

## How to Integrate Barracuda Web Application Firewall with AlienVault® USM Anywhere™

<https://campus.barracuda.com/doc/93192200/>

### Overview

AlienVault® USM Anywhere™ is a software-as-a-service (SaaS) security monitoring solution that centralizes threat detection, incident response, and compliance management across your on-premises, cloud, or hybrid environments. The Barracuda Web Application Firewall is integrated with AlienVault® USM Anywhere™ to send log data to the USM Anywhere.

### Supported Versions

- Firmware 8.1 or higher

### Configure the Barracuda Web Application Firewall to Send Logs to USM Anywhere

For setting up the log formats for various logs, see this [document](#) .

Steps for adding 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**.

**Add Export Log Server** Help

Name:

Log Server Type:  ▼  
Select the server type to which the logs needs to be exported.

IP Address:  .  .  .   
The IP address of the log server.

Port:   
The port associated with the IP address of the log server.

Connection Type:  UDP  TCP  SSL  
Select the connection type to transmit the logs from the Barracuda Web Application Firewall to the Syslog server.

Validate Server Certificate:  Yes  No  
Validates the syslog server certificate using the internal bundle of Certificate Authority's (CA's) certificates packaged with the system. If set to No, any certificate from the syslog server is accepted.

Client Certificate:  Yes  No  
Set to Yes to validate the syslog server certificate using the internal bundle of Certificate Authority's (CAs) certificates packaged with the system. If set to No, any certificate from the syslog server is accepted.

Log Timestamp and Hostname:  Yes  No  
Logs the date and time of the system events.

Comment:

To configure facilities for different log types:

1. Go to **ADVANCED > Export Logs**.
2. In **Export Logs**, select **Export Log Settings**.
3. In the **Syslog Settings** section of the **Export Log Settings** dialog box, select the appropriate facility (Local0 to Local7) from the list for each log type, and click **Save**.

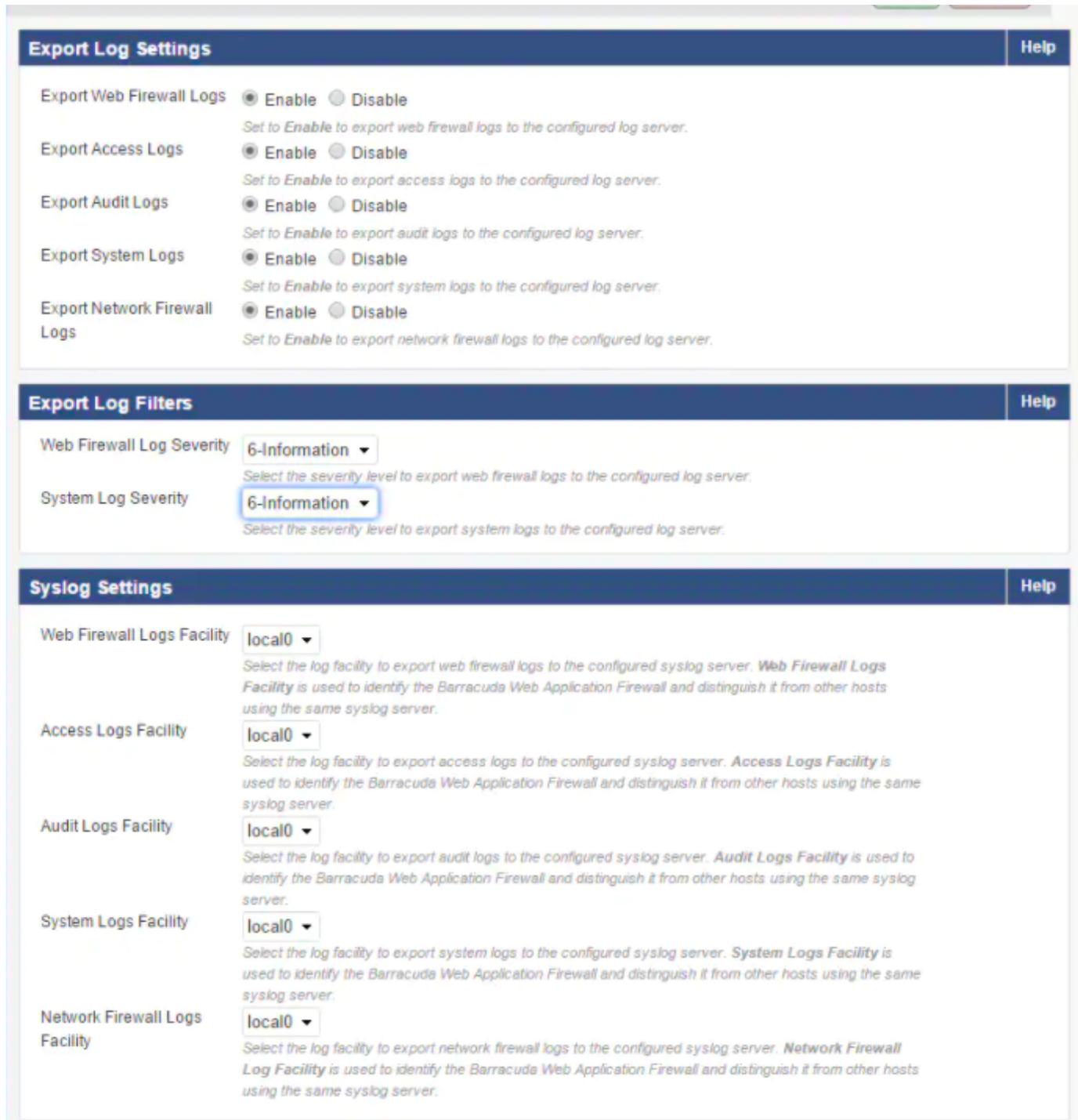
You can set the same facility for all log types. For example, you can set Local0 for System Logs, Web Firewall Logs, Access Logs, Audit Logs, and Network Firewall Logs.

In the **Export Log Settings** dialog box, you can do the following:

- Enable or disable the logs that need to be exported to the configured export log server(s) in **Export Log Settings**
- Set the severity level to export web firewall logs and system logs to the configured export log server(s) in **Export Log Filters**

The Barracuda Web Application Firewall exports the logs based on the selected severity level. For example, if Web Firewall Log Severity is set to 2-Critical, then logs with 0-2 are

sent to the external log server (in other words, 0-Emergency, 1-Alert, and 2-Critical).



The screenshot displays the configuration interface for the Barracuda Web Application Firewall, divided into three main sections: Export Log Settings, Export Log Filters, and Syslog Settings. Each section includes a 'Help' link in the top right corner.

- Export Log Settings:** This section contains five rows, each with a log type and two radio buttons for 'Enable' and 'Disable'. All 'Enable' options are selected.
  - Export Web Firewall Logs:  Enable  Disable. *Set to Enable to export web firewall logs to the configured log server.*
  - Export Access Logs:  Enable  Disable. *Set to Enable to export access logs to the configured log server.*
  - Export Audit Logs:  Enable  Disable. *Set to Enable to export audit logs to the configured log server.*
  - Export System Logs:  Enable  Disable. *Set to Enable to export system logs to the configured log server.*
  - Export Network Firewall Logs:  Enable  Disable. *Set to Enable to export network firewall logs to the configured log server.*
- Export Log Filters:** This section contains two rows, each with a severity level dropdown menu.
  - Web Firewall Log Severity: 6-Information. *Select the severity level to export web firewall logs to the configured log server.*
  - System Log Severity: 6-Information. *Select the severity level to export system logs to the configured log server.*
- Syslog Settings:** This section contains five rows, each with a log facility dropdown menu, all set to 'local0'.
  - 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: local0. *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: local0. *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: local0. *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: local0. *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.*

## Figures

1. VSMAnywhere\_1.png
2. ASM Anywhere\_2.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.