Cisco Systems, Inc.
Service Provider Video Technology Group

100 Middlefield Road
Scarborough, Ontario
Canada, M1S 4M6

Telephone (416) 299-6888
Fax (416) 299-7145

Application Note

Date: 12-Nov-13
Author: Fred Yee
Subject: Syslog

Capturing Receiver Log Files

November 12, 2013

Please read this entire document for important information about logging receivers, including problems you may encounter when running it.

Contents:

Requirements

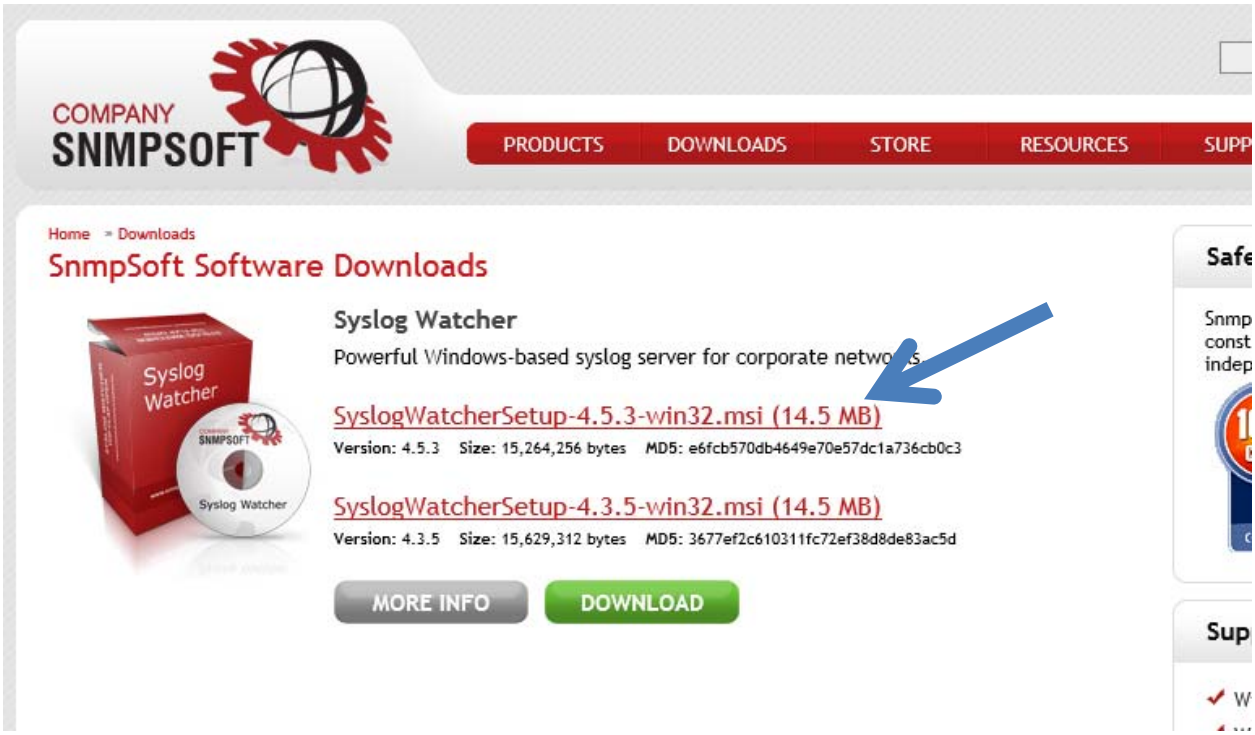
In attempts to troubleshoot problems with receivers, it is sometimes necessary to log the receiver for error messages. Previous versions of receivers required manual logging of diagnostic messages generated from the receiver. This was largely accomplished with telnet sessions, and issuing commands via CLI. With the release of v4.00 software, a new feature has facilitated the ability to capture all diagnostic messages via a Windows-based application known as a Syslog Server. The use of this feature provides a more universal solution to capturing receiver logs, which will be available in future products.

Implementation of Syslog requires that a third-party application be installed on a PC to capture the logs. Currently, we will support two free Syslog Servers:

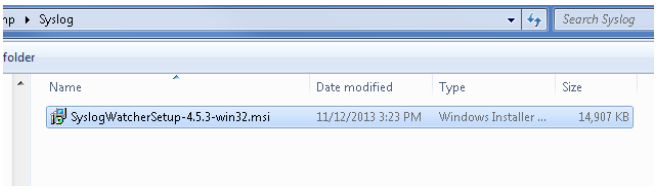
For Linux, we support 'syslog-ng' (from BalaBit)
http://www.balabit.com/network-security/syslog-ng/opensource-logging-system

For Windows, we support 'Syslog Watcher' (from SNMPSoft)
http://www.snmpsoft.com/syslogwatcher/syslog-server.html

Download the appropriate application and install in PC. In our example, we will be installing the SNMPSoft application on a Windows based PC.

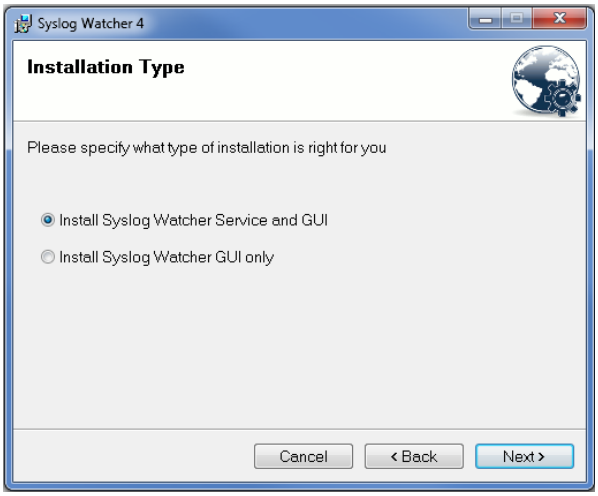


After downloading the application, locate the installer file and launch…



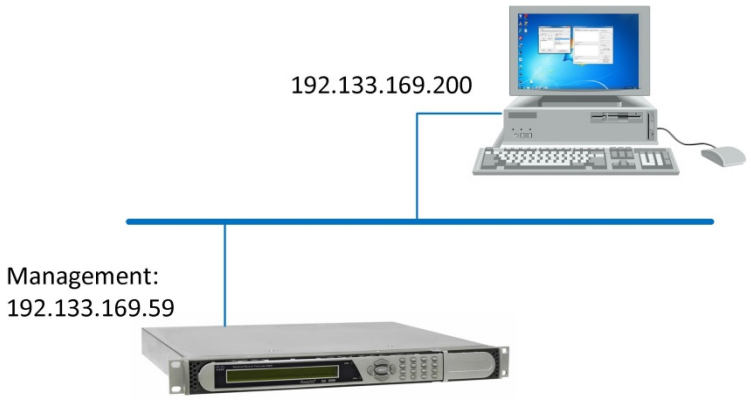
Choose 'Install Syslog Watcher Service and GUI' when prompted…

Continue to install the application.



Procedure

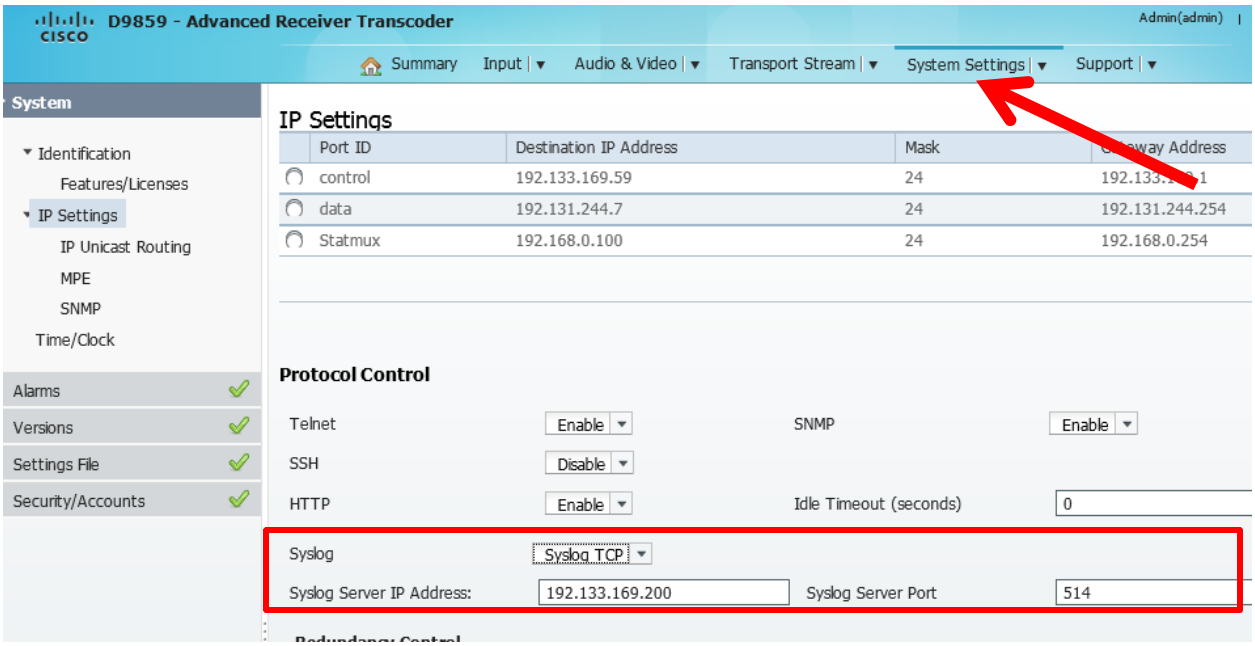
In our example, we have a D9859 receiver on our network. As well, the PC with the Syslog software is available configured with the IP addresses shown below:



STEP 1. Enable the logs from the receiver.
STEP 2. Launch the Syslog Watcher.
STEP 3. Capture logs to Syslog File.

STEP 1. Enable the logs from the receiver

Log in to the receiver via the Web interface (default username/password is admin/localadmin).
Access the **System Settings** screens and configure the **Protocol Control** fields:



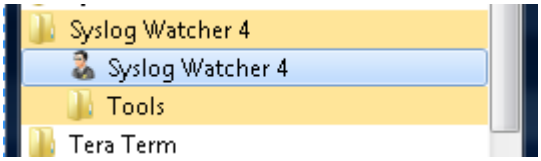
In this example, we have selected **Syslog TCP** protocol and entered the IP address of the PC (**192.133.169.200**) for the Syslog Server address. Also, we are using the default server port (**514**).

Alternatively, you may configure via the front panel:

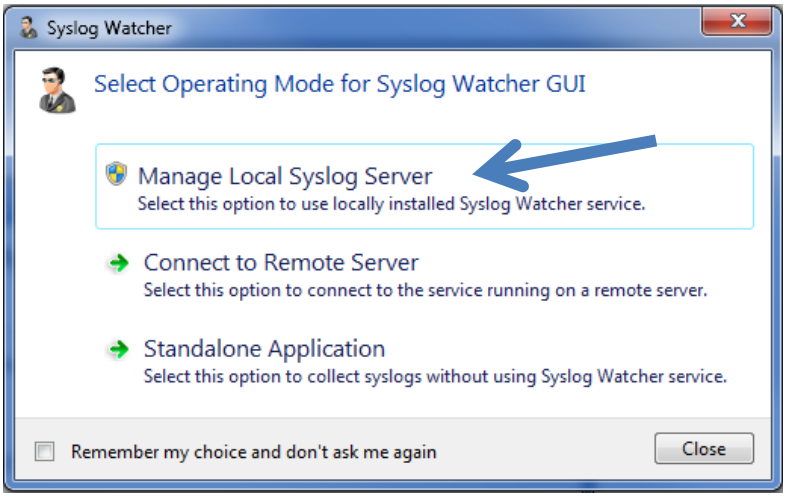
Main Menu – Setup – IP – Protocols
Scroll down until you see the menu above.

STEP 2. Launch the Syslog Watcher

Launch the Syslog Watcher application:



Choose 'Manage Local Syslog Server' when prompted…

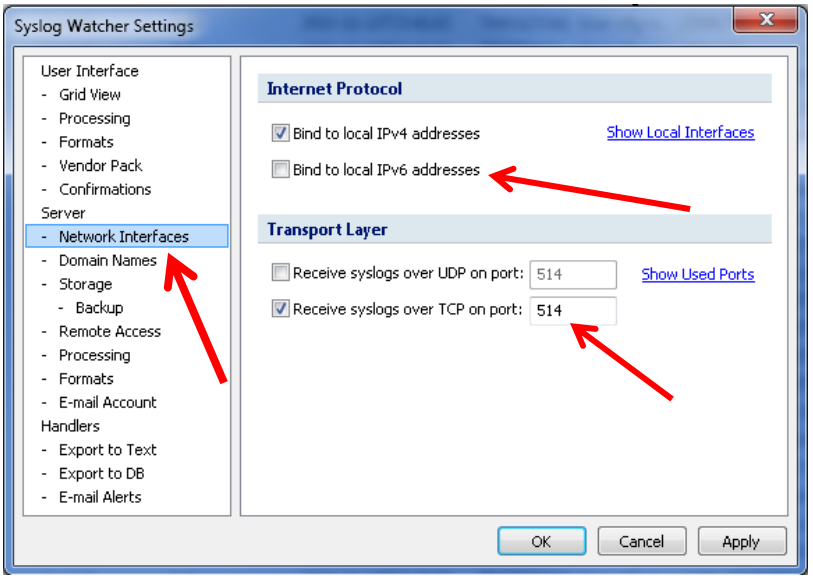


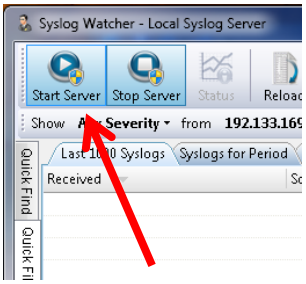
Click the 'Settings' icon…

Configure the **Transport Layer** in the **Network Interfaces** menu.

Uncheck ‘Bind to local IPv6 addresses’.

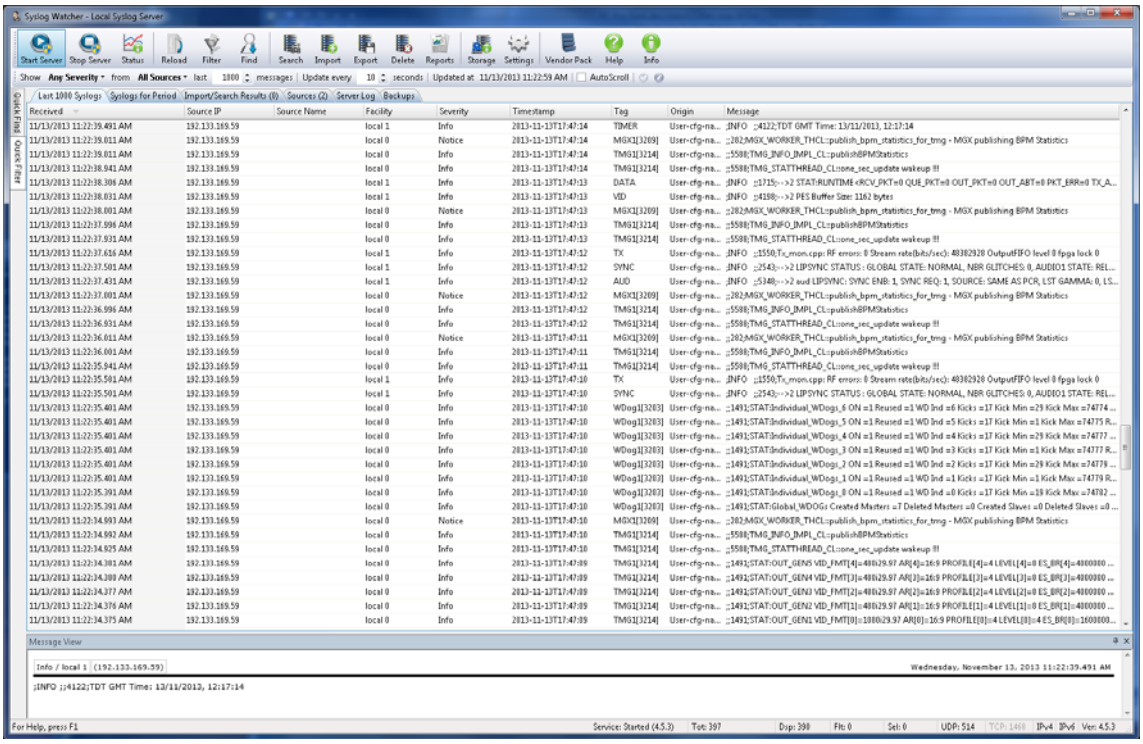
In this example, we used TCP protocol on port 514.





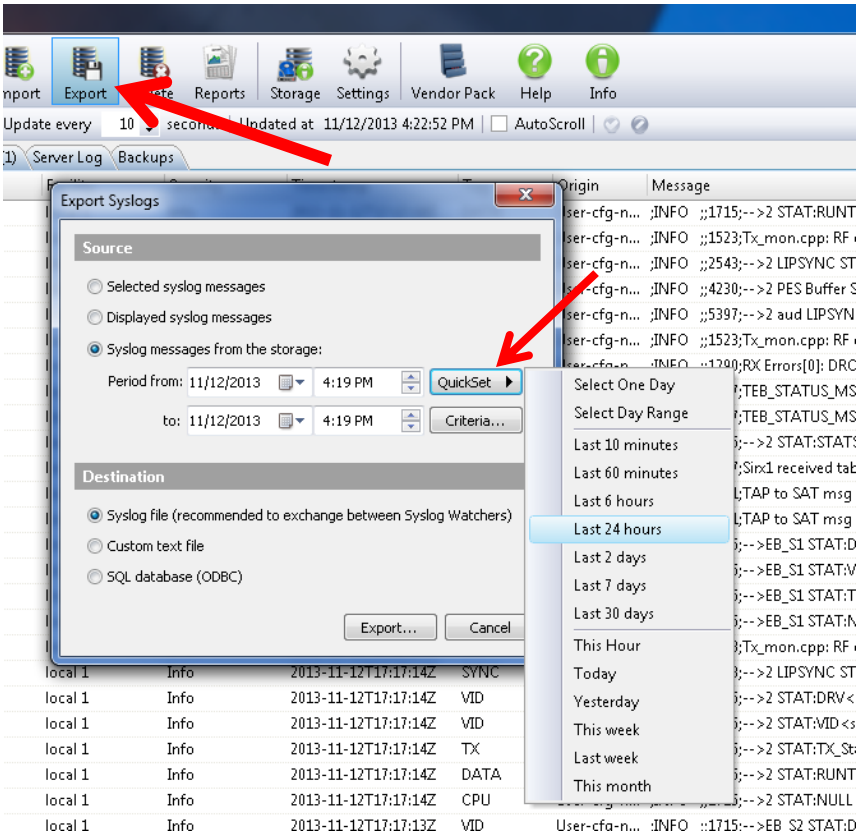
Start the Syslog Watcher server by clicking on the ‘Start Server’ icon…

Diagnostic log messages should begin to appear…



STEP 3. Capture logs to Syslog File

After a period of time when the diagnostic logs have captured the required event, click the **Export** icon…



Choose the source ‘Syslog messages from the storage’ and click on the **QuickSet** button…

Select an appropriate time period for the log capture.

Select ‘Syslog file’ for the destination.

Click the ‘Export’ button and save the file to your hard drive.

Forward the log file for analysis.

Common Questions about ....

Q: ***What is the difference between using UDP and TCP protocol? Can I use either one?***

A: UDP (User Datagram Protocol or Universal Datagram Protocol) is a connectionless protocol. It is used for applications which require fast transmission of data. The stateless nature of UDP data is also useful for servers that answer queries from a large number of clients. TCP (Transmission Control Protocol) is a connection-oriented protocol. It is generally slower than UDP and is considered reliable as packets are checked for errors. Although either protocol will work in this application, it is advisable to choose the TCP protocol as it is more reliable.

Q: ***Both my receiver and my Syslog Watcher PC are on my network, but I am not getting any results. What might be wrong?***

A: There may be a variety of reasons…

- Confirm that the port numbers are configured correctly. The port number is configured in both the Syslog Watcher configuration menus, as well as in the receiver's protocol configuration menu. If the receiver is on a different network segment, ensure that there is no firewall setting which may prevent the use of the port.
- Confirm that the protocols match in both the receiver and the Syslog Watcher application. If you are using TCP protocol in the receiver, you MUST configure the Syslog Watcher to receive syslogs via TCP protocol.
- Certain security software may also prevent Syslog from receiving the UDP data packets. If necessary, disable any firewall software which might prevent communication.
- Confirm that IPv6 addresses are not being used. Only IPv4 addressing is supported.

Q: ***Does this log contain all of the information you need?***

A: No, you may still need to provide the specific details for your receiver such as model, application code, FPGA code, etc. This information may be captured by exporting the Debug Support Data. Click the **Export** button, under **Support – Service Actions**: