

# D98xx シリーズ IRDs からのログをキャプチャするために Syslog サーバを設定して下さい

## 目次

[概要](#)

[背景説明](#)

[Syslog サーバを設定して下さい](#)

[Syslog 監視にログを送信するために IRD \( D9854/D9858/D9859 \) を設定して下さい](#)

[CSV ファイルへ保存されたメッセージをエクスポートすること](#)

[以前のメッセージの削除](#)

## 概要

この資料に D98xx シリーズ統合レシーバ/デコーダ ( IRDs ) からのログをキャプチャするために Syslog サーバを設定する方法を記述されています。

## 背景説明

D9859 サポート RFC-3164 対応 **syslog** メッセージの D9854 のソフトウェア リリース 4.0、D9858 及び D9824 およびリリース。顧客は今ストレージおよび検索のための Syslog サーバが付いているメッセージをキャプチャすることができます。さらに、このプロセスも新しい D9800 ネットワーク トランスポート レシーバによって使用することができます。

**Syslog 監視**は Windows マシンのためのサポートされた自由な **syslog** サーバです。Linux マシンに関しては、サポートされた **syslog** サーバは [http](http://www.balabit.com/network-security/syslog-ng/opensource-logging-system) から利用可能の **syslog NG** です: [://www.balabit.com/network-security/syslog-ng/opensource-logging-system](http://www.balabit.com/network-security/syslog-ng/opensource-logging-system)

この技術情報は Windows マシンの設定をだけ取扱います。

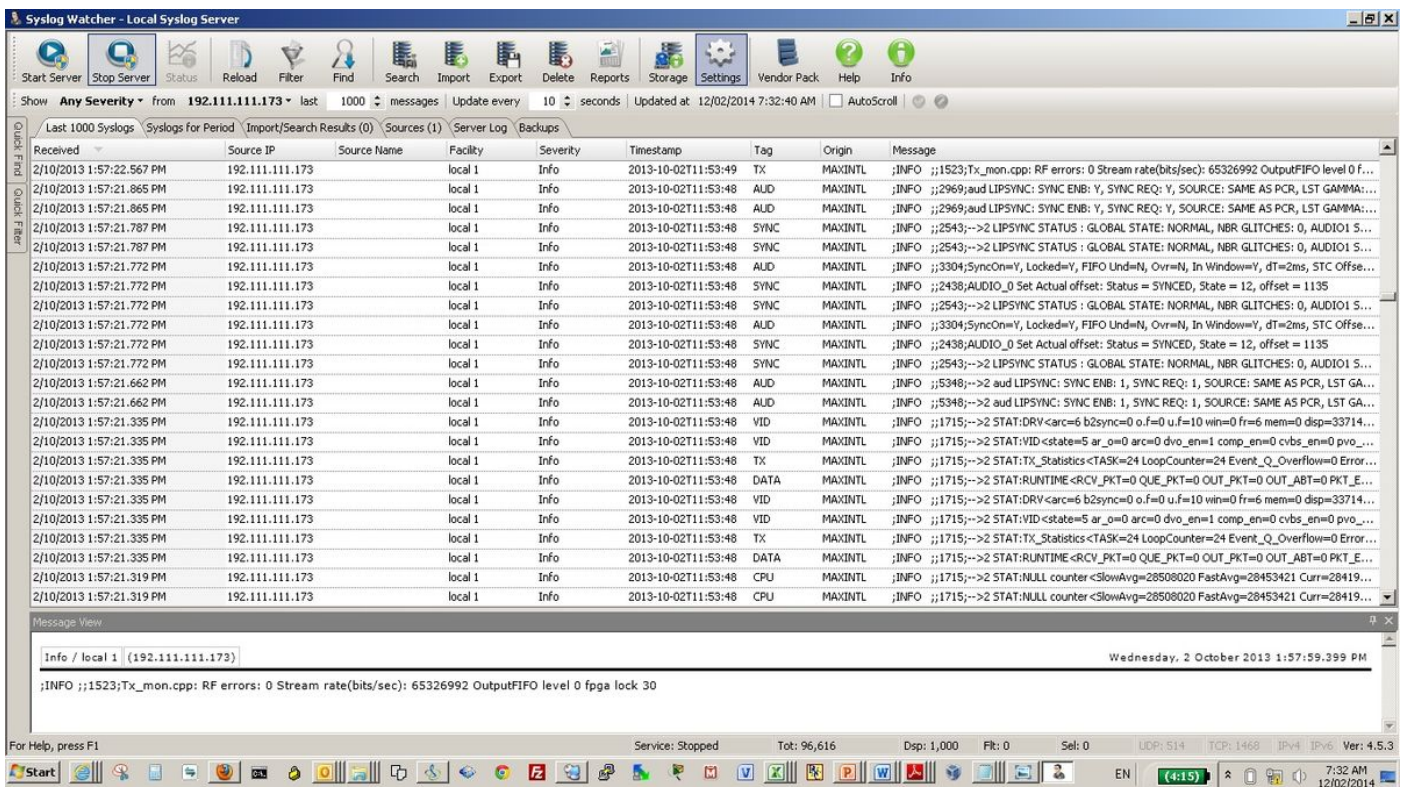
## Syslog サーバを設定して下さい

SysLog 監視をからダウンロードして下さい

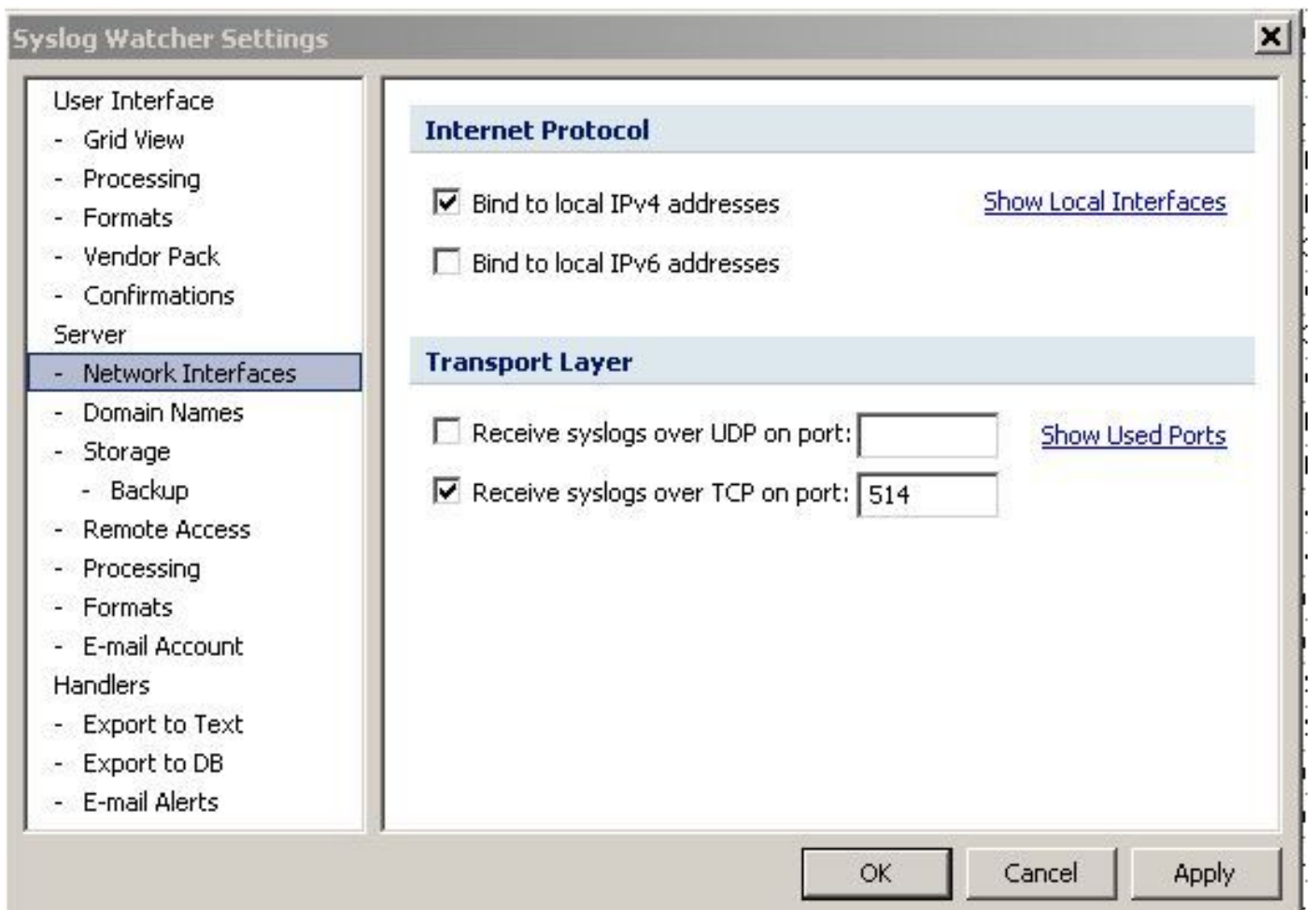
<http://www.snmpsoft.com/syslogwatcher/syslog-server.html>

そしてウィンドウ コンピュータにそれをインストールして下さい。

SysLog 監視を開始し、GUI に動作モードをよう管理しますローカル Syslog サーバ、示されているイメージ現われます選択して下さい:

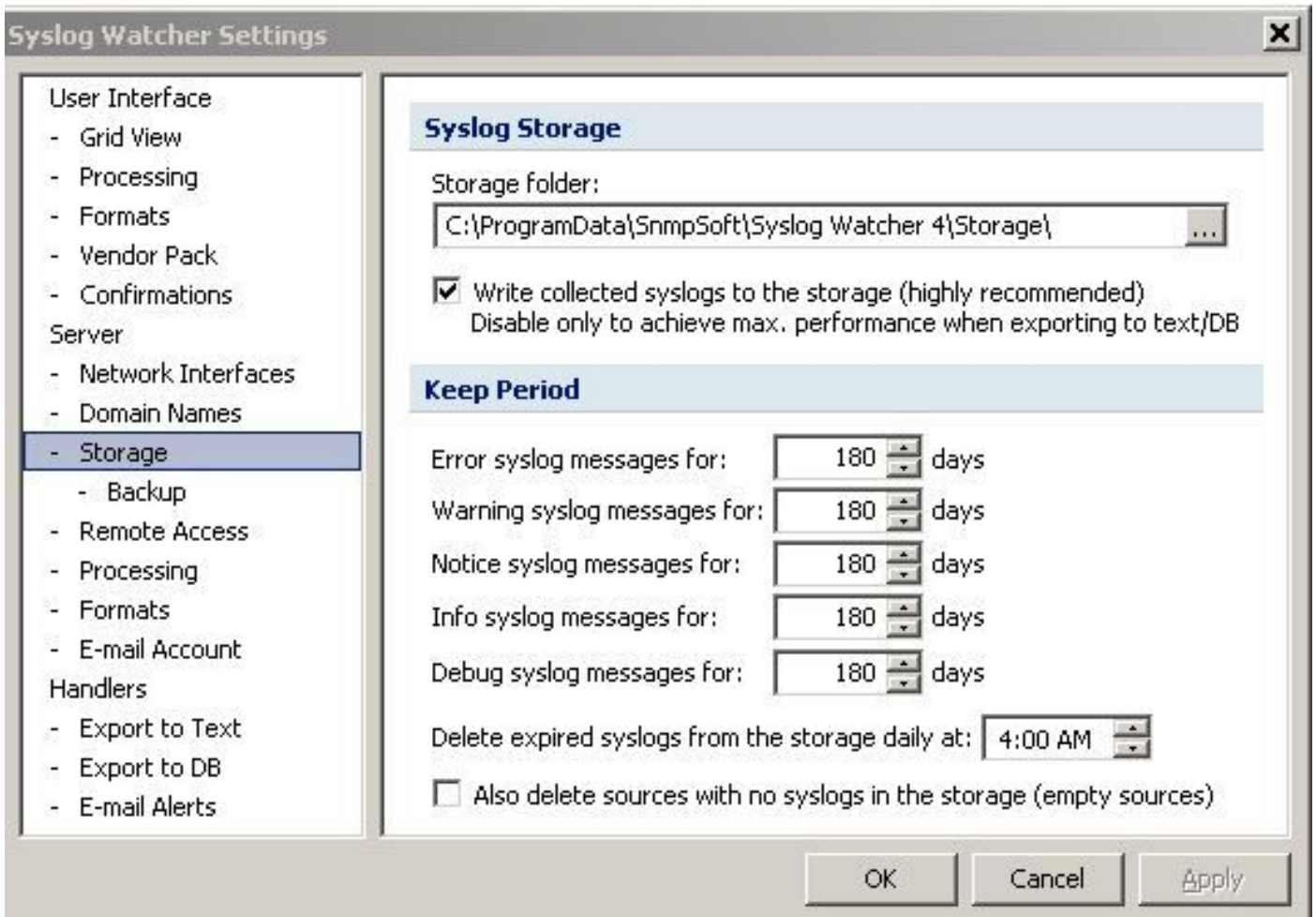


ツールバーの**設定**で ( 上記のピクチャで強調表示される )、示されているイメージ現われますクリックして下さい:



『Network Interfaces』を選択して下さい。ポートのUDP上のボックスをレシーブsyslogをチェックし、ポート番号を入力して下さい。同じポート数はからの設定されるSysLog監視がログを受け取る必要があるデバイスで必要があります。

この場合イメージに示すように SysLog 監視設定の下でストレージを、選択して下さい:



メッセージを保存するためのフォルダーの場所を規定して下さい、ボックスストレージへの Write によって集められる syslog をチェックして下さい。

ストレージで保存されるべき各メッセージのタイプのための日数を規定して下さい。

## Syslog 監視にログを送信するために IRD ( D9854/D9858/D9859 ) を設定して下さい

IRD GUI で、ツールバーからシステム設定 IP 設定を選択して下さい。示されているイメージは現われます:



D9854 - Advanced Program Receiver

Admin(admin) | About | Log Out

Summary | Input | Audio & Video | Transport Stream | System Settings | Support

System

Features/Licenses

IP Settings

IP Unicast Routing

MPE

SNMP

Alarms

Versions

Settings File

Security/Accounts

### IP Settings

Port ID	Destination IP Address	Mask	Gateway Address	PHY Mode
control	192.111.111.172	24	192.111.111.1	Auto
data	192.131.244.7	24	192.131.244.254	Auto

### Protocol Control

Telnet: Enable

SSH: Enable

HTTP: Enable

Syslog: Syslog TCP

Syslog Server IP Address: 192.111.111.170

Syslog Server Port: 514

SNMP: Enable

Idle Timeout (seconds): 0

### Redundancy Control

Mode: Manual: Data

Direction: Revertive

Delay Forward (ms): 0

Delay Back (seconds): 1

### Redundancy Status

Ports In Use	Change Reason	Change Date & Time
None	Setup+Link	2007/02/09 10:00:01

Settings ページ IP のプロトコル 制御 セクションではこれらを設定して下さい:

- **Syslog**は Syslog TCP か Syslog UDP を要求に応じて選択します。
- **Syslog サーバ IP アドレス**は SysLog 監視がインストールされているコンピュータの IP アドレスを入力します。
- **Syslog サーバポート**はポート番号を入力します。これは Syslog 監視設定で入るポート番号を一致する必要があります。

Syslog 監視 GUI の下で、イメージに示すようにサーバを『Start』を選択することからサービスを、開始して下さい:

Syslog Watcher - Local Syslog Server

Start Server | Stop Server | Status | Reload | Filter | Find | Search | Import | Export | Delete | Reports | Storage | Settings | Vendor Pack | Help | Info

Show: Any Severity from All Sources last 1000 messages Update every 10 seconds Updated at 2/12/2014 5:57:35 AM AutoScroll

Received	Source IP	Source Name	Facility	Severity	Timestamp	Tag	Origin	Message
2/12/2014 5:57:35.794 AM	192.111.111.172	local1	local1	Info	2014-02-12T05:53:14Z	VID	SETM	;INFO ;:0 -->2 STAPE: Cisco: NeedForUpdateReferenceList == TRUE
2/12/2014 5:57:35.744 AM	192.111.111.172	local1	local1	Info	2014-02-12T05:53:14Z	AUD	SETM	;INFO ;;2969;aud LIPSYNC: SYNC ENB: Y, SYNC REQ: Y, SOURCE: SAME AS PCR, LST GA...
2/12/2014 5:57:35.724 AM	192.111.111.173	local1	local1	Info	2014-02-12T05:53:14Z	AUD	MAXINT	;INFO ;;2969;aud LIPSYNC: SYNC ENB: Y, SYNC REQ: Y, SOURCE: SAME AS PCR, LST GA...
2/12/2014 5:57:35.704 AM	192.111.111.172	local1	local1	Info	2014-02-12T05:53:14Z	VID	SETM	;INFO ;:0 -->2 STAPE: Cisco: NeedForUpdateReferenceList == TRUE
2/12/2014 5:57:35.664 AM	192.111.111.172	local1	local1	Info	2014-02-12T05:53:14Z	SYNC	SETM	;INFO ;;2543;-->2 LIPSYNC STATUS: GLOBAL STATE: NORMAL, NBR GLITCHES: 0, AUD...
2/12/2014 5:57:35.649 AM	192.111.111.172	local1	local1	Info	2014-02-12T05:53:14Z	AUD	SETM	;INFO ;;3304;SyncOn=Y, Locked=Y, FIFO Und=N, Ovr=N, In Window=Y, dT=2ms, STC ...
2/12/2014 5:57:35.649 AM	192.111.111.173	local1	local1	Info	2014-02-12T05:53:14Z	SYNC	MAXINT	;INFO ;;2543;-->2 LIPSYNC STATUS: GLOBAL STATE: NORMAL, NBR GLITCHES: 0, AUD...
2/12/2014 5:57:35.649 AM	192.111.111.172	local1	local1	Info	2014-02-12T05:53:14Z	SYNC	SETM	;INFO ;;2438;AUDIO_0 Set Actual offset: Status = SYNCED, State = 12, offset = -647
2/12/2014 5:57:35.624 AM	192.111.111.173	local1	local1	Info	2014-02-12T05:53:14Z	AUD	MAXINT	;INFO ;;3304;SyncOn=Y, Locked=Y, FIFO Und=N, Ovr=N, In Window=Y, dT=0ms, STC ...
2/12/2014 5:57:35.624 AM	192.111.111.173	local1	local1	Info	2014-02-12T05:53:14Z	SYNC	MAXINT	;INFO ;;2438;AUDIO_0 Set Actual offset: Status = SYNCED, State = 12, offset = 580
2/12/2014 5:57:35.584 AM	192.111.111.172	local1	local1	Info	2014-02-12T05:53:14Z	VID	SETM	;INFO ;:0 -->2 STAPE: Cisco: NeedForUpdateReferenceList == TRUE
2/12/2014 5:57:35.584 AM	192.111.111.172	local1	local1	Info	2014-02-12T05:53:14Z	SYNC	SETM	;INFO ;;2543;-->2 LIPSYNC STATUS: GLOBAL STATE: NORMAL, NBR GLITCHES: 0, AUD...
2/12/2014 5:57:35.544 AM	192.111.111.173	local1	local1	Info	2014-02-12T05:53:14Z	VID	MAXINT	;INFO ;;4230;-->2 PES Buffer Size: 425 bytes
2/12/2014 5:57:35.539 AM	192.111.111.171	local1	local1	Info	2014-02-12T19:23:13Z	SYNC	User-cfg...	;INFO ;;2543;-->2 LIPSYNC STATUS: GLOBAL STATE: NORMAL, NBR GLITCHES: 0, AUD...
2/12/2014 5:57:35.534 AM	192.111.111.171	local1	local1	Info	2014-02-12T19:23:13Z	AUD	User-cfg...	;INFO ;;5940;-->2 aud_st_task: Stream Mode has changed from 0 to 1
2/12/2014 5:57:35.504 AM	192.111.111.171	local1	local1	Info	2014-02-12T19:23:13Z	AUD	User-cfg...	;INFO ;;5397;-->2 aud LIPSYNC: SYNC ENB: 1, SYNC REQ: 1, SOURCE: SAME AS PCR, LS...
2/12/2014 5:57:35.489 AM	192.111.111.173	local1	local1	Info	2014-02-12T05:53:14Z	VID	MAXINT	;INFO ;:0 -->2 STAPE: Cisco: NeedForUpdateReferenceList == TRUE
2/12/2014 5:57:35.469 AM	192.111.111.173	local1	local1	Info	2014-02-12T05:53:14Z	VID	MAXINT	;INFO ;:0 -->2 STAPE: Cisco: NeedForUpdateReferenceList == TRUE
2/12/2014 5:57:35.434 AM	192.111.111.173	local1	local1	Info	2014-02-12T05:53:14Z	VID	MAXINT	;INFO ;:0 -->2 STAPE: Cisco: NeedForUpdateReferenceList == TRUE
2/12/2014 5:57:35.354 AM	192.111.111.173	local1	local1	Info	2014-02-12T05:53:14Z	VID	MAXINT	;INFO ;:0 -->2 STAPE: Cisco: NeedForUpdateReferenceList == TRUE
2/12/2014 5:57:35.214 AM	192.111.111.173	local1	local1	Info	2014-02-12T05:53:14Z	VID	MAXINT	;INFO ;:0 -->2 STAPE: Cisco: NeedForUpdateReferenceList == TRUE
2/12/2014 5:57:35.199 AM	192.111.111.173	local1	local1	Info	2014-02-12T05:53:14Z	VID	MAXINT	;INFO ;:0 -->2 STAPE: Cisco: NeedForUpdateReferenceList == TRUE

Message View

CSV ファイルへ保存されたメッセージをエクスポートすること

SysLog 監視人 GUI で、イメージに示すように画面を表示するツールバーの Export ボタンでクリ

ックして下さい。

**Export Syslogs**

**Source**

Selected syslog messages

Displayed syslog messages

Syslog messages from the storage:

Period from: 7/02/2014 2:00 PM QuickSet ▶

to: 12/02/2014 2:00 PM Criteria...

**Destination**

Syslog file (recommended to exchange between Syslog Watchers)

Custom text file

SQL database (ODBC)

Next > Cancel

メッセージを対象の特定の期間の間にエクスポートするか、または特定の選択だけエクスポートするために選択できます。上の画面では期間の間に発生したメッセージをエクスポートすることを、選択します。

宛先の下で、カスタムテキストファイルを選択し、『Next』をクリックして下さい。

**Export to Text File** [X]

**Destination Files**

Export root folder:  [Explore Folder](#)

Subfolder:  \ Filename:  Tag ▶

Create next file when the size is more than:  KBytes

**Processing Options**

Trim large syslog messages to:  characters

Preprocess message for:

Line ending:  Encoding:

**File Format**

File header:  Tag ▶  
Lines: 0

Message conversion template:  Tag ▶  
Lines: 1

File footer:  Tag ▶  
Lines: 0

宛先フォルダを選択し、サブフォルダを追加し、.csv 拡張を用いるファイル名をつけて下さい。  
。サブフォルダがない場合、作成されます。

エクスポートでクリックして下さい。

## 以前のメッセージの削除

Syslog 監視 GUI で、イメージに示すように画面を表示するツールバーで『Delete』 をクリックして下さい:



メッセージを削除し、削除でクリックすることを望む期間を定義して下さい。、すぐに最後の1日または1週先祖などのようなあらかじめ定義された期間を選択するのにクイックセット ボタンを使用するためにまたかもしれないです