

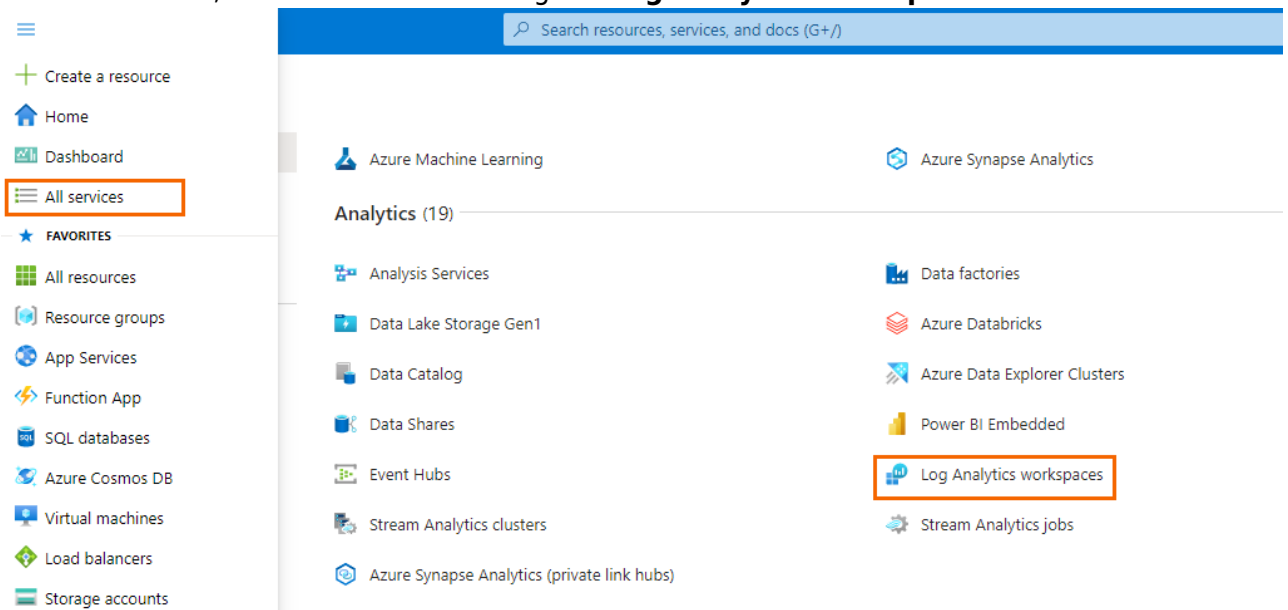
How to Configure Log Streaming to Microsoft Azure Log Analytics Workspace

<https://campus.barracuda.com/doc/98223629/>

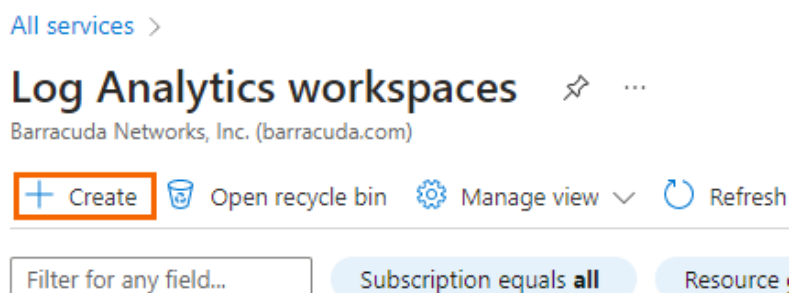
To stream log data to a Log Analytics workspace in Microsoft Azure, you must connect your Barracuda SecureEdge with the Log Analytics workspace. For more information on Microsoft Azure Log Analytics workspaces, see <https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/get-started-portal>.

Step 1. Create Log Analytics Workspace

1. Log into the Azure portal: <https://portal.azure.com>
2. In the left menu, click **All services** and go to **Log Analytics workspaces**.



3. In the **Log Analytics workspaces** menu, click **Create**.



4. The **Create Log Analytics workspace** blade opens. In the **Basics** blade, enter values for the following:
 - **Subscription** – Select your subscription.
 - **Resource Group** – Select an existing resource group, or create a new, dedicated resource group for your workspace.

- **Name** – Enter a name for the Log Analytics workspace.
- **Region** – Select the geographical location where the data for your workspace will be stored.

[All services](#) > [Log Analytics workspaces](#) >

Create Log Analytics workspace ...

Basics Tags Review + Create

i A Log Analytics workspace is the basic management unit of Azure Monitor Logs. There are specific considerations you should take when creating a new Log Analytics workspace. [Learn more](#)

With Azure Monitor Logs you can easily store, retain, and query data collected from your monitored resources in Azure and other environments for valuable insights. A Log Analytics workspace is the logical storage unit where your log data is collected and stored.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ

NetSec-cust2



Resource group * ⓘ

(New) Campus-LogAnalytic

[Create new](#)

Instance details

Name * ⓘ

Campus-LogAnalytic-workspace ✓

Region * ⓘ

West Europe

Review + Create


« Previous

Next : Tags >

5. Click **Next : Tags**.
6. The **Tags** blade opens. Specify values for your tags.
7. Click **Review + Create**.
8. The **Review + Create** blade opens. Verify your settings:

[All services](#) > [Log Analytics workspaces](#) >

Create Log Analytics workspace ...

 Validation passedBasics Tags **Review + Create****Log Analytics workspace**
by Microsoft

Basics

Subscription	NetSec-cust2
Resource group	Campus-LogAnalytic
Name	Campus-LogAnalytic-workspace
Region	West Europe

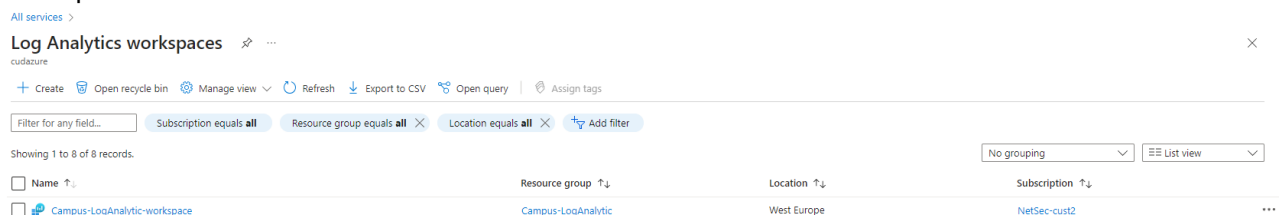
Pricing

Pricing tier	Pay-as-you-go (Per GB 2018)
--------------	-----------------------------

The cost of your workspace depends on the volume of data ingested and how long it is retained. Regional pricing details are available on the [Azure Monitor pricing page](#). You can change to a different pricing tier after the workspace is created. [Learn more](#) about Log Analytics pricing models.

Tags


9. Click **Create**.
10. Click **Refresh** in the **Log Analytics workspaces** blade to display the new Log Analytics workspace.



Log Analytics workspaces ...

Filter for any field... Subscription equals all Resource group equals all Location equals all Add filter

Showing 1 to 8 of 8 records.

Name ↑↓	Resource group ↑↓	Location ↑↓	Subscription ↑↓
 Campus-LogAnalytic-workspace	Campus-LogAnalytic	West Europe	NetSec-cust2

Step 2. Retrieve Workspace ID and Workspace Key

To connect Barracuda SecureEdge with the newly created Log Analytics workspace, you need the **Workspace ID** and **Workspace Key**.

1. Log into the Azure portal: <https://portal.azure.com>
2. In the left menu, click **All services** and go to **Log Analytics workspaces**.
3. Click on the Log Analytics workspace created in Step 1.
4. In the left menu, click **Agents**.

All services > Log Analytics workspaces > Campus-LogAnalytic-workspace

Campus-LogAnalytic-workspace | Agents

Log Analytics workspace

Search

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Logs

Settings

- Tables
- Agents**
- Usage and estimated costs
- Data export
- Network isolation
- Linked storage accounts
- Properties
- Locks

Classic

- Legacy agents management
- Legacy activity log connector
- Legacy storage account logs
- Legacy computer groups
- Legacy solutions

Windows servers Linux servers

0 Windows computers connected
via Azure Monitor Windows agent
[See them in Logs](#)

Want to setup the new Azure Monitor agent? Go to 'Data Collection Rules'

[Data Collection Rules](#)

Log Analytics agent instructions

Download agent

Download an agent for your operating system, then install :
You'll need the Workspace ID and Key to install the agent.

[Download Windows Agent \(64 bit\)](#)
[Download Windows Agent \(32 bit\)](#)

Workspace ID	ff025bf5-713e
Primary key	4bB4QtGTPJ50
Secondary key	1amllwX6HXHl

Log Analytics Gateway

If you have machines with no internet connectivity to Log A

[Learn more about Log Analytics Gateway](#)
[Download Log Analytics Gateway](#)

5. In the **Agents** window, select **Linux servers**.

All services > Log Analytics workspaces > Campus-LogAnalytic-workspace

Campus-LogAnalytic-workspace | Agents

Log Analytics workspace

Search

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Logs

Settings

Tables

Agents

Usage and estimated costs

Data export

Network isolation

Linked storage accounts

Properties

Locks

Classic

Legacy agents management

Legacy activity log connector

Legacy storage account logs

Windows servers

Linux servers

0 Linux computers connected

via Azure Monitor Linux agent

[See them in Logs](#)

Want to setup the new Azure Monitor agent? Go to 'Data Collection Rules'

Data Collection Rules

Log Analytics agent instructions

Download agent

Download an agent for your operating system, then install it. You'll need the Workspace ID and Key to install the agent.

[Download Linux Agent](#)

Download and onboard agent for Linux

```
wget https://raw.githubusercontent.com/Microsoft/OMS-A
```

Workspace ID

ff025bf5-713e-

Primary key

4bB4QtGTPJ5O

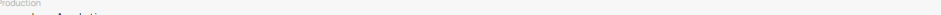
Secondary key

lamllwX6HXHlv

6. Copy **WORKSPACE ID** and **PRIMARY KEY** and save it locally.



- Integration ×
- CloudGen Firewalls
- Azure Log Analytics

- 
- Integration > Azure Log Analytics
- Enabled ☒
- Workspace ID * f5e8b1e7-e8fe-48e1-bf91-c9eE
- Workspace Key *




4. Click **Save**.

Additional Information

(Optional) Configure Azure Log Analytics as the Logstream Destination on the CloudGen Firewall

If you want to configure the CloudGen Firewall to send the logstream to Microsoft Azure Log Analytics, select **Microsoft OMS Security** from the **Logstream Destination** list. For more information, see [How to Configure Log Streaming to Microsoft Azure Log Analytics](#).

Destination Address

Logstream Destination	<input type="text" value="Microsoft OMS Security"/>	
Destination IP Address	<input type="text"/>	
Destination Port	<input type="text" value="5143"/>	

To stream logs to Microsoft Azure Log Analytics using the CEF format, you must configure **Microsoft OMS Security** as the streaming destination.

Data sent to Log Analytics will show up under the **Syslog** tag in Azure Log Analytics. Data sent to **Microsoft OMS Security** can be found under **CommonSecurityLog**, which requires **Security and Audit** to be enabled in the workspace (select **Configure monitoring solutions** and search for the solution).

Figures

1. goto-allservice-log.png
2. click-create.png
3. create-logAnalytic.png
4. logAnalytic-validation.png
5. LogAnalytic-ws.png
6. LAW-agents.png
7. goto-linux-servers.png
8. workspace-ID-key.png
9. goto-azureLogAnalytics-9.0.png
10. azure-log-analytics-9.0.png
11. select_dest_oms_security_via_cef.png

© Barracuda Networks Inc., 2024 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.