Установите Сервер системного журнала для Получения Журналов от серии D98xx IRDs

Содержание

Введение

Этот документ описывает, как установить Сервер системного журнала для получения журналов от серии D98xx Интегрированные Приемники/Декодеры (IRDs).

Общие сведения

Выпуск ПО 4.0 из D9854, D9858 и D9824 и любого выпуска D9859 поддерживает RFC 3164 совместимые **сообщения системного журнала**. Клиенты могут теперь перехватить сообщения с Сервером системного журнала для хранилища и извлечения. Кроме того, эта процедура может также использоваться с новым Сетевым Транспортным Получателем D9800.

Наблюдатель системного журнала является поддерживаемым свободным **сервером системного журнала** для машин Windows. Для машин Linux поддерживаемый **сервер системного журнала** является **наногра**ммом системного журнала, который доступен от http://www.balabit.com/network-security/syslog-ng/opensource-logging-system

Эта статья имеет дело только с устанавливанием на машинах Windows.

Настройте сервер системного журнала

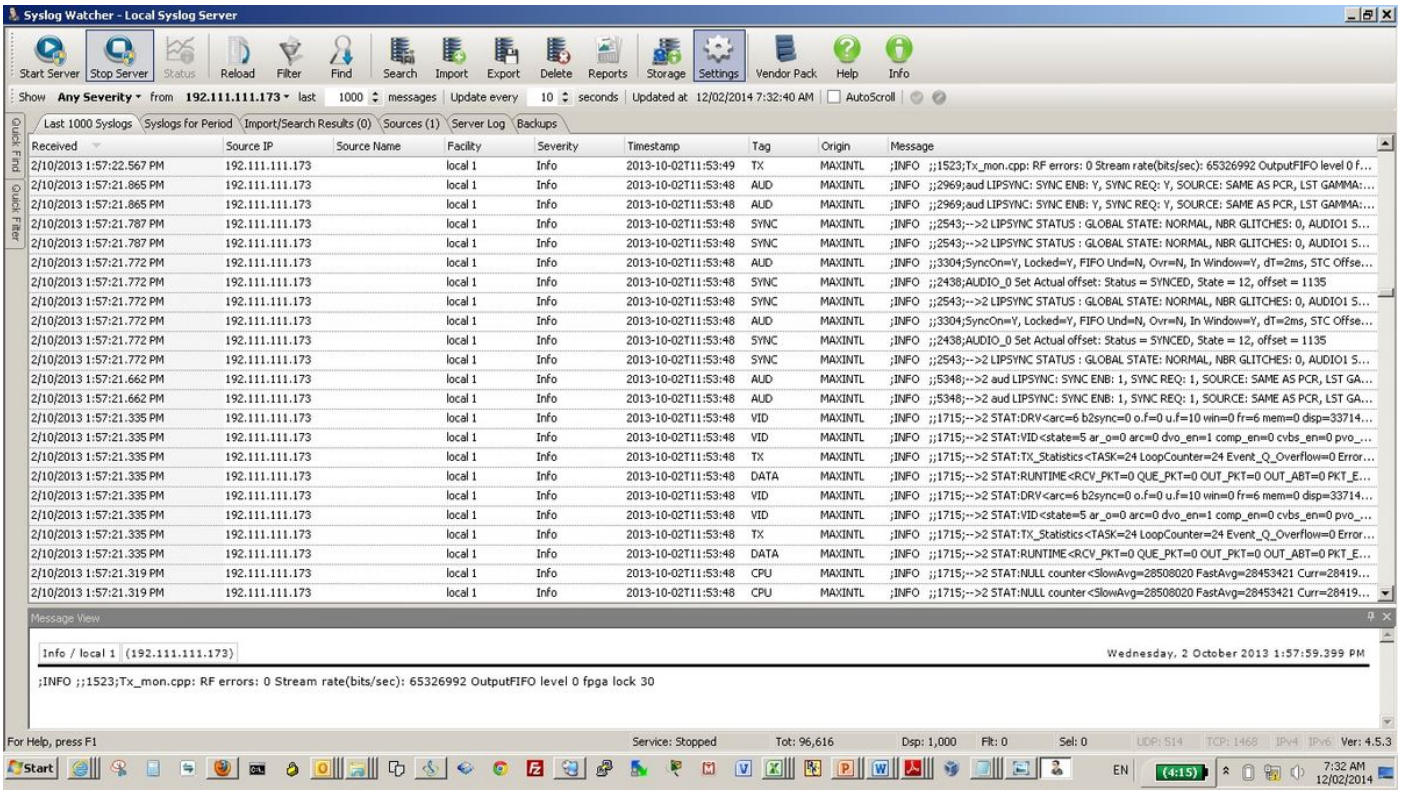
Загрузите **наблюдателя SysLog** от

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

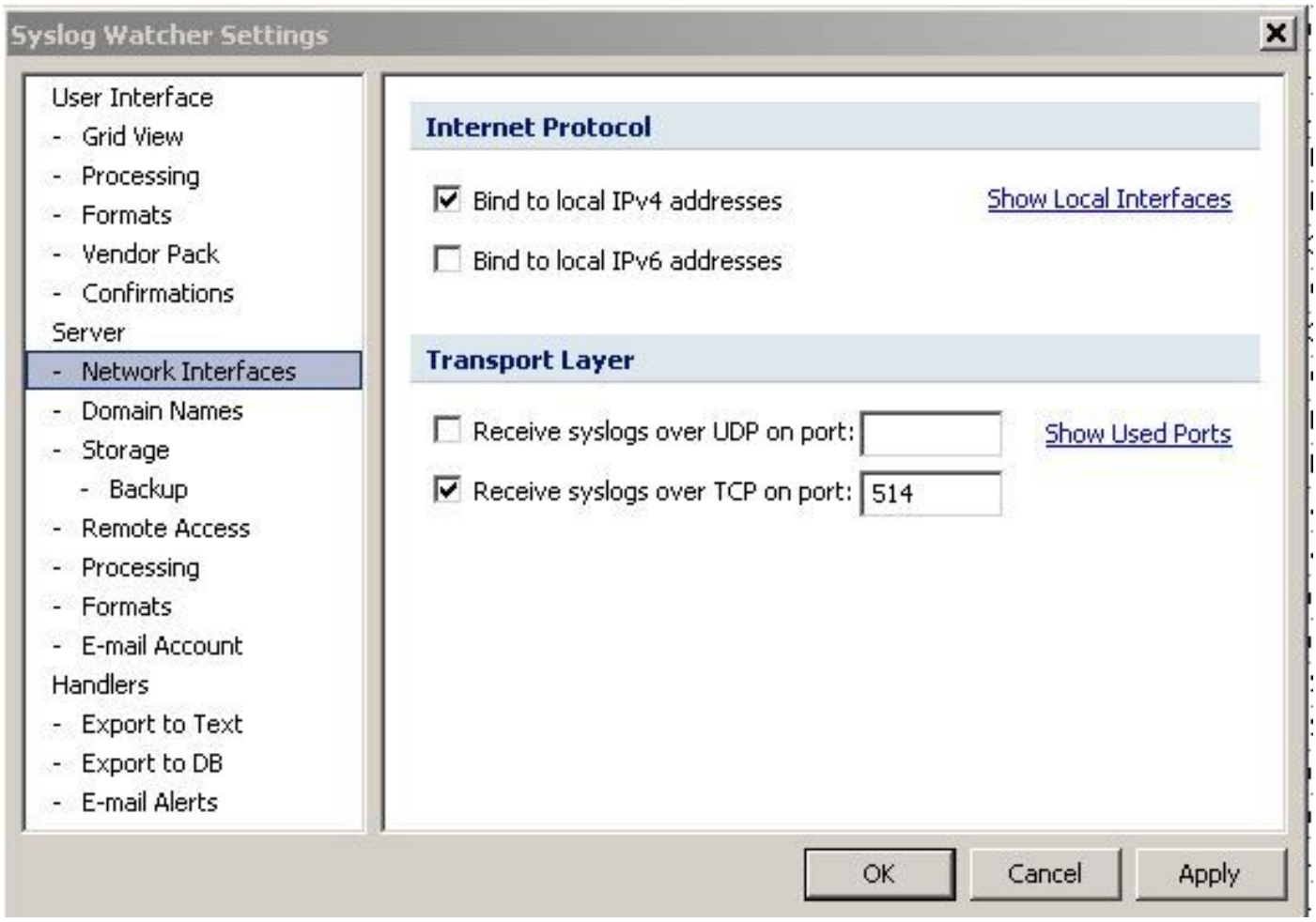
и установите его в своем компьютере под управлением Windows.

Запустите Наблюдателя SysLog и выберите Рабочий режим для GUI, как **Управляют**

Локальным Сервером системного журнала, показанный образ появляется:



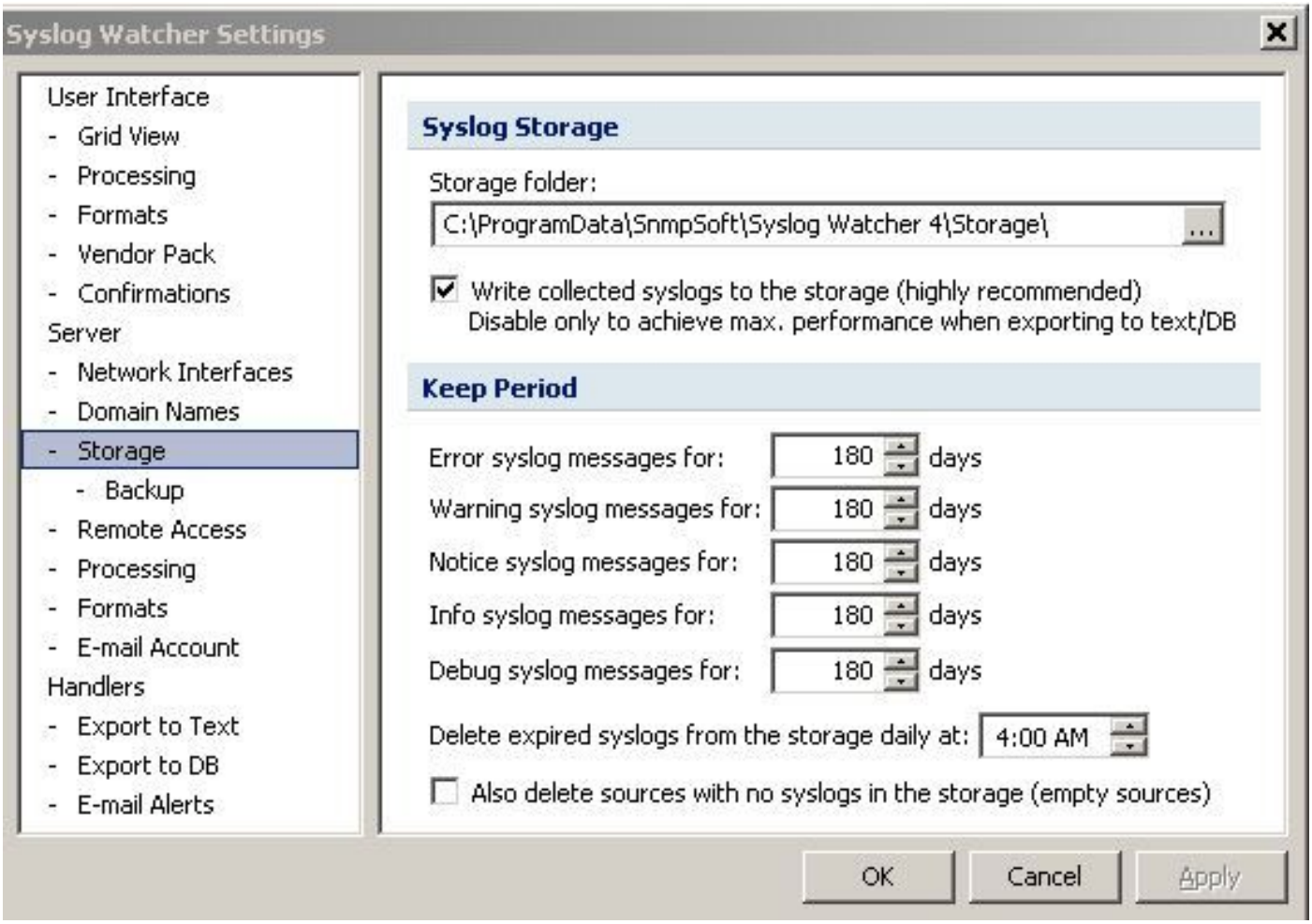
Нажмите в **Параметрах настройки** (выделенный в вышеупомянутом изображении) в строке инструментов, показанный образ появляется:



Выберите **Network Interfaces**. Установите флажок**, Получают** системные журналы **по UDP на**

порту и вводят номер порта. Номер того же порта должен быть настроен на устройствах от того, где Наблюдатель SysLog должен получить журналы.

Теперь выберите **Storage** при **Параметрах настройки Наблюдателя SysLog**, как показано в образе:

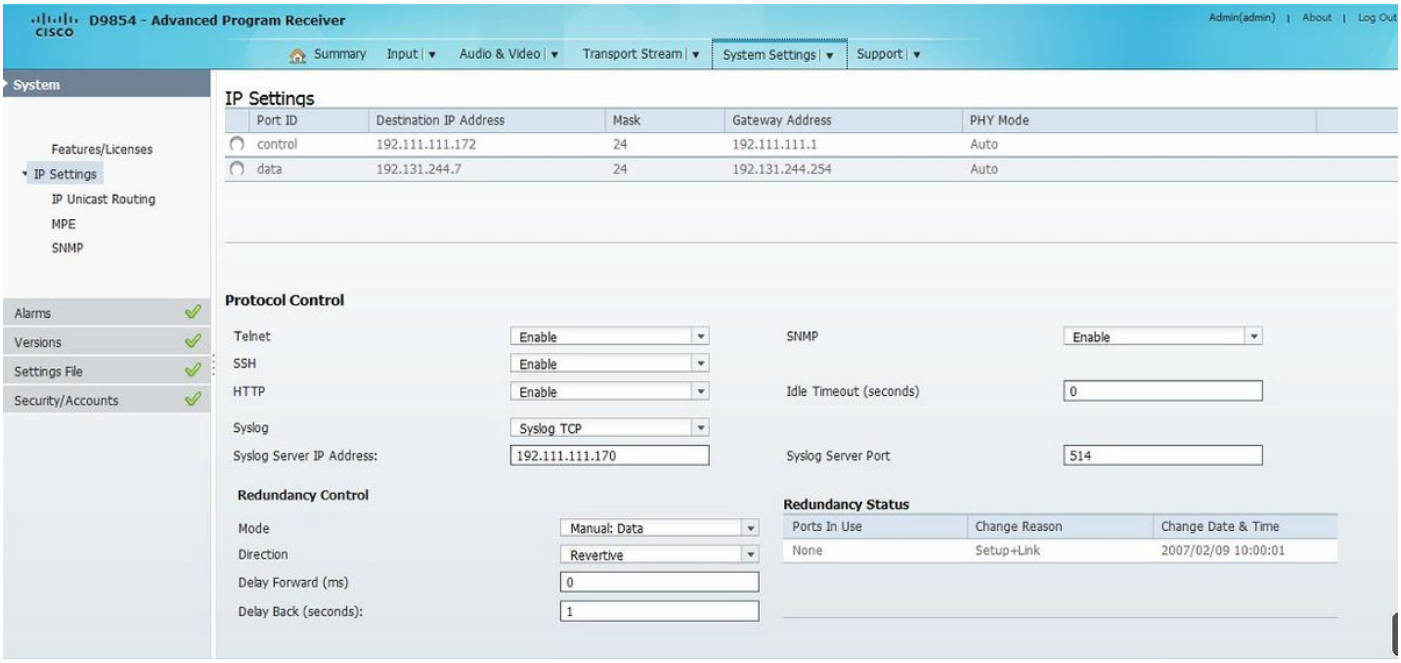


Задайте расположение папки для того, чтобы хранить сообщения, проверьте**, что Запись** коробки **собрала** системные журналы **к хранилищу**.

Задайте число дней для каждого типа сообщения, который будет сохранен в хранилище.

Настройте IRD (D9854/D9858/D9859), чтобы передать журналы Наблюдателю Системного журнала

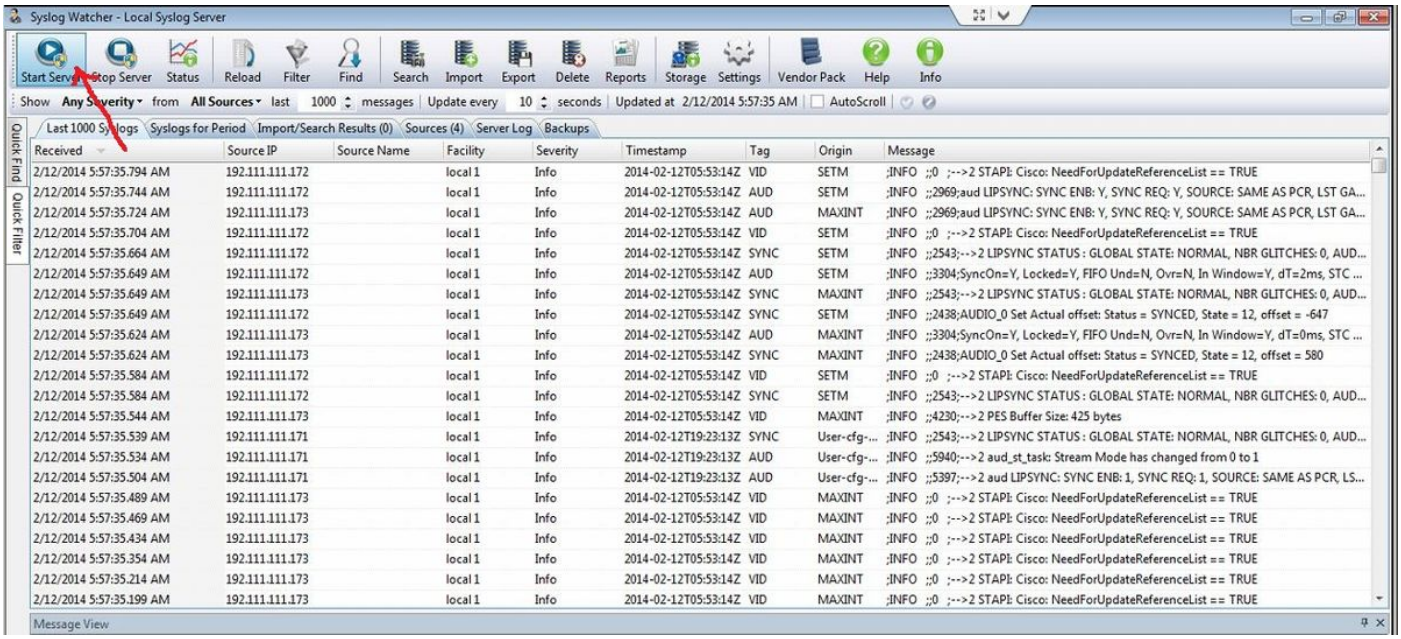
На GUI IRD выберите **System Settings / Параметры настройки IP** от строки инструментов. Показанный образ появляется:



В разделе **Контроля протокола** Страницы настроек IP настройте их:

- **Системный журнал** - Выбирает Syslog TCP или Syslog UDP как требуется.
- **IP-адрес Сервера системного журнала** - Вводит IP-адрес компьютера, где установлен Наблюдатель SysLog.
- **Порт Сервера системного журнала** - Вводит номер порта. Это должно совпасть с номером порта, введенным в **Параметры настройки Наблюдателя Системного журнала**.

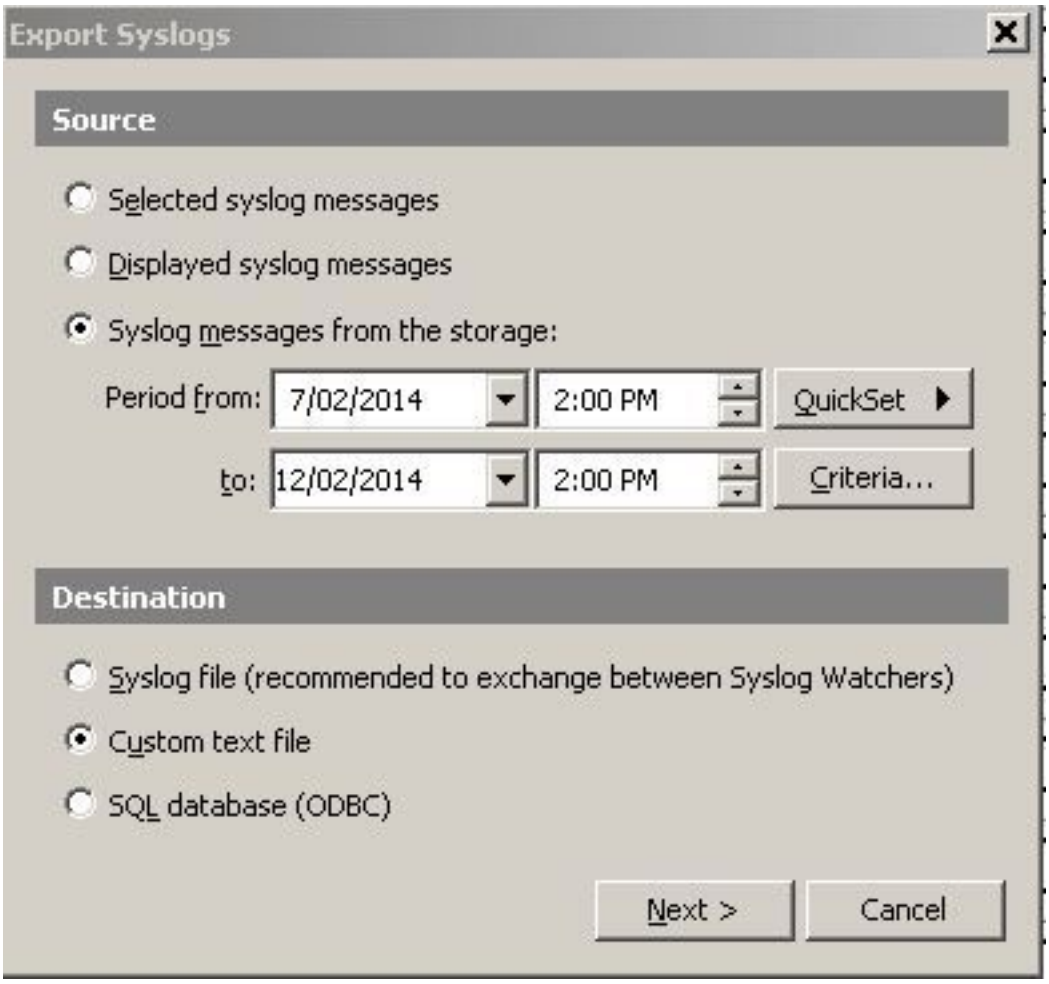
Под GUI Наблюдателя Системного журнала запустите сервис путем выбора **Start Server**, как показано в образе:



Экспортирование хранивших сообщений к Файлу csv

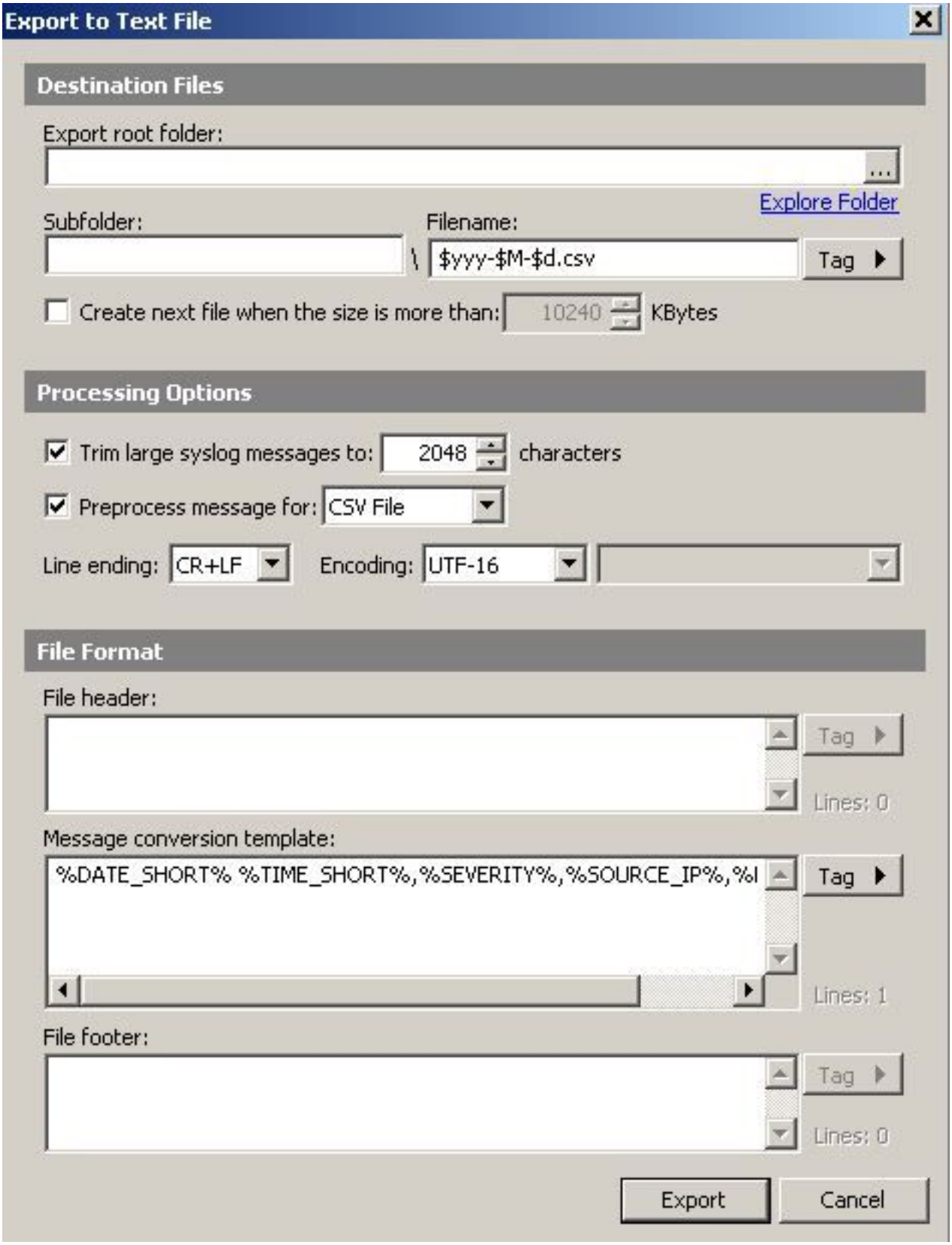
На GUI Наблюдателя SysLog нажмите в кнопке Export на строку инструментов, которая

переводит экран в рабочее состояние, как показано в образе.



Можно выбрать, чтобы экспортировать сообщения в течение определенного периода интереса или экспортировать только определенный выбор. На вышеупомянутом экране это выбрано для экспортирования сообщений, которые произошли в течение периода.

При Назначении выберите файл Пользовательского текста и нажмите **Next**.

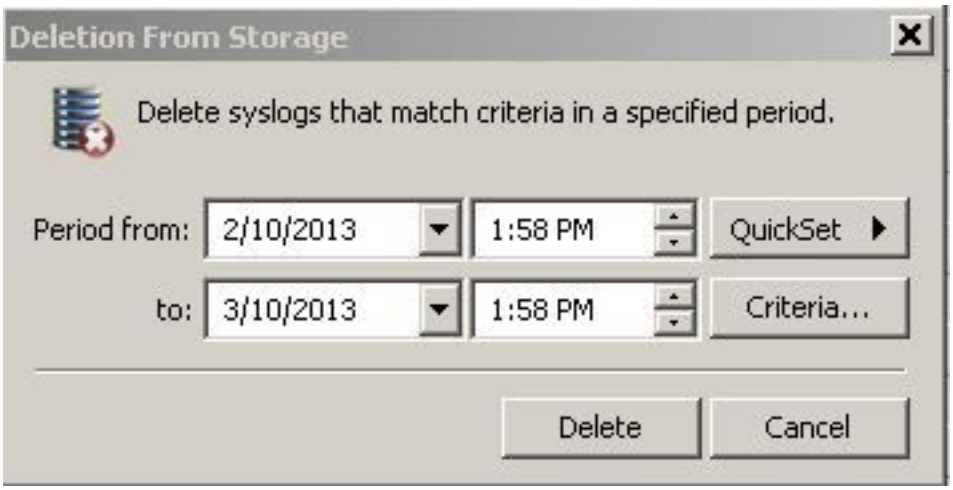


Выберите Нужную папку, добавьте Подпапку и дайте имя файла с расширением .csv. Если Подпапка не существует, она создана.

Нажмите в **экспорте**.

Удаление старых сообщений

На GUI Наблюдателя Системного журнала нажмите **Delete** на строке инструментов, которая переводит экран в рабочее состояние, как показано в образе:



Определите период, в течение которого требуется удалить сообщения, и щелчок в **Удаляют**. Вы можете также, использовать кнопку QuickSet для быстрого выбора предопределенных периодов как в последний раз один день или одна неделя и т.д.