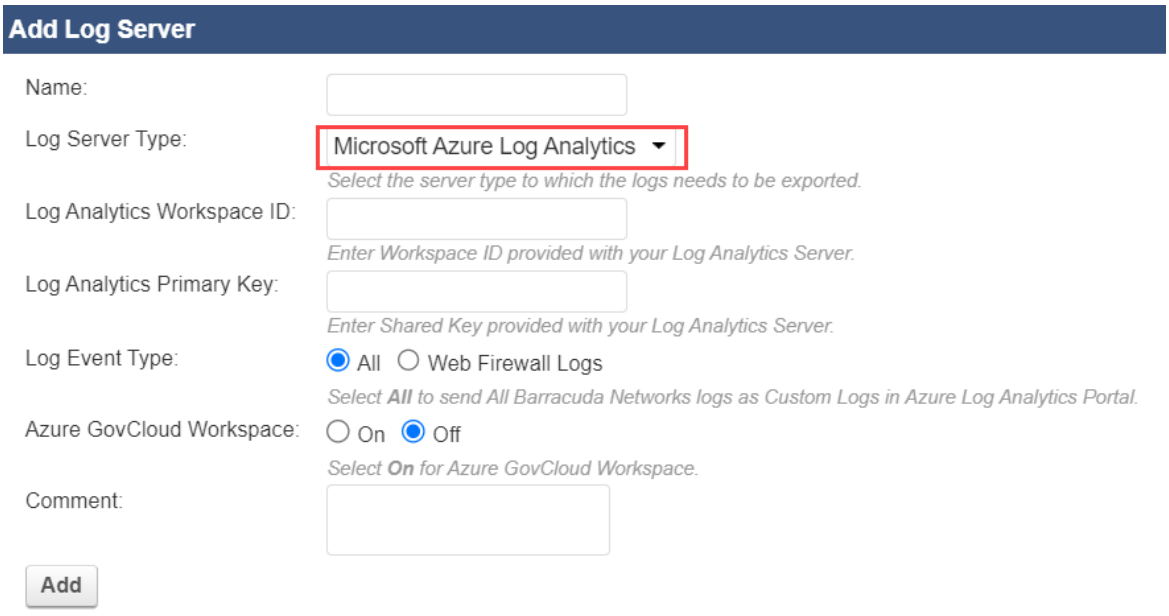
Configure the Barracuda Web Application Firewall to Integrate with the Log Analytics Server and Export Logs

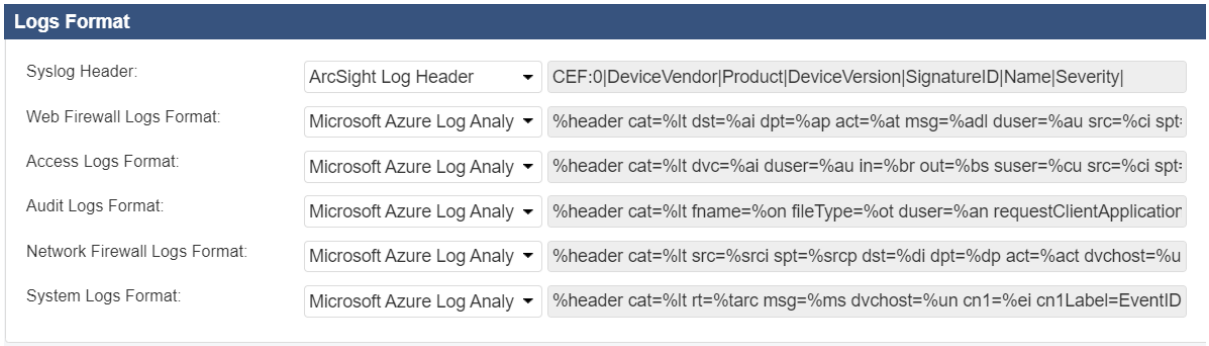
https://campus.barracuda.com/doc/73696965/

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 Worspace** field is set to **No**), the endpoint is mapped to *ods.opinsights.azure.com"
5. Click **Add**.

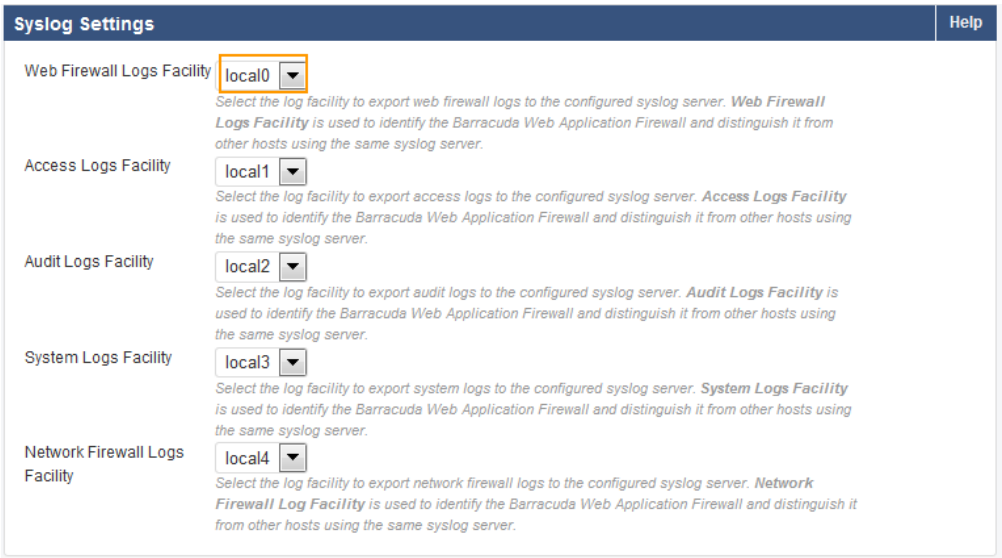


6. In the **Logs Format** section:

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**.



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)



9. Click **Save**.

Next Step

Continue with Log Search.

Figures

1. Add_Log_Server.png
2. Logs_Format.png
3. Syslog_Settings.png