



Micro Focus Security ArcSight Connectors

SmartConnector for McAfee Firewall Enterprise Syslog

Configuration Guide

June, 2018

Configuration Guide

SmartConnector for McAfee Firewall Enterprise Syslog

June, 2018

Copyright © 2003 – 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	Added encryption parameters to Global Parameters.
11/30/2016	Updated installation procedure for setting preferred IP address mode.
09/30/2016	Updated mappings for 'Destination Address' and 'Destination Port.' Added a 'File Size' mapping.
08/30/2016	Updated mappings. Removed support for versions 5.2 through 8.2 due to end of support by vendor.
05/15/2015	Added new parameters for Syslog File.
02/16/2015	Added parameter for Syslog Daemon connector configuration.
02/14/2014	Added support for version 8.3. Updated mappings table.
05/15/2012	Added new installation procedure.

SmartConnector for McAfee Firewall Enterprise Syslog

This guide provides information for installing the SmartConnector for McAfee Enterprise Firewall Syslog (formerly Secure Computing Sidewinder Syslog) and configuring the device for syslog event collection. Firewall Enterprise Appliance Software version 8.3 is supported.

Product Overview

The McAfee Enterprise Firewall is a network security gateway that lets you connect your organization to the Internet while protecting your network from unauthorized users and network attackers. It combines an application-layer firewall, IPSec VPN capabilities and clientless VPN access, anti-spam/anti-fraud and anti-virus/anti-spyware filtering engines, and SSL decryption into one Unified Threat Management (UTM) security appliance, designed to offer centralized perimeter security.



Although syslog pipe and file have a default event length of 2048 characters, the Enterprise Firewall device is limited to a default event length of 1032 characters. Events with a greater length are truncated.

Configuration

Configure Firewall Enterprise

For complete information about McAfee Firewall Enterprise logging, see the Auditing chapter in the *McAfee Firewall Enterprise Product Guide*, from which information in this section has been derived.

From the **Audit Management** window, you can export log files in various formats to a specified host.

Click **Monitor -> Audit Management** to display the Audit Management window.

The screenshot shows the 'Audit Management Firewall Reporter/Syslog' configuration window. It is divided into several sections:

- Audit Options:** Contains three checkboxes: 'Show system statistics in audit log' (checked), 'Require change ticket' (unchecked), and 'Create backups before each change ticket' (unchecked). Below these is a text input field for 'Number of automatic backups to keep:' with the value '50'.
- Logfile Options:** Features a toolbar with icons for adding, editing, deleting, and refreshing, followed by a 'Find:' search box. Below this is a table with three columns: 'Export Entry Name', 'Type', and 'Summary'. The table is currently empty.
- Export logfiles:** Shows the status 'disabled (35 minutes after every hour.)' with a 'Change' button and an 'Export All Now' button.
- Roll logfiles:** Shows the status 'daily at 2:00am.' with 'Change' and 'Roll Now' buttons.
- Delete logs after export:** A checkbox that is currently unchecked.
- Signature Options:** Includes a checkbox for 'Sign exported files', two radio buttons for 'Append signature to exported file' (selected) and 'Put signature in separate file', and a 'Sign with:' dropdown menu currently set to '<None>'.

To capture network and system utilization statistics, make sure "Show system statistics in audit log" is selected. This option is enabled by default and should rarely, if ever, require disabling.

When you configure and enable a schedule, the firewall automatically checks to determine whether any log files are to be exported, and, if so, exports them.

You can configure a schedule, or export or roll log files on request.

Export Audit Data

Use the **Firewall Reporter/Syslog** tab to export audit data to designated syslog servers.

- 1 Select **Monitor -> Audit Management**.
- 2 Click the **Firewall Reporter/Syslog** tab.

Audit Management Firewall Reporter/Syslog

Export audit to McAfee Firewall Reporter

Use McAfee Firewall Reporter

Remote facility: local0

IP address:

Filter: <No Filtering>

Encrypt traffic to McAfee Firewall Reporter

Certificate: Default_SSL_Cert

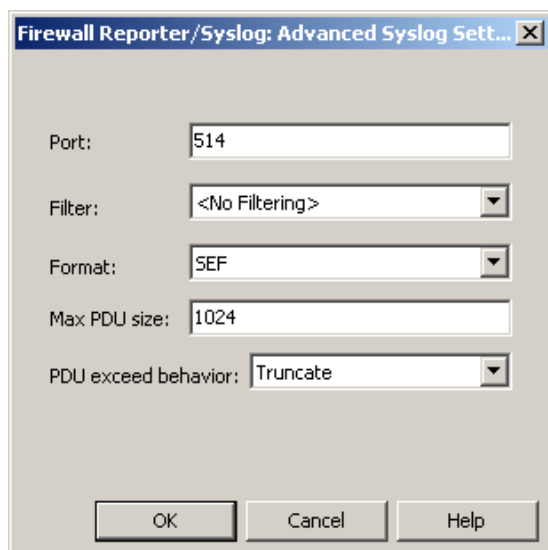
Export audit to syslog servers

Enabled	IP Address	Remote Facility	Description

This pane lets you manage audit data exports to a syslog server.

To create a syslog server export entry:

- 1 Do not select the "Use McAfee Firewall Reporter" checkbox.
- 2 From the toolbar, click **New**.
- 3 Click the **IP Address** cell, and enter the IP address of the syslog server to which you are sending audit data.
- 4 From the **Remote Facility** drop-down list, select a syslog facility to help identify the audit export.
- 5 (Optional) Click in the **Description** cell and enter a further description of the audit export entry.
- 6 (Optional) To define additional parameters for an export entry, select the entry and click **Advanced**. The Advanced Syslog Settings window is displayed.



Specify the additional parameters:

Port: The default port is 514.

Filter: From the drop-down list, select a filter to include or exclude certain types of audit records.

Format: From the drop-down list, select the format to convert the audit data into.

Max PDU size: Enter the maximum size of the syslog record.

PDU exceed behavior: Select a method for auditing export records that exceed the maximum PDU size.

- 7 Click **OK**.

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.

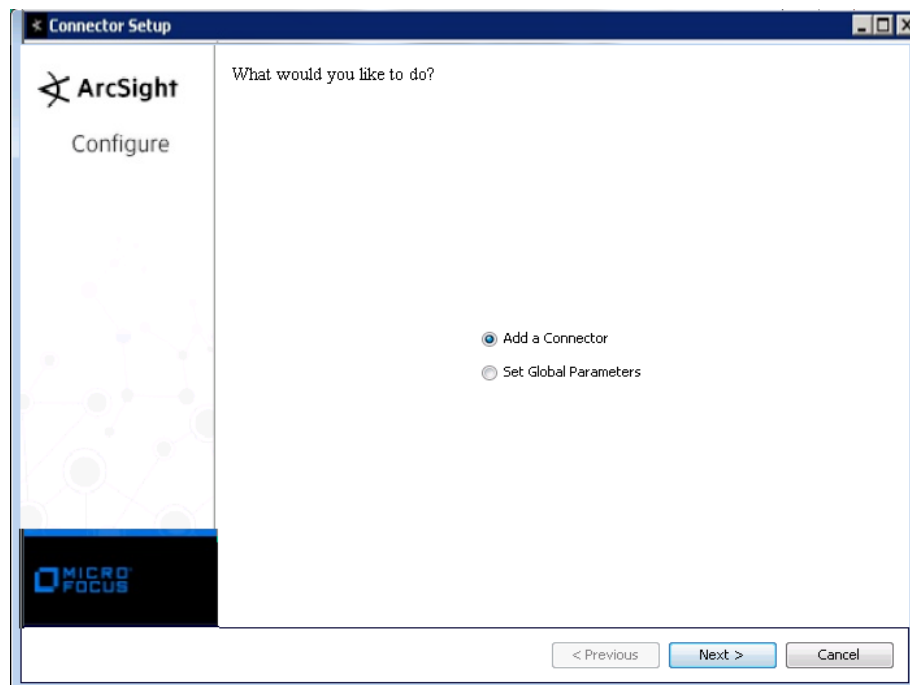


When installing a syslog daemon SmartConnector in a UNIX environment, run the executable as 'root' user.

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 Daemon, File, or Pipe** 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.
Syslog Pipe Parameter	<i>Pipe Absolute Path Name</i>	Absolute path to the pipe, or accept the default: <code>/var/tmp/syspipe</code>
Syslog File Parameters	<i>File Absolute Path Name</i>	<p>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).</p> <p>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.</p> <p>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:</p> <pre>filename'yyy-MM-dd'.log;</pre> <p>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:</p> <pre>filename'%d,1,99,true'.log;</pre> <p>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.</p>
	<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.

McAfee Firewall Enterprise Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	p_critical = Very High; p_major = High; p_trivial = Medium; p_minor = Low
Base Event Count	num_events
Bytes In	One of (bytes_written_to_server, ibytes)
Bytes Out	One of (bytes_written_to_client, obytes)
Destination Address	One of (dstip, dest_ip)
Destination DNS Domain	dstburb
Destination Geo Location Info	dst_geo
Destination Host Name	dsthost
Destination Port	One of (dstport, dest_port)
Destination Process Name	service_name
Destination User Name	One of (user_name, udb_user, user_auth_name)
Device Action	One of (alert_type, udb_action, status)
Device Custom IPv6 Address 2	scrip (Source IPv6 Address)
Device Custom IPv6 Address 3	dstip (Destination IPv6 Address)
Device Custom String 1	rule_name (Rule Name)
Device Custom String 2	auth_method (Authentication Method)
Device Custom String 3	submessage2 (Continued Message)
Device Event Category	fac
Device Event Class ID	type
Device Host Name	hostname
Device Inbound Interface	interface
Device Process ID	pid
Device Process Name	module
Device Product	'Firewall Enterprise'
Device Receipt Time	date
Device Severity	pri
Device Vendor	'McAfee'
End Time	end_time
Event Outcome	result (1=Success, 0=Failure)
External ID	netsessid
File Name	file
File Size	max_pdu_size
File Type	filetype
Message	Both (reason, information)
Name	One of (event, 'continued message', type (without t_))
Reason	result_code
Request Client Application	application
Request Method	request_command
Request URL	url
Source Address	scrip
Source DNS Domain	srcburb
Source Geo Location Info	src_geo

ArcSight ESM Field	Device-Specific Field
Source Host Name	srchost
Source Port	srcport
Source Process Name	cmd
Source User ID	logid
Source User Name	admin
Start Time	start_time
Transport Protocol	One of (protocol, protocolname)

Troubleshooting

How can I check whether auditd is sending messages to syslogd?

To check whether auditd is sending messages to syslogd using the local1 facility (as outlined above), add this line to `/etc/syslog.conf` and restart syslogd.

```
local1.* /var/log/testlocal1
```

All audit messages should now appear in that file (check using `tail -f /var/log/testlocal1`). You might want to undo this step after the test is successful.

How can I check whether the loghost is receiving messages from Sidewinder and writing to the syslog pipe?

To check whether the loghost is receiving messages from Sidewinder and writing to the pipe:

- 1 Make sure no other process is listening on the pipe on the loghost.
- 2 Start listening on the pipe:

```
"cat /path/to/pipe"
```

- 3 On the Sidewinder appliance, enter the command

```
"logger -p local1.notice This is a test from sidewinder"
```

- 4 If everything is correctly configured, the above message should now be displayed on the terminal where step 2 was performed.

Make sure that the cat process is killed before starting the connector, as only one process may read from the pipe.