Installez un serveur de Syslog pour saisir des logs de la gamme D98xx IRDs

Contenu

Introduction

Ce document décrit comment installer un serveur de Syslog pour saisir des logs des récepteurs/des décodeurs intégrés par gamme D98xx (IRDs).

Informations générales

Version de logiciel 4.0 de D9854, D9858 et D9824, et toute version D9859 des messages conformes de **Syslog du** support RFC-3164. Les clients peuvent maintenant capturer les messages avec un serveur de Syslog pour la mémoire et la récupération. En outre, cette procédure peut également être utilisée avec le nouveau récepteur de transport du réseau D9800.

Le watcher de Syslog est le **serveur** libre pris en charge de **Syslog** pour des ordinateurs Windows. Pour des machines Linux, le **serveur** pris en charge de **Syslog** est le Syslog-**NG** qui est fourni par le HTTP [: /www.balabit.com/network-security/syslog-ng/opensource-logging-system](#)

Cet article traite seulement l'établissement sur des ordinateurs Windows.

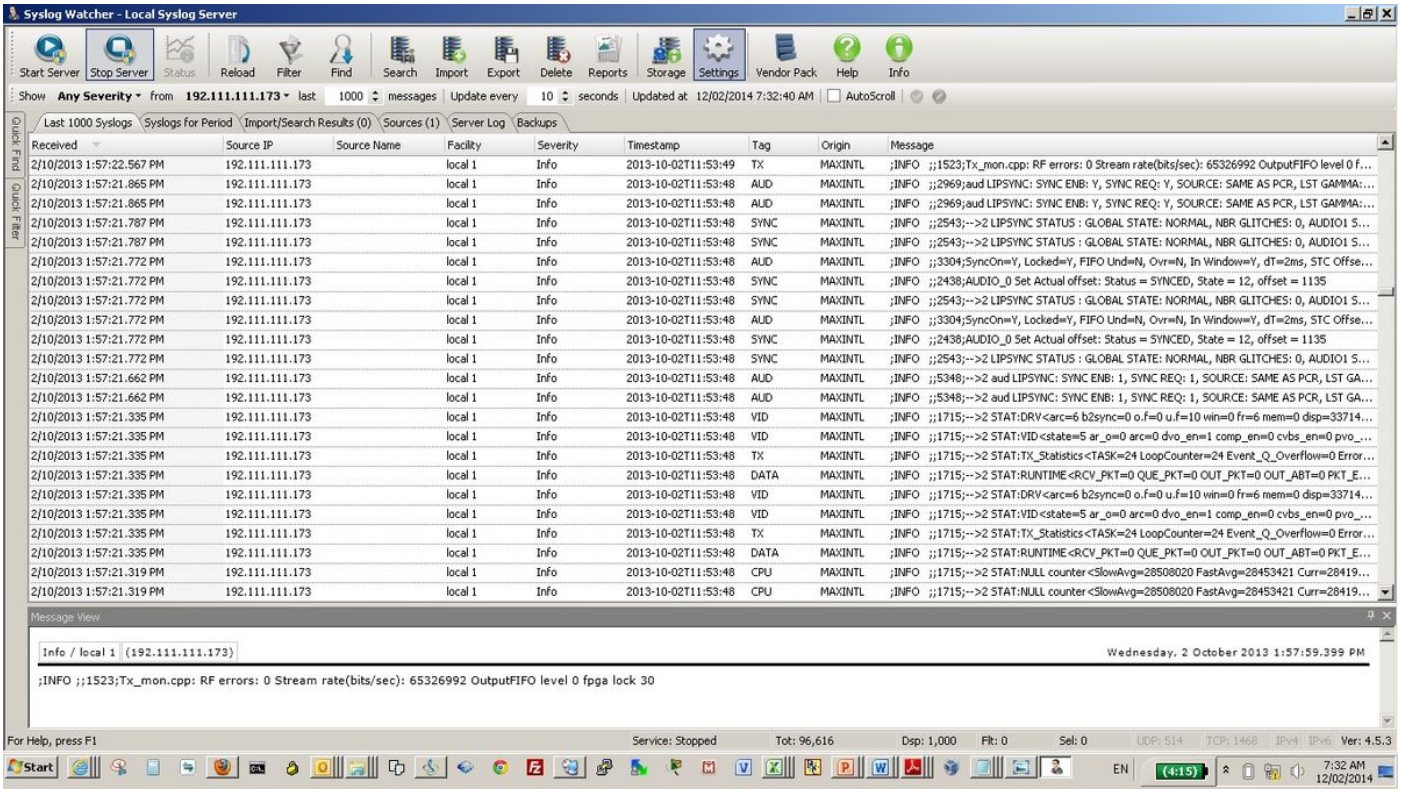
Configurez le serveur de Syslog

Téléchargez le **watcher de Syslog** de

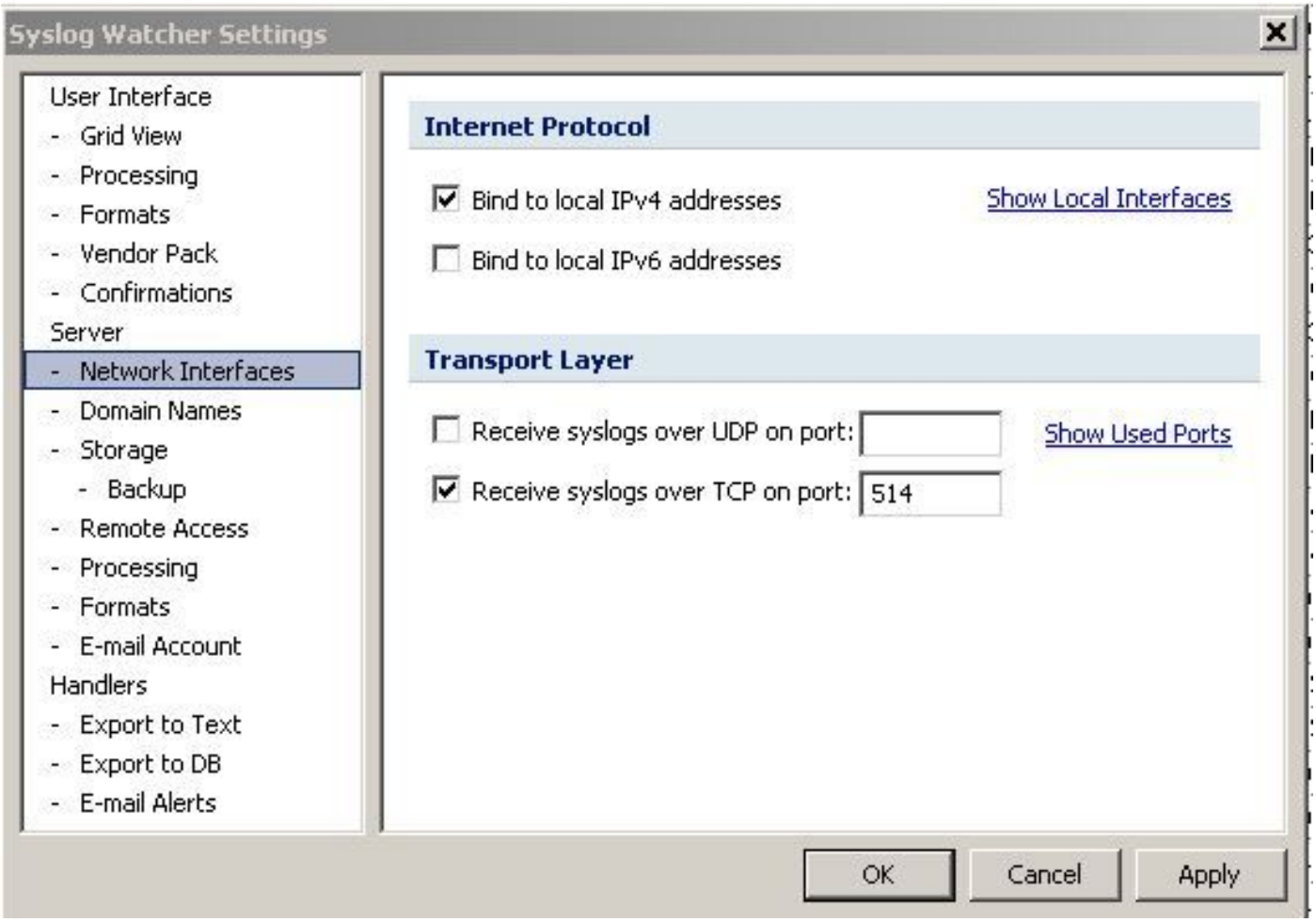
HTTP [: /www.snmpsoft.com/syslogwatcher/syslog-server.html](#)

et installez-le dans votre ordinateur de fenêtres.

Commencez le watcher de Syslog et sélectionnez le mode de fonctionnement pour le GUI comme **gèrent serveur local de Syslog**, l'image affichée apparaît :

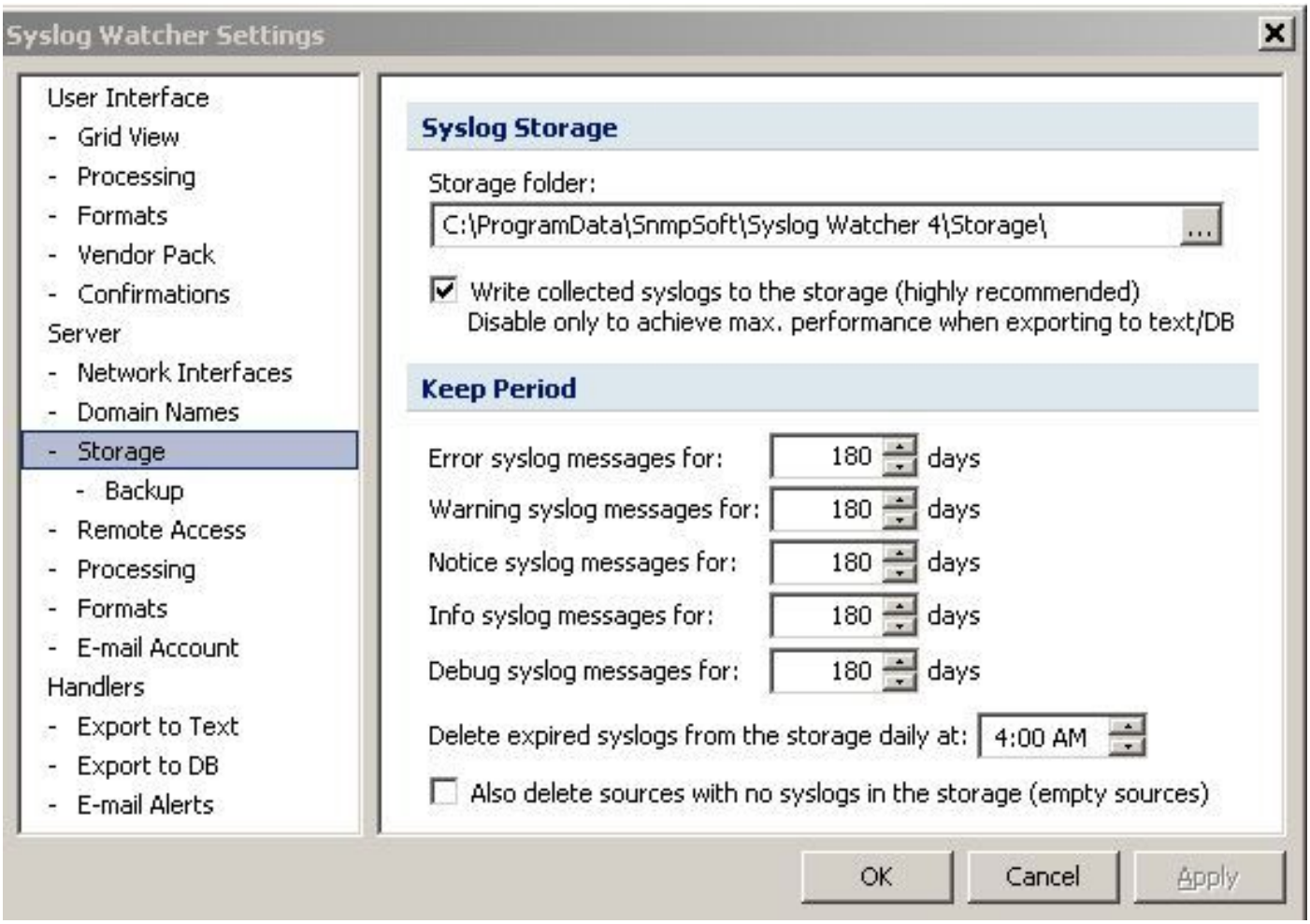


Cliquez sur dans les **configurations** (mises en valeur dans l'image ci-dessus) dans la barre d'outil, l'image affichée apparaît :



Interfaces réseau choisies. Cochez la case **reçoivent des** Syslog **au-dessus d'UDP sur le port** et introduisent un numéro de port. Le même numéro de port doit être configuré sur les périphériques d'où le watcher de Syslog doit recevoir des logs.

Mémoire maintenant choisie sous des **configurations de watcher de Syslog**, suivant les indications de l'image :

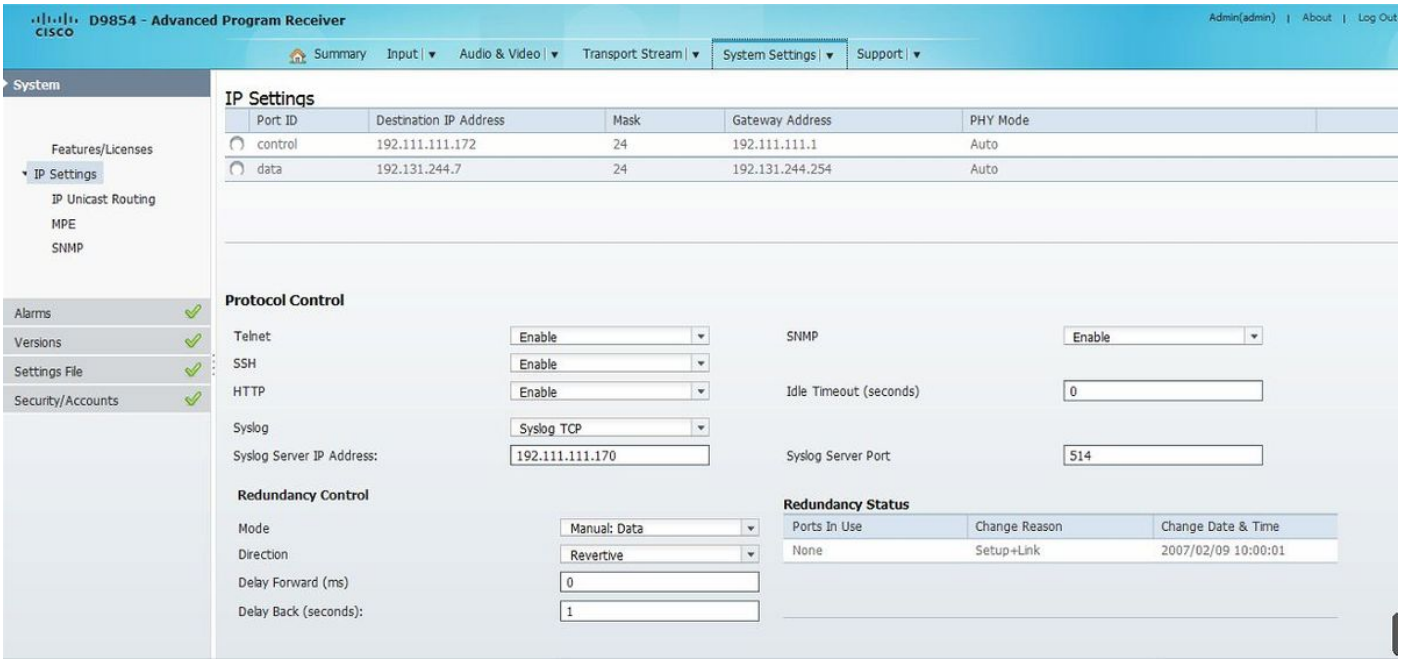


Spécifiez un emplacement de répertoire pour enregistrer les messages, cochez les Syslog **collectés Write de** case à la **mémoire**.

Spécifiez le nombre de jours pour chaque type de message à maintenir dans la mémoire.

Configurez l'IRD (D9854/D9858/D9859) pour envoyer des logs au watcher de Syslog

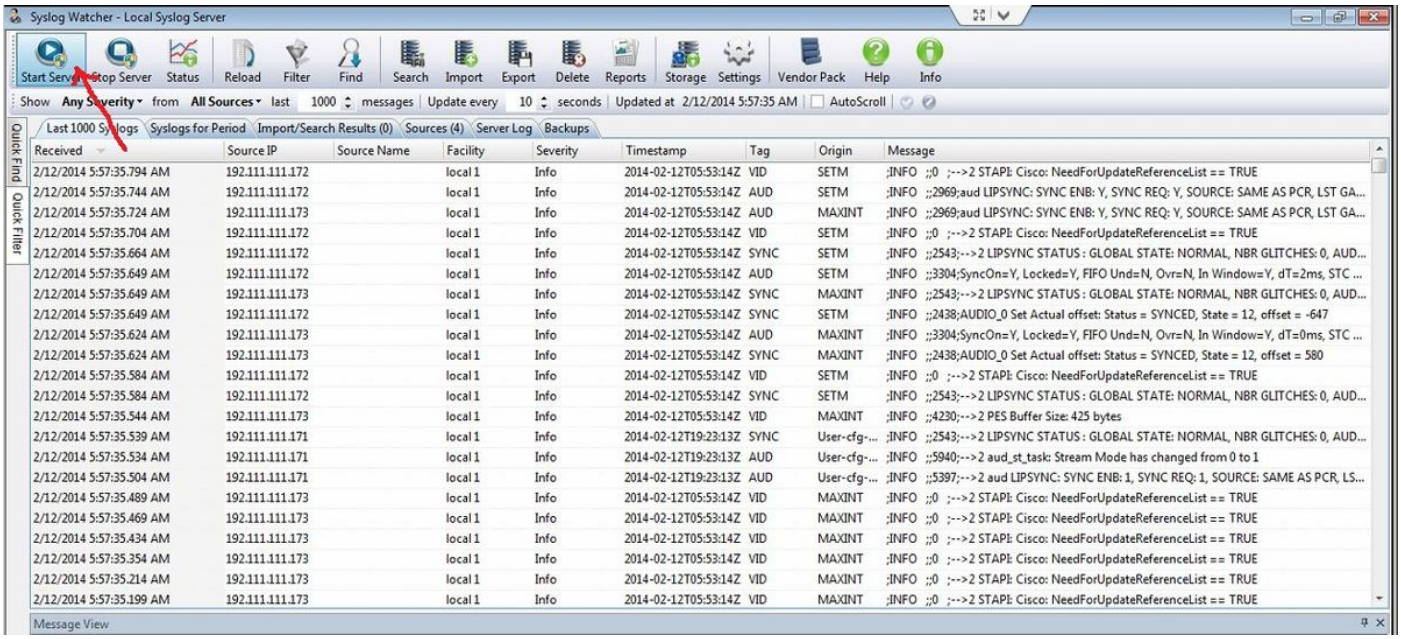
Sur le GUI IRD, sélectionnez les **paramètres IP de configurations de système de la** barre d'outil. L'image affichée apparaît :



Dans l'unité de **commande de Protocol des** paramètres IP paginez, configurez ces derniers :

- **Sgf** sélectionnez le TCP de Syslog ou l'UDP de Syslog au besoin.
- **L'adresse IP de serveur de Syslog** écrivent l'adresse IP de l'ordinateur où le watcher de Syslog est installé.
- **Le port de serveur de Syslog** introduisent un numéro de port. Ceci devrait apparier le numéro de port introduit dans les **configurations de watcher de Syslog**.

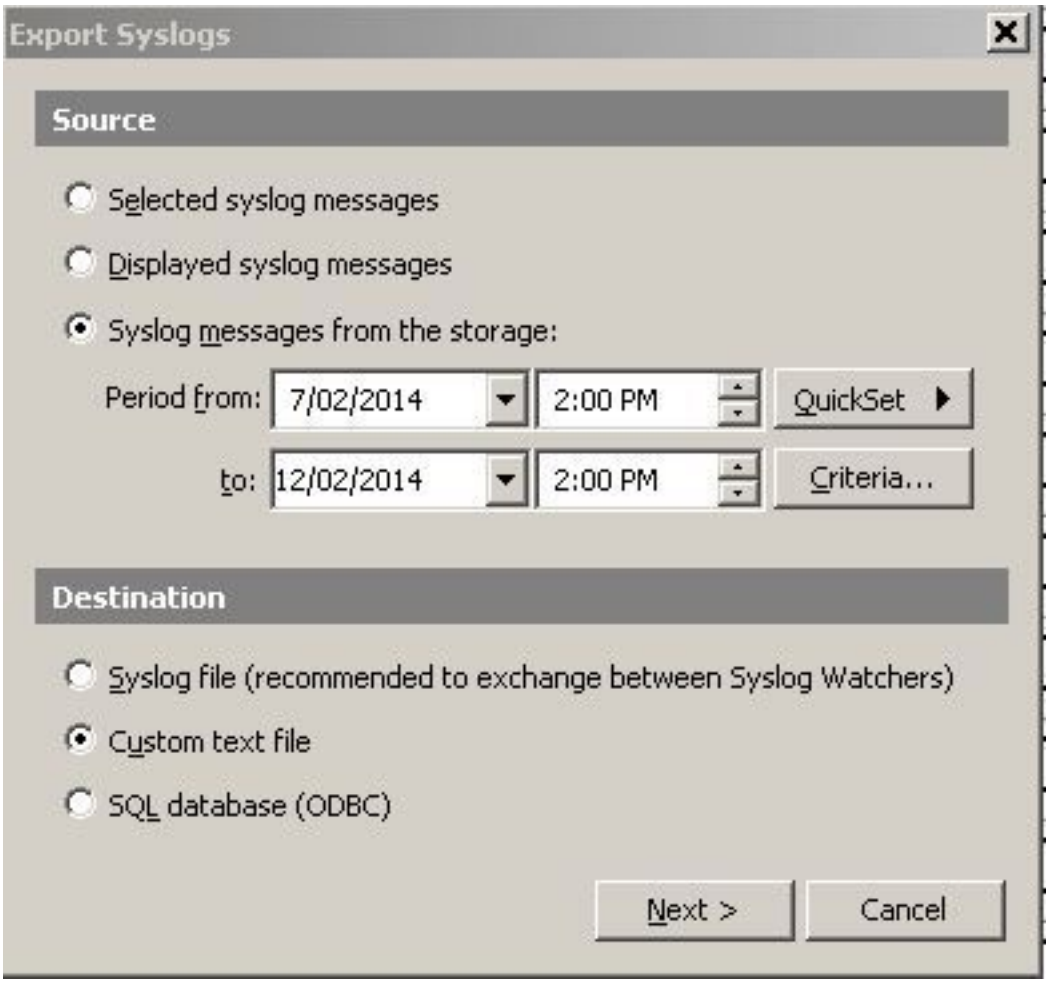
Sous le GUI de watcher de Syslog, commencez le service par sélectionner le **serveur de début**, suivant les indications de l'image :



Exporter les messages enregistrés à un fichier CSV

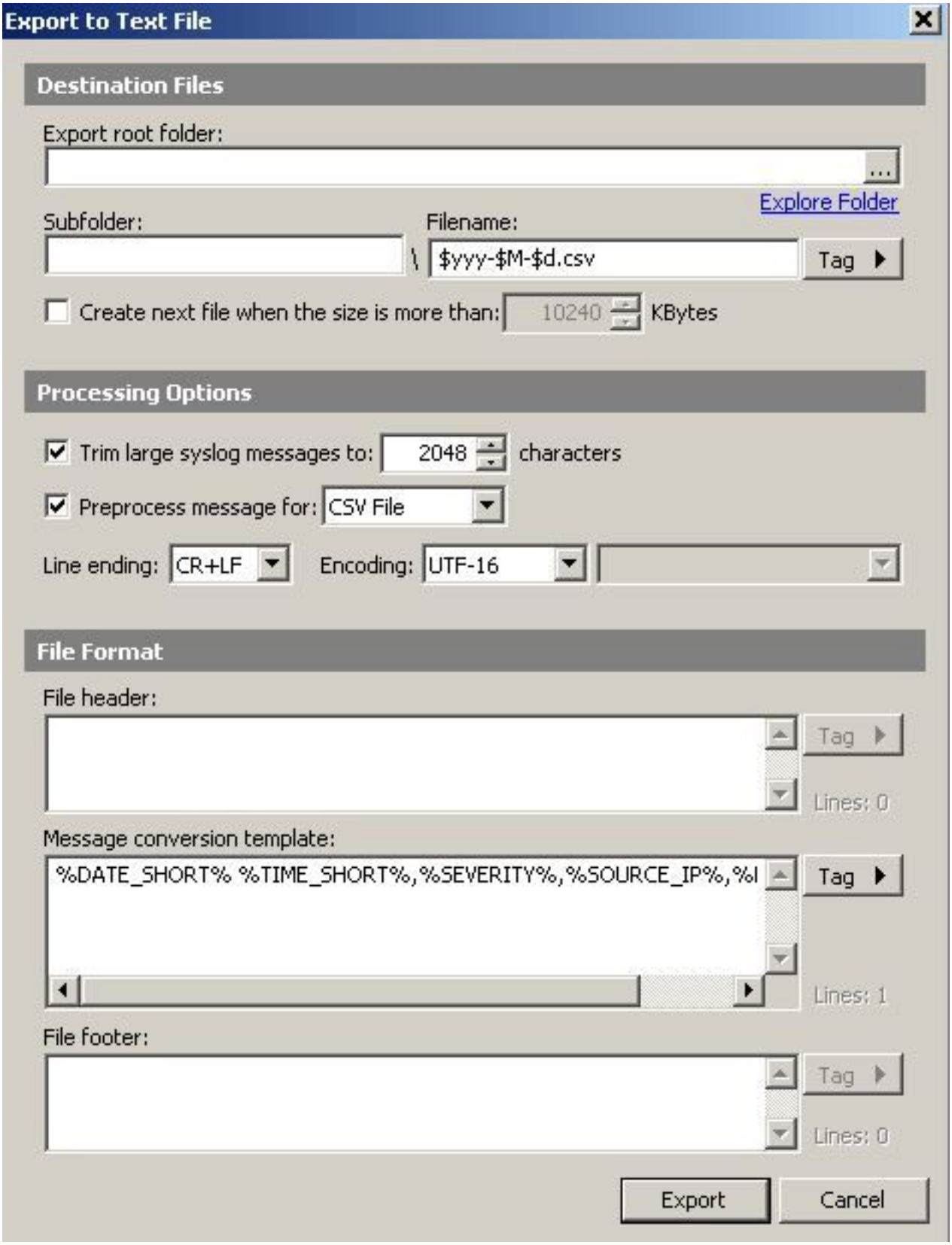
Sur le GUI de watcher de Syslog, clic dans le bouton d'exportation sur la barre d'outil, qui apporte

l'écran, suivant les indications de l'image.



Vous pouvez sélectionner pour exporter des messages au cours d'une période spécifique d'intérêt ou pour exporter seulement une sélection particulière. Dans l'écran ci-dessus, il est sélectionné pour exporter les messages qui se sont produits au cours d'une période.

Sous la destination, sélectionnez le fichier texte fait sur commande et cliquez sur Next.

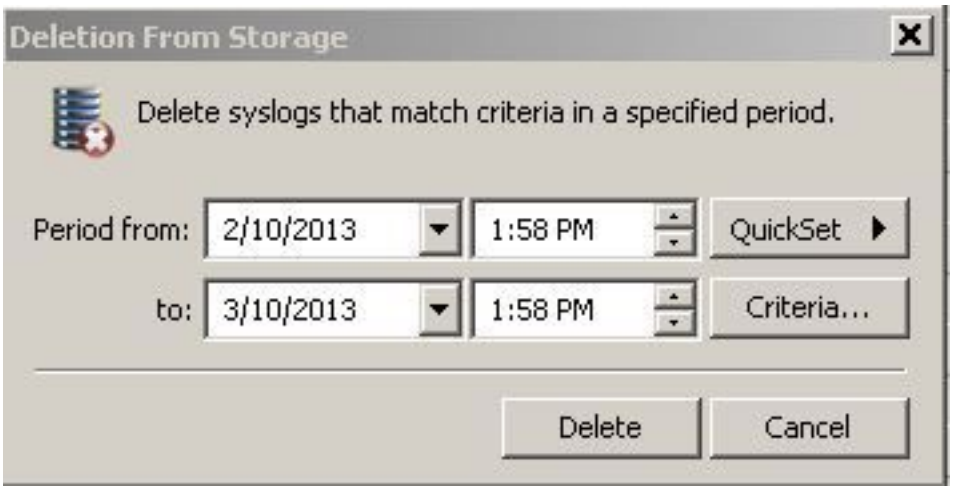


Sélectionnez un répertoire de destination, ajoutez un sous-dossier et donnez un nom du fichier avec l'extension .csv. Si le sous-dossier n'existe pas, il est créé.

Clic dans l'**exportation**.

Supprimer de vieux messages

Sur le GUI de watcher de Syslog, cliquez sur Delete sur la barre d'outil, qui apporte l'écran, suivant les indications de l'image :



Définissez la période l'où vous voudriez supprimer les messages et cliquer sur dans l'**effacement**. Vous pouvez également, utiliser le bouton à congélation rapide pour sélectionner rapidement des périodes de prédéfinis comme l'un jour passé ou une semaine etc.