

How to Manually Configure Cloud Integration for AWS

<https://campus.barracuda.com/doc/73719776/>

To allow an on-premises firewall or a firewall not running in AWS to connect to AWS services such as AWS CloudWatch, you must manually configure authentication credentials. For firewalls running in AWS, use IAM roles instead. Cloud integration allows your firewall to exchange information with the underlying cloud platform for things like streaming logs to AWS CloudWatch. The IAM user uses the same IAM policies that are assigned to the AWS IAM role.

Before You Begin

Create the required IAM policies for your firewall. For more information, see [How to Create an IAM Role for a CloudGen Firewall in AWS](#).

Step 1. Create the IAM User

Create the IAM user that is used to connect the firewall instance to the cloud fabric.

1. Go to AWS IAM: <https://console.aws.amazon.com/iam>.
2. In the left menu, click **Users**.
3. Click **Create New Users**.
4. Enter the **User name**.
5. In the **Select AWS access type** section, select the **Programmatic access** check box.

Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name*

[+ Add another user](#)

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

- Access type* **Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.
- AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

6. Click **Next: Permissions**.
7. Click **Attach existing policies directly**.

Set permissions for firewalladmin1



8. From the **Filter** drop-down list, select **Customer Managed**.
9. Select the IAM policies required for the AWS services you need to access. E.g., **NGF_CloudWatch** to send logs to AWS CloudWatch

Attach one or more existing policies directly to the users or create a new policy. [Learn more](#)

Filter: Customer managed

	Policy name	Type	Attachments	Description
<input type="checkbox"/>	▶ NGF_AutoScaling	Customer managed	0	
<input type="checkbox"/>	▶ NGF_CloudInformation_Element	Customer managed	0	
<input checked="" type="checkbox"/>	▶ NGF_CloudWatch	Customer managed	0	
<input type="checkbox"/>	▶ NGF_Route_Shifting	Customer managed	0	

10. Click **Next: Review**.
11. Review the settings, and click **Create user**.
12. Download or click **show** to write down the user's security credentials (access key ID and secret access key).

User	Access key ID	Secret access key
▶ firewalladmin1	AKIAJIQFLRMAOS5GZW3Q	***** Show

Step 2. Configure Cloud Integration

Add the access key ID and secret access key to allow the firewall to connect to the AWS cloud fabric.

1. Log into the firewall instance.
2. Go to **CONFIGURATION > Configuration Tree > Box > Advanced Configuration > Cloud Integration**.

3. Click **Lock**.
4. In the left menu, click **AWS Integration**.
5. From the **Enable AWS Integration** list, select **Enabled**.
6. Enter the **Access Key ID** from the IAM user created in Step 1.
7. Enter the **Secret Access Key** from the IAM user created in Step 1.
8. Enter a **Route Check Interval** between 10 and 300 seconds.

AWS Integration	
Enable AWS Integration	<input checked="" type="checkbox"/> Enabled <input type="text"/>
Access Key ID	<input checked="" type="checkbox"/> <input type="text"/>
Secret Access Key	<input checked="" type="checkbox"/> <input type="text"/>
Route Check Interval	<input type="text" value="300"/>

9. Click **Send Changes** and **Activate**.

The firewall instance can now connect to the AWS APIs allowed by the IAM policies.

Next Steps

Configure log streaming to AWS CloudWatch. For more information, see [How to Configure Log Streaming to AWS CloudWatch](#) .

Figures

1. AWS_IAM_01.png
2. AWS_IAM_02.png
3. AWS_IAM_03.png
4. AWS_IAM_04.png
5. aws_integration_2020.png

© Barracuda Networks Inc., 2020 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.