

# How to Deploy a Workbook via Microsoft Sentinel

#### https://campus.barracuda.com/doc/99616884/

To add a Log Analytics workspace to Microsoft Sentinel in Microsoft Azure, you must first connect your Barracuda SecureEdge with a Log Analytics workspace. Microsoft Sentinel allows you to create custom workbooks across your data. Workbooks are used for querying data from multiple sources in Azure and visualising data for reporting and analysis. The template used will deploy a workbook into a new or existing Log Analytics workspace and provide basic information on VPN Status, Device Availability, Device Performance, Device Bandwidth, and WAN Latency.

#### Barracuda SecureEdge Workbook

The Barracuda SecureEdge workbook is available in the Barracuda Networks GitHub account:

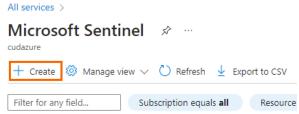
https://github.com/barracudanetworks/secureedge/tree/main/azure-workbook

### **Before You Begin**

- Create a Microsoft Azure account.
- Create a Log Analytics workspace and connect Barracuda SecureEdge with the Microsoft Azure Log Analytics workspace. For more information, see <u>How to Configure Log Streaming to</u> <u>Microsoft Azure Log Analytics Workspace</u>.

### Step 1. Add Log Analytics Workspace to Microsoft Sentinel

- 1. Log into the Azure portal: https://portal.azure.com
- 2. In the left menu, click **All services** and search for **Microsoft Sentinel**.
- 3. Click **Create**.



4. Select the newly created Log Analytics workspace. For example, in this case: **Campus-LogAnalytics-workspace.** 



Add Microsoft Continul to a	workspace			
Add Microsoft Sentinel to a	aworkspace			
+ Create a new workspace 💍 Refresh				
Microsoft Sentinel offers a 31-day free trial. See Mic	rosoft Sentinel pricing for more details.			
Filter by name				
Filter by name Workspace ↑↓	Location ↑↓	ResourceGroup ↑↓	Subscription $\uparrow_\downarrow$	Directory $\uparrow_\downarrow$
	Location ↑↓ westeurope	ResourceGroup ↑↓ campus-loganalytic	Subscription ↑↓ NetSec-cust2	Directory ↑↓ cudazure
Workspace ↑↓				



5. Click **Add**.

### Step 2. Deploy a Workbook

- 1. Log into the Azure portal: <u>https://portal.azure.com</u>
- 2. In the left menu, click **All services**, search for the Log Analytics workspace you created, and pin it to your dashboard.
- 3. In the **Campus-LogAnalytic-workspace** menu, select **Workbooks**. Create an **Empty** workbook.



#### All services > Campus-LogAnalytic-workspace

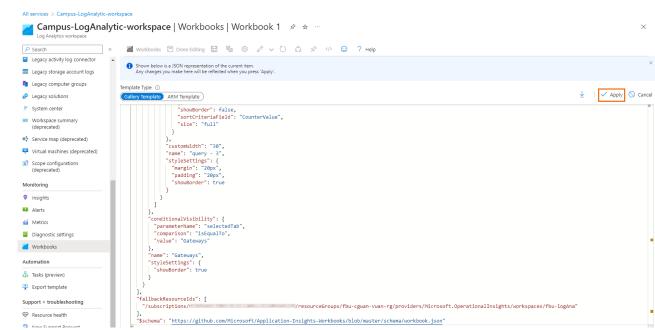
♀ Search <	🛛 🕂 🕂 New 💍 Refresh 😳 Feedback 🤶 Help 🎧 Community Git repo 🗸 🎽
Legacy activity log connector	All Workbooks Public Templates My Templates
Legacy storage account logs	
Legacy computer groups	
Legacy solutions	∧ Quick start
System center	Default Template Empty
Workspace summary (deprecated)	A report with text and query sections. A completely empty workbook.
Service map (deprecated)	<ul> <li>Recently modified workbooks (0)</li> <li>No items found.</li> </ul>
Virtual machines (deprecated)	∧ Log Analytics Workspace Insights (7)
Scope configurations (deprecated)	Insights Overview
onitoring	
Insights	Query Audit Change Log
Alerts	
Metrics	<ul> <li>Activity Logs Insights (1)</li> </ul>
Diagnostic settings	Activity Logs Insights
Workbooks	Activity Logs Insights

4. Click the **Advanced Editor** icon and delete the existing content of **Gallery Template**.

~	Campus-LogAna	alytic	-workspace   Workbooks   Workbook 2 🛷 🛧 …
2	Search	] «	🎽 Workbooks 🖳 Done Editing 🔜 🖷 🚳 🖉 🗸 🖒 🖒 🍰 🕫 🖓 😳 🤶 Help
	Legacy activity log connector	-	
-	Legacy storage account logs		This Workbook has no content.
F	Legacy computer groups		
P	Legacy solutions		Use the add button below to add items.
8	System center		$\checkmark$
	Workspace summary (deprecated)		+ Add $\sim$

- 5. Open the SecureEdge workbook. For example, in this case: **SecureEdgeWorkbook.json**.
- 6. Click **Raw** to copy the content of a workbook and paste it in your workbook's **Gallery Template**.





- 7. Click **Apply**. You can see that a new workbook has been created. Wait briefly to fetch the log data.
- 8. To save this workbook, select **Done Editing** in **Advanced Editor**, and then click **Save**.
- 9. The **Save As** page opens. Enter the name of workbook.



Save As Campus-LogAnalytic-workspace	×
Title * 🔅	
Myworkbook	$\checkmark$
Subscription * 🕡	
NetSec-cust2	$\sim$
Resource group * 🕡	
Campus-LogAnalytic	$\sim$
Location * (i)	
(US) East US	$\checkmark$

Save content to an Azure Storage Account. 🛈

Cancel		
--------	--	--

### 10. Click Apply.

You can now see the log data streaming to a Log Analytics workspace. On the SecureEdge workbook, the **Overview** page opens. Select the **Site device** and **Time frame** from the drop-down list.

The **Overview** page provides following details:



#### • SecureEdge Device Availability

	-		
₽ Search	«	🞽 Workbooks 🖉 Edit 🔜 🖒 🏡 🔗 😳 🦩 Help 🕄 Auto refresh: Off	
Classic	^		
😤 Legacy agents management		SecureEdge Workbook	
Legacy activity log connector			
😐 Legacy storage account logs		SecureEdge Portal	
Legacy computer groups		Overview Gateways Sites User SD-WAN	
Legacy solutions			
System center		Overview	
<ul> <li>Workspace summary (deprecated)</li> </ul>		SiteDevice: All V	
Service map (deprecated)	18	SecureEdge Device Availability (30Days)	
Virtual machines (deprecated)			
Scope configurations		P Search	
(deprecated)		DOC-T-VIE	
Monitoring		99.9%	
💡 Insights			
Alerts			
Metrics			
Diagnostic settings			
Workbooks			

#### • SecureEdge Site Performance Summary

host ↑↓ Latency (Ma DOC-T-VIE	x)↑↓ (Min)↑↓ (Avg.)↑↓ 42 0 23.2		Upload Max (Mbps)↑↓ 47	Download Max (MB/s)↑↓ 6.816 MB/s	Upload Max (MB/s) $\uparrow \downarrow$	
DOC-T-VIE	42 0 23.5	54	47	6.816 MB/s		
				0.010 (10)/3	5.994 MB/s	
Up WAN connections by Device			₹			
	оос-т-ч  1	ne				

### Accessing Information on the Gateways Page

The **Gateways** tab provides the information on gateway throughput. You can see a graphical representation of the egress and ingress traffic. In addition, it displays information on connected sites and connected remote clients.

At the top of the workbook, click **Gateways**. Select **Gateways** and specify the **Time frame** from the drop-down list. Note: To get the complete result for gateways, you must wait several hours.



SecureEdge Workbook	
SecureEdge Portal	
Overview Gateways Sites User SD-WAN	
Gateways	
Gateways: 2 selected V	
GW Throughput	\$ U
600.0k8/s	egress
500.0k8/s	ingress
400.018/s 300.018/s	
200.0k8/s	
100.0k8/s	
0.048/s	
10 10.02 Ingress egress	10:45
hgress 505.0 kR/s 508.0 kB/s	

### Accessing Information on the Sites Page

The **Sites** tab provides information on the load over a range of time, the latest WAN bandwidth measurements, and new connections. In addition, it displays information on the firmware version and the VPN tunnels currently up. In the **Load over time** illustration, you can see a graphical representation of the load during a specified time range. The **Latest WAN Bandwidth measurement** illustration provides a bar graph.

At the top of the workbook, click **Sites**. Select **Sites** and specify the **Time frame** from the drop-down list. The **Sites** page provides following details:

SecureEdge Workbook					
SecureEdge Portal					
Overview Gateways <u>Sites</u> User SD-WAN					
tes					
Sites: DOC-T-VIE $\checkmark$ TimeFrame: Last hour $\checkmark$					
Load over time					
2				-	
	-		•	-	
0		10:17			

• Latest WAN Bandwidth measurement and New Connections.



atest WAN Bandwidth Measurement	New Connections (
ома 2007	SecureEdge Site CPU Temperature (Celsius)
P Search	P Search
doc-T-VIE 45.5	DOC-T-VIE 53
irmware Version and VPN Tunnels UP	· · · · · · · · · · · · · · · · · · ·
Firmware Version	VPN Tunnels UP
P Search	
Computer         ↑↓         DeviceVersion         ↑↓           DOC-T-VIE         9.0.0-0511	DOC-T-VIE

#### Accessing Information on the SD-WAN Page

The **SD-WAN** tab provides the aggregated data on latency, download bandwidth utilisation, and upstream bandwidth utilisation. Each of these elements provides an illustration of the data within a specified time range.

At the top of the workbook, click **SD-WAN**. Select **Sites** and specify the **Time frame** and **Transport** from the drop-down list. The **SD-WAN** page provides following details:

• Latency

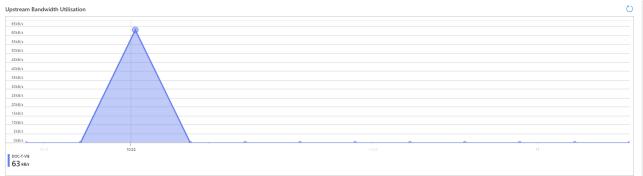


© SecureEdge Workbook secureEdge Rotal Overview Gateways Sites Ure DUWN SD-WAN SD-WAN Ster DOCT-VIE → TimeFarme List hour → Turnsport: PW2PW-wanhub-Sabe97c5-sate → Latency		ulde a a le					
Overview Gateways Site User SD-WAN   Determine List hour >   Transport: FW2PW-wanhub-c3eb97c5-ase>   Latency   Image: Image	- SecureLage Wo	ORKDOOK					
Overview Gateways Site User SD-WAN   Determine List hour >   Transport: FW2PW-wanhub-c3eb97c5-ase>   Latency   Image: Image							
iD-WAN  Stes: DCC-T-VIE  Transport: FWZPW-wanhub-c3eb97c5-ae8  Last hour	SecureEdge Portal						
SD-WAN  Stes: DCC-T-VIE  Transport: RWZPW-wanhub-c3eb97c5-ae8   Latcop  Letop  Leto	Overview Gateways Sites	User SD-WAN					
Sites:       DOC-T-VE V         Transport:       FWZFW-wanhub-c3eb97c5-ae8 V	,						
Transport: PV2PW-wanhub-c3eb97c5-ae8 V	D-WAN						
Transport: PW2PW-wanhub-c3eb97c5-ae8   Latency		meErame: Last hour X					
	Trease to participation of the state	7-5					
	Iransport: FW2FW-wanhub-c3eb9	9/c5-ae8 V					
	Latency						
				_			
			•		0	• •	
	20ms						
	20ms						
See 10.19							
See 10.19							
0m 10.19							
0m 10.19	15ms						
0ms 10.19	15ms						
10:19	15mg						
10:19	15ms						
Litinov	15ms						
Latency	15ms 10ms 5ms						
	15ma 19ma 5ma Oms	1019					

#### • Download Bandwidth Utilisation



## • Upstream Bandwidth Utilisation





#### Figures

- 1. ms-sentinel.png
- 2. add-ms-sentinel-ws.png
- 3. LAW-Workbook.png
- 4. AdvancedEditor.png
- 5. GallertyTemplate.png
- 6. myworkbook.png
- 7. Overview.png
- 8. SE-SitePerformance.png
- 9. Gateways.png
- 10. Site-Load over time.png
- 11. BW-NewConnection.png
- 12. SE-SiteTemp.png
- 13. Firmware-version.png
- 14. VPN-Tunnel-UP.png
- 15. SDWAN.png
- 16. Download-BW-Utilization.png
- 17. Upstram-BW-Utilization.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.