

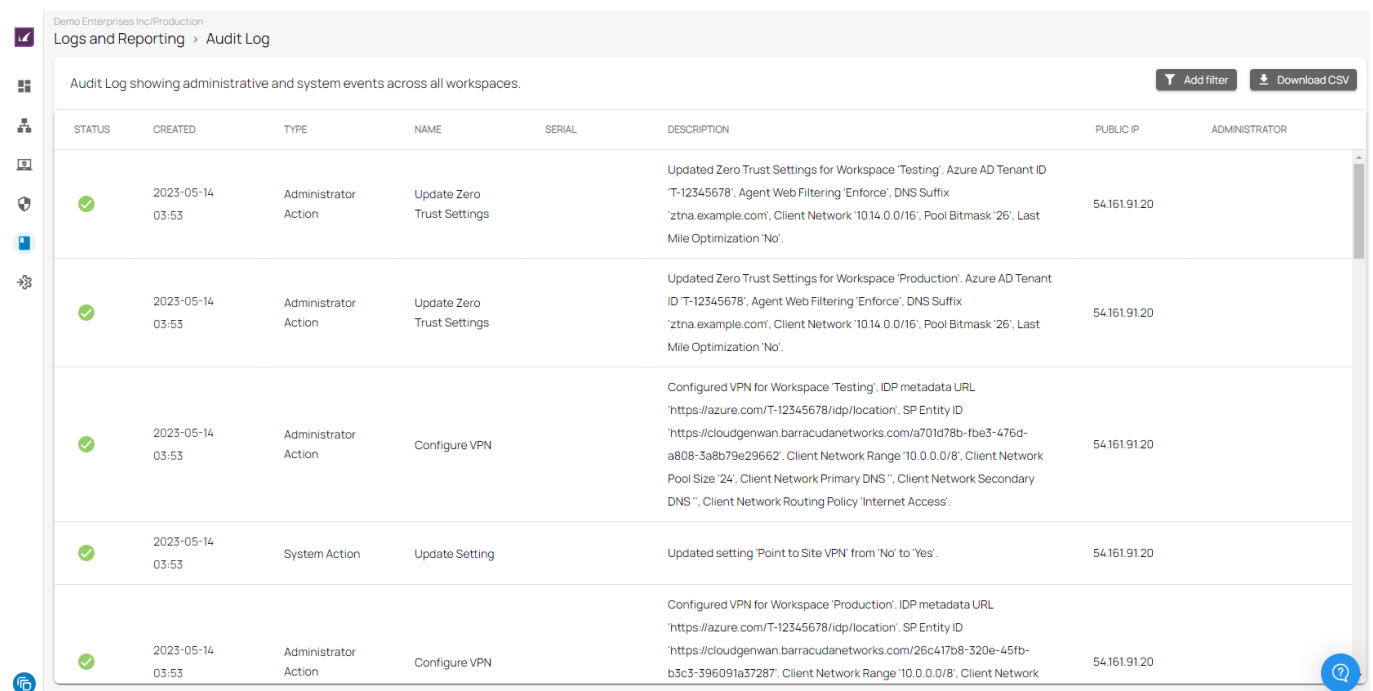
Logs and Monitoring

<https://campus.barracuda.com/doc/98223628/>

Barracuda SecureEdge offers multiple audit and reporting functionalities to help you monitor activities throughout your network.

Audit Log

The Audit Log contains all administrative actions and displays the user and the public IP address of the user who performs an action. It can be accessed in the Audit Log tab of the Cloud UI <https://se.barracudanetworks.com>. Actions performed directly on the [Local Web UI](#) are logged with the username **root**. You can also download the entries as a CSV file.



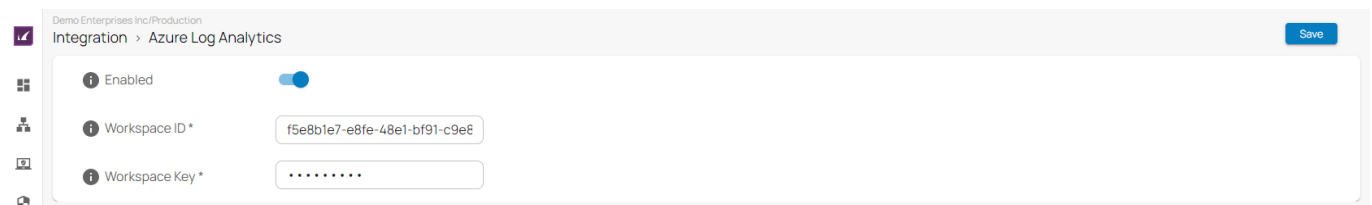
STATUS	CREATED	TYPE	NAME	SERIAL	DESCRIPTION	PUBLIC IP	ADMINISTRATOR
✓	2023-05-14 03:53	Administrator Action	Update Zero Trust Settings		Updated Zero Trust Settings for Workspace 'Testing', Azure AD Tenant ID 'T-12345678', Agent Web Filtering 'Enforce', DNS Suffix 'ztna.example.com', Client Network '10.14.0.0/16', Pool Bitmask '26', Last Mile Optimization 'No'.	54.161.91.20	
✓	2023-05-14 03:53	Administrator Action	Update Zero Trust Settings		Updated Zero Trust Settings for Workspace 'Production', Azure AD Tenant ID 'T-12345678', Agent Web Filtering 'Enforce', DNS Suffix 'ztna.example.com', Client Network '10.14.0.0/16', Pool Bitmask '26', Last Mile Optimization 'No'.	54.161.91.20	
✓	2023-05-14 03:53	Administrator Action	Configure VPN		Configured VPN for Workspace 'Testing', IDP metadata URL 'https://azure.com/T-12345678/idp/location', SP Entity ID 'https://cloudgenwan.barracudanetworks.com/a701d78b-fbe3-476d-a808-3a8b79e29662', Client Network Range '10.0.0.0/8', Client Network Pool Size '24', Client Network Primary DNS '', Client Network Secondary DNS '', Client Network Routing Policy 'Internet Access'.	54.161.91.20	
✓	2023-05-14 03:53	System Action	Update Setting		Updated setting 'Point to Site VPN' from 'No' to 'Yes'.	54.161.91.20	
✓	2023-05-14 03:53	Administrator Action	Configure VPN		Configured VPN for Workspace 'Production', IDP metadata URL 'https://azure.com/T-12345678/idp/location', SP Entity ID 'https://cloudgenwan.barracudanetworks.com/26c417b8-320e-45fb-b3c3-396091a37287', Client Network Range '10.0.0.0/8', Client Network	54.161.91.20	

Log Files

Barracuda SecureEdge appliances generate log files for the following system processes:

- FW Activity Log
- Threag Log
- Web Log
- SD-WAN Log

Log files are stored and are accessible directly on the appliance. To limit the size of a single log file, the appliance creates a new log file for each service every four hours. All log files are stored in plain text in the system's /var/phion/logs directory. You can easily stream your log files to Microsoft Azure and analyze them there. For more information, see [How to Configure Log Streaming to Microsoft Azure Log Analytics Workspace](#) .



Format and Types

Log file entries are divided into the following segments:

- **Time** – The time when an event has taken place. This indicator marks individual log entries.
- **Type** – Shows the following types of the log files.
 - **Warning** – Uncritical log event (e.g., login to the system)
 - **Error** – Log event error (e.g., system calls or clock skew)
 - **Fatal** – System-critical log events.
 - **Notice** – Normal system log events.
 - **Security** – Security-relevant log events.
 - **Panic** – Marks critical log events compromising the system's functionality and stability.
- **TZ** – Displays the UTC time zone offset compared to the local box time.
- **Message** – Description of the log event.

Stream Log Files to Microsoft Azure

Log files can be easily streamed to a Log Analytics workspace in Microsoft Azure.

- To stream log files to a Log Analytics workspace in Microsoft Azure, see [How to Configure Log Streaming to Microsoft Azure Log Analytics Workspace](#).
- To get started with Microsoft Log Analytics, see <https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/get-started-portal>.

Firewall Activity Log

- Action taken
- Source IP
- Source port
- Destination IP
- Destination port

Firewall Threat Log

- Threat description
- Action taken
- Source IP
- Destination IP
- Destination port
- Protocol
- User name

VPN User Accounting Log

- Event (login/logout)
- Tunnel name
- User name
- Peer
- Start time
- End time
- Duration
- Bytes in
- Bytes out

SDWan Data Log

- Tunnel name
- Host name
- Transport state
- Sample timestamp
- Number of samples
- Effective upstream bandwidth minimum
- Effective upstream bandwidth average
- Effective upstream bandwidth maximum
- Effective downstream bandwidth minimum
- Effective downstream bandwidth average
- Effective downstream bandwidth maximum
- Latency minimum
- Latency average
- Latency maximum
- Usage standard upstream minimum
- Usage standard upstream average
- Usage standard upstream maximum
- Usage standard downstream minimum
- Usage standard downstream average
- Usage standard downstream maximum
- Usage non-delay upstream minimum
- Usage non-delay upstream average

- Usage non-delay upstream maximum
- Usage non-delay downstream minimum
- Usage non-delay downstream average
- Usage non-delay downstream maximum

Barracuda Own Metrics

- SSL VPN clients
- Connections total
- Connections new
- Connections failed
- Connections dropped
- Connections blocked
- Forwarding connections total
- Forwarding connections new
- Site-to-site VPN tunnels up
- Site-to-site VPN tunnels down
- Client-to-site VPN tunnels
- Protected IPS
- IPS hits
- Packets total
- Packets in
- Packets out
- Bytes total
- Bytes in
- Bytes out
- Metered bytes total
- Used memory
- Free memory
- Load

Generic Performance Metrics

- Hard disk i/o measurements
- RAM usage
- Network interface statistics
- CPU usage
- File system usage
- Temperature data

Home > Campus-OMS-workspace > Advanced settings >

Logs

Campus-OMS-workspace

New Query 1* +

Example queries Query explorer Settings Bookmarks

Campus-OMS-workspace Select scope Run Time range: Last 24 hours Save Copy link New alert rule Export Pin to dashboard Format query

Tables Queries Filter

Search

Group by: Solution Filters: not selected

Favorites

You can add favorites by clicking on the star icon

LogManagement

- Alert
- AppCenterError
- ComputerGroup
- Heartbeat
- Operation
- Perf
- ReservedCommonFields
- Usage

```
// Virtual Machine available memory
// Chart the VM's available memory over the last hour.
Perf
where ObjectName == "Free_Memory"
```

Results Chart Columns Display time (UTC+00:00) Group columns

Completed. Showing results from the last 24 hours. 00:00:00.919 1,439 records

TimeGenerated [UTC]	Computer	ObjectName	CounterName	InstanceName	Min	Max	SampleCount	CounterValue	Bucket
6/16/2020, 2:02:08.943 PM	ca-tesseract-394	Free_Memory	Free_Memory.value	BNGF				86,164	
6/16/2020, 2:02:08.943 PM	ca-tesseract-394	Free_Memory	Free_Memory.value	BNGF				84,532	
6/16/2020, 2:05:08.950 PM	ca-tesseract-394	Free_Memory	Free_Memory.value	BNGF				84,636	
6/16/2020, 1:54:08.923 PM	ca-tesseract-394	Free_Memory	Free_Memory.value	BNGF				86,040	
6/16/2020, 1:54:08.927 PM	ca-tesseract-394	Free_Memory	Free_Memory.value	BNGF				86,204	
6/16/2020, 1:56:08.940 PM	ca-tesseract-394	Free_Memory	Free_Memory.value	BNGF				86,812	
6/16/2020, 1:57:08.957 PM	ca-tesseract-394	Free_Memory	Free_Memory.value	BNGF				86,432	
6/16/2020, 1:57:08.957 PM	ca-tesseract-394	Free_Memory	Free_Memory.value	BNGF				86,632	
6/16/2020, 1:58:08.943 PM	ca-tesseract-394	Free_Memory	Free_Memory.value	BNGF				86,404	
6/16/2020, 2:00:08.917 PM	ca-tesseract-394	Free_Memory	Free_Memory.value	BNGF				86,264	
6/16/2020, 2:00:08.923 PM	ca-tesseract-394	Free_Memory	Free_Memory.value	BNGF				85,040	
6/16/2020, 2:04:08.947 PM	ca-tesseract-394	Free_Memory	Free_Memory.value	BNGF				83,280	

Notifications

Barracuda SecureEdge allows you to create notifications for certain events. These notifications are sent to one or more specified email addresses. You can also download a list of notifications as a CSV file. For more information, see [How to Create a Notification](#).

Demo Enterprises Inc/Production

Logs and Reporting > Notifications

Add

Configure notifications for administrative and system events across all workspaces. Add filter Download CSV

STATUS	NAME ↑	EVENTS	ADMINISTRATORS	ACTIONS
🔴	Notify Admin	Reset Policy Category	admin@barracuda.com	✎ 🗑
🔴	Notify IT	Create Azure Gateway Create Explicit Policy Create Site Update Policy Category	it@barracuda.com	✎ 🗑

Further Information

- [How to Configure Syslog Streaming in SecureEdge](#)
- [How to Configure Barracuda XDR in SecureEdge](#)
- [How to Deploy a Workbook via Microsoft Sentinel](#)
- [How to Update Notification Email Addresses](#)

- [Barracuda Report Creator](#)
- [Telemetry Data](#)

Figures

1. audit-log-9.0.png
2. azure-log-analytics-9.0.png
3. free_memory.png
4. notification-9.0.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.