

---

## How to Integrate Barracuda Web Application Firewall with Symantec™ Managed Security Services (MSS)

<https://campus.barracuda.com/doc/77401181/>

### Overview

---

Symantec™ Managed Security Services (MSS) provides 24x7 real-time security monitoring, analysis and reporting, and early warning intelligence. The Barracuda Web Application Firewall is integrated with Symantec™ MSS and is configured to send logs to the Symantec MSS Log Collection Platform (LCP).

### Supported Versions

---

- Firmware 9.0 or higher

## Configure the Barracuda Web Application Firewall to Send Logs to Symantec MSS

---

Steps to add a syslog server

1. Go to the **ADVANCED > Export Logs** page.
2. In the **Export Logs** section, click **Add Export Log Server**. The **Add Export Log Server** window opens. Specify values for the following:
  - **Name** - Enter a name for the syslog NG server.
  - **Log Server Type** - Select *Syslog NG*.
  - **IP Address or Hostname** - Enter the IP address or the hostname of the syslog NG server.
  - **Port** - Enter the port associated with the IP address of the syslog NG server.
  - **Connection Type** - Select the connection type to transmit the logs from the Barracuda Web Application Firewall to the syslog server. UDP is the default port for syslog communication. UDP, TCP or SSL can be used in case of NG Syslog server.
  - **Validate Server Certificate** - Set to *Yes* to validate the syslog server certificate using the internal bundle of Certificate Authority (CA) certificates packaged with the system. If set to *No*, any certificate from the syslog server is accepted.
  - **Client Certificate** - When set to *Yes*, the Barracuda Web Application Firewall presents the certificate while connecting to the syslog server.
  - **Certificate** - Select a certificate for the Barracuda Web Application Firewall to present when connecting to the syslog server. Certificates can be uploaded on the **BASIC > Certificates** page. For more information on how to upload a certificate, see [How to Add](#)

[an SSL Certificate.](#)

- **Log Timestamp and Hostname** - Set to Yes if you want to log the date and time of the event, and the hostname configured on the **BASIC > IP Configuration > Domain Configuration** section.

3. Click **Add**.

4. To configure the logs format, in the **Logs Format** section, specify the following values for each feature:

- From the **Syslog Header** drop-down list, select **ArcSight Log Header**.
- From the **Web Firewall Logs Format** drop-down list, select **HPE Arcsight CEF:0**.
- From the **Access Logs Format** drop-down list, select **HPE Arcsight CEF:0**.
- From the **Audit Logs Format** drop-down list, select **HPE Arcsight CEF:0**.
- From the **Network Firewall Logs Format** drop-down list, select **HPE Arcsight CEF:0**.
- From the **System Logs Format** drop-down list, select **HPE Arcsight CEF:0**.

Logs Format		
Syslog Header:	ArcSight Log Header	CEF:0 DeviceVendor Product DeviceVersion SignatureID Name Severity
Web Firewall Logs Format	HPE Arcsight CEF:0	%header cat=%lt dst=%ai dpt=%ap act=%at msg=%adl duser=%au src=%ci spt=%s
Access Logs Format	HPE Arcsight CEF:0	%header cat=%lt dvc=%ai duser=%au in=%br out=%bs suser=%cu src=%ci spt=%s
Audit Logs Format	HPE Arcsight CEF:0	%header cat=%lt fname=%on fileType=%ot duser=%an requestClientApplication=%
Network Firewall Logs Format	HPE Arcsight CEF:0	%header cat=%lt src=%srci spt=%srcp dst=%di dpt=%dp act=%act start=%ta dvc
System Logs Format	HPE Arcsight CEF:0	%header cat=%lt rt=%tarc externalid=%uid msg=%ms dvchost=%sun start=%ta

## Figures

### 1. MSSIntegration.png

© Barracuda Networks Inc., 2020 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.