Configure a un servidor de Syslog para capturar los registros de las D98xx Series IRDs

Contenido

Introducción

Este documento describe cómo configurar a un servidor de Syslog para capturar los registros de los receptores/de los decodificadores integrados las D98xx Series (IRDs).

Antecedentes

Software Release 4.0 de D9854, D9858 y D9824, y cualquier versión de los **mensajes de Syslog** obedientes del RFC-3164 del soporte D9859. Los clientes pueden ahora capturar los mensajes con un servidor de Syslog para el almacenamiento y la extracción. Además, este procedimiento se puede también utilizar con el nuevo receptor del transporte de la red D9800.

El vigilante del Syslog es el **servidor de Syslog** libre soportado para las máquinas de Windows. Para las máquinas de Linux, el **servidor de Syslog** soportado es el Syslog-**NG** que es disponible desde HTTP: /www.balabit.com/network-security/syslog-ng/opensource-logging-system

Este artículo se ocupa solamente de configurar en las máquinas de Windows.

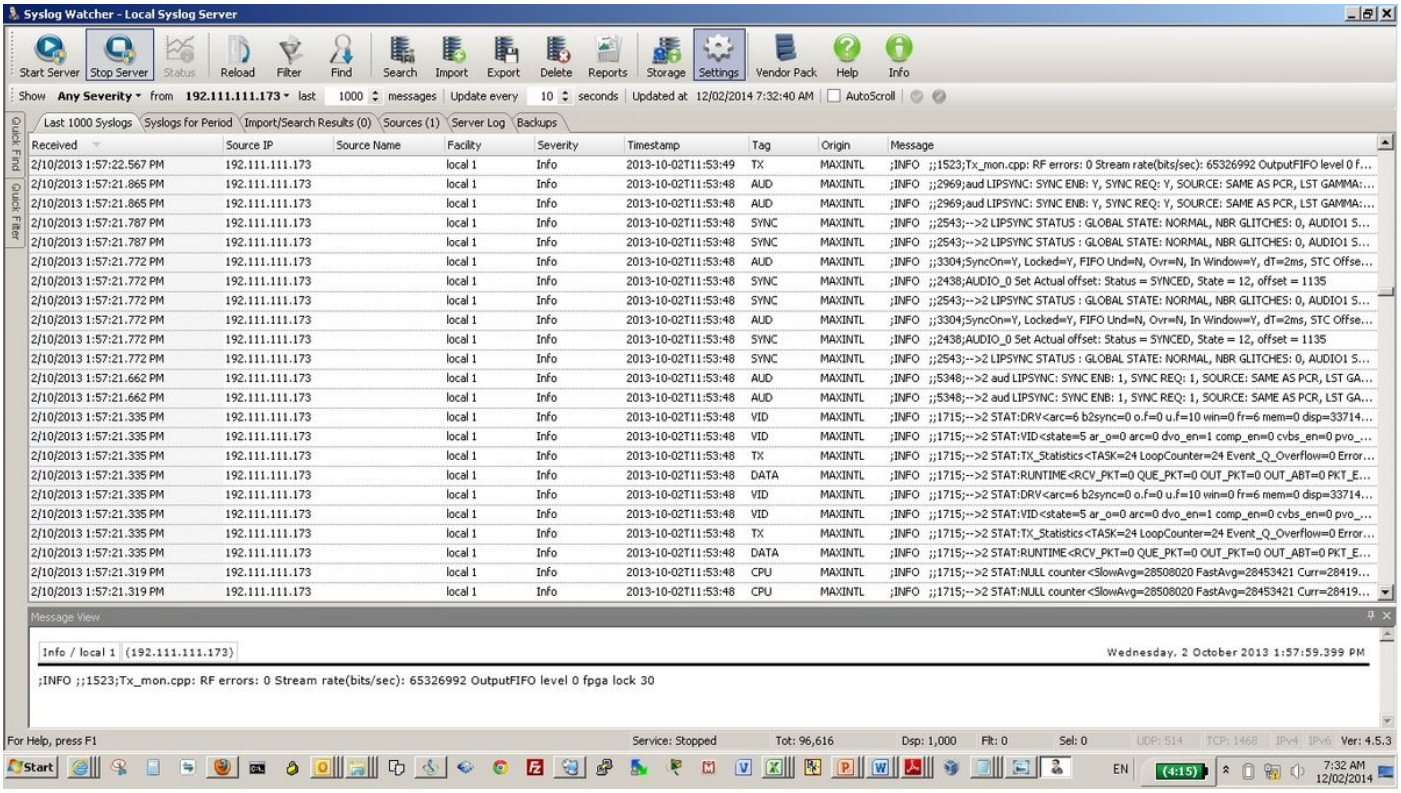
Configure al servidor de Syslog

Descargue al **vigilante del Syslog** de

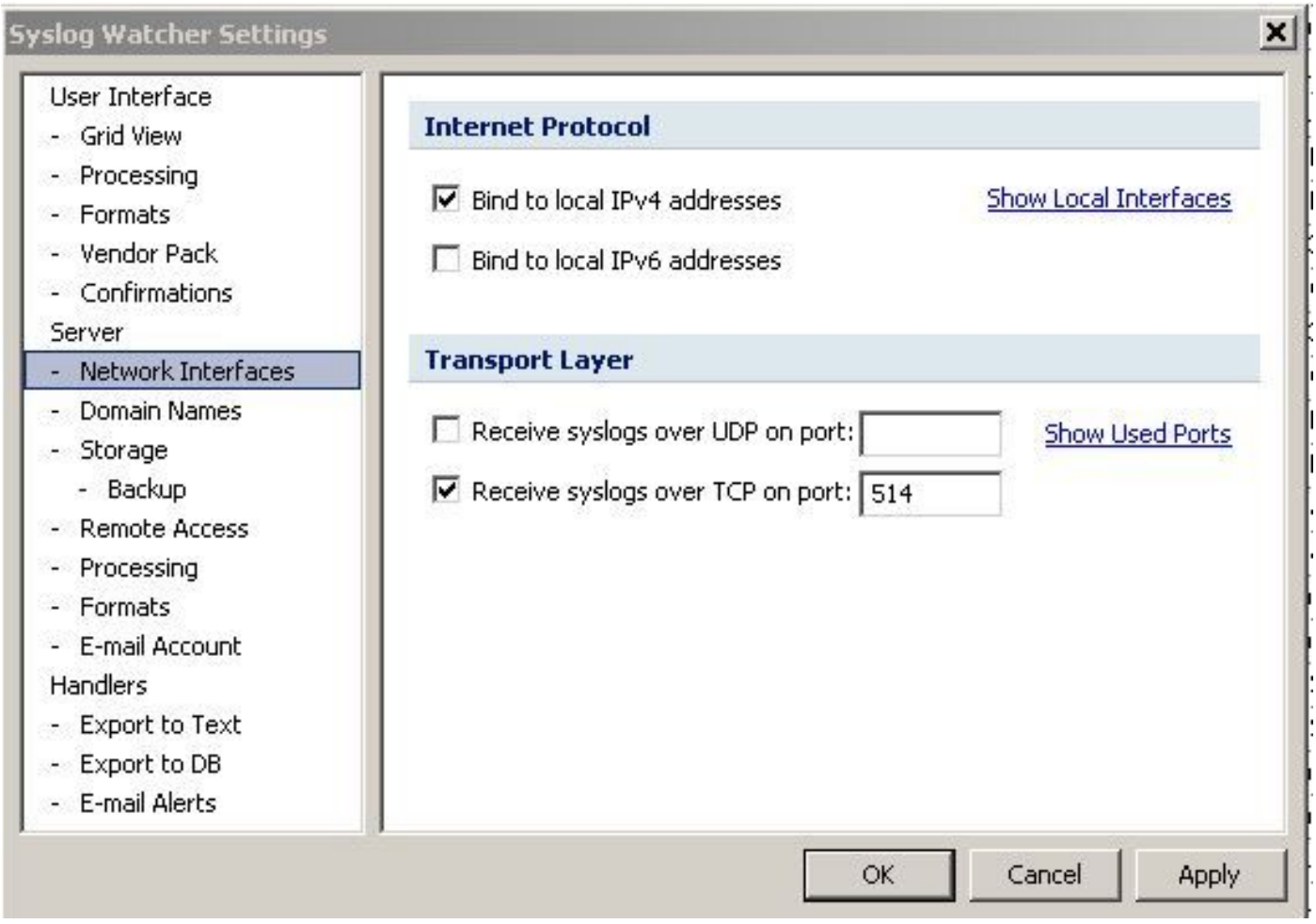
HTTP: /www.snmpsoft.com/syslogwatcher/syslog-server.html

y instalelo en su computador con Windows.

Comience al vigilante del Syslog y seleccione al modo de operación para el GUI como **manejan servidor de Syslog local**, la imagen mostrada aparece:

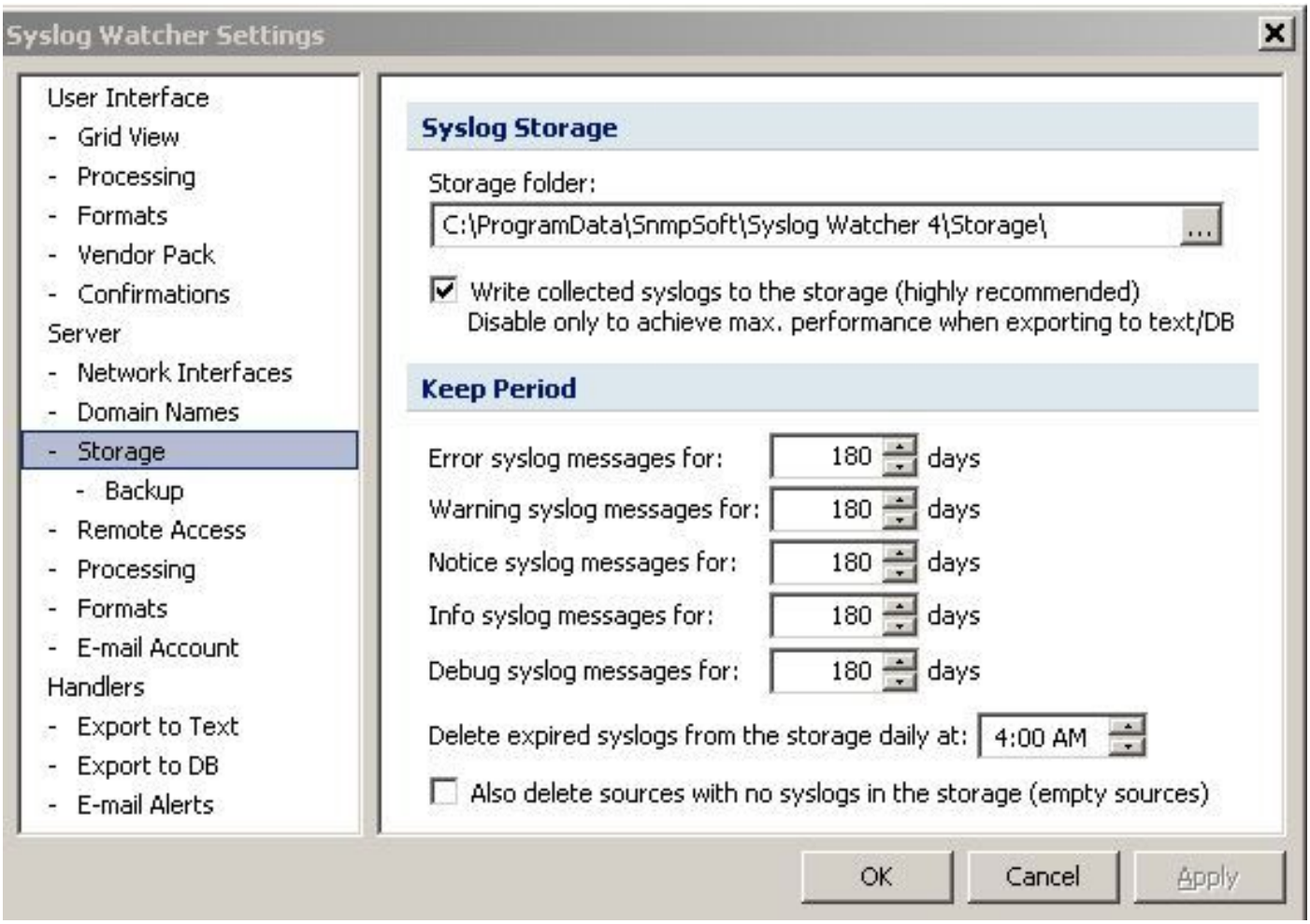


Haga clic en las **configuraciones** (resaltadas en la ilustración superior) en la barra de herramienta, la imagen mostrada aparece:



Seleccione las **interfaces de la red**. Marque el rectángulo **reciben los** Syslog **sobre el UDP en el puerto** y ingresan un número del puerto. El número del mismo puerto necesita ser configurado en los dispositivos de donde el vigilante del Syslog necesita recibir los registros.

Ahora seleccione el **almacenamiento** bajo **configuraciones del vigilante del Syslog**, tal y como se muestra en de la imagen:

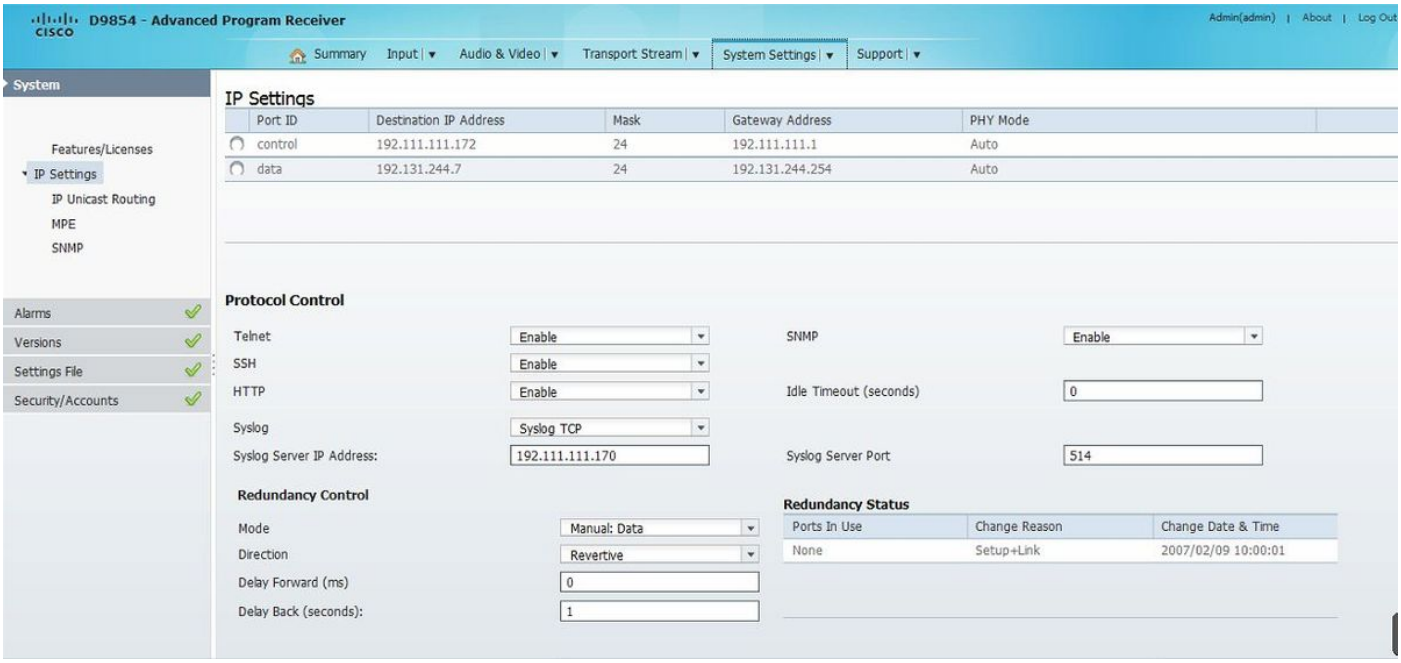


Especifique una ubicación de la carpeta para salvar los mensajes, marque los Syslog **recogidos Write del** cuadro al **almacenamiento**.

Especifique el número de días para que cada tipo de mensaje sea mantenido el almacenamiento.

Configure el IRD (D9854/D9858/D9859) para enviar los registros al vigilante del Syslog

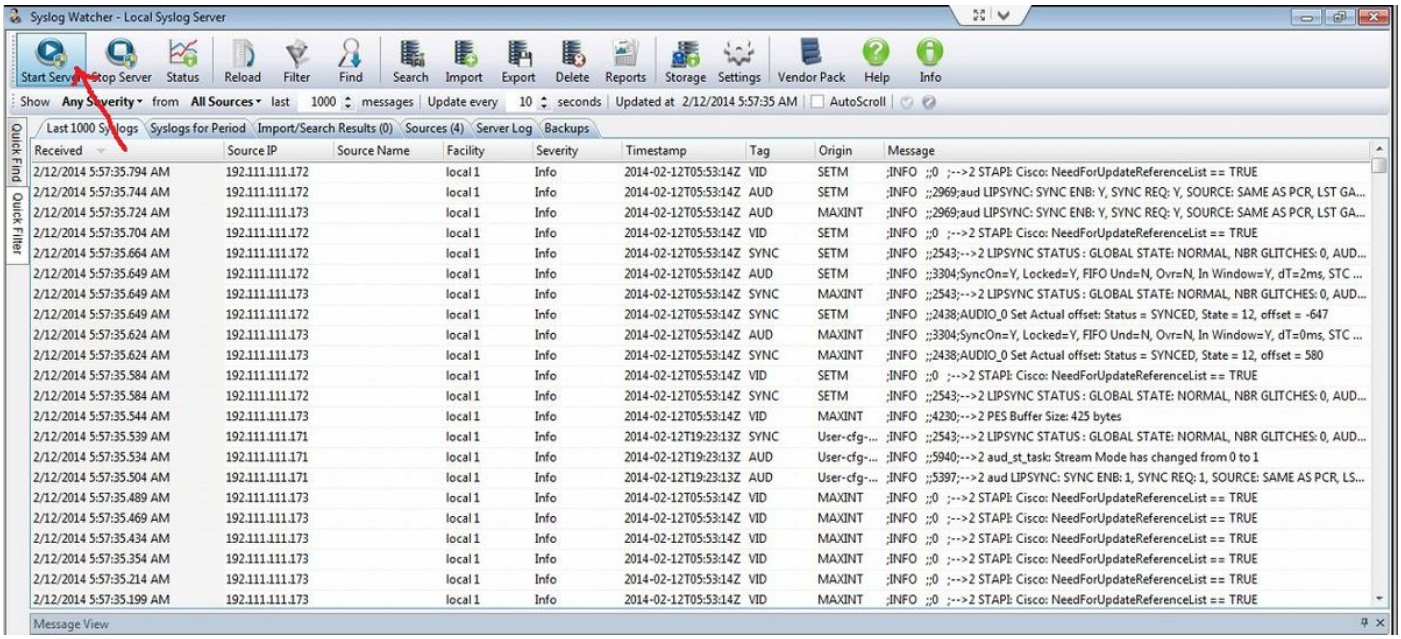
En el IRD GUI, seleccione las **configuraciones IP de las configuraciones del sistema de la** barra de herramienta. La imagen mostrada aparece:



En la sección de **control del protocolo de la** página Configuración IP, configure éstos:

- **Syslog** seleccione el Syslog TCP o el Syslog UDP como sea necesario.
- **El direccionamiento IP del servidor de Syslog** ingresa el IP Address del ordenador donde el vigilante del Syslog está instalado.
- **El puerto de servidor de Syslog** ingresa un número del puerto. Esto debe corresponder con el número del puerto ingresado en las **configuraciones del vigilante del Syslog**.

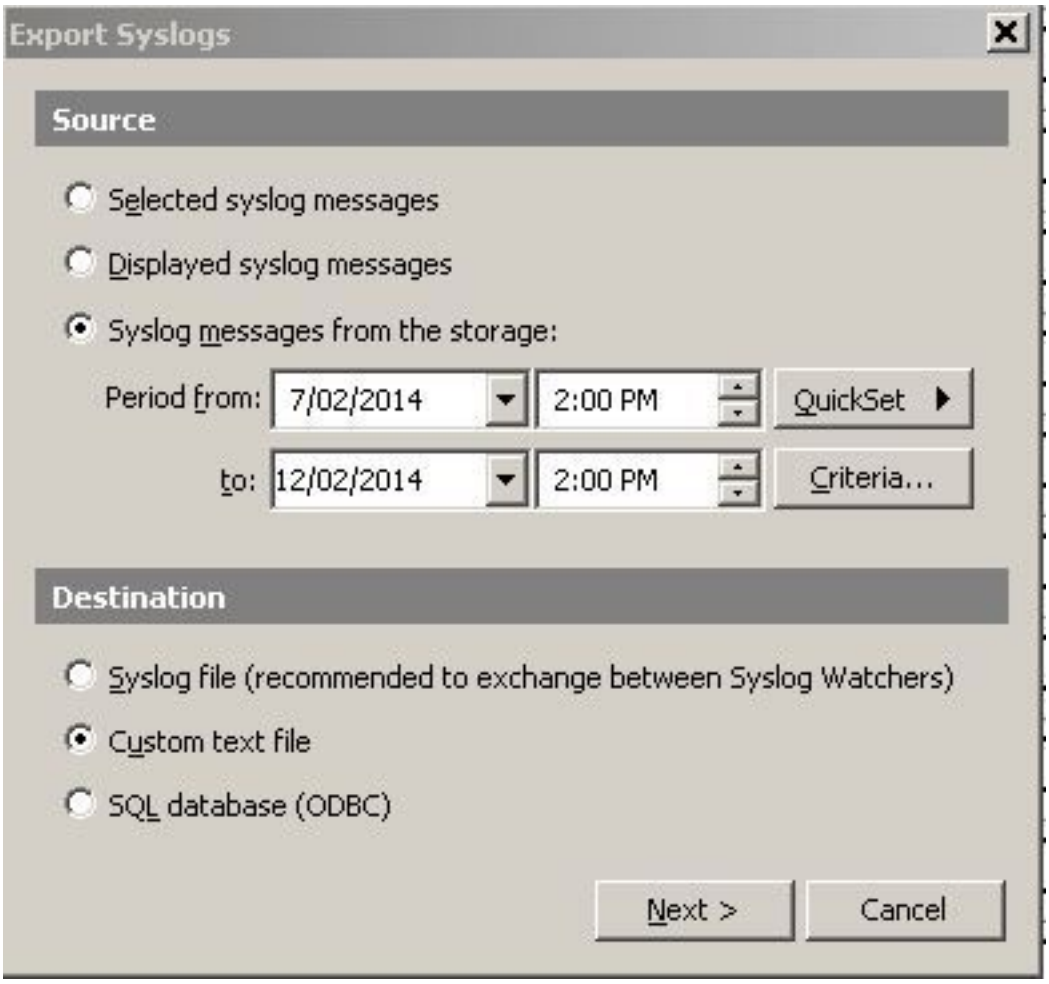
Bajo el vigilante GUI del Syslog, comience el servicio seleccionando el **servidor del comienzo**, tal y como se muestra en de la imagen:



Exportando los mensajes salvados a archivo CSV

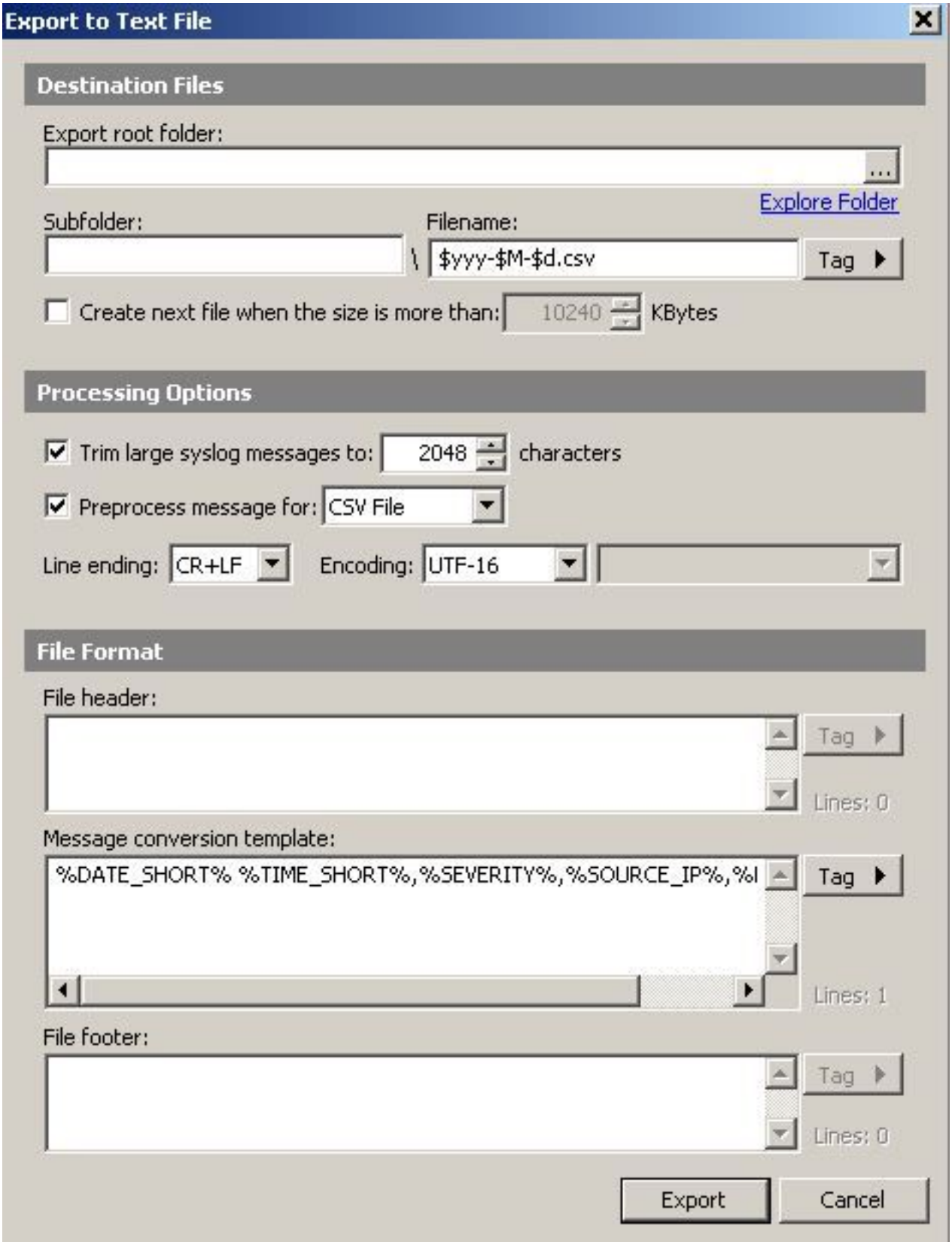
En el vigilante GUI del Syslog, tecleo en el botón de la exportación en la barra de herramienta,

que trae para arriba la pantalla, tal y como se muestra en de la imagen.



Usted puede seleccionar para exportar los mensajes durante un período específico de interés o para exportar solamente una selección determinada. En la pantalla antedicha, se selecciona para exportar los mensajes que ocurrieron durante un período.

Bajo el destino, seleccione el archivo de texto de encargo y haga clic **después**.

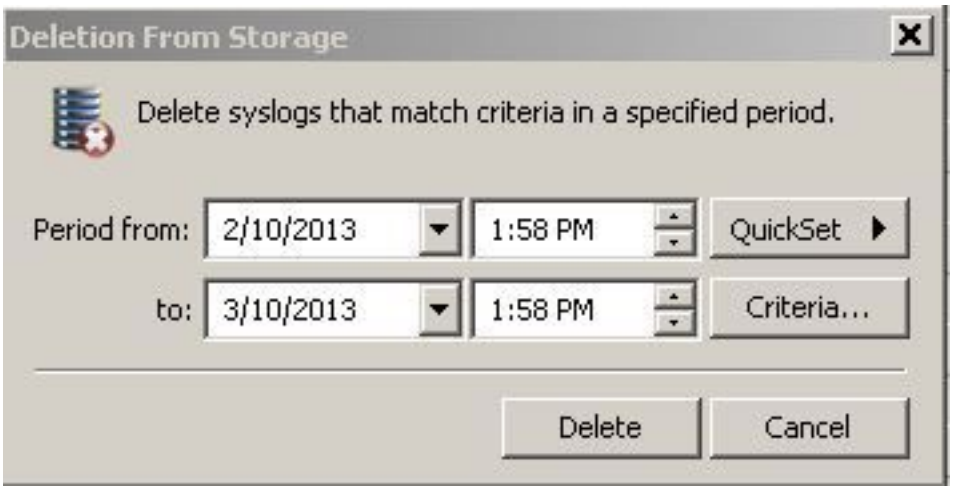


Seleccione una carpeta de destino, agregue un Subfolder y dé un nombre del archivo con la extensión del .csv. Si no existe el Subfolder, se crea.

Tecleo en la **exportación**.

Borrar los viejos mensajes

En el vigilante GUI del Syslog, **cancelación del** tecleo en la barra de herramienta, que trae para arriba la pantalla, tal y como se muestra en de la imagen:



Defina el período para el cual usted quisiera borrar los mensajes y hacer clic en la **cancelación**. Usted puede también, utilizar el botón de solidificación rápida para seleccionar rápidamente los períodos predefinidos como el último un día o una semana etc.