

## 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/securedge/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 [How to Configure Log Streaming to Microsoft Azure Log Analytics Workspace](#).

### 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**.

[All services](#) >

**Microsoft Sentinel** ⚙️ ...

cudazure

**+ Create** ⚙️ Manage view ▾ ↻ Refresh ⬇️ Export to CSV

Filter for any field...

Subscription equals **all**

Resource

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

[All services](#) > [Microsoft Sentinel](#) >

## Add Microsoft Sentinel to a workspace ...

[+ Create a new workspace](#) [Refresh](#)

Microsoft Sentinel offers a 31-day free trial. See [Microsoft Sentinel pricing](#) for more details.

Filter by name—				
Workspace ↑↓	Location ↑↓	ResourceGroup ↑↓	Subscription ↑↓	Directory ↑↓
 Campus-LogAnalytic-workspace	westeurope	campus-loganalytic	NetSec-cust2	cudazure
 mzxamplecotLogAnalytics	westeurope	mz-xamplecowan	NetSec-cust2	cudazure

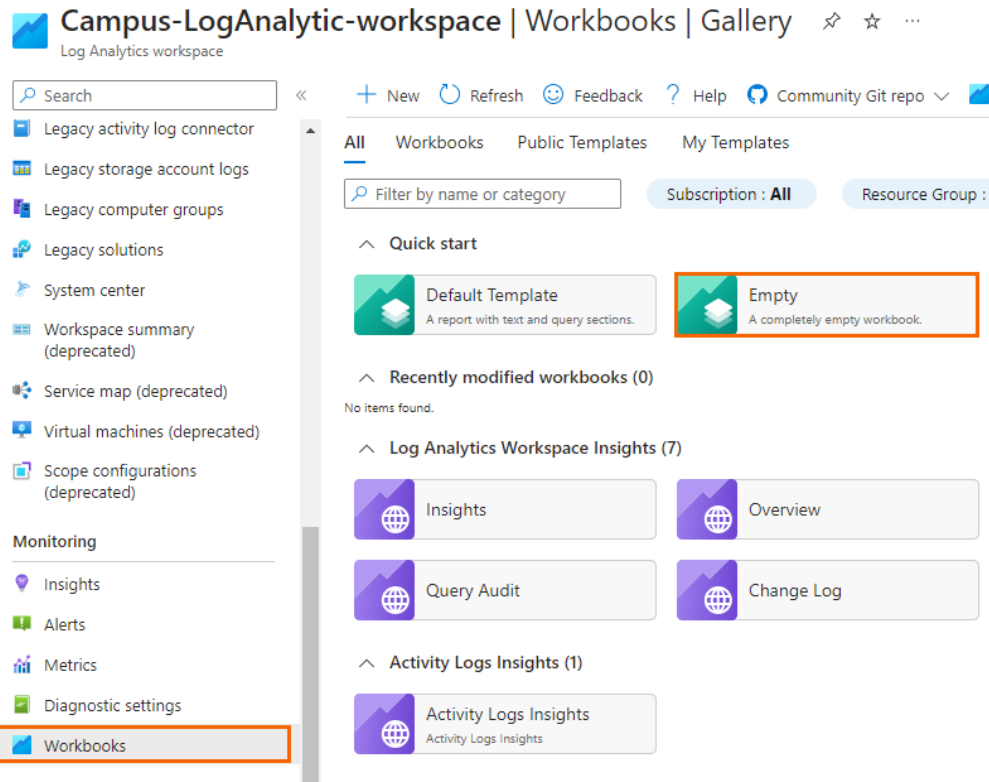
Add

Cancel

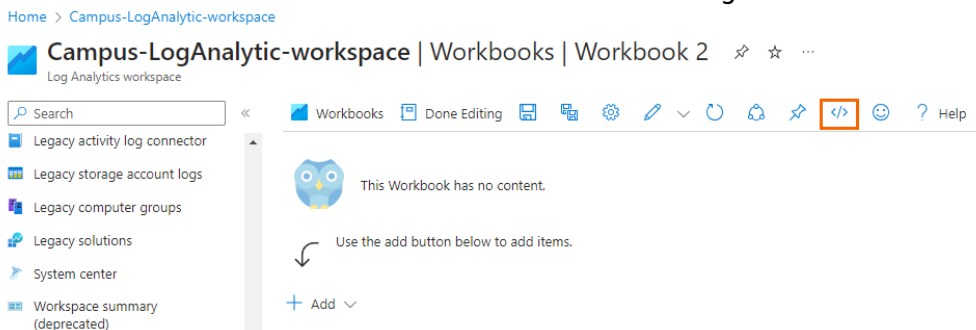
5. Click **Add**.

## Step 2. Deploy a Workbook

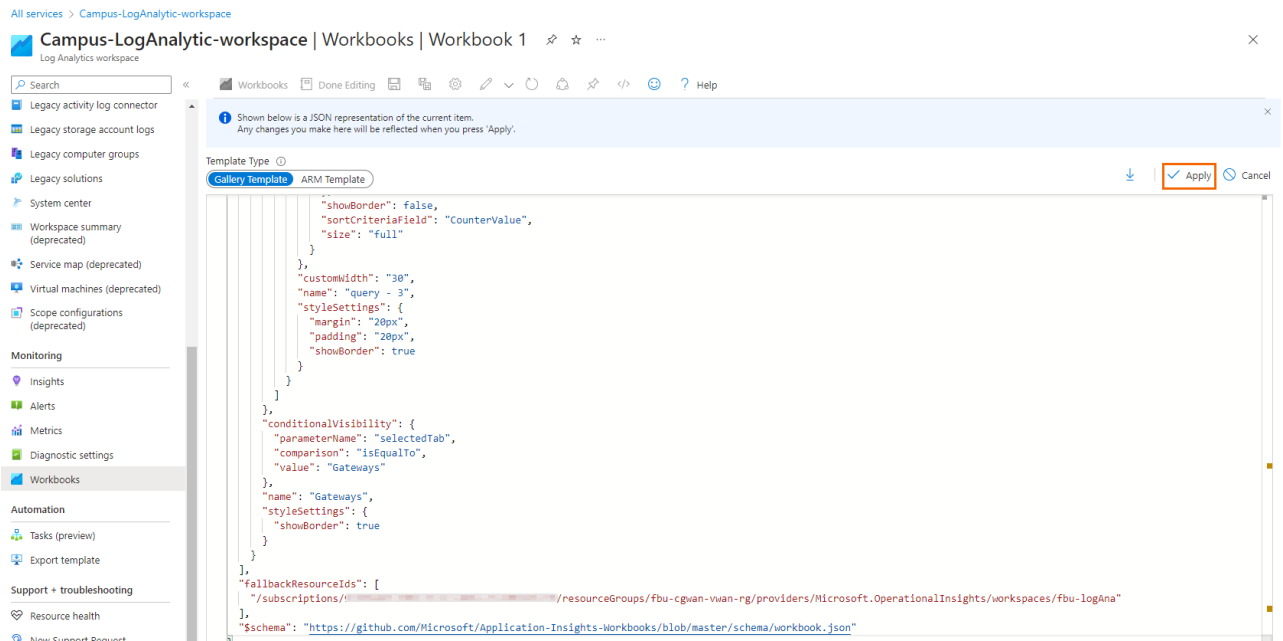
1. Log into the Azure portal: <https://portal.azure.com>
2. In the left menu, click **All services**, search for the Log Analytics workspace you created, and pin it to your dashboard.
3. In the **Campus-LogAnalytic-workspace** menu, select **Workbooks**. Create an **Empty** workbook.

[All services](#) > [Campus-LogAnalytic-workspace](#)

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



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 ✓

Subscription \* ⓘ

NetSec-cust2 ▼

Resource group \* ⓘ

Campus-LogAnalytic ▼

Location \* ⓘ

(US) East US ▼



Save content to an Azure Storage Account. ⓘ

**Apply**

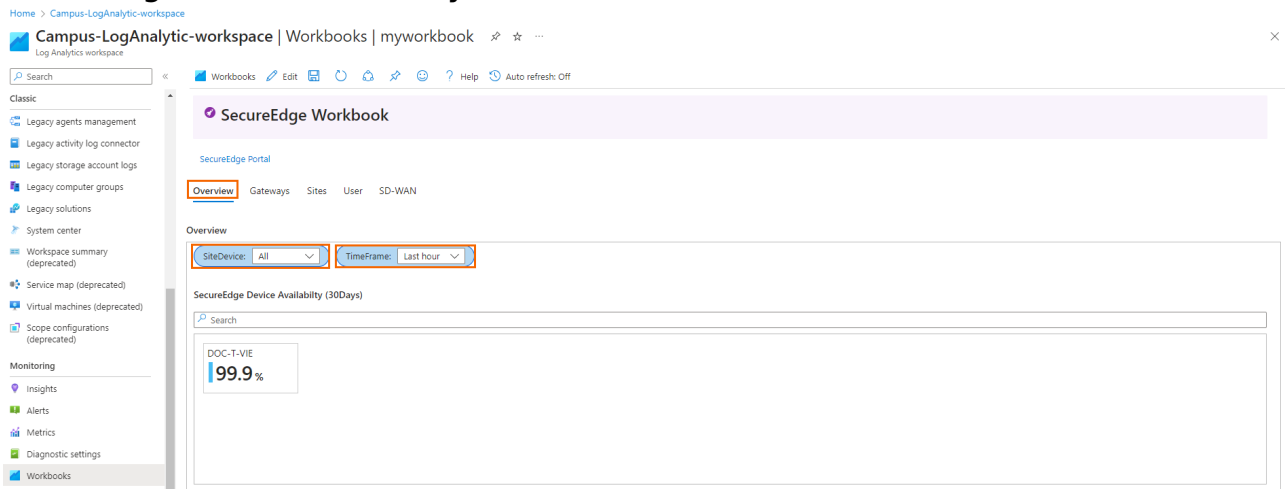
Cancel

10. Click **Apply**.

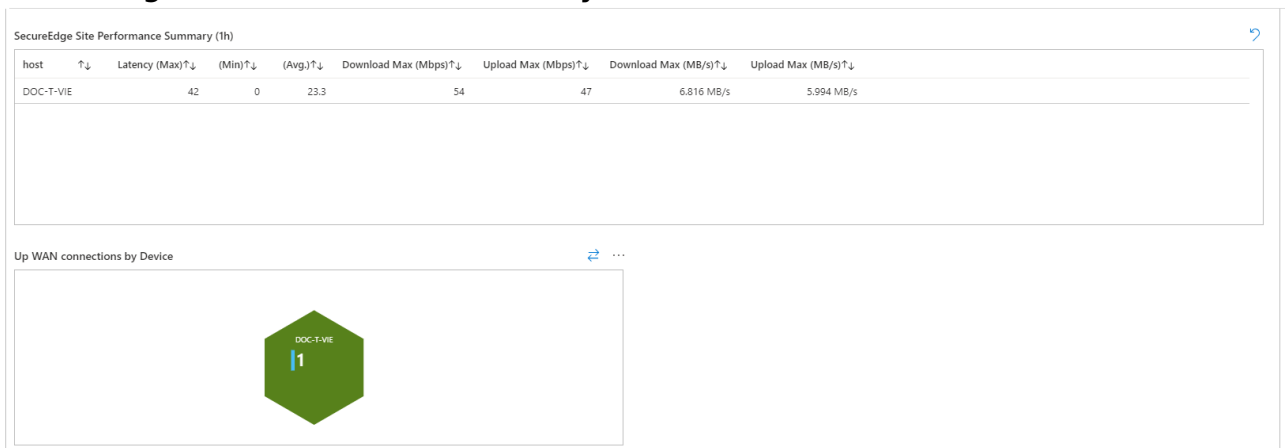
You can now see the log data streaming to a Log Analytics workspace. On the SecureEdge workbook, the **Overview** page opens. Select the **Site device** and **Time frame** from the drop-down list.

The **Overview** page provides following details:

• SecureEdge Device Availability



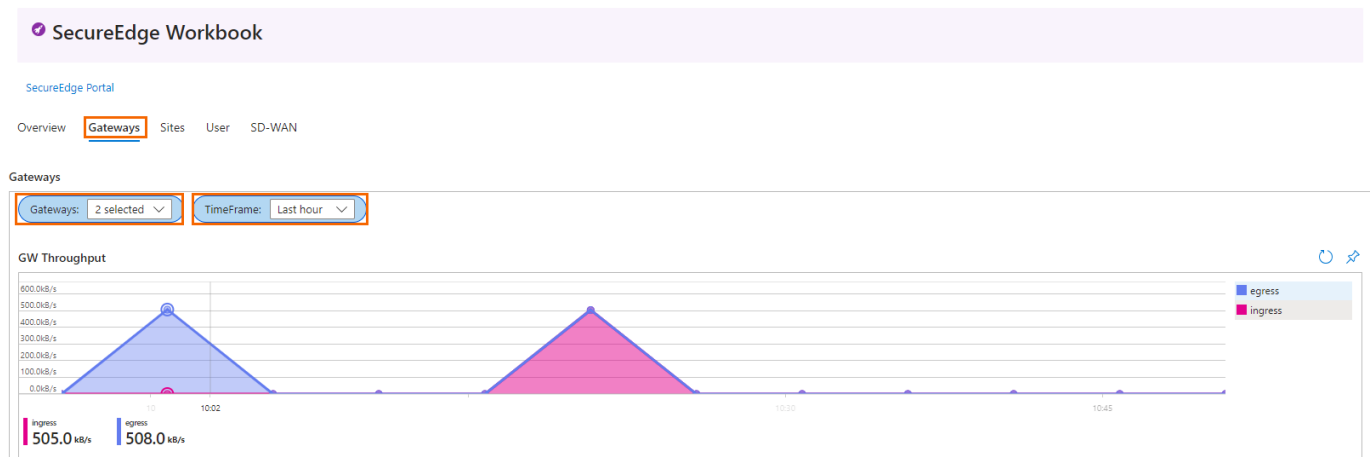
• SecureEdge Site Performance Summary



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.

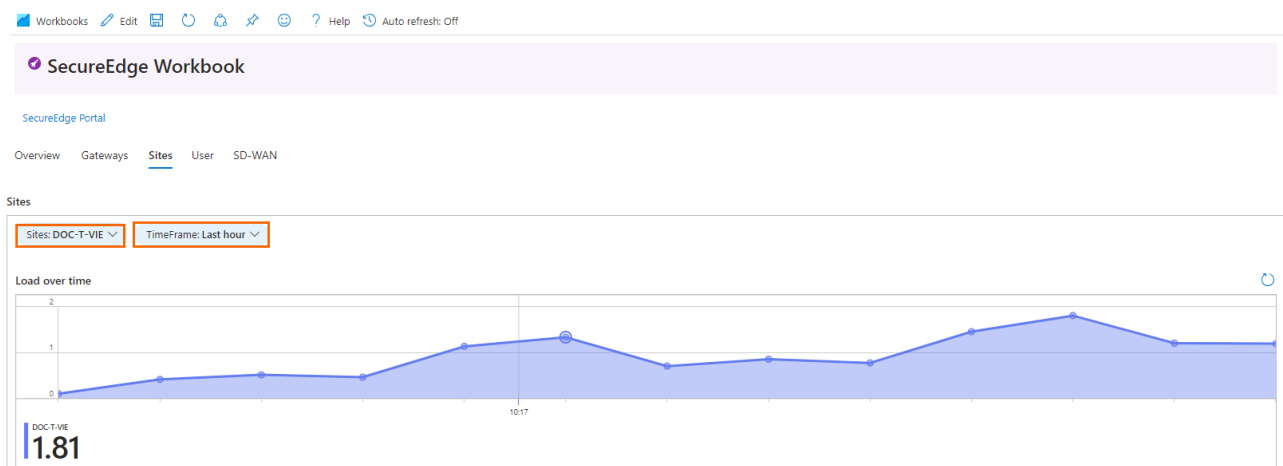


## Accessing Information on the Sites Page

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.

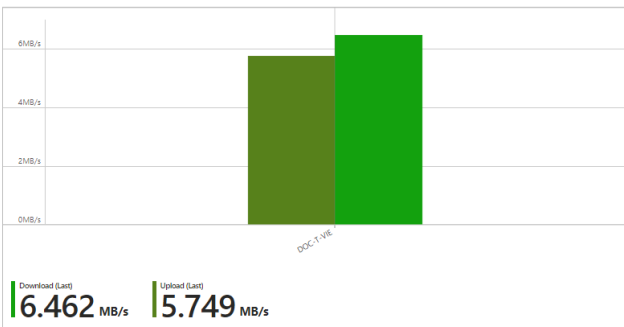
At the top of the workbook, click **Sites**. Select **Sites** and specify the **Time frame** from the drop-down list. The **Sites** page provides following details:

- **Load over time.**

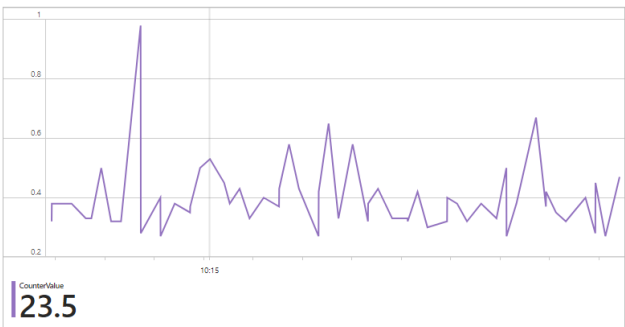


- **Latest WAN Bandwidth measurement and New Connections.**

Latest WAN Bandwidth Measurement

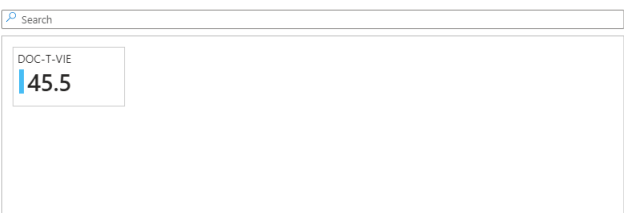


New Connections

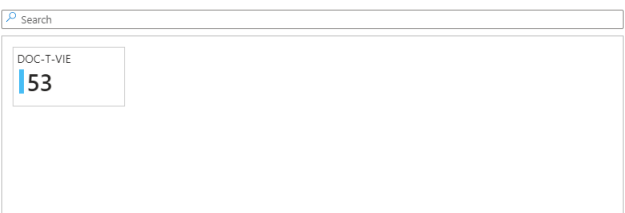


• **Site Device and Site CPU Temperature.**

SecureEdge Site Device Temperature (Celsius)



SecureEdge Site CPU Temperature (Celsius)



• **Firmware Version and VPN Tunnels UP.**

Firmware Version

Computer	DeviceVersion
DOC-T-VIE	9.0.0-0511



**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

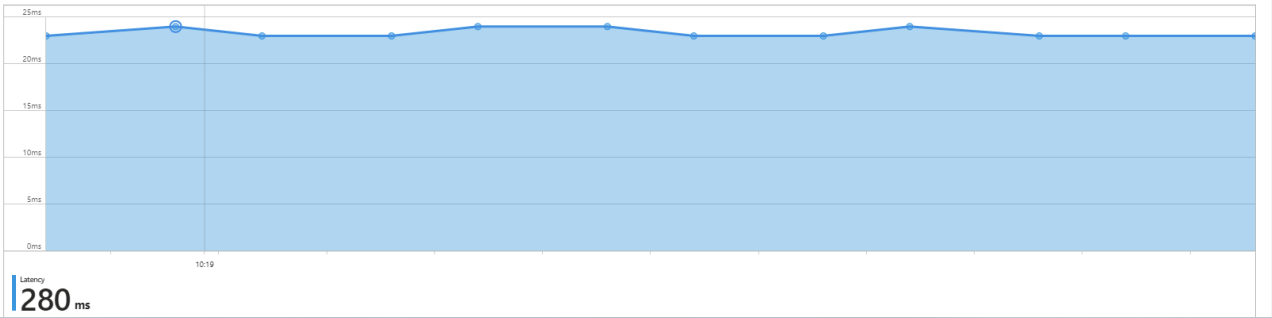
SecureEdge Portal

Overview Gateways Sites User **SD-WAN**

SD-WAN

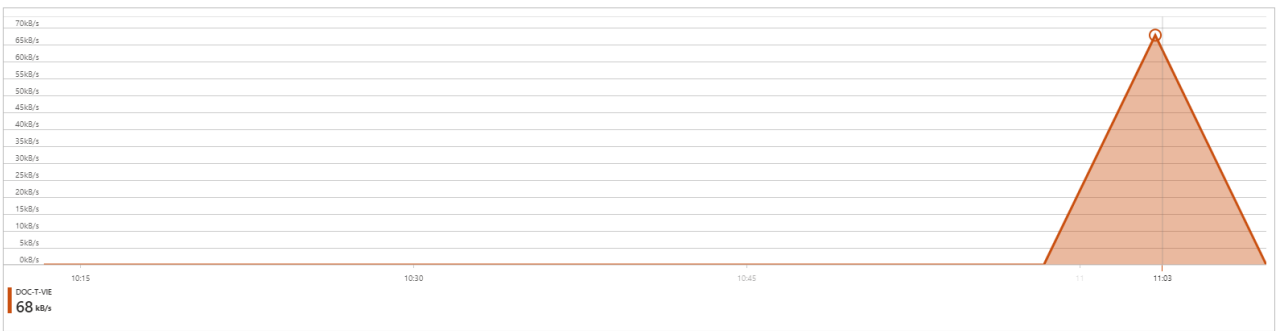
Sites: DOC-T-VIE TimeFrame: Last hour  
Transport: FW2FW-wanhub-c3eb97c5-ae8...

Latency



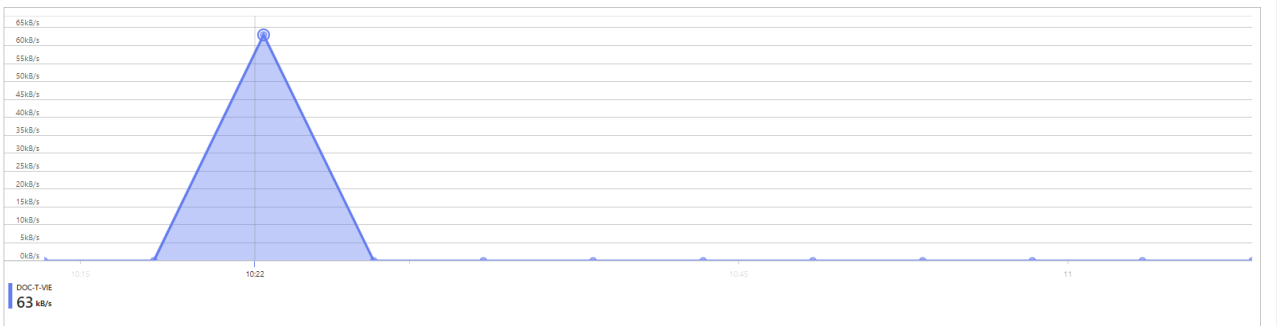
• Download Bandwidth Utilisation

Download Bandwidth Utilisation



• Upstream 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.