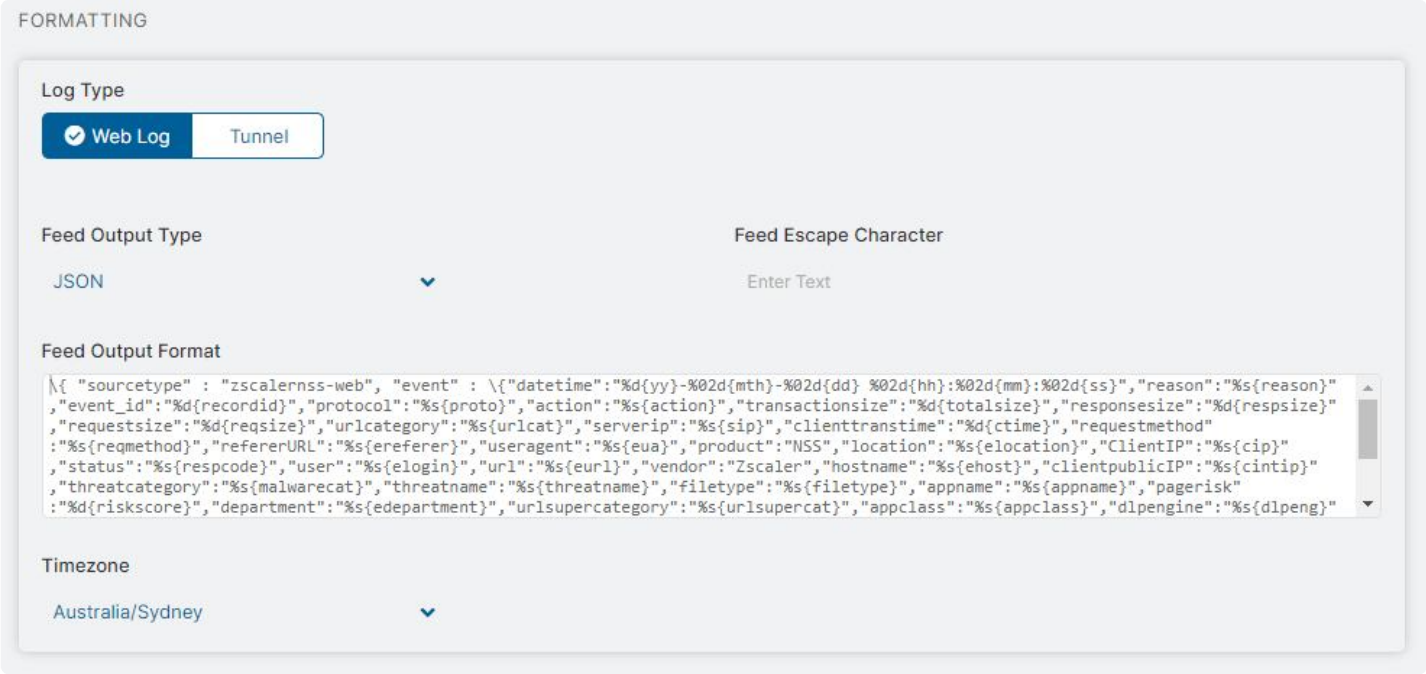
- For easier identification, use log_to_saasyan as Feed Name. The NSS Type should be NSS for Web. The Status should be set to Enabled and SIEM Rate set to Unlimited.



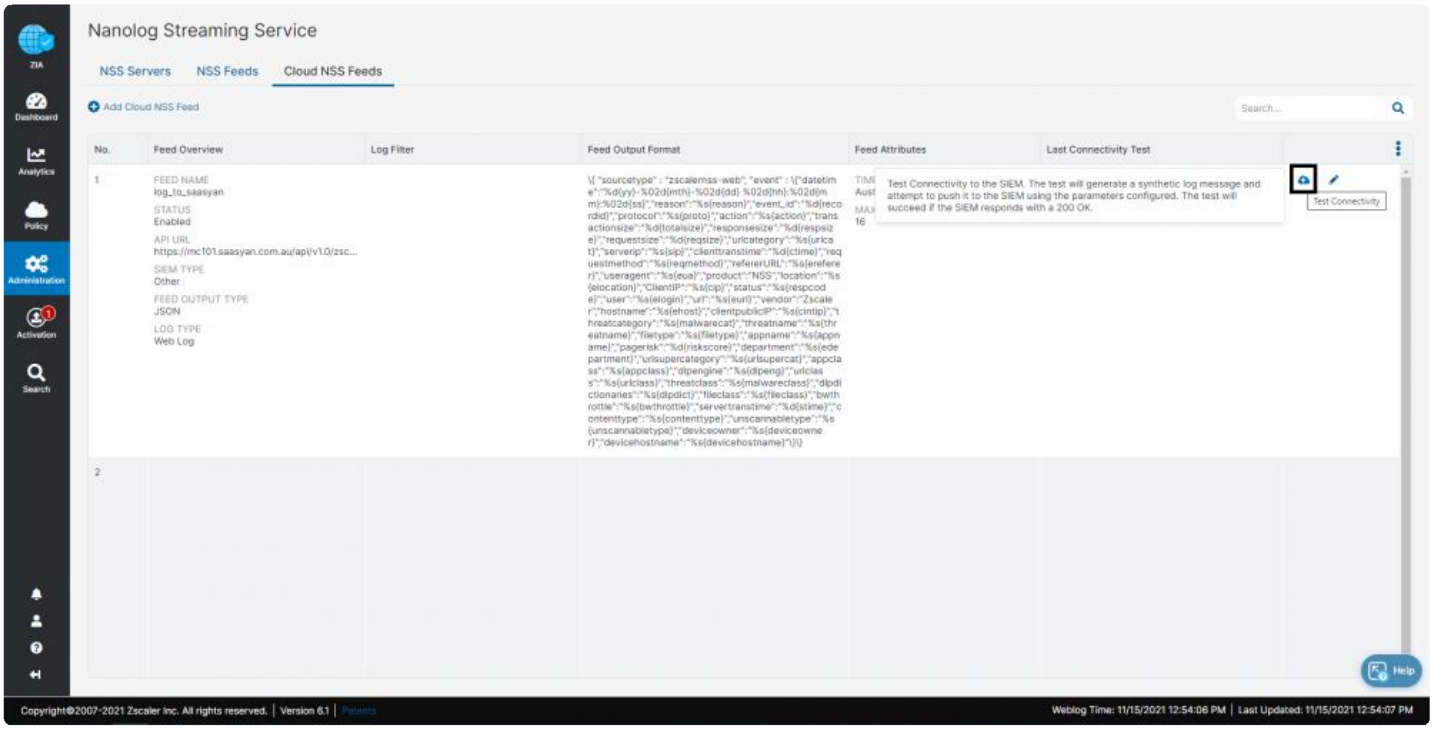
- Set the SIEM type to Other, Max Batch Size to 16 KB. For the API URL, use https://mc101.saasyan.com.au/api/v1.0/zsc/logs. Under HTTP Headers, set the Key 1 to Authorization and for Value 1 use the unique key provided by Saasyan.



- Set the Log Type to Web Log and the Feed Output Type to JSON. No need to customise the Feed Output Format but make sure the native one is there. Set the Timezone.



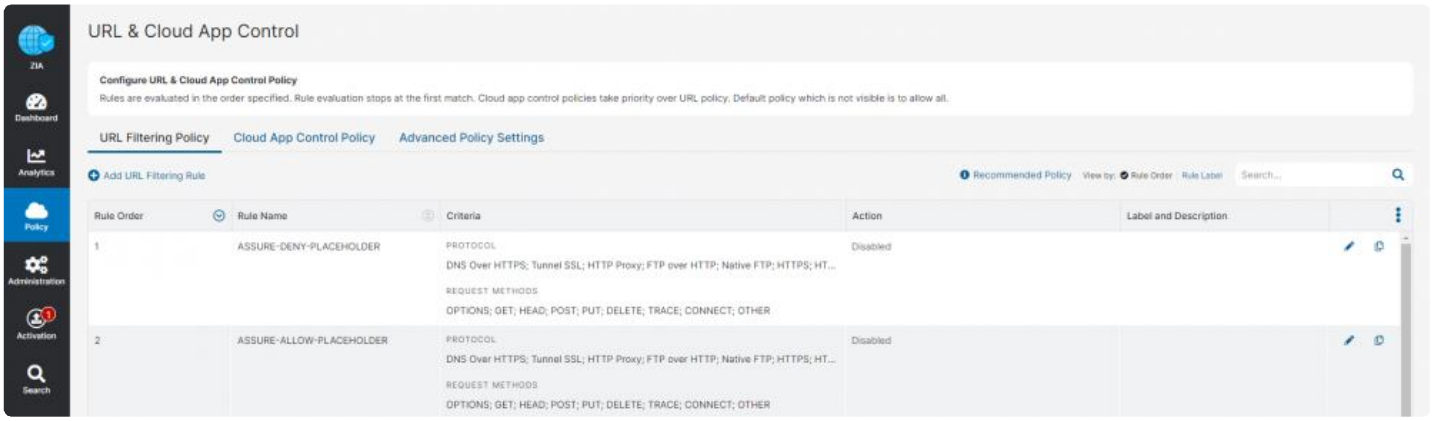
- After saving the new Cloud NSS Feed, make sure you click on the Test Connectivity to the SIEM and the test is successful.



Create Rule Placeholders

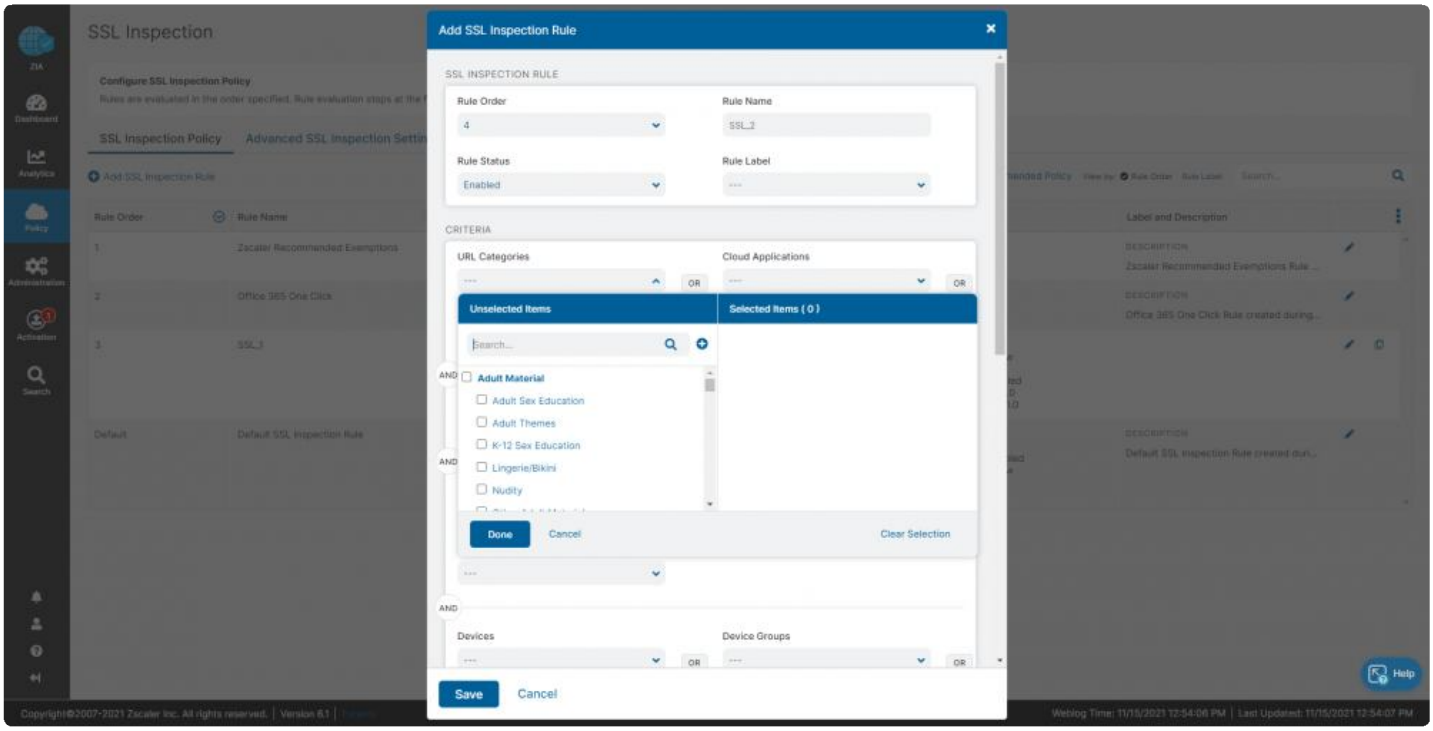
- Navigate to Policy -> URL & Cloud App Control to create the following rules as placeholders. Make sure they're disabled. These rules should never match any traffic but should be strategically placed. Assure will use these to determine where to place the programmatically created override rules in the URL Filtering Policy.

ASSURE-DENY-PLACEHOLDER
ASSURE-ALLOW-PLACEHOLDER



SSL Inspection

- Navigate to Policy -> SSL Inspection and click on Add SSL Inspection Policy. Make sure the different URL Categories for search engines, streaming media and social networking are selected.



Activate the config

- Navigate to Activation, click on Activate and make sure you get the successful activation message.

Sophos XG Specific Configuration Steps