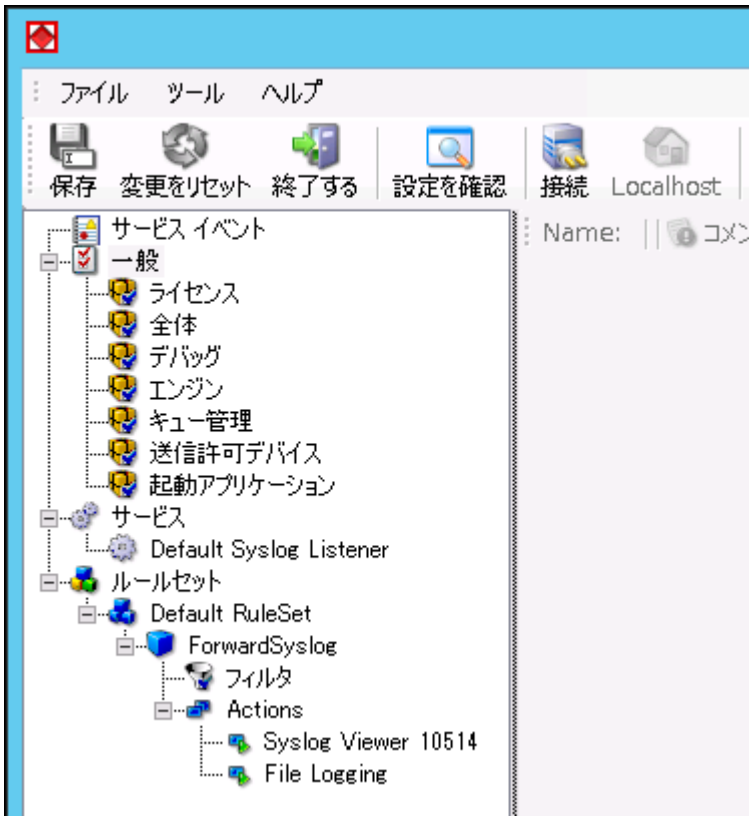
2017 年 7 月 3 日

SNMP トラップ送信と MIB ブラウザ

受信したログで条件に合致したログを SNMP トラップとして送信する方法を説明します。
本書では、既存のルールへ「SNMP トラップの送信」アクションを追加する方法を紹介しています。

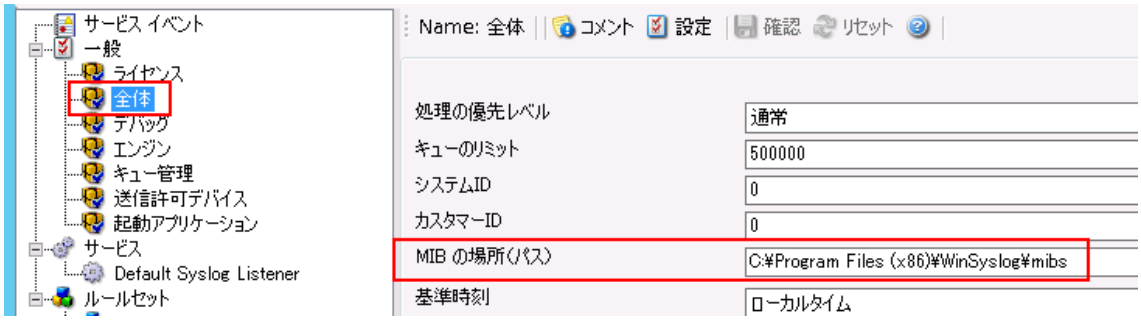
1 MIB データの設定

1. WinSyslog Configuration Client を起動します。



デフォルトでは、左ペインのツリーには、上記のサービスとルールセットが設定されています。

2. ツリーから、「一般」>「全体」を選択します。ここで MIB データの場所を指定します。

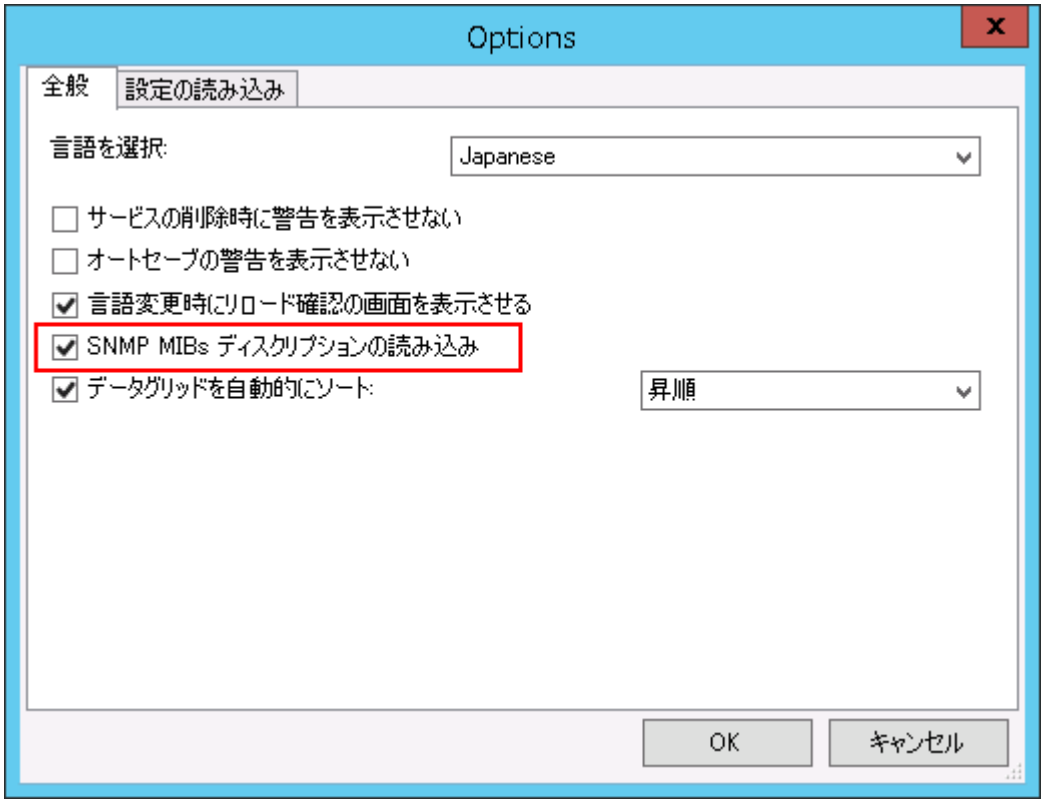


MIB の場所（パス）

MIB データの場所を指定します。「参照」ボタンを押下し、ブラウザより MIB ファイルを選択するか、MIB ファイルが入るフォルダを指定の場合は、パスを指定してください。
デフォルト値は、C:¥Program Files (x86)¥WinSyslog¥mibs です。

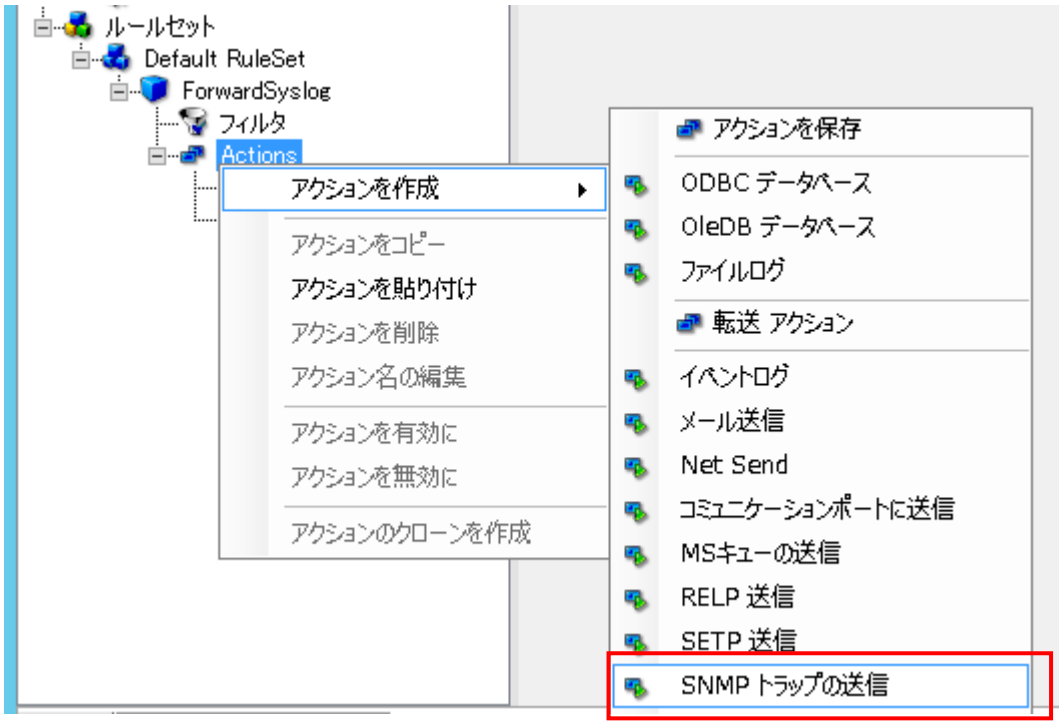
3. トップメニューから、「ファイル」>「オプション」を選択し、
「全般」タブで、
☐ SNMP Mibs ディスクリプションの読み込み
にチェックします。

このオプションを有効にすると、クライアント(WinSyslog Configuration Client)を開いたとき MIB データが直ちにロードされます。
無効の場合、「MIB ブラウザ(OID)」を開く時に MIB データがロードされるため、遅延を感じることになります。

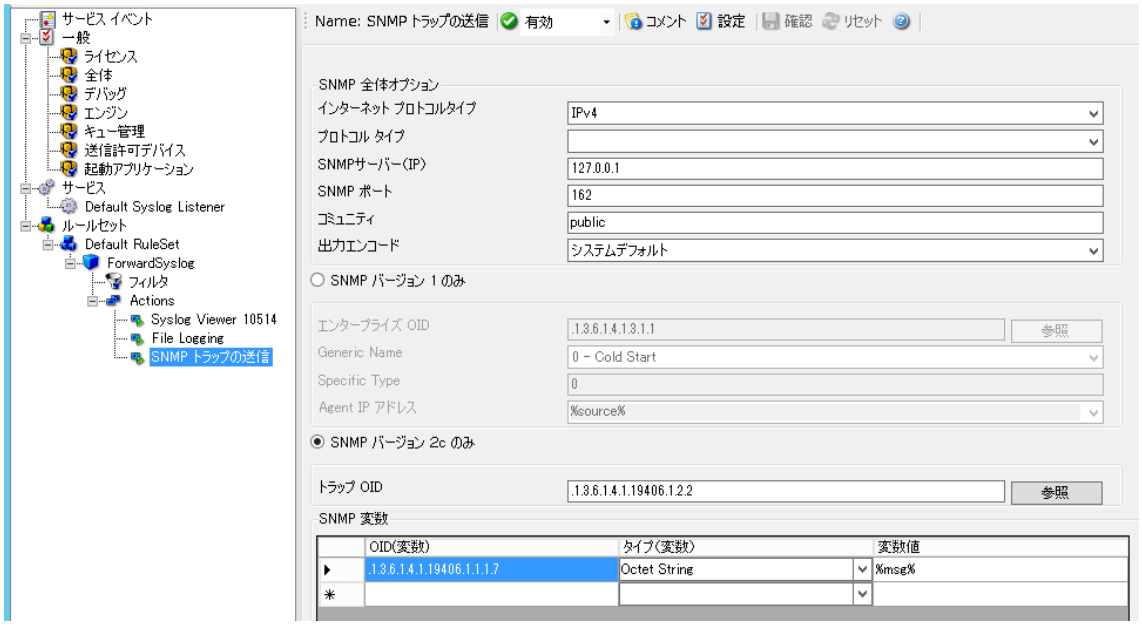


2 「SNMP トラップの送信」アクションを追加

1. 左ペインの「ルールセット」>「Default RuleSet」>「ForwardSyslog」>「Actions」上で右クリックし、「アクションを作成」>「SNMP トラップの送信」をクリックします。



左ペインの Actions ツリー下に「SNMP トラップの送信」が追加され、右ペインは以下の表示になります。



右ペインで設定を行います。

「SNMP　全体オプション」

インターネットプロトコルタイプ

送信時の IP タイプを指定します。IPv4、IPv6 のどちらかを選択します。

プロトコルタイプ

ここでは、UDP または TCP を指定します。

SNMP サーバー(IP)

SNMP トラップを受信するエージェントを IP アドレスで指定します。

SNMP ポート

ここでは、ポート番号を指定します。

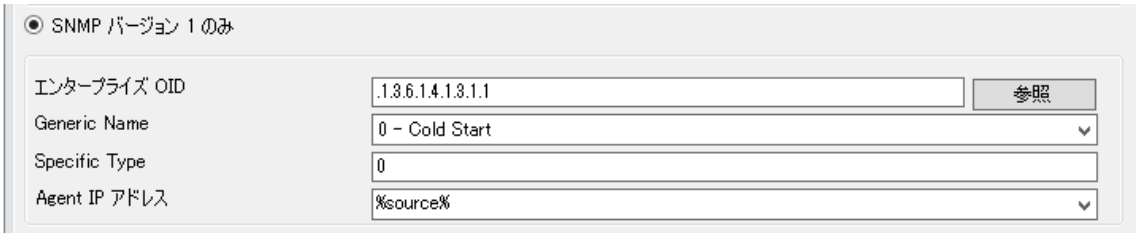
実際に使用する値については、サーバーリファレンスをご参照下さい。

一般的に、メールサーバーはポート 25、ウェブサーバーは、ポート 80 を使用します。

コミュニティ

メッセージの属する SNMP コミュニティを指定します。

○SNMP バージョン 1 のみ



SNMP バージョン 1 で送信する場合に、こちらのオプションを選択します。

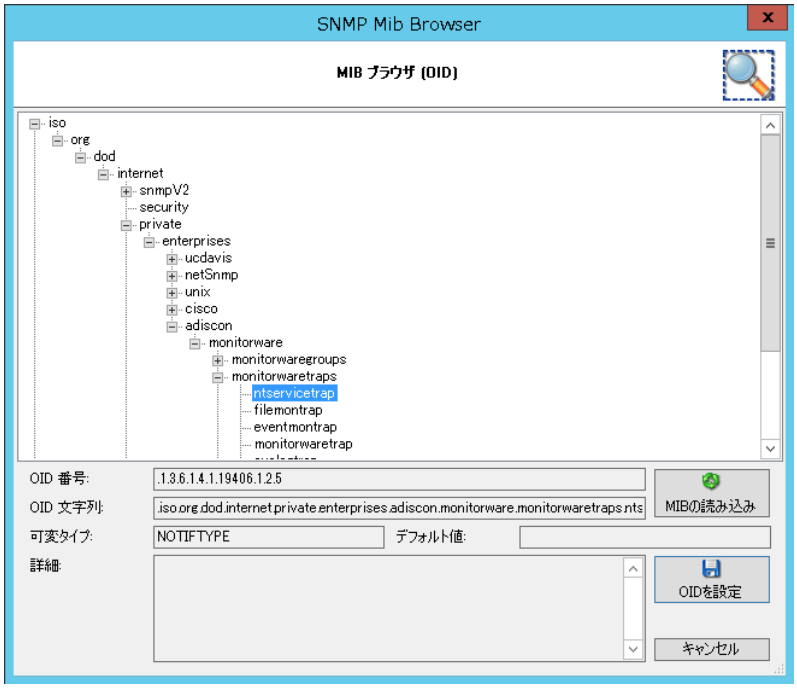
このグループボックスでは、SNMP バージョン 1 に関するパラメータを設定できます。

エンタープライズ OID

ここでは、エンタープライズ OID を指定します。

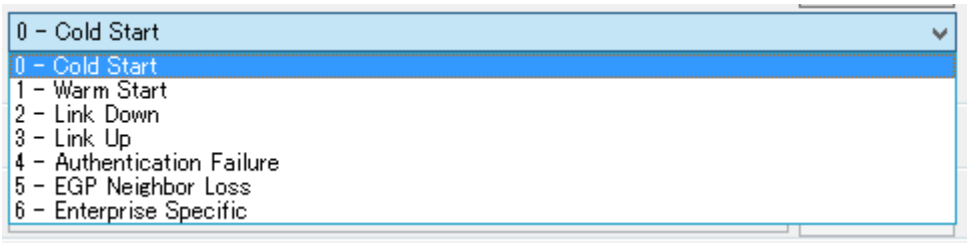
「参照」をクリックすると下記画面「SNMP Mib Browser MIB ブラウザ(OID)」が現れます。

MIB の場所(パス)で指定した MIB データから OID の選択が可能となります。



Generic Name

トラップの一般名をプルダウンメニューから指定します。



0 - Cold Start

1 - Warm Start

2 - Link Down

3 - Link Up

4 - Authentication Failure

5 - EGP Neighbor Loss

6 - Enterprise Specific

から、Generic Name を指定することができます。

Specific Type

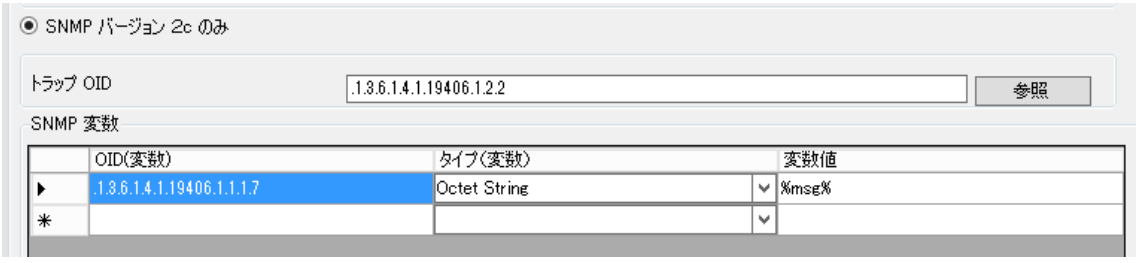
トラップの追加コードを定義できます。整数値です。

Agent IP アドレス

Trap を発生させた SNMP エージェントの IP アドレスを示す SNMP v1 の Agent Address フィールドを、他の IP アドレスに設定できます。可能であれば、ホスト名は自動的に解決されます。 デフォルトでは、**%source%**プロパティに設定されます。

トラップデータに含まれる agent IP のプロパティを設定する場合は、**%snmp_agentip%**とします。プルダウンからの選択も可能です。

○SNMP バージョン 2c のみ



SNMP バージョン 2c で送信する場合に、こちらのオプションを選択します。

このグループボックスでは、SNMP バージョン 2c に関するパラメータを設定できます。

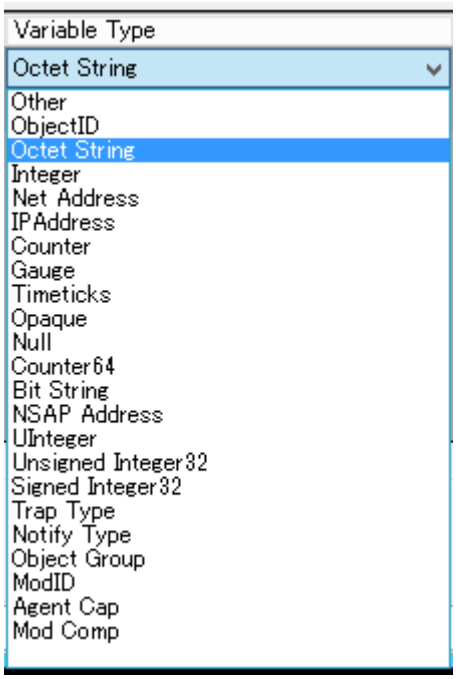
トラップ OID

ここでは、OID を指定します。トラップコードをご存知の場合、それらを入力することも可能です。そうでない場合は、「参照」をクリックすると「SNMP Mib Browser　MIB ブラウザ

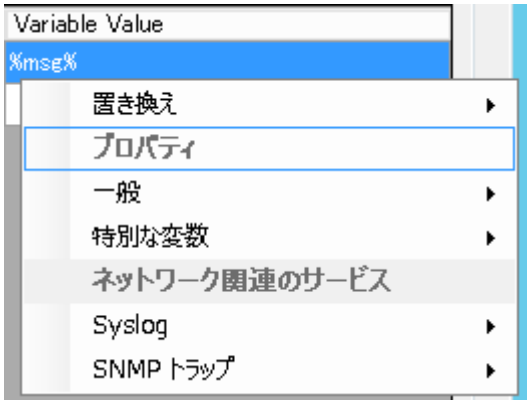
(OID)」が現れます。
MIB の場所（パス）で指定した MIB データから OID を確認してください。

SNMP 変数（SNMP トラップに送信する変数）
各カラムに指定します。
・OID（変数）
SNMP トラップの OID を指定します。利用できる OID については、「SNMP Mib Browser MIB ブラウザ(OID)」のリストをご利用下さい。

・タイプ（変数）
Octet String や Integer などのタイプ。
このタイプによっては、変数を正確にフォーマットする必要があります。(IP Address など)



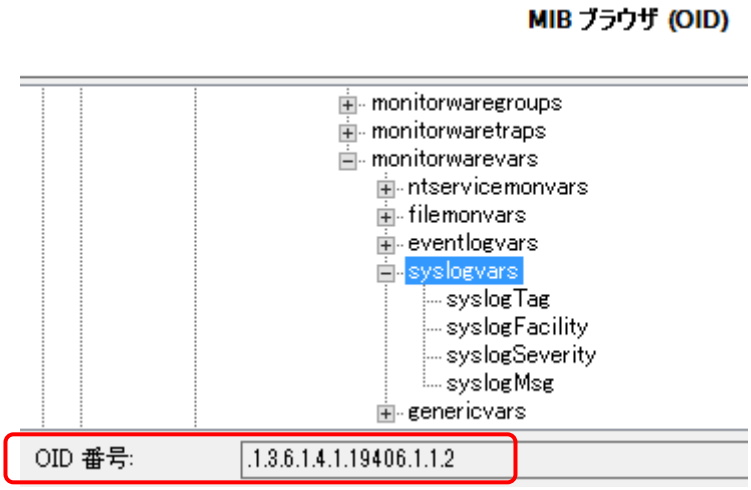
・変数値
タイプによってフォーマットされる必要があります。
カラム上にカーソルを置き、右クリックで、プロパティ値を入力可能です。



2. 設定例

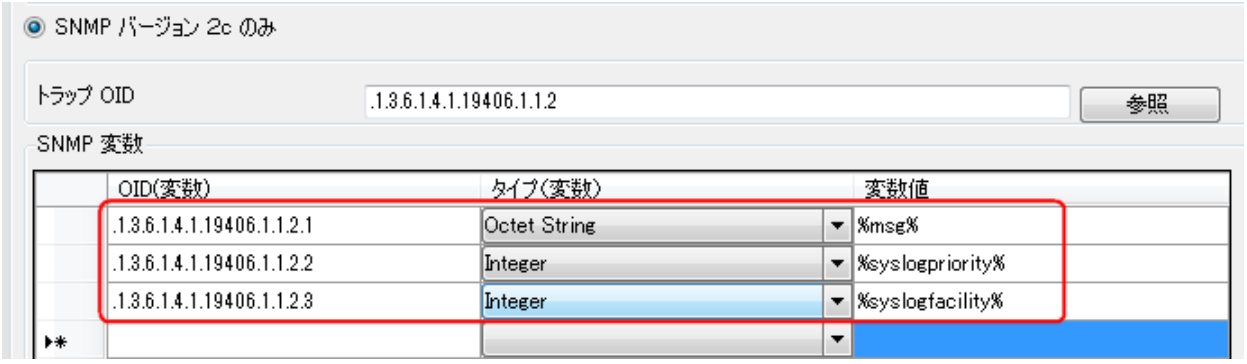
以下に、SNMP トラップ送信の設定例と、受信先で出力した表示のサンプルを記します。

トラップ OID： syslogvars(.1.3.6.1.4.1.19406.1.1.2)



その他の SNMP 変数（VariableOID）として、以下を追加します。

- syslogMSG (.1.3.6.1.4.1.19406.1.1.2.1)
- syslogSeverity (.1.3.6.1.4.1.19406.1.1.2.2)
- syslogFacility (.1.3.6.1.4.1.19406.1.1.2.3)



SNMP トラップとして転送する Syslog メッセージ:

2016-07-07　15:52:50,　Syslog.Warning,　192.168.91.156,　SampleTest

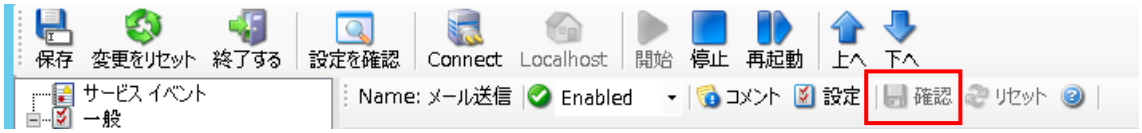
転送先トラップ出力例 1(OID が変換される場合):

2016-07-07,15:53:50,source="192.168.91.156" community="public" version="Ver2" variables: snmp_var_1 = 'DISMAN-EVENT-MIB::sysUpTimeInstance: 'Timeticks: (1269809507) 146 days, 23:14:55.07" , snmp_var_2 = 'SNMPv2-MIB::snmpTrapOID.0: 'OID: ADISCON-MONITORWARE-MIB::syslogvars" , snmp_var_3 = 'ADISCON-MONITORWARE-MIB::syslogFacility: 'INTEGER: syslog(5)" , snmp_var_4 = 'ADISCON-MONITORWARE-MIB::syslogSeverity: 'INTEGER: warning(4)" , snmp_var_5 = 'ADISCON-MONITORWARE-MIB::syslogMsg: 'STRING: "SampleTest""

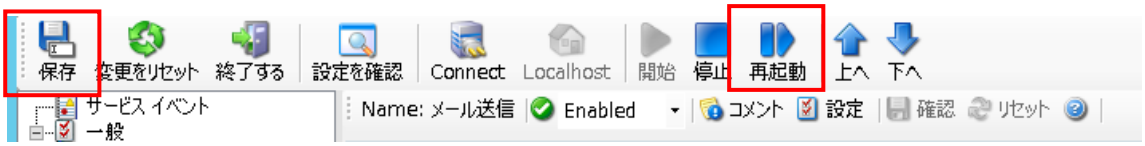
転送先トラップ出力例 2(OID が変換されない場合):

2016-07-07 15:54:05 Local7.Debug　192.168.91.156 community=public, enterprise=1.3.6.1.4.1.19406.1.1.2, uptime=1269777817, agent_ip=, version=Ver2, 1.3.6.1.4.1.19406.1.1.2.1=SampleTest, 1.3.6.1.4.1.19406.1.1.2.2=4, 1.3.6.1.4.1.19406.1.1.2.3=5

3. 設定した後は、問題がないか「確認」ボタンを押します。問題なければ、以下のようにグレーアウト表示になります。



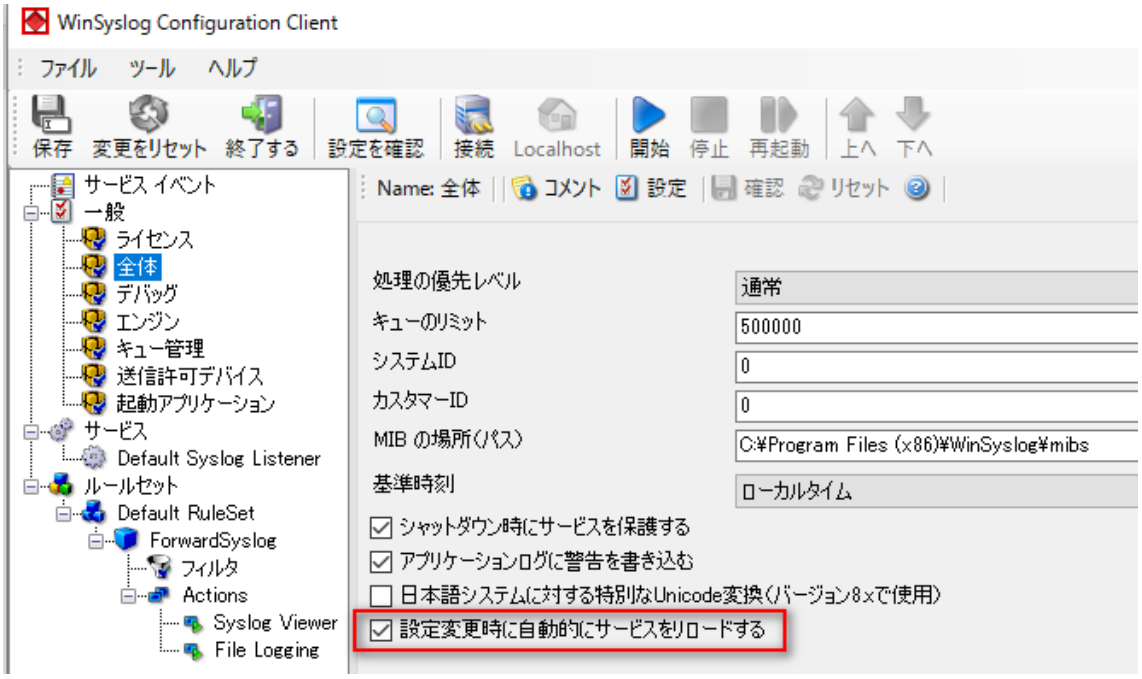
次に、「保存」アイコンを押下し、設定を保存後、「再起動」アイコンをクリックして、サービスを再起動し、設定を反映させます。



※WinSyslog ver.14.1 以降、「設定変更時に自動的にサービスをリロードする」オプションが追加となりました。

このオプションはデフォルト設定では有効ですので、**設定変更後「保存」ボタンのみで変更が反映されます。**

この機能を無効にしたい場合は、チェックを外してください。


WinSyslog Configuration Client
ファイル
ツール
ヘルプ
保存
変更をリセット
終了する
設定を確認
接続
Localhost
開始
停止
再起動
上へ
下へ
サービス イベント
一般
ライセンス
全体
デバッグ
エンジン
キュー管理
送信許可デバイス
起動アプリケーション
サービス
Default Syslog Listener
ルールセット
Default RuleSet
ForwardSyslog
フィルタ
Actions
Syslog Viewer
File Logging
Name: 全体
コメント
設定
確認
リセット
処理の優先レベル
通常
キューのリミット
500000
システムID
0
カスタマーID
0
MIB の場所(パス)
C:¥Program Files (x86)¥WinSyslog¥mibs
基準時刻
ローカルタイム
シャットダウン時にサービスを保護する
アプリケーションログに警告を書き込む
日本語システムに対する特別なUnicode変換(バージョン8.xで使用)
設定変更時に自動的にサービスをリロードする

以上