

## 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 <a href="https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/get-started-portal">https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/get-started-portal</a>.

## Step 1. Create Log Analytics Workspace

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

=	$\mathcal{P}$ Search resources, services, and docs (G-	+/)			
+ Create a resource					
숨 Home					
Z Dashboard	Azure Machine Learning	Azure Synapse Analytics			
E All services	Analytics (19)				
<b>★</b> FAVORITES					
All resources	🚰 Analysis Services	🔛 Data factories			
间 Resource groups	Data Lake Storage Gen1	e Azure Databricks			
📀 App Services	📕 Data Catalog	X Azure Data Explorer Clusters			
🎸 Function App					
🧃 SQL databases	S Data Shares	Power BI Embedded			
🧕 Azure Cosmos DB	🗈 Event Hubs	Log Analytics workspaces			
📮 Virtual machines	🍢 Stream Analytics clusters	🐳 Stream Analytics jobs			
💠 Load balancers	Azure Synapse Analytics (private link hubs)				
Storage accounts	• • • • • • •				
3. In the Log Analytics	<b>workspaces</b> menu, click <b>Create</b> .				
All services >					
Log Analytics Barracuda Networks, Inc. (I	<b>s workspaces</b> ☆ … barracuda.com)				
🕂 Create 🐻 Open	🕂 Create 🗑 Open recycle bin 🔅 Manage view 🗸 🖒 Refresh				
Filter for any field	Subscription equals all Resource				

- 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.



 $\circ~\textbf{Name}$  – 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	
A Log Analytics workspace is the l you should take when creating a r	pasic management unit of Azure Monitor Logs. There are specific considerations $$\times$$ new Log Analytics workspace. Learn more
With Azure Monitor Logs you can easi and other environments for valuable ir is collected and stored.	ly store, retain, and query data collected from your monitored resources in Azure nsights. A Log Analytics workspace is the logical storage unit where your log data
Project details	
Select the subscription to manage dep manage all your resources.	loyed resources and costs. Use resource groups like folders to organize and
Subscription * 🕡	NetSec-cust2 V
Resource group * 🛈	(New) Campus-LogAnalytic 🗸 🗸
Instance details	
Name * 🕡	Campus-LogAnalytic-workspace 🗸
Region * 🛈	West Europe
Review + Create « Previou	is 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 >	All services	> Log Analytics workspa	aces >
---	--------------	-------------------------	--------

✓ Validation passed	
Basics Tags Review +	· Create
Log Analytics workspa	ice
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 d are available on the Azure Mo Learn more about Log Analyt	epends on the volume of data ingested and how long it is retained. Regional pricing details mitor pricing page. You can change to a different pricing tier after the workspace is created. ics pricing models.
Tags	

workspace.				
All services >				
Log Analytics workspaces 🔗 … cudazure				×
+ Create 🗟 Open recycle bin 🛞 Manage view 🗸 🖒 Refresh 🛓 Export to C	SV 😚 Open query 🛛 🖉 Assign tags			
Filter for any field Subscription equals all Resource group equals all	$ imes$ Location equals all $ imes$ $^+\!$			
Showing 1 to 8 of 8 records.			No grouping ✓ == List view	$\vee$
□ 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: <u>https://portal.azure.com</u>
- 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**.

# Barracuda SecureEdge



₽ Search «		
Overview	Windows servers   Linux s	ervers
Activity log	<ol> <li>0 Windows computer</li> </ol>	s connected
ccess control (IAM)	via Azure Monitor Windows agen	t
Tags	See them in Logs	
agnose and solve problems	Want to setup the new Azure M	onitor agent? Go to '
Logs	Data Collection Rules	
Settings		
Tables	∧ Log Analytics agent instruct	ions
	Download agent	
Usage and estimated costs	Download an agent for your op	erating system, then in
Data export	You'll need the Workspace ID an	d Key to install the age
Network isolation	Download Windows Agent (64 b	pit)
Linked storage accounts	Download Windows Agent (52 t	лсу 
Properties	Workspace ID	ff025bf5-
Locks	Primary key	4bB4OtG
ssic	Cocondany kay	lam!!
Legacy agents management	Secondary Key	TamiiwX6
Legacy activity log connector	Log Analytics Gateway	,
Legacy storage account logs	If you have machines with no in	ternet connectivity to L
	Learn more about Log Analytics	Gateway
Legacy computer groups	Download Log Applicities Cotown	

# Barracuda SecureEdge



Search «	
I Overview	Windows servers
Activity log	O Linux computers connected
Access control (IAM)	See them in Logs
🗳 Tags	See them in Edgs
Diagnose and solve problems	Want to setup the new Azure Monitor agent? Go
P Logs	Data Collection Rules
Settings	
Tables	<ul> <li>Log Analytics agent instructions</li> </ul>
🥔 Agents	Download agent
<ul> <li>Usage and estimated costs</li> </ul>	Download an agent for your operating system, ther
Data export	Download Linux Agent
Network isolation	Download Linux Agent
Linked storage accounts	Download and onboard agent for Linux
Properties	wget https://taw.githubusercontent.com/wicroso
🔒 Locks	Workspace ID ff0258
Classic	Primary key 4bB40
Classic	
Classic Cassic	Secondary key

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

## Barracuda SecureEdge



Overview	Windows servers	
Activity log	0 Linux computers connected	3 Linux computers connected
Access control (IAM)	via Azure Monitor Linux agent	via Log Analytics Linux agent (legacy)
🗳 Tags	See them in Logs	See them in Logs
Diagnose and solve problems	Want to setup the new Azure Monitor agent? Go	to 'Data Collection Rules'
₽ Logs	Data Collection Rules	
Settings Tables	∧ Log Analytics agent instructions	
	Download agent	
<ul> <li>Usage and estimated costs</li> </ul>	Download an agent for your operating system, then install and configure it using the keys for your workspace ID.	
Data export     Network isolation	You'll need the Workspace ID and Key to install the Download Linux Agent	agent.
Linked storage accounts	Download and onboard agent for Linux	
Properties	wget https://raw.githubusercontent.com/Microso	ft/OMS-Agent-for-Linux/master/installer/scripts/onboard_agent.s
A Locks	Workspace ID	015-7138-46c2-9509-956010958278
L LOCKS		

# Step 3. Connect Barracuda SecureEdge with Microsoft Azure Log Analytics Workspace

- 1. Log into Barracuda SecureEdge: https://se.barracudanetworks.com/
- 2. Go to Integration > Azure Log Analytics.

1	Integration	×
5	CloudGen Firewalls	
±.	Azure Log Analytics	

- 3. The **Azure Log Analytics** page opens, specify values for the following:
  - **Enabled** Set the switch to **Enable**.
  - Workspace ID Enter the WORKSPACE ID retrieved in Step 2.
  - Workspace Key Enter the **PRIMARY KEY** retrieved in Step 2.

	Demo Enterprises Inc/Production Integration > Azure Log Analytics		
	(i) Enabled		
A	Workspace ID *	f5e8b1e7-e8fe-48e1-bf91-c9e8	
0	Workspace Key *		
0			



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 <u>How to Configure Log Streaming to Microsoft Azure Log Analytics</u>.

Destination Address		
Logstream Destination	Microsoft OMS Security 💌	Ē۰
Destination IP Address	ũ E	Ð
Destination Port	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.