



Micro Focus Security ArcSight Connectors

SmartConnector for Barracuda Firewall NG F-Series Syslog

Configuration Guide

June, 2018

Configuration Guide

SmartConnector for Barracuda Firewall NG F-Series Syslog

June, 2018

Copyright © 2017; 2018 Micro Focus and its affiliates and licensors.

Warranty

The only warranties for products and services of Micro Focus and its affiliates and licensors ("Micro Focus") are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Except as specifically indicated otherwise, a valid license from Micro Focus is required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated. Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation. UNIX® is a registered trademark of The Open Group.

Revision History

Date	Description
10/17/2017	First edition of this Configuration Guide.

SmartConnector for Barracuda Firewall NG F-Series Syslog

This guide provides information for installing the SmartConnector for Barracuda Firewall NG F-Series Syslog and configuring the device for syslog event collection. Barracuda Firewall NG version 7 is supported.

Product Overview

The Barracuda NextGen (NG) Firewall F-Series is a family of hardware, virtual, and cloud-based appliances that protect and enhance your dispersed network infrastructure. They deliver advanced security by tightly integrating a comprehensive set of next-generation firewall technologies, including Layer 7 application profiling, intrusion prevention, web filtering, malware and advanced threat protection, antispy protection, and network access control.

The product uses syslog messages as a means of logging, which are sent to a text file on the Security Gateway, as well as to a remote server configurable by the product administrator.

Configuration

For complete information about monitoring and logging Barracuda Firewall NG F-Series devices, see <https://campus.barracuda.com/product/nextgenfirewallf/article/NGF71/Logs/>. The information in this section is derived from that documentation.

Logging

Configuring logging requires the following steps:

- Configure Log Daemon
- Enable Audit Logs
- Configure Syslog Streaming
- Configure Web Log Streaming

Configure Log Daemon

To configure the log daemon:

- 1 Go to **CONFIGURATION > Full Configuration > Box > Infrastructure Services > Log Configuration**.
- 2 Click **Lock**.
- 3 Set the parameters for **Generate Log Data** and **Store Log Data**. For logs to be sent to the syslog service and written to disk, select **Yes** for both **Generate Log Data** and **Store Log Data**. For logs to be sent to the syslog service but not written to disk, select **Yes** for **Generate Log Data** and **No** for **Store Log Data**.

- 4 Click **Send Changes and Activate**.

Enable Audit Logs

- 1 Go to **CONFIGURATION > Full Configuration > Box > Infrastructure Services > General Firewall Configuration**.
- 2 In the left menu, select **Audit and Reporting**.
- 3 Expand the **Configuration Mode** menu and select **Switch to Advanced View**.
- 4 Click **Lock**.
- 5 In the **Log Policy** section enable **Generate Audit Log**.
- 6 Click **Set** next to **Audit Log Data**.
- 7 From the **Audit Delivery** list and select **Syslog-Proxy** from the drop-down list.
- 8 Click **OK**.
- 9 Click **Send Changes** and **Activate**.

Configure Syslog Streaming

The syslog streaming configuration defines the handling of log files. Log messages of centrally managed firewalls can be transmitted to the NextGen Control Center Syslog service, but they can just as well be transmitted to any other system designed for log file collection or to another Barracuda NextGen Firewall F-Series.

Configuring syslog streaming comprises the following steps:

- Enable the Syslog Service
- Upload External SSL Certificates (optional)
- Configure Logdata Filters
- Configure Log Stream Destinations

Enable the Syslog Service

- 1 Go to **CONFIGURATION > Full Configuration > Box > Infrastructure Services > Syslog Streaming**.
- 2 Click **Lock**
- 3 Under **Operational Setup**, set **Enable Syslog Streaming** to **yes**.
- 4 Click **Send Changes** and **Activate**.

Upload External SSL Certificates (optional)

If the syslog stream is SSL encrypted, by default the box certificate and key are used. To upload custom SSL certificates:

- 1 Go to **CONFIGURATION > Full Configuration > Box > Infrastructure Services > Syslog Streaming**.
- 2 Click **Lock**.
- 3 In the left menu expand the **Configuration Mode** section and click **Switch to Advanced View**.
- 4 From the **Use Box Certificate/Key** drop-down list select **no**.
- 5 Import the **SSL Private Key** and **SSL Certificate**.
- 6 Click **Send Changes** and **Activate**.

Configure Logdata Filters

Define profiles specifying the log file types to be streamed.

- 1 Go to **CONFIGURATION > Full Configuration > Box > Infrastructure Services > Syslog Streaming**.
- 2 In the left menu, select **Logdata Filters**.
- 3 Expand the **Configuration Mode** menu and select **Switch to Advanced View**.
- 4 Click **Lock**.
- 5 Click the plus (+) icon to add a new entry.
- 6 Enter a descriptive name in the **Filters** dialog and click **OK**.
- 7 In the **Data Selection** table, you can add the log files to be streamed. Select **Firewall_Audit_Log**.
- 8 In the **Affected Box Logdata** section, define what kind of box logs are to be affected by the syslog daemon from the **Data Selection** list.
- 9 When choosing **Selection** (default):
 - a Click the plus (+) icon next to **Data Selection** to add an entry.
 - b Enter a descriptive name for the group and click **OK**. The **Data Selection** window opens.
 - c Add the **Log Groups** for selection or select **Other** and specify an explicit selection.
 - d Set a **Log Message Filter**. When choosing **Selection**, add the explicit log type to the **Selected Message Types** table.
 - e Click **OK**,
- 10 Click **Send Changes** and **Activate**.

Configure Logstream Destinations

For selective syslog streaming a configured logstream destination is required.

- 1 Go to **CONFIGURATION > Full Configuration > Box > Infrastructure Services > Syslog Streaming**.
- 2 In the left menu, select **Logstream Destinations**.
- 3 Expand the **Configuration Mode** menu and select **Switch to Advanced View**.
- 4 Click **Lock**.
- 5 Click the plus (+) icon to add a new entry.
- 6 Enter a descriptive name in the upcoming dialog and click **OK**. The **Destinations** window opens.
- 7 Select the **Logstream Destination**. When an external log host is used, select **Explicit IP** (default) and enter the destination IP address in the Destination IP Address field.
- 8 Enter the **Destination Port** for delivering syslog messages. The Barracuda Networks CC syslog service listens on port TCP 5143 for SSL connections and on TCP and UDP port 5144 for unencrypted streaming. The default is to use encryption for delivery, therefore port 5143 is preconfigured. When changing the port, you must also adapt the host firewall rule for syslog traffic to use the new port.
- 9 Select the **Transmission Mode** (TCP or UDP - default; for SSL connections TCP is automatically set).
- 10 Click .
- 11 Click **Send Changes** and **Activate**.

Configure Web Log Streaming

Web Log streaming lets you send a syslog stream to an external device. Although TCP and TCP/TLS are supported as streaming protocols, UDP is recommended for performance reasons.

To stream an HTTPS session, the web traffic must match an access rule using SSL Interception. For HTTP traffic streaming no additional access rules are required.

Depending on the target device, it is possible to customize the log format to match the target device using streaming templates. See the Barracuda documentation at the following location for more information.

<https://campus.barracuda.com/product/nextgenfirewallf/article/NGF71/LogsConfigWebLogStreaming/>

Configuring Web Log streaming comprises the following steps:

- Configure Web Log Streaming on the Firewall
- Create an Access Rule Matching HTTPS Traffic
- Configure the Syslog Service on the Destination Device

Before You Begin

When using the Barracuda Web Security Gateway as the destination syslog server, update the Web Security Gateway to the latest available firmware and contact [Barracuda Networks Technical Support](#) to set up your Web Security Gateway appliance.

Collect the following information for your destination device:

- Destination IP address
- Destination port
- Supported streaming protocols
- Log format
- Syslog facility
- Syslog level

Configure Web Log Streaming on the Firewall

Configure the Barracuda NG Firewall F-Series to stream every HTTP and HTTPS request to the configured syslog server using the streaming template as the log format.

- 1 Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > Syslog Streaming**.
- 2 Click **Lock**.
- 3 In the left menu, click **Web Log Streaming**.
- 4 From the **Enable Web Log Streaming** drop-down list, select **yes**.

Operational Setup

Enable Web Log Streaming	yes	
Streaming Template	[: %timestamp% 1 %srcip% %dstip% %content-type% %srcip% %uri% %con	
Streaming Protocol	UDP	
Destination IP Address	172.16.0.111	
Destination Port	514	
Syslog Server SSL Certificate	<input type="button" value="Show..."/> <input type="button" value="Ex/Import"/> No certificate present	

- 5 Enter the **Streaming Template** as required by the destination device. Use the **template placeholders** and plain text. The default value matches the required log format for the Barracuda Web Security Gateway.
- 6 Select the **Streaming Protocol**. Use **UDP** because it has the least performance impact on the F-Series.

- 7 Enter the **Destination IP Address**.
- 8 Enter the **Destination Port** (514 for the Barracuda Web Security Gateway).
- 9 Click **Send Changes** and **Activate**.

Create an Access Rule Matching HTTPS Traffic (HTTPS Only)

To be able to stream information about HTTPS connections, ensure that the access rule matching the HTTPS traffic is using SSL Interception.

- 1 Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > Firewall > Forwarding Rules**.
- 2 Double-click to edit the access rule matching HTTPS traffic.
- 3 Click on the **Application Policy** link and select **Application Control** and **SSL Interception**.
- 4 Click **OK**.
- 5 Click **Send Changes** and **Activate**.

Configure the Syslog Service on the Destination Device

Configure the remote device running the syslog service to receive and process the syslog stream from the firewall.

Configure the Syslog SmartConnectors

The three ArcSight Syslog SmartConnectors are:

- Syslog Daemon
- Syslog Pipe
- Syslog File

The Syslog Daemon SmartConnector

The Syslog Daemon SmartConnector is a syslogd-compatible daemon designed to work in operating systems that have no syslog daemon in their default configuration, such as Microsoft Windows. The SmartConnector for Syslog Daemon implements a UDP receiver on port 514 (configurable) by default that can be used to receive syslog events. Use of the TCP protocol or a different port can be configured manually.

If you are using the SmartConnector for Syslog Daemon, simply start the connector, either as a service or as a process, to start receiving events; no further configuration is needed.



Messages longer than 1024 bytes may be split into multiple messages on syslog daemon; no such restriction exists on syslog file or pipe.

The Syslog Pipe and File SmartConnectors

When a syslog daemon is already in place and configured to receive syslog messages, an extra line in the syslog configuration file (`rsyslog.conf`) can be added to write the events to either a **file** or a

system **pipe** and the ArcSight SmartConnector can be configured to read the events from it. **In this scenario, the ArcSight SmartConnector runs on the same machine as the syslog daemon.**

The **Syslog Pipe** SmartConnector is designed to work with an existing syslog daemon. This SmartConnector is especially useful when storage is a factor. In this case, syslogd is configured to write to a named pipe, and the Syslog Pipe SmartConnector reads from it to receive events.

The **Syslog File** SmartConnector is similar to the Pipe SmartConnector; however, this SmartConnector monitors events written to a syslog file (such as `messages.log`) rather than to a system pipe.

Configure the Syslog Pipe or File SmartConnector

This section provides information about how to set up your existing syslog infrastructure to send events to the ArcSight Syslog Pipe or File SmartConnector.

The standard UNIX implementation of a syslog daemon reads the configuration parameters from the `/etc/rsyslog.conf` file, which contains specific details about which events to write to files, write to pipes, or send to another host. First, create a pipe or a file; then modify the `/etc/rsyslog.conf` file to send events to it.

For syslog pipe:

- 1 Create a pipe by executing the following command:

```
mkfifo /var/tmp/syspipe
```

- 2 Add the following line to your `/etc/rsyslog.conf` file:

```
*.debug /var/tmp/syspipe
```

or

```
*.debug | /var/tmp/syspipe
```

depending on your operating system.

- 3 After you have modified the file, restart the syslog daemon either by executing the scripts `/etc/init.d/syslogd stop` and `/etc/init.d/syslogd start`, or by sending a `configuration restart` signal.

On RedHat Linux, you would execute:

```
service syslog restart
```

On Solaris, you would execute:

```
kill -HUP `cat /var/run/syslog.pid`
```

This command forces the syslog daemon to reload the configuration and start writing to the pipe you just created.

For syslog file:

Create a file or use the default for the file into which log messages are to be written.

After editing the `/etc/rsyslog.conf` file, be sure to restart the syslog daemon as described above.

When you follow the SmartConnector Installation Wizard, you will be prompted for the absolute path to the syslog file or pipe you created.

Install the SmartConnector

The following sections provide instructions for installing and configuring your selected SmartConnector.

Syslog Installation

Install this SmartConnector (on the syslog server or servers identified in the *Configuration* section) using the SmartConnector Installation Wizard appropriate for your operating system. The wizard will guide you through the installation process. When prompted, select one of the following **Syslog** connectors (see *Configure the Syslog SmartConnectors* in this guide for more information):

- Syslog Daemon
- Syslog Pipe
- Syslog File

Because all syslog SmartConnectors are sub-connectors of the main syslog SmartConnector, the name of the specific syslog SmartConnector you are installing is not required during installation.

The syslog daemon connector by default listens on port 514 (configurable) for UDP syslog events; you can configure the port number or use of the TCP protocol manually. The syslog pipe and syslog file connectors read events from a system pipe or file, respectively. Select the one that best fits your syslog infrastructure setup.

Prepare to Install Connector

Before you install any SmartConnectors, make sure that the ArcSight products with which the connectors will communicate have already been installed correctly (such as ArcSight ESM or ArcSight Logger).

For complete product information, read the *Administrator's Guide* as well as the *Installation and Configuration* guide for your ArcSight product before installing a new SmartConnector. If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* for instructions, and start the installation procedure at "Set Global Parameters (optional)" or "Select Connector and Add Parameter Information."

Before installing the SmartConnector, be sure the following are available:

- Local access to the machine where the SmartConnector is to be installed
- Administrator passwords

Install Core Software

Unless specified otherwise at the beginning of this guide, this SmartConnector can be installed on all ArcSight supported platforms; for the complete list, see the *SmartConnector Product and Platform Support* document, available from the Micro Focus SSO and Protect 724 sites.

- 1 Download the SmartConnector executable for your operating system from the Micro Focus SSO site.
- 2 Start the SmartConnector installation and configuration wizard by running the executable.

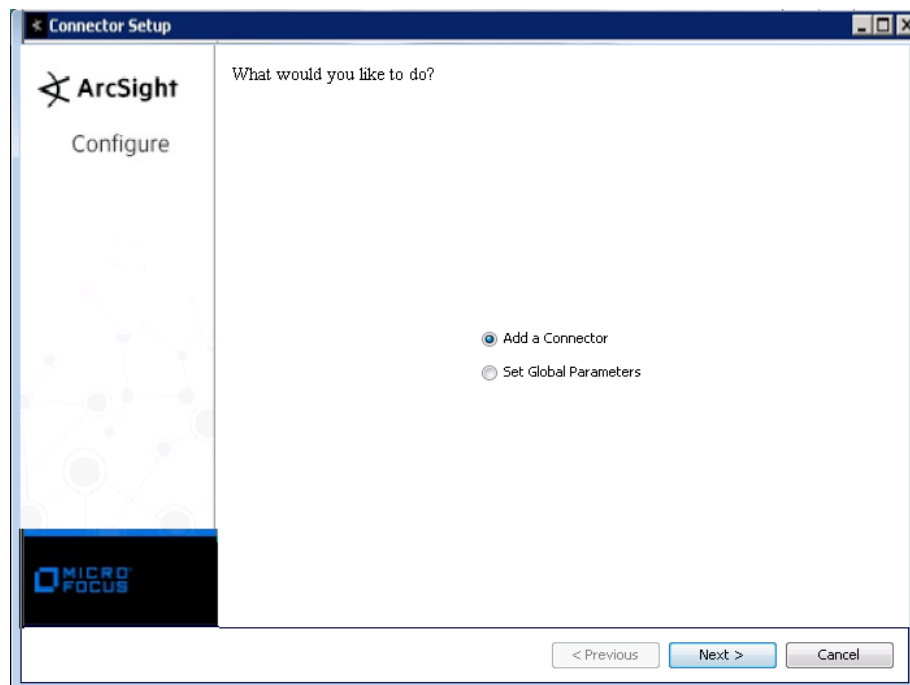


When installing a syslog daemon SmartConnector in a UNIX environment, run the executable as 'root' user.

Follow the wizard through the following folder selection tasks and installation of the core connector software:

Introduction
 Choose Install Folder
 Choose Shortcut Folder
 Pre-Installation Summary
 Installing...

- 3 When the installation of SmartConnector core component software is finished, the following window is displayed:



Set Global Parameters (optional)

If you choose to perform any of the operations shown in the following table, do so before adding your connector. You can set the following parameters:

Parameter	Setting
FIPS mode	Select 'Enabled' to enable FIPS compliant mode. To enable FIPS Suite B Mode, see the SmartConnector User Guide under "Modifying Connector Parameters" for instructions. Initially, this value is set to 'Disabled'.
Remote Management	Select 'Enabled' to enable remote management from ArcSight Management Center. When queried by the remote management device, the values you specify here for enabling remote management and the port number will be used. Initially, this value is set to 'Disabled'.
Remote Management Listener Port	The remote management device will listen to the port specified in this field. The default port number is 9001.
Preferred IP Version	When both IPv4 and IPv6 IP addresses are available for the local host (the machine on which the connector is installed), you can choose which version is preferred. Otherwise, you will see only one selection. The initial setting is IPv4.

The following parameters should be configured only if you are using Micro Focus SecureData solutions to provide encryption. See the *Micro Focus SecureData Architecture Guide* for more information.

Parameter	Setting
Format Preserving Encryption	Data leaving the connector machine to a specified destination can be encrypted by selecting 'Enabled' to encrypt the fields identified in 'Event Fields to Encrypt' before forwarding events. If encryption is enabled, it cannot be disabled. Changing any of the encryption parameters again will require a fresh installation of the connector.
Format Preserving Policy URL	Enter the URL where the Micro Focus SecureData Server is installed.
Proxy Server (https)	Enter the proxy host for https connection if any proxy is enabled for this machine.
Proxy Port	Enter the proxy port for https connection if any proxy is enabled for this machine.
Format Preserving Identity	The Micro Focus SecureData client software allows client applications to protect and access data based on key names. This key name is referred to as the identity. Enter the user identity configured for Micro Focus SecureData.
Format Preserving Secret	Enter the secret configured for Micro Focus SecureData to use for encryption.
Event Fields to Encrypt	Recommended fields for encryption are listed; delete any fields you do not want encrypted and add any string or numeric fields you want encrypted. Encrypting more fields can affect performance, with 20 fields being the maximum recommended. Also, because encryption changes the value, rules or categorization could also be affected. Once encryption is enabled, the list of event fields cannot be edited.

After making your selections, click **Next**. A summary screen is displayed. Review the summary of your selections and click **Next**. Click **Continue** to return to proceed with "Add a Connector" window. Continue the installation procedure with "Select Connector and Add Parameter Information."

Select Connector and Add Parameter Information

- 1 Select **Add a Connector** and click **Next**. If applicable, you can enable FIPS mode and enable remote management later in the wizard after SmartConnector configuration.
- 2 Select **Syslog Pipe, File, or Daemon** and click **Next**.
- 3 Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.

Syslog Daemon Parameters	<i>Network port</i>	The SmartConnector for Syslog Daemon listens for syslog events from this port.
---------------------------------	---------------------	--

	<i>IP Address</i>	The SmartConnector for Syslog Daemon listens for syslog events only from this IP address (accept the default (ALL) to bind to all available IP addresses).
	<i>Protocol</i>	The SmartConnector for Syslog Daemon uses the selected protocol (UDP or Raw TCP) to receive incoming messages.
	<i>Forwarder</i>	Change this parameter to 'true' only if the events being processed are coming from another SmartConnector sending to a CEF Syslog destination, and that destination also has CEF forwarder mode enabled. That allows attributes of the original connector to be retained in the original agent fields.
	<i>Syslog Pipe Parameter</i>	<i>Pipe Absolute Path Name</i> Absolute path to the pipe, or accept the default: <code>/var/tmp/syspipe</code>
<i>Syslog File Parameters</i>	<i>File Absolute Path Name</i>	Enter the full path name for the file from which this connector will read events or accept the default: <code>\var\adm\messages</code> (Solaris) or <code>\var\log\messages</code> (Linux). A wildcard pattern can be used in the file name; however, in realtime mode, rotation can occur only if the file is over-written or removed from the folder. Realtime processing mode assumes following external rotation. For date format log rotation, the device writes to 'filename.timestamp.log' on a daily basis. At a specified time, the device creates a new daily log and begins to write to it. The connector detects the new log and terminates the reader thread to the previous log after processing is complete. The connector then creates a new reader thread to the new 'filename.timestamp.log' and begins processing that file. To enable this log rotation, use a date format in the file name as shown in the following example: <code>filename 'yyy-MM-dd'.log;</code> For index log rotation, the device writes to indexed files - 'filename.log.001', 'filename.log.002', 'filename.log.003', and so on. At startup, the connector processes the log with highest index. When the device creates a log with a greater index, the connector terminates the reader thread to the previous log after processing completes, creates a thread to the new log, and begins processing that log. To enable this log rotation, use an index format, as shown in the following example: <code>filename '%d,1,99,true'.log;</code> Specifying 'true' indicates that it is allowed for the index to be skipped; for example, if 5 appears before 4, processing proceeds with 5 and will not read 4, even if 4 appears later. Use of 'true' is optional.
	<i>Reading Events Real Time or Batch</i>	Specify whether file is to be read in batch or realtime mode. For batch mode, all files are read from the beginning. The 'Action Upon Reaching EOF' and 'File Extension if Rename Action' parameters apply for batch mode only.
	<i>Action Upon Reaching EOF</i>	For batch mode, specify 'None', 'Rename', or 'Delete' as the action to be performed to the file when the connector has finished reading and reaches end of file (EOF). For realtime mode, leave the default value of 'None' for this parameter.
	<i>File Extension If Rename Action</i>	For batch mode, specify the extension to be added to the file name if the action upon EOF is 'Rename' or accept the default value of '.processed'.

Select a Destination

- 1 The next window asks for the destination type; select a destination and click **Next**. For information about the destinations listed, see the *ArcSight SmartConnector User Guide*.
- 2 Enter values for the destination. For the ArcSight Manager destination, the values you enter for **User** and **Password** should be the same ArcSight user name and password you created during the ArcSight Manager installation. Click **Next**.

- 3 Enter a name for the SmartConnector and provide other information identifying the connector's use in your environment. Click **Next**. The connector starts the registration process.
- 4 If you have selected ArcSight Manager as the destination, the certificate import window for the ArcSight Manager is displayed. Select **Import the certificate to the connector from destination** and click **Next**. (If you select **Do not import the certificate to connector from destination**, the connector installation will end.) The certificate is imported and the **Add connector Summary** window is displayed.

Complete Installation and Configuration

- 1 Review the **Add Connector Summary** and click **Next**. If the summary is incorrect, click **Previous** to make changes.
- 2 The wizard now prompts you to choose whether you want to run the SmartConnector as a stand-alone process or as a service. If you choose to run the connector as a stand-alone process, select **Leave as a standalone application**, click **Next**, and continue with step 5.
- 3 If you chose to run the connector as a service, with **Install as a service** selected, click **Next**. The wizard prompts you to define service parameters. Enter values for **Service Internal Name** and **Service Display Name** and select **Yes** or **No** for **Start the service automatically**. The **Install Service Summary** window is displayed when you click **Next**.
- 4 Click **Next** on the summary window.
- 5 To complete the installation, choose **Exit** and Click **Next**.

For instructions about upgrading the connector or modifying parameters, see the *SmartConnector User Guide*.

Run the SmartConnector

SmartConnectors can be installed and run in stand-alone mode, on Windows platforms as a Windows service, or on UNIX platforms as a UNIX daemon, depending upon the platform supported. On Windows platforms, SmartConnectors also can be run using shortcuts and optional Start menu entries.

If the connector is installed in stand-alone mode, it must be started manually and is not automatically active when a host is restarted. If installed as a service or daemon, the connector runs automatically when the host is restarted. For information about connectors running as services or daemons, see the *ArcSight SmartConnector User Guide*.

To run all SmartConnectors installed in stand-alone mode on a particular host, open a command window, go to `$ARCSIGHT_HOME\current\bin` and run: `arcsight connectors`

To view the SmartConnector log, read the file `$ARCSIGHT_HOME\current\logs\agent.log`; to stop all SmartConnectors, enter `Ctrl+C` in the command window.

Device Event Mapping to ArcSight Fields

The following section lists the mappings of ArcSight data fields to the device's specific event definitions. See the *ArcSight Console User's Guide* for more information about the ArcSight data fields.

Barracuda Firewall NG F-Series Event Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Panic = Very High; Security, Fatal, Error = High; Warning = Medium; Notice, Info, Internal = Low
Device Product	'Firewall NG F-Series'
Device Severity	Severity
Device Vendor	'Barracuda'
Old File Name	Log

Barracuda Firewall NG F-Series Web Streaming Event Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	emerg, crit, alerth = Very High; err = High; warning = Medium; info, notice, debug = Low
Destination Address	DestinationIP
Destination Host Name	Host
Device Action	ActionNum (0=ALLOWED, 1=BLOCKED)
Device Custom Number 1	ContentLength
Device Custom String 4	URLCategory
Device Event Class ID	'ALLOWED CLEAN'
Device Product	'Firewall NG F-Series'
Device Receipt Time	Timestamp
Device Severity	_SYSLOG_PRIORITY
Device Vendor	'Barracuda'
File Type	ContentType
Name	'ALLOWED CLEAN'
Request URL	URI
Source Address	SourceIP
Source User Name	User