Estabelecer um servidor de SYSLOG para capturar logs do D98xx Series IRDs

Índice

[Introdução](#)
[Informações de Apoio](#)
[Configurar o servidor de SYSLOG](#)
[Configurar o IRD (D9854/D9858/D9859) para enviar logs ao observador do Syslog](#)
[Exportando mensagens armazenadas para um arquivo CSV](#)
[Suprimindo de mensagens velhas](#)

Introdução

Este documento descreve como estabelecer um servidor de SYSLOG para capturar logs dos receptores/decodificadores integrados D98xx Series (IRDs).

Informações de Apoio

Software Release 4.0 de D9854, D9858 & D9824, e alguma liberação de **mensagens do syslog** complacentes do RFC-3164 do apoio D9859. Os clientes podem agora capturar as mensagens com um servidor de SYSLOG para o armazenamento e a recuperação. Além, este procedimento pode igualmente ser usado com o receptor novo do transporte da rede D9800.

O observador do Syslog é o **servidor de SYSLOG** livre apoiado para máquinas de Windows. Para máquinas de Linux, o **servidor de SYSLOG** apoiado é o Syslog-**NG** que está disponível do HTTP: /www.balabit.com/network-security/syslog-ng/opensource-logging-system

Este artigo trata somente a fundação em máquinas de Windows.

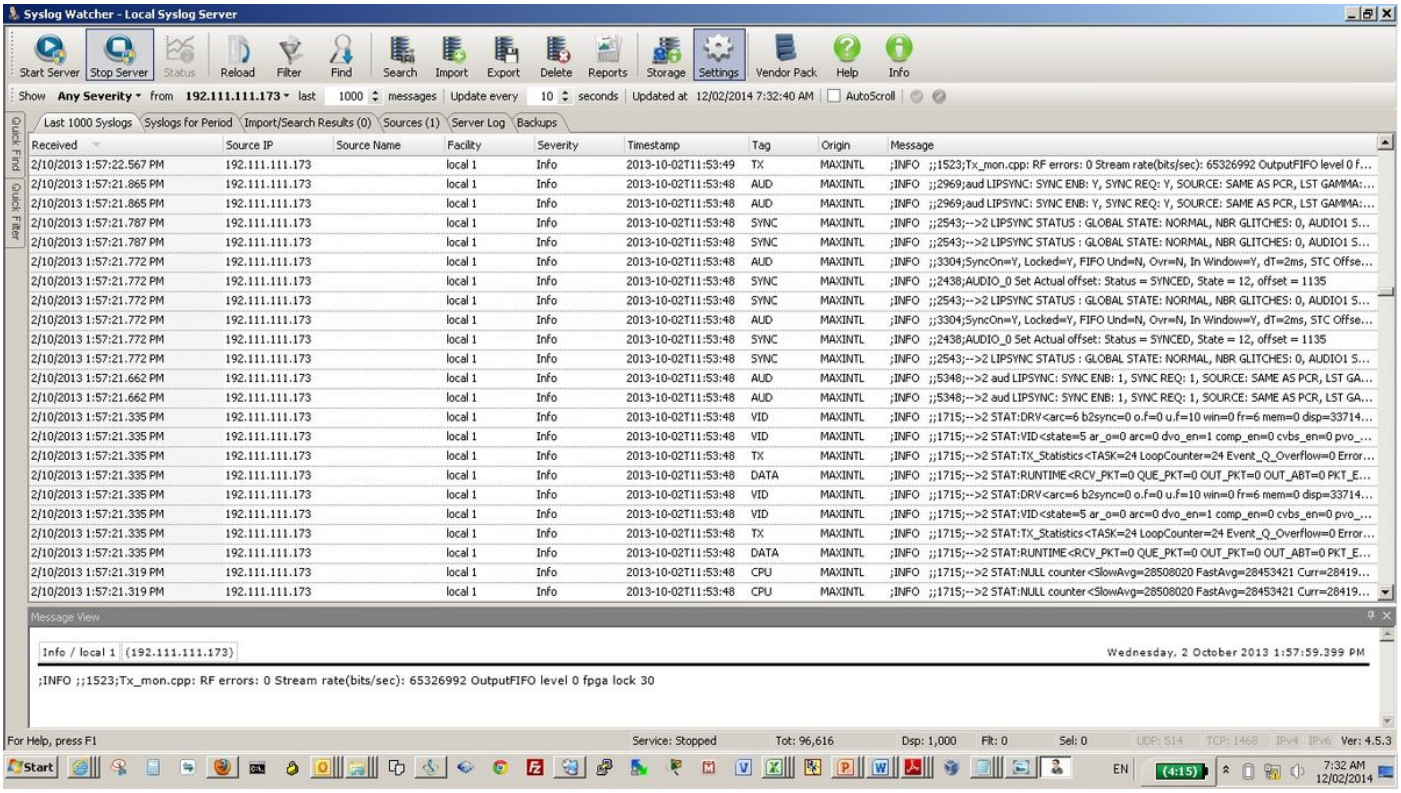
Configurar o servidor de SYSLOG

Transfira o **observador do Syslog** de

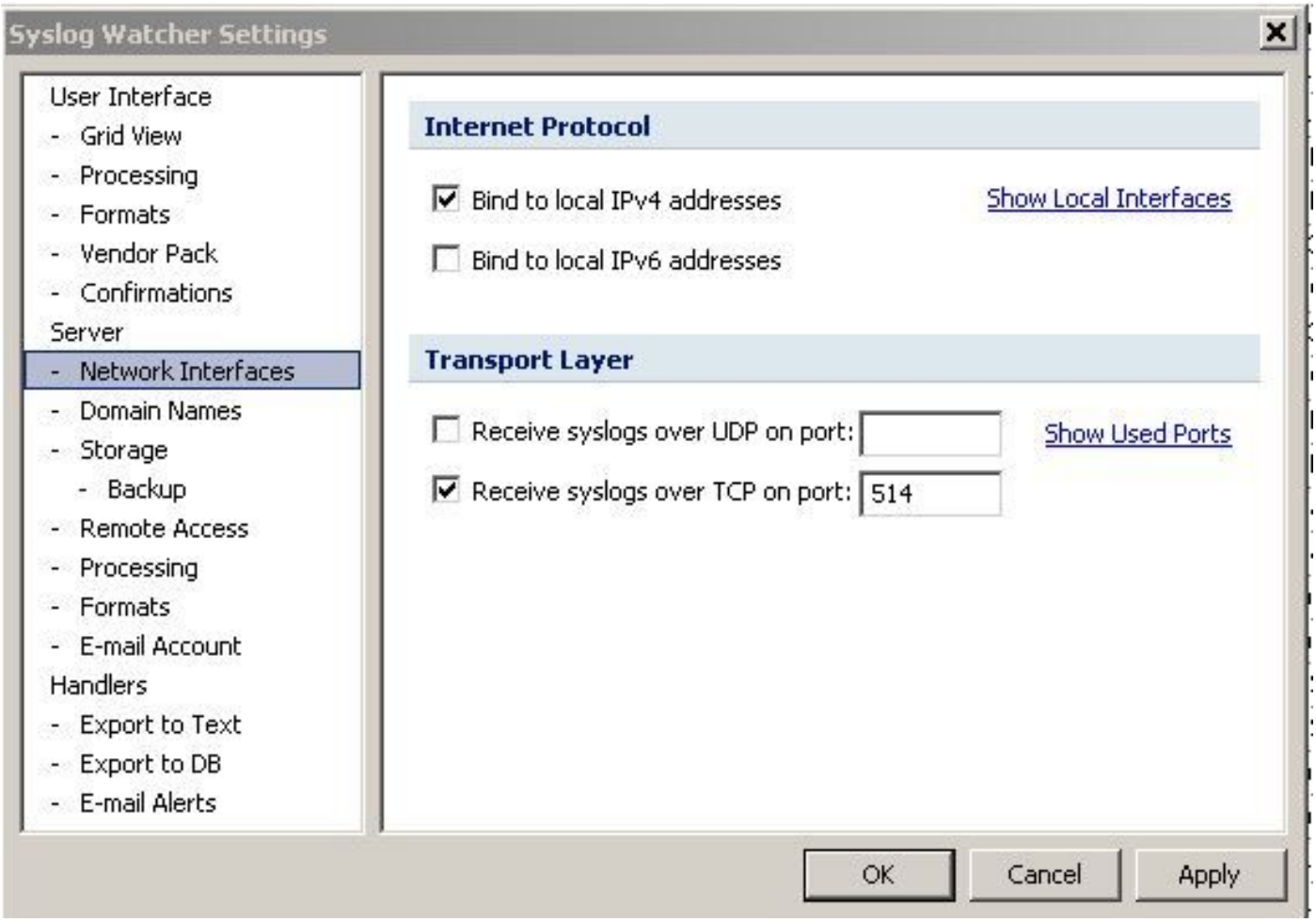
HTTP: /www.snmpsoft.com/syslogwatcher/syslog-server.html

e instale-o em seu computador Windows.

Comece o observador do Syslog e selecione o modo operacional para o GUI como **controlam servidor de SYSLOG local**, a imagem mostrada aparece:

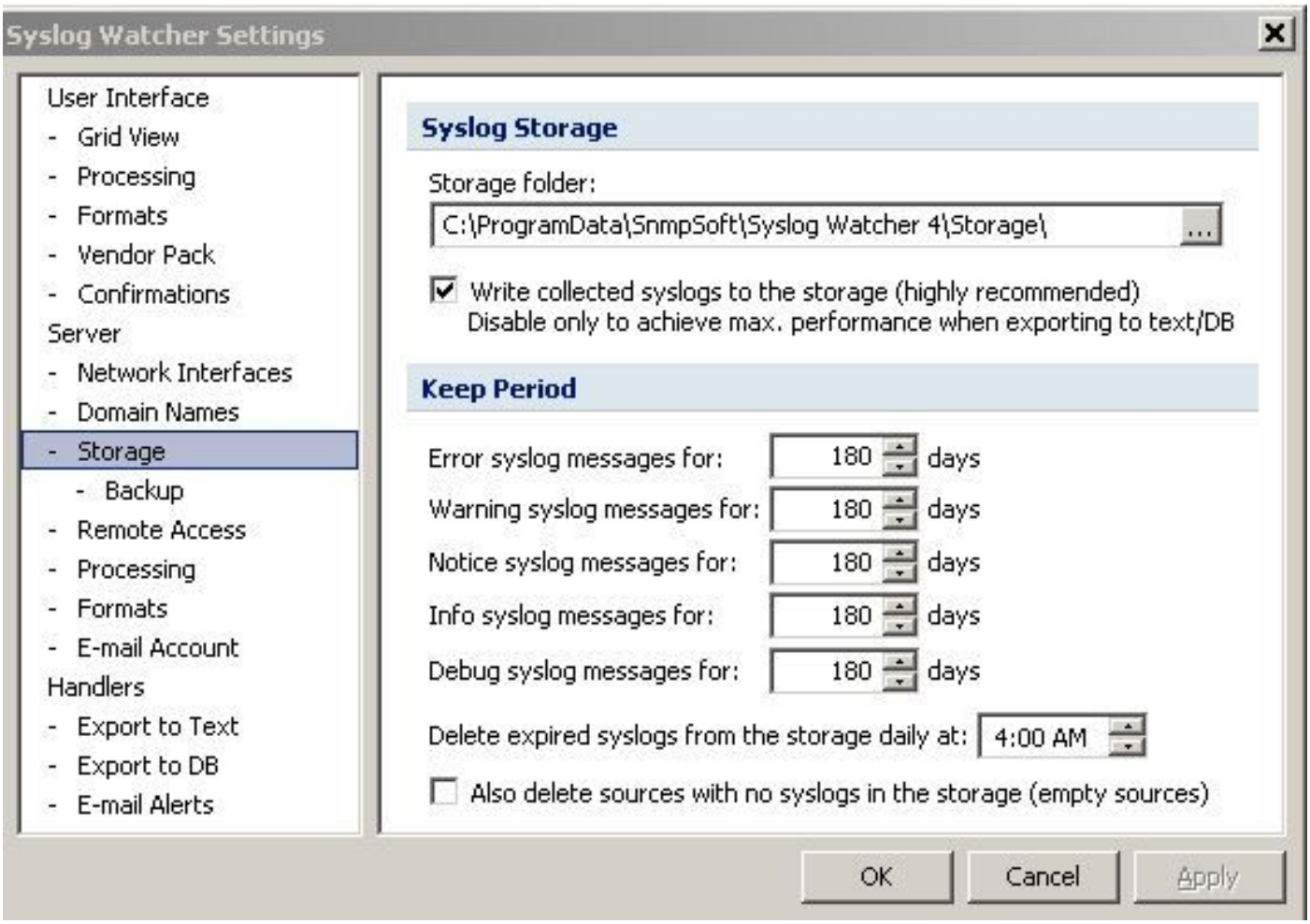


Clique nos **ajustes** (destacados na imagem acima) na barra de ferramentas, a imagem mostrada aparece:



Selecione **interfaces de rede**. Verifique a caixa **recebem** Syslog **sobre o UDP na porta** e entram em um número de porta. O número de mesma porta precisa de ser configurado nos dispositivos de onde o observador do Syslog precisa de receber logs.

Selecione agora o **armazenamento** sob **ajustes do observador do Syslog**, segundo as indicações da imagem:

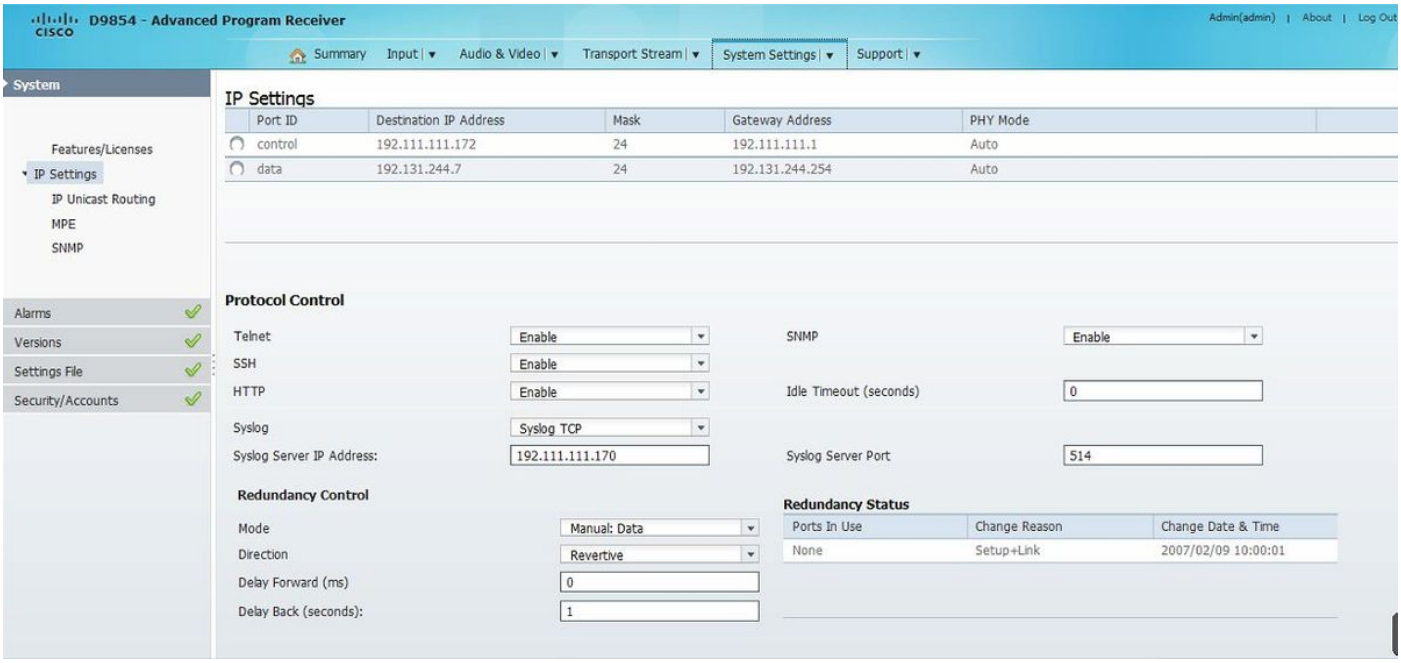


Especifique um local da pasta armazenando as mensagens, verifique os Syslog **recolhidos Write da** caixa ao **armazenamento**.

Especifique o número de dias para que cada tipo de mensagem seja mantido no armazenamento.

Configurar o IRD (D9854/D9858/D9859) para enviar logs ao observador do Syslog

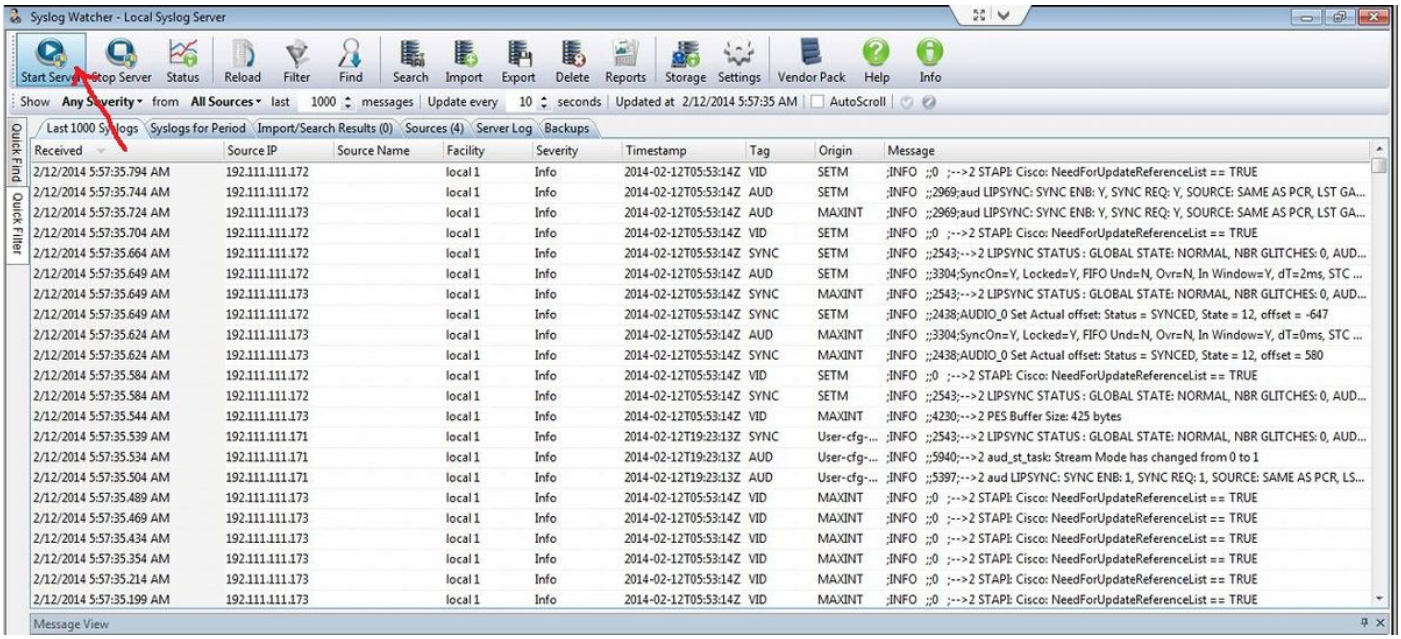
No IRD GUI, selecione os **ajustes IP dos ajustes do sistema da** barra de ferramentas. A imagem mostrada aparece:



Na seção de **controle de protocolo do** IP os ajustes paginam, configuram estes:

- **O Syslog** seleciona o Syslog TCP ou o Syslog UDP como necessário.
- **O endereço IP do servidor de SYSLOG** incorpora o endereço IP de Um ou Mais Servidores Cisco ICM NT do computador onde o observador do Syslog é instalado.
- **A porta de servidor de SYSLOG** entra em um número de porta. Isto deve combinar o número de porta inscrito nos **ajustes do observador do Syslog**.

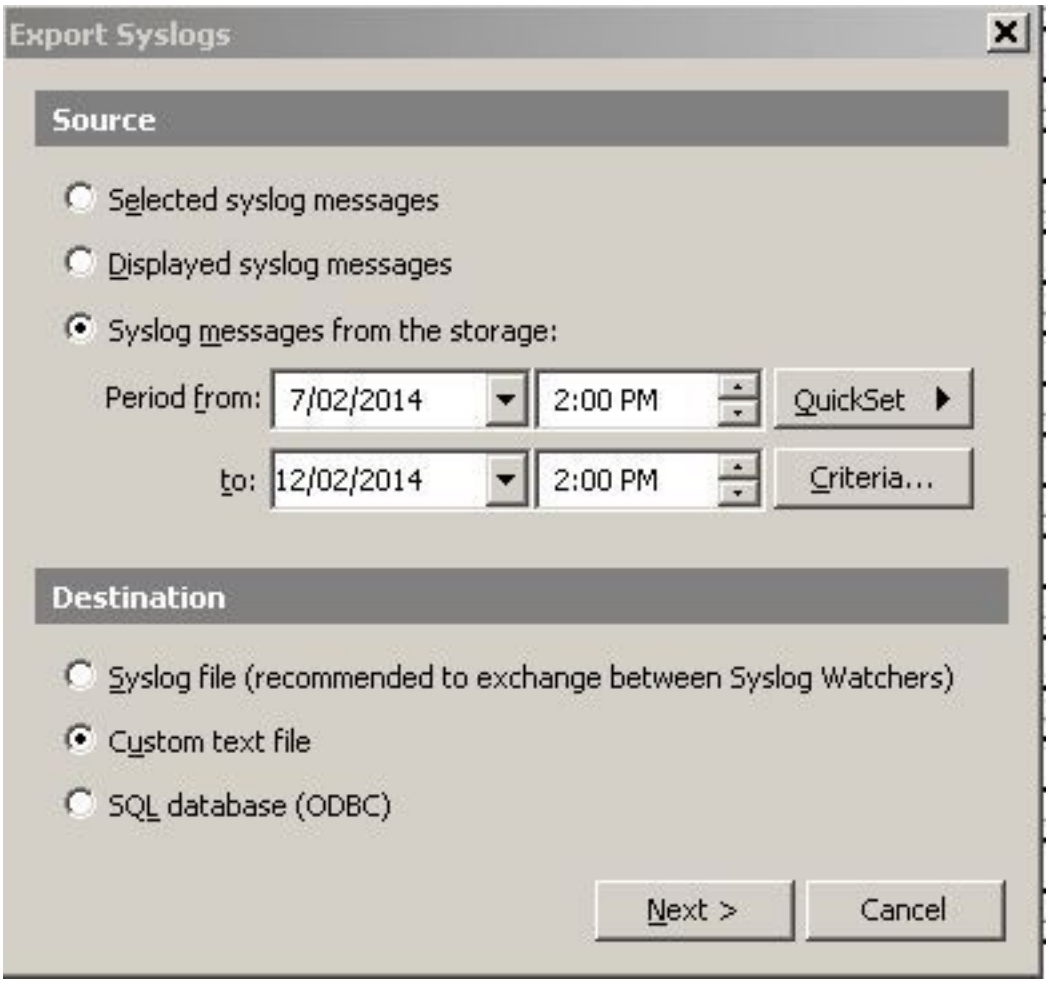
Sob o observador GUI do Syslog, comece o serviço selecionando o **server do começo**, segundo as indicações da imagem:



Exportando mensagens armazenadas para um arquivo CSV

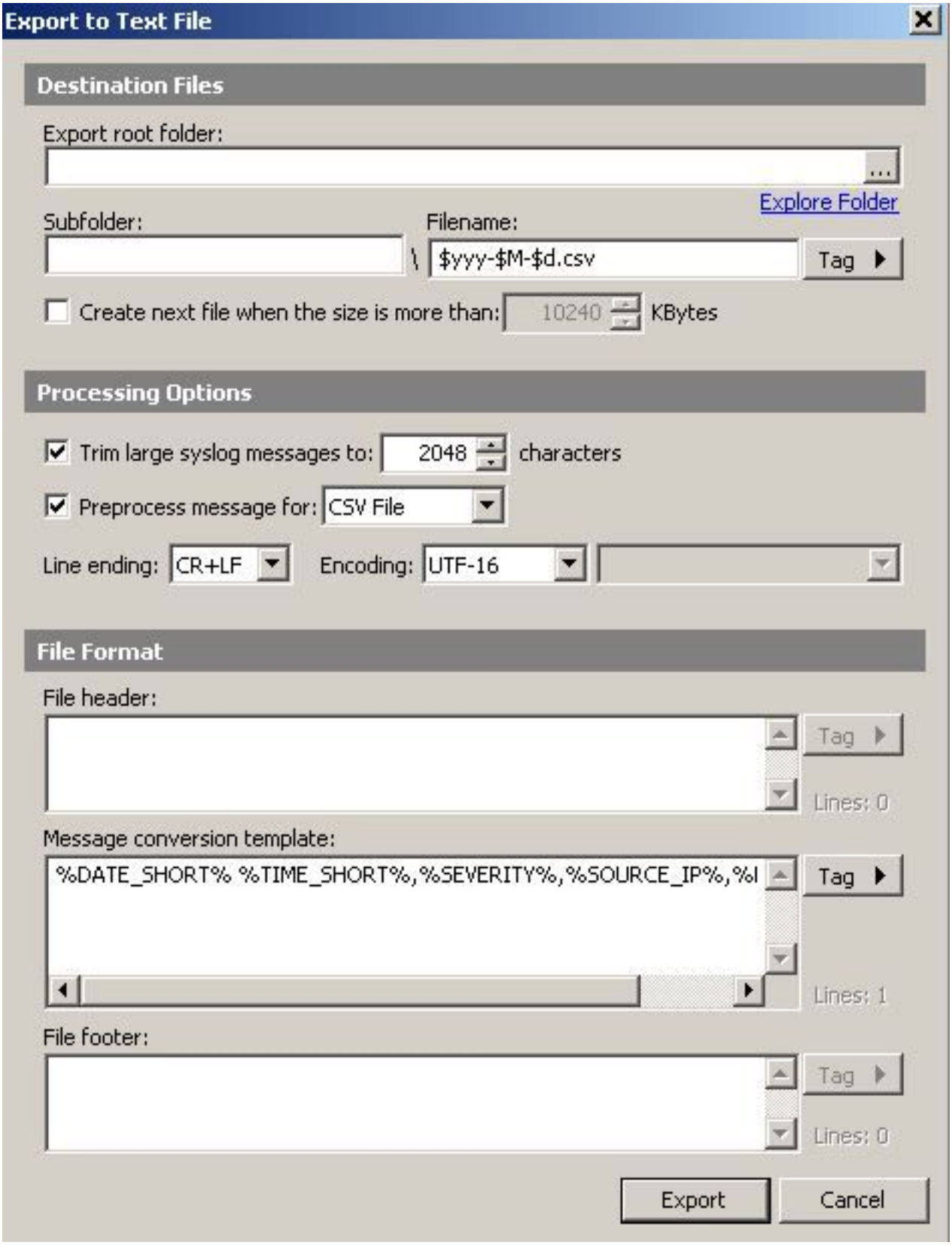
No observador GUI do Syslog, clique no botão da exportação na barra de ferramentas, que traz

acima a tela, segundo as indicações da imagem.



Você pode selecionar para exportar mensagens durante um período específico de interesse ou para exportar somente uma seleção particular. Na tela acima, é selecionada para exportar as mensagens que ocorreram durante um período.

Sob o destino, selecione o arquivo de texto feito sob encomenda e clique-o em seguida.

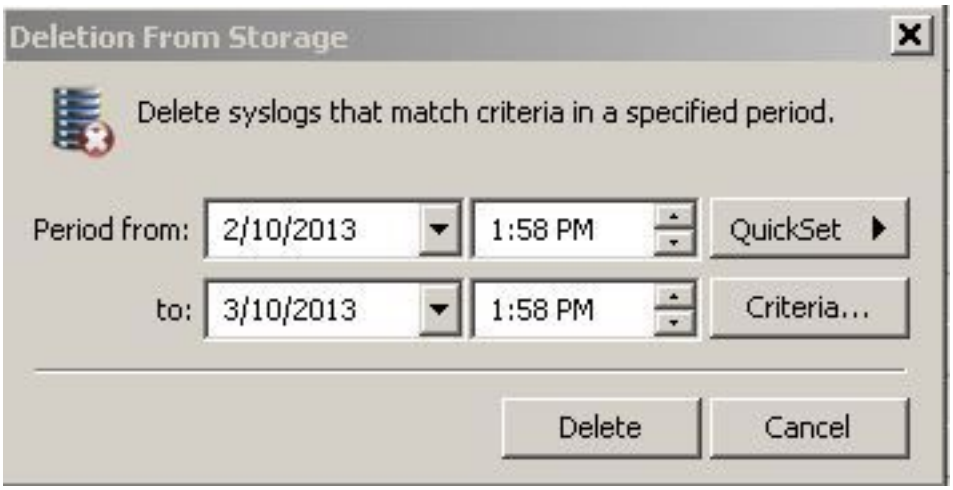


Selecione uma pasta de destino, adicionar uma subpasta e dê um nome de arquivo com extensão .csv. Se a subpasta não existe, está criada.

Clique na **exportação**.

Suprimindo de mensagens velhas

No observador GUI do Syslog, **supressão do** clique na barra de ferramentas, que traz acima a tela, segundo as indicações da imagem:



Defina o período para que você gostaria de suprimir das mensagens e das clicar na **supressão**. Você pode igualmente, para usar o botão do QuickSet para selecionar rapidamente períodos predefinidos como o último um dia ou a uma semana etc.