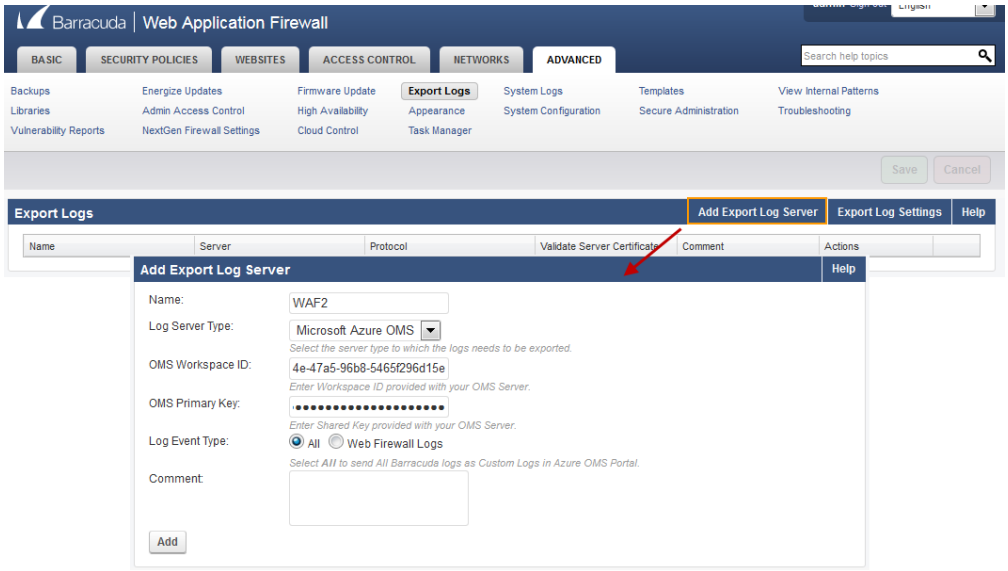
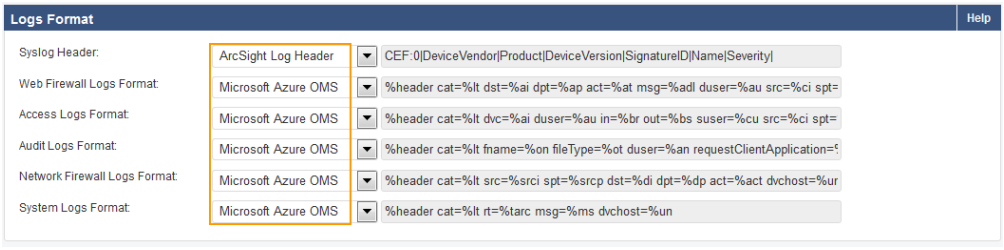
# Configure the Barracuda Web Application Firewall to Integrate with the OMS Server and Export Logs

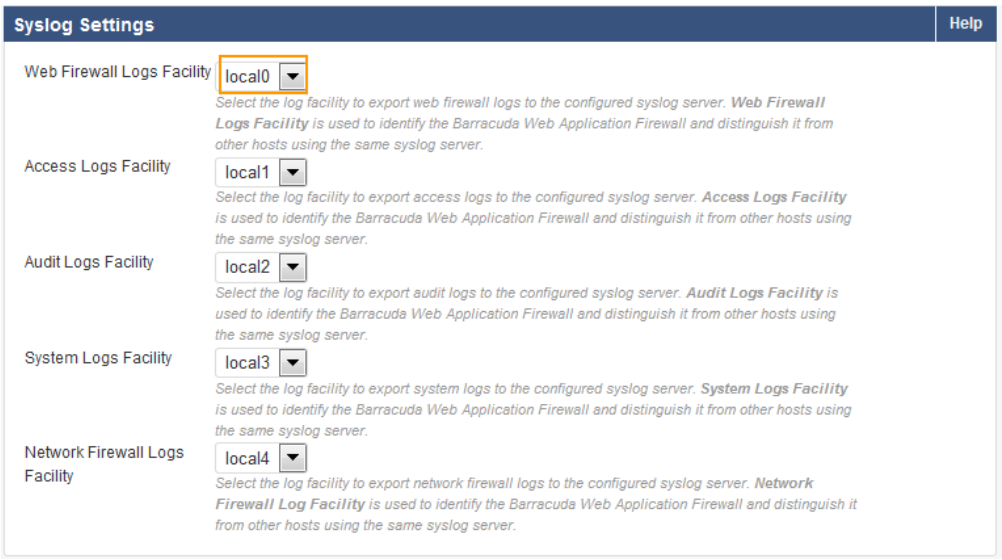
1. Log into the Barracuda Web Application Firewall web interface that needs to be connected to the OMS server.
2. Go to the **ADVANCED > Export Logs** page.
3. In the **Export Logs** section, click **Add Export Log Server**.
4. In the **Add Export Log Server** window:
    1. **Name**: Enter a name for the Microsoft Azure OMS server.
    2. **Log Server Type**: Select **Microsoft Azure OMS**.
    3. **OMS Workspace ID**: Enter the Workspace ID copied in step **13.b** in the Deploying the ARM Template article.
    4. **OMS Primary Key**: Enter the primary key copied in step **13.b** in the Deploying the ARM Template article.
    5. **Log Event Type**: Select which log events you want to send as custom logs to the Microsoft Azure OMS server.
        1. **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 OMS portal. In this case, Web Firewall Logs are also sent as CommonSecurityEvents logs.
    6. Click **Add**.




5. In the **Logs Format** section:
    1. Select **ArcSight Log Header** as **Syslog Header**.
    2. Select **Microsoft Azure OMS** 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**.



6. In the **Export Logs** section, click **Export Log Settings**.
7. In the **Export Logs Settings** window, scroll down to the **Syslog Settings** section, and set **Web Firewall Logs Facility** to **local0** and 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)




8. Click **Save**.

**Next Step**

Continue with Log Search.

## Figures