Set up a Syslog Server to Capture Logs from D98xx series IRDs

Contents

Introduction

This document describes how to set up a Syslog server to capture logs from D98xx series Integrated Receivers/Decoders (IRDs).

Background Information

Software release 4.0 of D9854, D9858 & D9824, and any release of D9859 support RFC-3164 compliant **syslog** messages. The customers can now capture the messages with a Syslog Server for storage and retrieval. In addition, this procedure can also be used with the new D9800 Network Transport Receiver.

Syslog Watcher is the supported free **syslog server** for Windows machines. For Linux machines, the supported **syslog server** is **syslog-ng** which is available from http://www.balabit.com/network-security/syslog-ng/opensource-logging-system

This article deals only with setting up on Windows machines.

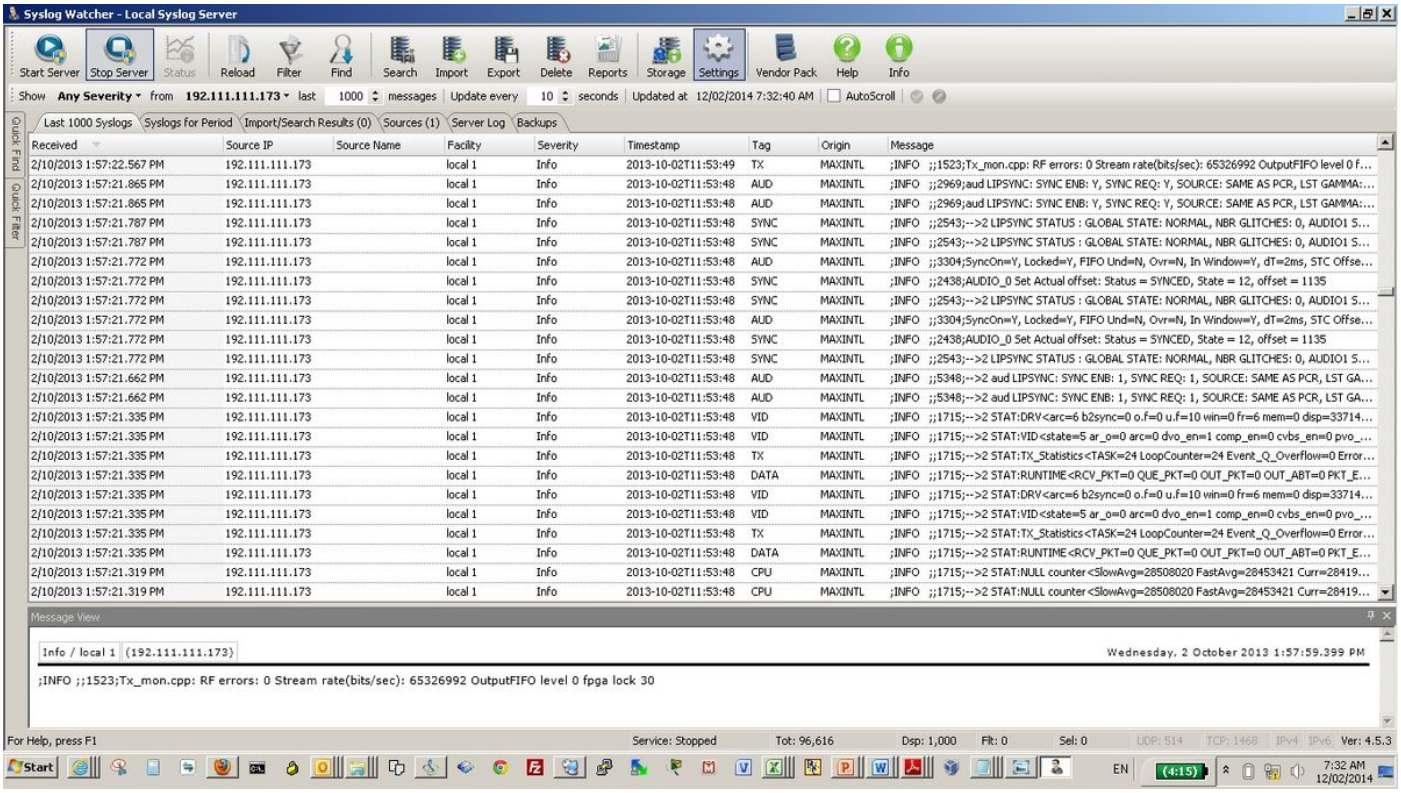
Configure the Syslog Server

Download the **SysLog Watcher** from

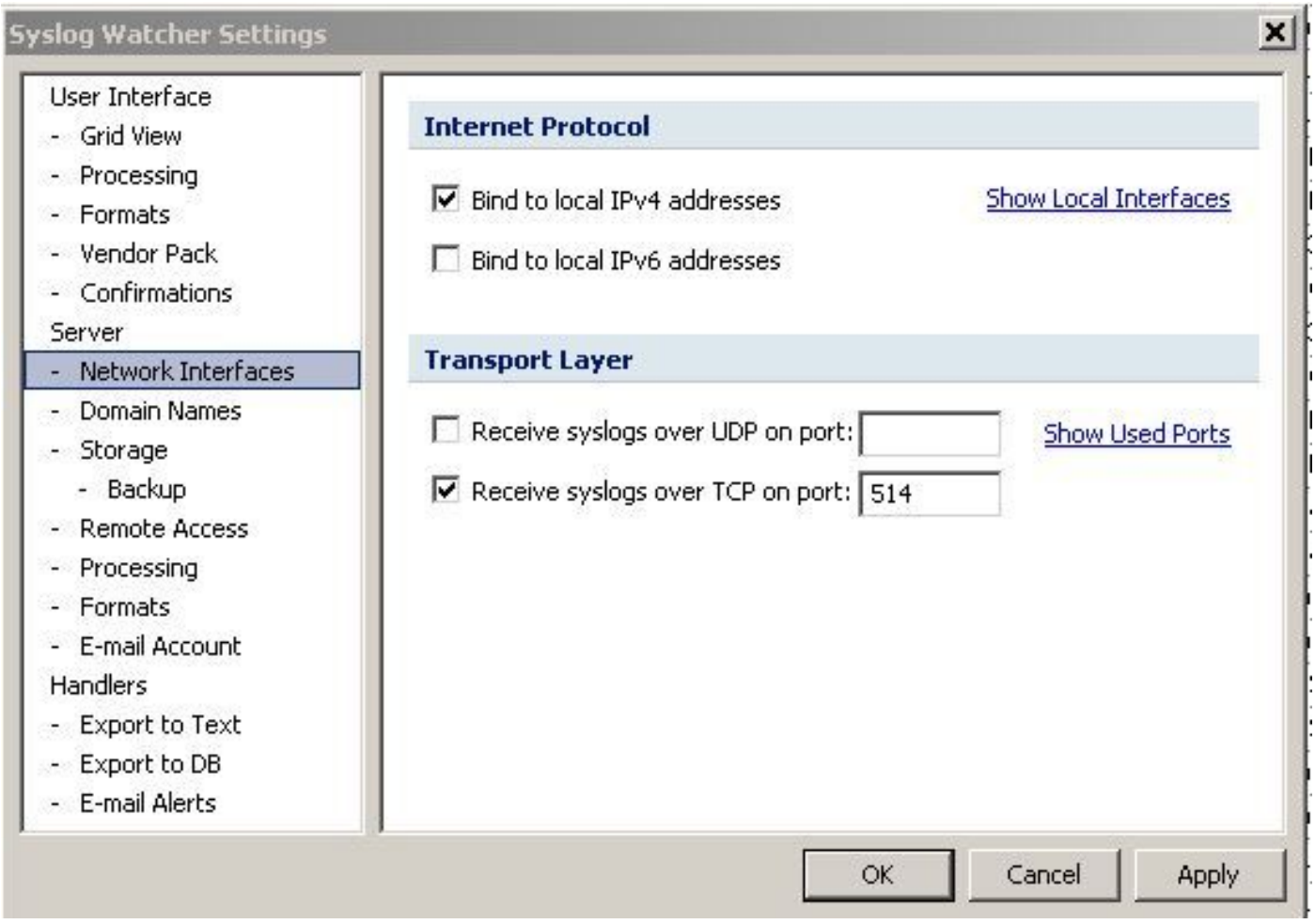
http://www.snmpsoft.com/syslogwatcher/syslog-server.html

and install it in your windows computer.

Start the SysLog Watcher and select the Operating mode for the GUI as **Manage Local Syslog Server**, the image shown appears:

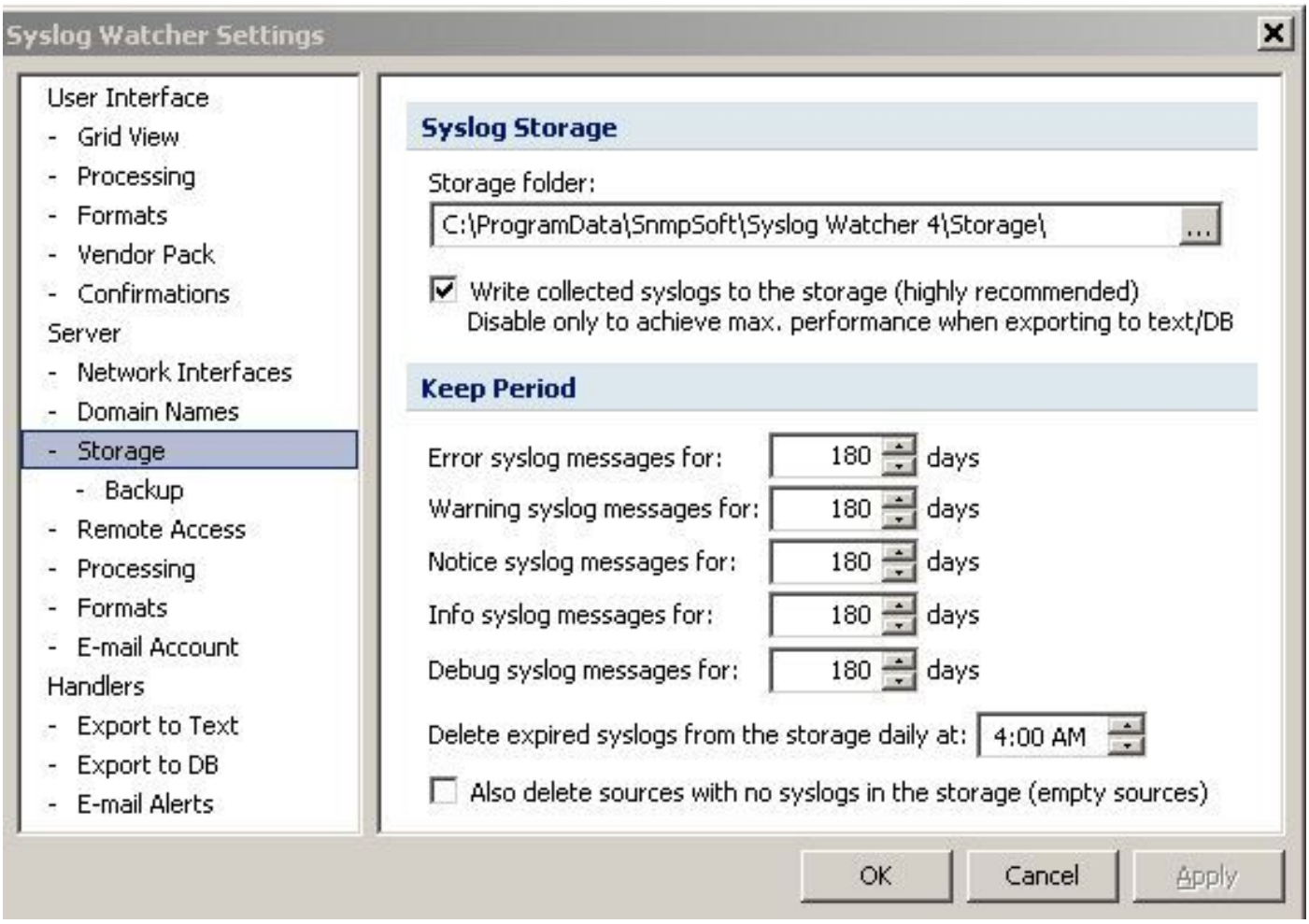


Click in **Settings** (highlighted in the above picture) in the tool bar, the image shown appears:



Select **Network Interfaces**. Check the box **Receive** syslogs **over UDP on port** and enter a port number. The same port number needs to be configured on the devices from where the SysLog Watcher needs to receive logs.

Now select **Storage** under **SysLog Watcher Settings**, as shown in the image:

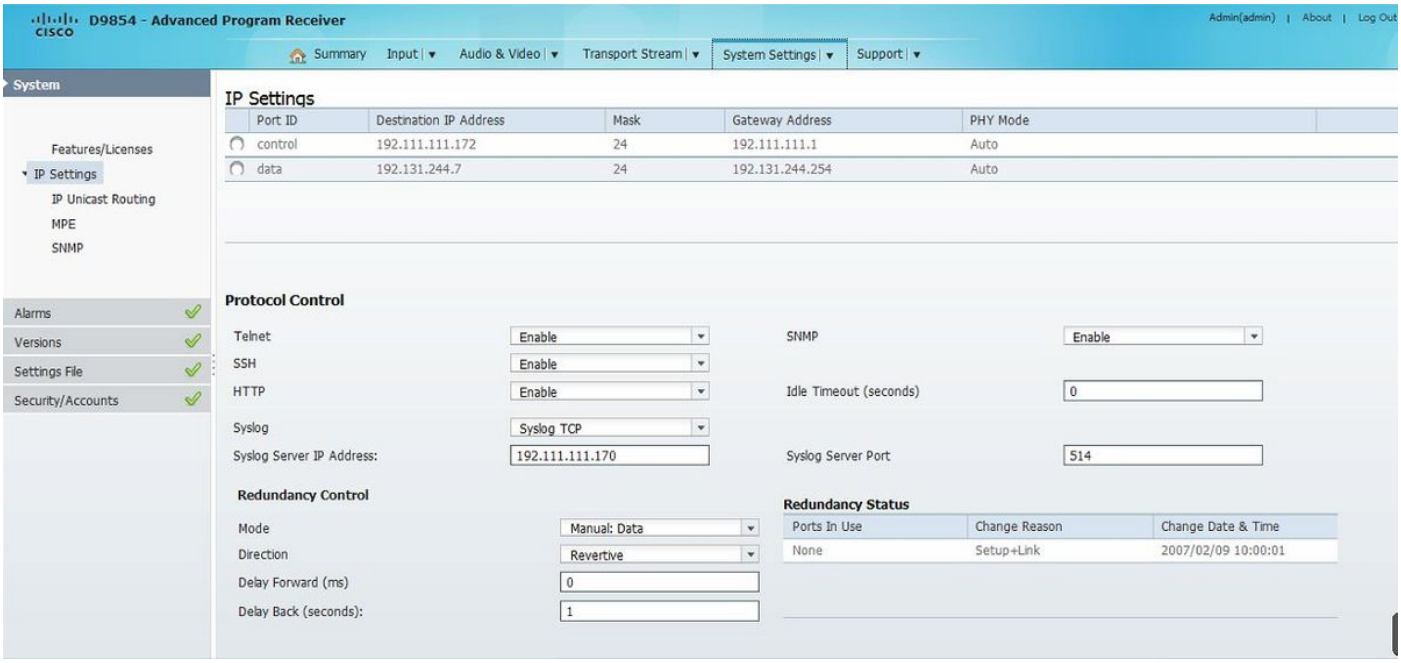


Specify a folder location for storing the messages, check the box **Write collected** syslogs **to the storage**.

Specify the number of days for each type of message to be kept in storage.

Configure the IRD (D9854/D9858/D9859) to send logs to Syslog Watcher

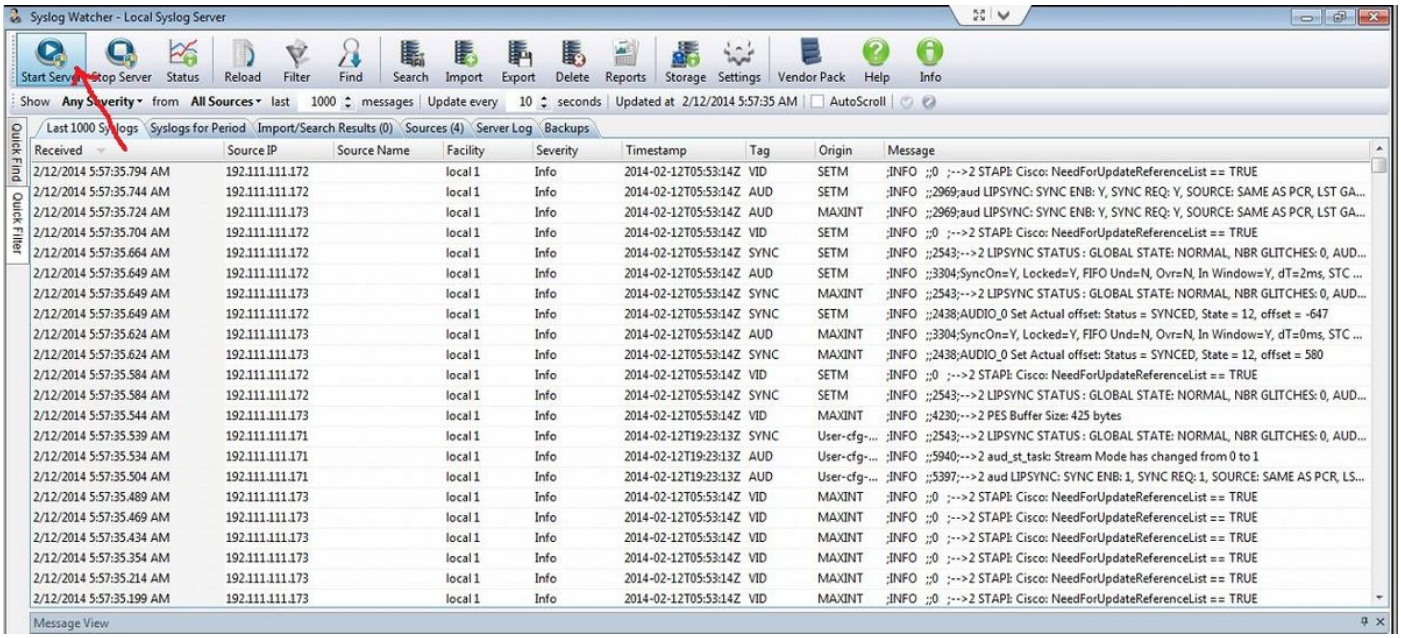
On the IRD GUI, select the **System Settings/ IP Settings** from the tool bar. The image shown appears:



In the **Protocol Control** section of the IP Settings page, configure these:

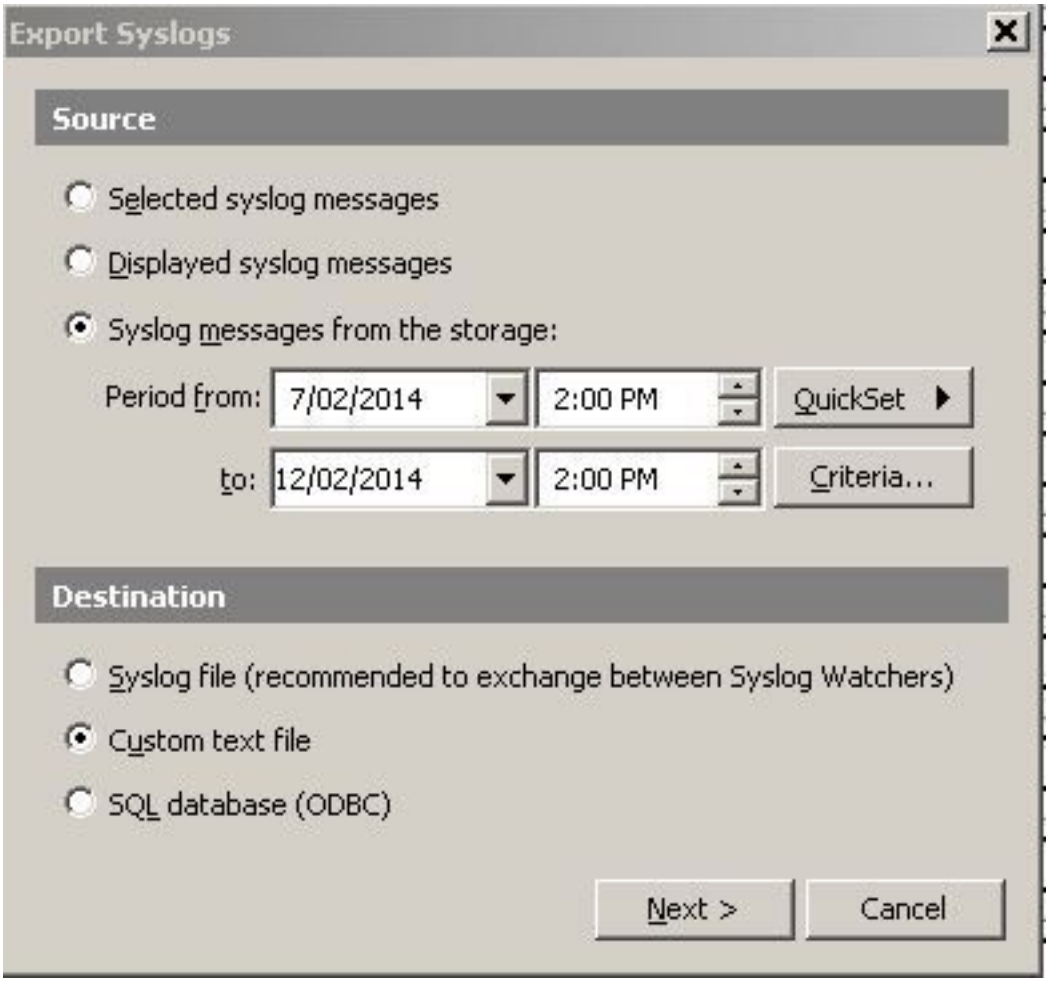
- **Syslog**- Select either Syslog TCP or Syslog UDP as required.
- **Syslog Server IP Address**- Enter the IP address of the computer where the SysLog Watcher is installed.
- **Syslog Server Port**- Enter a port number. This should match the port number entered in the **Syslog Watcher Settings**.

Under Syslog Watcher GUI, start the service by selecting **Start Server**, as shown in the image:



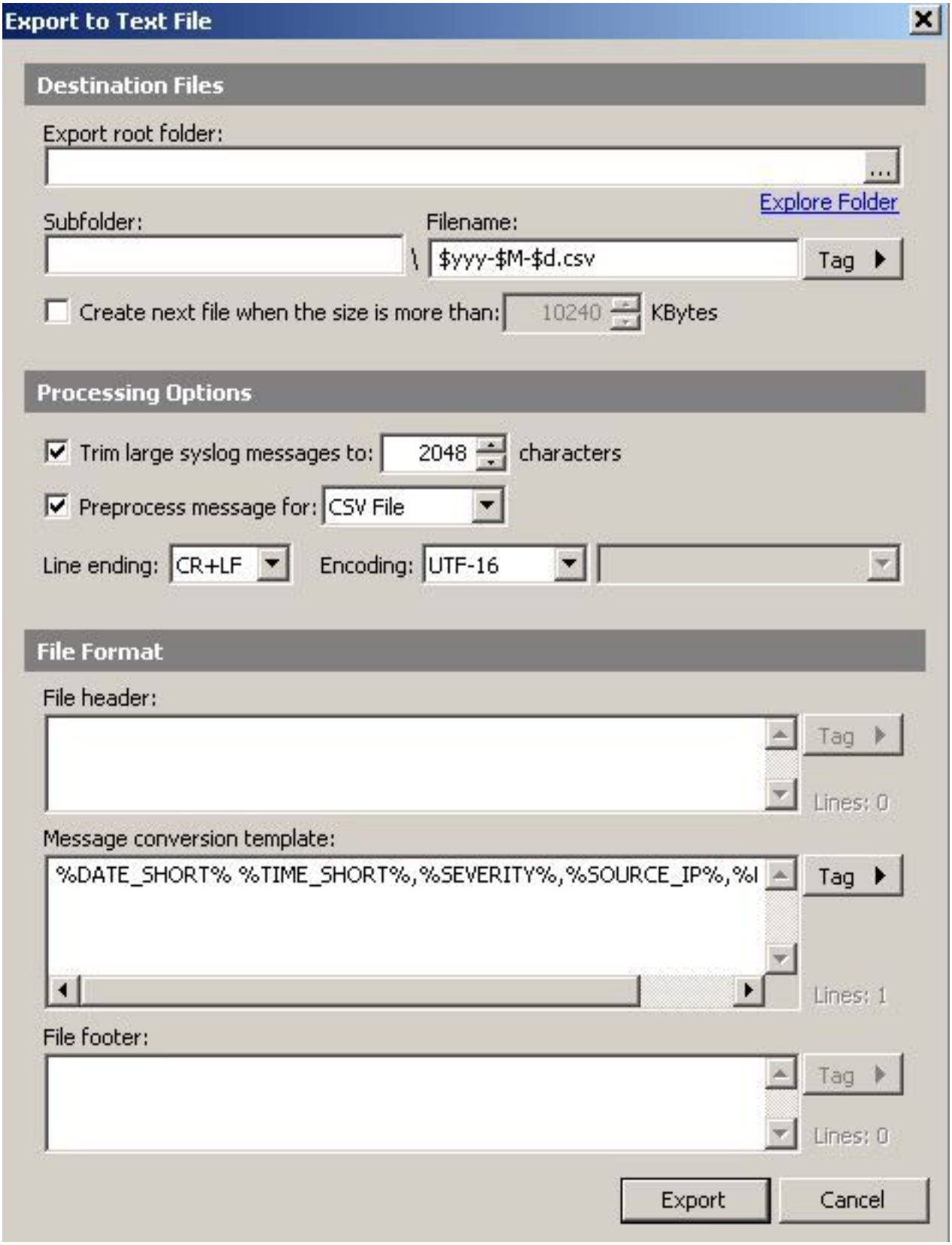
Exporting stored messages to a CSV file

On the SysLog Watcher GUI, click in the Export button on the tool bar, which brings up the screen, as shown in the image.



You can select to export messages during a specific period of interest or export only a particular selection. In the above screen, it is selected to export messages that occurred during a period.

Under Destination, select the Custom text file and click **Next**.

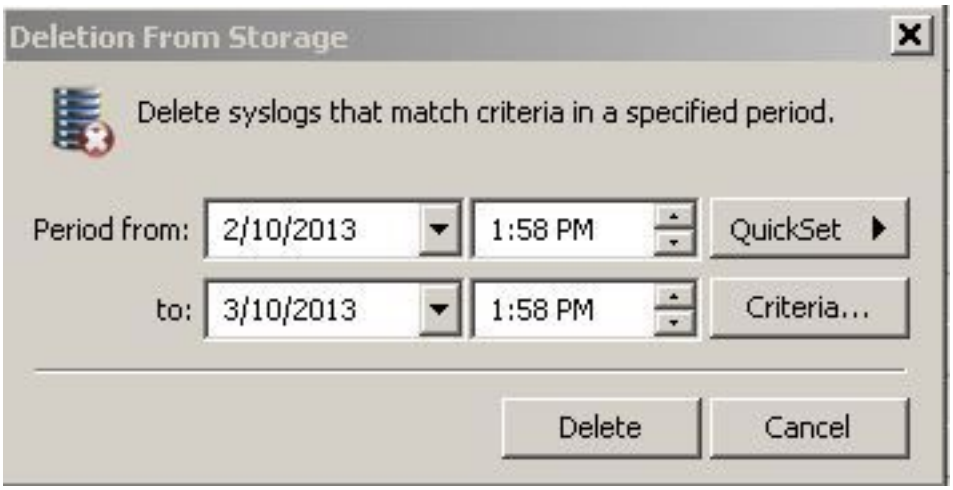


Select a Destination folder, add a Subfolder and give a file name with .csv extension. If the Subfolder does not exist, it is created.

Click in **Export**.

Deleting old messages

On Syslog Watcher GUI, click **Delete** on the tool bar, which brings up the screen, as shown in the image:



Define the period for which you would like to delete the messages and click in **Delete**. You may also, use the QuickSet button to quickly select predefined periods like last one day or one week etc.