Micro Focus Security ArcSight SmartConnectors

Software Version: 8.3.0

Configuration Guide for Dell SonicWALL Firewall Syslog SmartConnector

Document Release Date: February 2022
Software Release Date: February 2022

Legal Notices

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK

https://www.microfocus.com

Copyright Notice

Trademark Notices

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

https://www.microfocus.com/support-and-services/documentation

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

Contents

Configuration Guide for Dell SonicWALL Firewall Syslog SmartConnector

Configuration Guide for Dell SonicWALL Firewall Syslog SmartConnector

This guide provides information for installing the SmartConnector for Dell SonicWALL Firewall Syslog and configuring a SonicWALL Firewall device to send syslog events.

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight SmartConnectors.

Additional Documentation

The ArcSight SmartConnectors documentation library includes the following resources:

- *Installation Guide for ArcSight SmartConnectors*, which provides detailed information about installing SmartConnectors.
- *Configuration Guides for ArcSight SmartConnectors*, which provide information about configuring SmartConnectorss to collect events from different sources.
- *Release Notes for ArcSight SmartConnectors*, which provides information about the latest release

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the documentation site for ArcSight SmartConnectors.

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to Documentation-Feedback@microfocus.com.

For specific product issues, contact Micro Focus Customer Care.

Product Overview

SonicWALL's family of Internet security appliances provide the first line of defense against Internet security threats. Designed to increase security by reducing complexity, SonicWALL Internet security appliances eliminate the cost and complexity of installing and managing separate devices and software packages for comprehensive security.

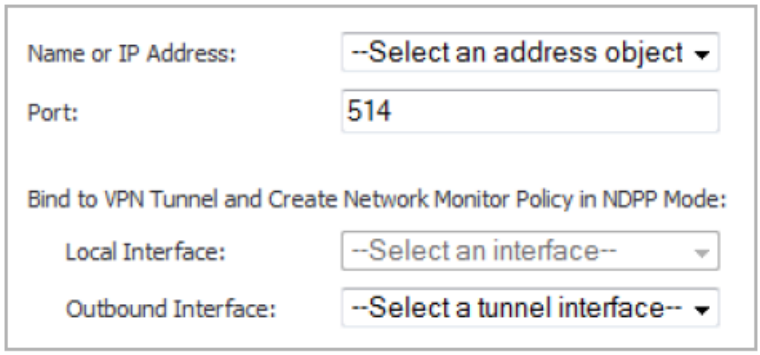
Configuration

Configuring the SonicWALL Device for SonicOS 6.2

In addition to displaying event messages in the GUI, the Dell SonicWALL security appliance can send the same messages to an external, user-configured Syslog server for viewing. The Syslog message format can be selected in Syslog Settings and the destination Syslog Servers can be specified in the table of Syslog Servers. See the Administration Guide for SonicOS 6.2 for details

To configure the SonicWALL device to send syslog events:

1. Login to the SonicWALL management interface with the **admin** account.
2. Go to **Log > Syslog**.
3. In the Syslog Servers section, click **Add**.



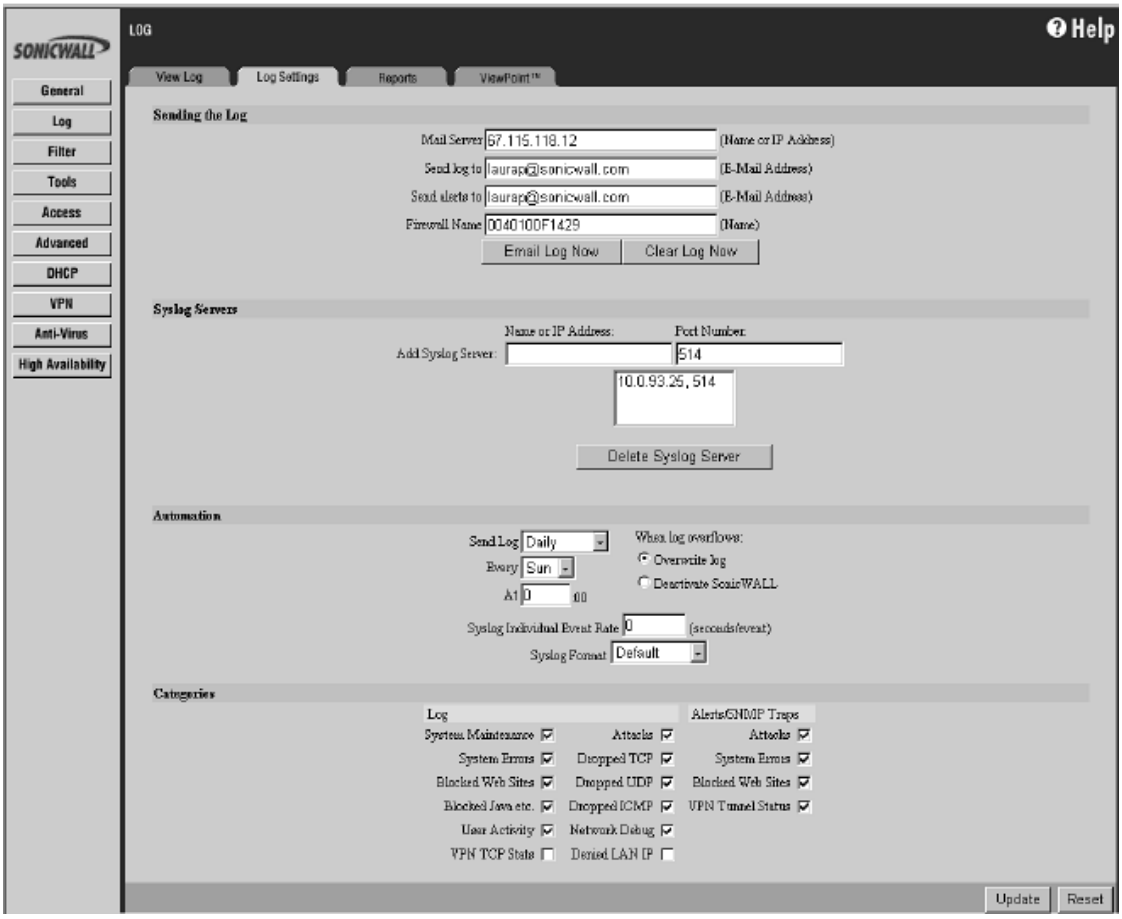
4. Select the syslog server name or IP address from the **Name or IP Address** drop-down menu. Messages from the firewall are then sent to the servers.
5. Select the default port 514, or specify another port number in the **Port Number** field.
6. Click **OK**.
7. Click **Accept** to save all Syslog Server settings.

Configuring the SonicWALL Device for SonicOS 5.8

The SonicWALL Syslog captures all log activity and includes every connection source and destination IP address, IP service, and number of bytes transferred. The SonicWALL Syslog support requires an external server running a syslog daemon on UDP Port 514.

To configure the SonicWALL device to send syslog events:

1. Login to the SonicWALL management interface with the **admin** account.
2. Click **Log,**then click the **Log Settings** tab.
3. In the Syslog Servers section, enter the syslog server name or IP address in the **Add Syslog Server** field. Messages from the SomnicWALL device are then sent to the servers. You can configure up to three Syslog Server IP addresses.



4. In the Automation section, select options to configure the frequency at which the logs need to be sent and the action to be taken when there is a log overflow.

   Set the **Syslog Individual Event Rate** as appropriate. This setting prevents repetitive messages from being written to Syslog. If duplicate events occur during the period specified in the **Syslog Individual Event Rate** field, they are not written to Syslog as unique events. Instead the additional events are counted, and then at the end of the period, a message is written to the Syslog that includes the number of times the event occurred. The Syslog Individual Event Rate default value is 60 seconds and the maximum value is 86,400 seconds (24 hours). Setting this value to 0 seconds sends all Syslog messages without filtering.

   You can choose the format of the Syslog to be **Default** or **WebTrends**. If you select Webtrends, however, you must have WebTrends software installed on your system.
5. Click **Update** to save your settings.

Configuring for the Syslog SmartConnectors

The syslog SmartConnectors use a sub-connector architecture that lets them receive and process syslog events from multiple devices. There is a unique regular expression that identifies the device. For example, the same SmartConnector can process events from a Cisco Router and a NetScreen Firewall simultaneously. The SmartConnector inspects all incoming messages and automatically detects the type of device that originated the message.

You can install the syslog SmartConnector as a syslog daemon, pipe, or file connector. You can use the Syslog Deamon, Syslog Deamon NG, or Syslog File connector types depending on your requirement. The Syslog File type SmartConnectors also support Syslog Pipe.

Syslog Daemon SmartConnector

The Syslog Deamon 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 by default, or can be configured on another port to receive syslog events. You can also configure to use the TCP protocol.

To use the SmartConnector for Syslog Daemon, add the following statement in the *rsyslog.conf* file:

```
*.* @@(remote/local-host-IP):514
```

Example: `local1.warning @@10.0.0.1:514`

- To read all Syslog events, use *.*
- To filter specific events, replace regex with the specific event name.
- For example: *.* @@(remote/local-host-IP):514 and local1.warning @@10.0.0.1:514.
- To send events over a TCP connection, use @@ and to send events over an UDP connection, use @.

If you are running SmartConnector for Syslog Daemon on the same machine as the server, you must provide the IP address of the local host. If you want to forward events to other machines, you must provide the IP address of the same.

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

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 additional configurations for the ArcSight syslog file or syslog pipe SmartConnectors in the system where all Syslog Daemon SmartConnector configurations are done.

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.

Using the SmartConnector for Syslog Pipe or File

This section provides information 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.

For Syslog Pipe:

1. Execute the following command to create a pipe:

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

2. Add one of the following lines depending on your OS to the */etc/rsyslog.conf* file:

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

or

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

3. Restart the syslog daemon in one of the following methods:
Enter the following commands:

```
/etc/init.d/syslogd stop
/etc/init.d/syslogd start
```

or

Execute the following command to send a configuration restart signal:

On RedHat Linux:

```
service syslog restart
```

On Solaris:

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

For Syslog File:

1. Create a file or use the default file into which log messages must be written.
2. Modify the /etc/rsyslog.conf file

The syslog daemon is forced to reload the configuration and start writing to the pipe.

3. Restart the syslog daemon in one of the following methods:
   a. Restart the syslog daemon in one of the following methods:
   Enter the following commands:

```
/etc/init.d/syslogd stop
/etc/init.d/syslogd start
```

or

Execute the following command to send a configuration restart signal:

On RedHat Linux:

```
service syslog restart
```

On Solaris:

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

Installing the SmartConnector

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

Preparing to Install Connector

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

For complete product information, refer to the *Administrator's Guide to ArcSight Platform* guide, available on ArcSight Documentation.

If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* for instructions.

Start the installation procedure from step 3.

Before installing the SmartConnector, make sure that the following are available:

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

Installing and Configuring the SmartConnector by Using the Wizard

The installation steps described in this section are specific to the Citrix NetScaler Syslog Connector. For detailed installation steps or for manual installation steps, see SmartConnector Installation and User Guide.

To install and configure the Citrix NetScaler Syslog Connector:

1. Start the installation wizard.
2. Follow the instructions in the wizard to install the core software.
3. Specify the relevant Global Parameters, when prompted.
4. Select a Syslog Deamon or Syslog File connector from the **Type** drop-down, then click **Next**.

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

5. Specify the following information depending on the type SmartConnector that you are installing:

   For Syslog Deamon, specify the following parameters:

Syslog Daemon Parameters	**Network port**	The SmartConnector for Syslog Daemon listens for syslog events from this port.
	IP Address	The SmartConnector for Syslog Daemon listens for syslog events only from this IP address, apart from the default (ALL) to bind to all available IP addresses.
	Reading Events Real Time or Batch	Specify whether to read files in batch mode or real-time mode. In batch mode, all files are read from the beginning.
	Action Upon Reaching EOF	This option applies to Batch Mode only. Specify **None**, **Rename**, or **Delete** as the action to be performed to the file when the connector finishes reading and reaches end of file . For the real-time mode, retain the default value **None**.
	File Extension If Rename Action	This option applies to Batch Mode only. Specify the extension to be added to the file name if the action on reaching the end of file is specified as **Rename**. The default value is **Processed**, which adds a `.processed` extension.

   For Syslog File Type, specify the following parameters:

Syslog Pipe Parameter	**Pipe Absolute Path Name**	Specify an absolute path to the pipe, or accept the default value: `/var/tmp/syspipe`.
Syslog File Parameters	**File Absolute Path Name**	Specify the full path name for the file from which this connector will read events. The following are default values: • **Solaris:** `\var\adm\messages` • **Linux:** `\var\log\messages` You can use a wildcard pattern in the file name. In the real-time mode, rotation can occur only if the file is over-written or removed from the folder. The real-time processing mode assumes the following external rotation: • **Date format log rotation:** The device creates a new log at a specified time in the with the naming convention `filename.timestamp.log`. The connector detects the new log and terminates the reader thread to the previous log after the 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, specify timestap in yyyy-MM-dd date format. For example, `filename.yyyy-MM-dd.log` • **Index log rotation:** The device writes to indexed files in the following format: `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:`filename'%d,1,99,true'.log;` Specifying `true` indicates that the index can be skipped. For example, if 5 appears before 4, processing proceeds with 5 and will not read 4. Use of `true` is optional.
	Reading Events Real Time or Batch	Specify whether to read files in batch mode or real-time mode. In batch mode, all files are read from the beginning.
	Action Upon Reaching EOF	This option applies to Batch Mode only. Specify **None**, **Rename**, or **Delete** as the action to be performed to the file when the connector finishes reading and reaches end of file . For the real-time mode, retain the default value **None**.
	File Extension If Rename Action	This option applies to Batch Mode only. Specify the extension to be added to the file name if the action on reaching the end of file is specified as **Rename**. The default value is **Processed**, which adds a `.processed` extension.

6. Select a destination and configure parameters.
7. Specify a name for the connector.
8. 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.
9. Select whether you want to run the connector as a service or in the standalone mode.
10. The connector cannot detect the network drive when running as a service on a Windows platform. This problem does not occur when the connector and IIS Server are installed on the same host.
11. Complete the installation.
12. Run the SmartConnector.

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

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.

Dell SonicWALL Firewall Field Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Very High when Device Severity = 0, 1; High when Device Severity = 2, 3; Medium when Device Severity = 4, 5; Low when Device Severity = 6, 7
Bytes In	rcvd or bytesRX
Bytes Out	sent or bytesTX
Destination Address	dadress or dst
Destination Dns Domain	part of dst
Destination Host Name	dstname or part of msg
Destination MAC Address	dstMac
Destination NT Domain	dstZone
Destination Port	dport or dst or part of msg
Destination Service Name	proto
Destination Translated Address	natDst
Destination User ID	rcptTo
Destination User Name	usr
Detect Time	DetectTime
Device Action	fw_action, af_action
Device Address	WanIP
Device Custom IPv6 Address 2	srcV6 or natSrcV6
Device Custom IPv6 Address 2 Label	"Source IPv6 Address" or "Source IPv6 NAT Address"
Device Custom IPv6 Address 3	dstV6 or natDstV6 (Destination IPv6 Address or Destination IPv6 NAT Address)

ArcSight ESM Field	Device-Specific Field
Device Custom Number 1	n (Event Count)
Device Custom Number 2	icmpCode (ICMP Code)
Device Custom Number 3	cdur (Connection Duration)
Device Custom String 1	rule (Rule)
Device Custom String 2	result (Result)
Device Custom String 3	vpnpolicy (Source VPN Policy)
Device Custom String 4	appName (Application Name)
Device Custom String 5	sess (Session Type)
Device Custom String 6	dur (Session Duration)
Device Event Category	One of (ipscat, spycat, gcat, f)
Device Event Class ID	m or sid
Device External ID	bid
Device Inbound Interface	part of dst
Device Mac Address	mac
Device Outbound Interface	ai or part of src
Device Product	'SonicWALL Firewall'
Device Severity	pri, ipspri, or syprpi
Device Vendor	'Dell'
Event Name	msg
File ID	appid
File Name	arg
File Path	arg
File Type	appcat
Message	Submessage
Name	msg
Old File ID	af_polid
Old File Name	af_policy
Old File Type	af_type
Request Method	op
Request URL	arg

ArcSight ESM Field	Device-Specific Field
Source Address	saddress or src or part of msg
Source Dns Domain	part of src
Source Host Name	src or part of msg
Source MAC Address	srcMac
Source NT Domain	srcZone
Source Port	sport or src or part of msg
Source Service Name	af_service
Source Translated Address	natSrc
Source User Name	mailFrom
Transport Protocol	proto

Additional Data Mappings

Additional_Information=note	Application_Applied_Syslog=app
Application_Policy_Object_Name=af_object	Blocking_Code_Description=category
Broadcast_Packets_Received=bcastRX	Broadcast_Packets_Sent=bcastTX
Code=code	Configuration_Change_Webpage=change
Connections_In_Use=conns	Content_Object=contentObject
CPU_Utilization=cpuUtil	Destination_Interface=dst
Destination_VPN_Policy_Name=vpnpolicyDst	Device_Management_Port=pt
Firewall_Devices_With_Limited_Nodes=lic	Firewall_LAN_Zone_IP=fwlan
GMS_Message_Interval=i	HA_And_Dialup_Connection_State=dyn
ICMP_Type_Code=type	Interface_Statistics_Report=if
Message_Category=c	Number_Of_Packet_Sent=spkt
Packet_Receive=rpkt	RAM_Utilization=ramUtil
returncode=result	Rule_Category_ID=catid
SonicPoint_Radio=radio	SonicPoint_Station=station
Standby_SA_In_Use=usesstandbysa	Time_Since_Last_Change=unsynched
Unicast_Packets_Received=ucastRx	Unicast_Packets_Sent=ucastTx
URL_Of_Network_Packet_Capture_System=npcs	Well_Formed_Packets_Received=goodRxBytes
Well_Formed_Packets_Sent=goodTxBytes	

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on Configuration Guide for Dell SonicWALL Firewall Syslog SmartConnector (SmartConnectors 8.3.0)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to Documentation-Feedback@microfocus.com.

We appreciate your feedback!