

## Configure the Barracuda Web Application Firewall to Integrate with the Log Analytics Server and Export Logs

<https://campus.barracuda.com/doc/73696965/>

1. Log into the Barracuda Web Application Firewall that has to be connected to the Log Analytics server.
2. Go to the **ADVANCED > Export Logs** page.
3. In the **Export Logs** section, click **Add Export Log Server**.
4. In the **Add Export Log Server** window, edit the following settings:
  - **Name** – Enter a name for the Microsoft Azure Log Analytics server.
  - **Log Server Type** – Select **Microsoft Azure Log Analytics**.
  - **Log Analytics Workspace ID** – Enter the workspace ID copied in Step **12.b** in the [Deploying the ARM Template](#) article.
  - **Log Analytics Primary Key** – Enter the primary key copied in Step **12.b** in the [Deploying the ARM Template](#) article.
  - **Log Event Type** – Select which log events you want to send as custom logs to the Microsoft Azure Log Analytics server.
    - **All** - When selected, the Barracuda Web Application Firewall sends all logs (Access Logs, Audit Logs, Web Firewall Logs, Network Firewall Logs and System Logs) as custom logs to the Microsoft Azure Log Analytics server. In this case, Web Firewall Logs are also sent as CommonSecurityEvents logs.
  - **Azure GovCloud Workspace**: Select **On** to turn on Azure GovCloud support. This will internally map to a different endpoint on Log Analytics. Azure GovCloud endpoint is \*ods.opinsights.azure.us\*  
If the above field is disabled (**Azure GovCloud Workspace** field is set to **No**), the endpoint is mapped to \*ods.opinsights.azure.com"
5. Click **Add**.

**Add Log Server**

Name:	<input type="text"/>
Log Server Type:	<div>Microsoft Azure Log Analytics ▾</div> <small>Select the server type to which the logs needs to be exported.</small>
Log Analytics Workspace ID:	<input type="text"/> <small>Enter Workspace ID provided with your Log Analytics Server.</small>
Log Analytics Primary Key:	<input type="text"/> <small>Enter Shared Key provided with your Log Analytics Server.</small>
Log Event Type:	<input checked="" type="radio"/> All <input type="radio"/> Web Firewall Logs <small>Select <b>All</b> to send All Barracuda Networks logs as Custom Logs in Azure Log Analytics Portal.</small>
Azure GovCloud Workspace:	<input type="radio"/> On <input checked="" type="radio"/> Off <small>Select <b>On</b> for Azure GovCloud Workspace.</small>
Comment:	<input type="text"/>
<input type="button" value="Add"/>	

6. In the **Logs Format** section:

1. Select **ArcSight Log Header** as **Syslog Header**.
2. Select **Microsoft Azure Log Analytics** for all log types (**Web Firewall Logs Format**, **Access Logs Format**, **Audit Logs Format**, **Network Firewall Logs Format** and **System Logs Format**).
3. Click **Save**.

Logs Format		
Syslog Header:	ArcSight Log Header	CEF:0 DeviceVendor Product DeviceVersion SignatureID Name Severity
Web Firewall Logs Format:	Microsoft Azure Log Analy	%header cat=%lt dst=%ai dpt=%ap act=%at msg=%adl duser=%au src=%ci spt:
Access Logs Format:	Microsoft Azure Log Analy	%header cat=%lt dvc=%ai duser=%au in=%br out=%bs suser=%cu src=%ci spt:
Audit Logs Format:	Microsoft Azure Log Analy	%header cat=%lt fname=%on fileType=%ot duser=%an requestClientApplication
Network Firewall Logs Format:	Microsoft Azure Log Analy	%header cat=%lt src=%srci spt=%srcp dst=%di dpt=%dp act=%act dvchost=%u
System Logs Format:	Microsoft Azure Log Analy	%header cat=%lt rt=%tarc msg=%ms dvchost=%un cn1=%ei cn1Label=EventID

7. In the **Export Logs** section, click **Export Log Settings**.
8. In the **Export Logs Settings** window, scroll down to the **Syslog Settings** section, and set **Web Firewall Logs Facility** to **local0**. All other log's facility (Access Logs Facility, Audit Logs Facility, System Logs Facility and Network Logs Facility) should be anything other than local0 (i.e., local1 to local7)

Syslog Settings		Help
Web Firewall Logs Facility	local0	Select the log facility to export web firewall logs to the configured syslog server. Web Firewall Logs Facility is used to identify the Barracuda Web Application Firewall and distinguish it from other hosts using the same syslog server.
Access Logs Facility	local1	Select the log facility to export access logs to the configured syslog server. Access Logs Facility is used to identify the Barracuda Web Application Firewall and distinguish it from other hosts using the same syslog server.
Audit Logs Facility	local2	Select the log facility to export audit logs to the configured syslog server. Audit Logs Facility is used to identify the Barracuda Web Application Firewall and distinguish it from other hosts using the same syslog server.
System Logs Facility	local3	Select the log facility to export system logs to the configured syslog server. System Logs Facility is used to identify the Barracuda Web Application Firewall and distinguish it from other hosts using the same syslog server.
Network Firewall Logs Facility	local4	Select the log facility to export network firewall logs to the configured syslog server. Network Firewall Log Facility is used to identify the Barracuda Web Application Firewall and distinguish it from other hosts using the same syslog server.

9. Click **Save**.

## Next Step

Continue with [Log Search](#).

## Figures

1. Add\_Log\_Server.png
2. Logs\_Format.png
3. Syslog\_Settings.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.