Kiwi Syslog Server

ver.9.5.0

リリースノート

Release Note

Rev. 1.0

2015.10.06

ジュピターテクノロジー

目次

変更履歴

この資料の変更履歴は以下の通りです。

版	発行日	変更内容
第 1.0 版	2015/10/06	・新規 v9.5.0 リリースノート

1 はじめに

このドキュメントは、Kiwi Syslog Server v9.5.0 リリースノートです。
Kiwi Syslog Server v9.5.0 は、2015 年 8 月 11 日にリリースされました。

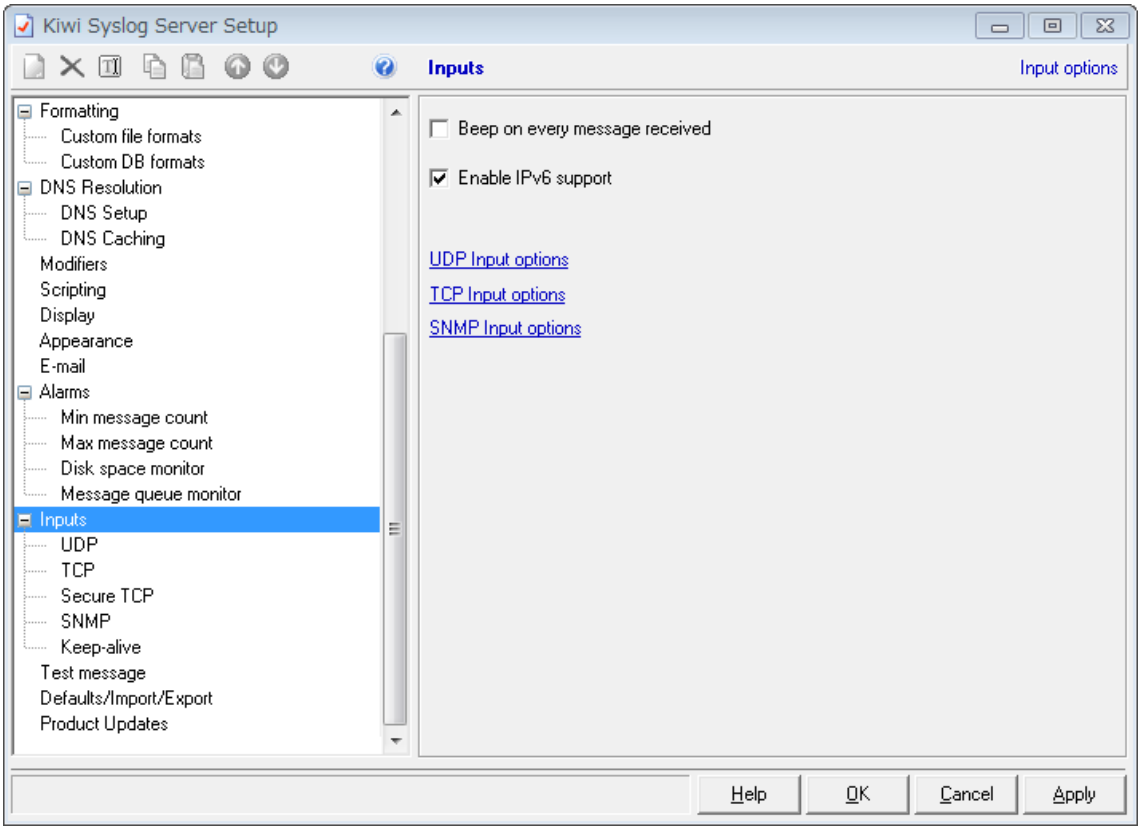
ご質問、ご不明な点は、弊社カスタマーポータルで受付けております。
詳細は、4.「問い合わせ窓口について」をご参照ください。

2 リリースノート

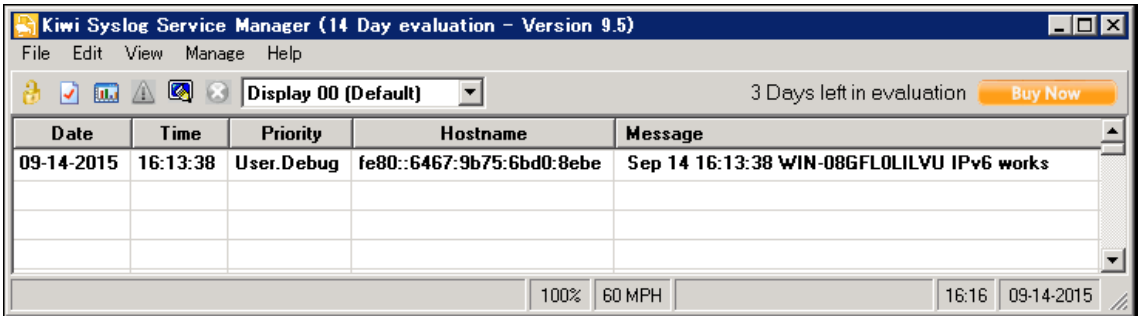
2.1 新機能と改善点

2.1.1 IPv6 をサポート

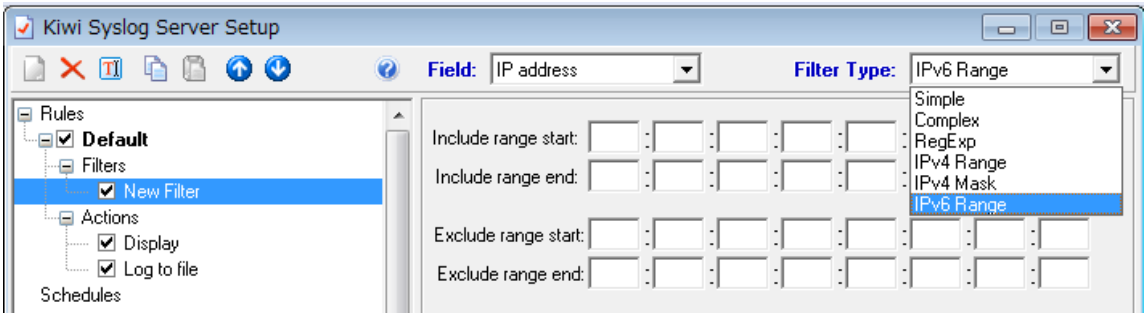
1. IPv6 アドレスからのログを受信するには、以下の設定を行います。
   Inputs > ☑Enable IPv6 support



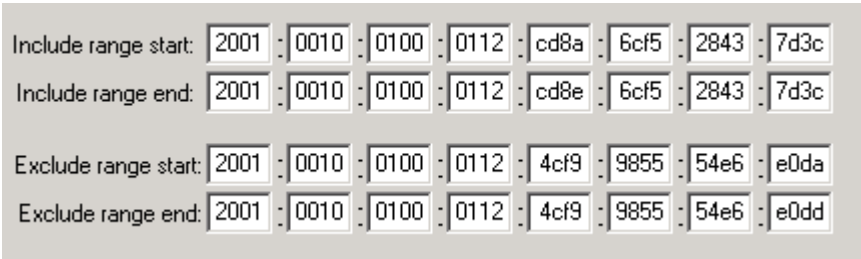
受信例:



2. 新しいフィルタータイプ Filter Type: IPv6 Range（IPv6 レンジ）での指定方法



例 1：



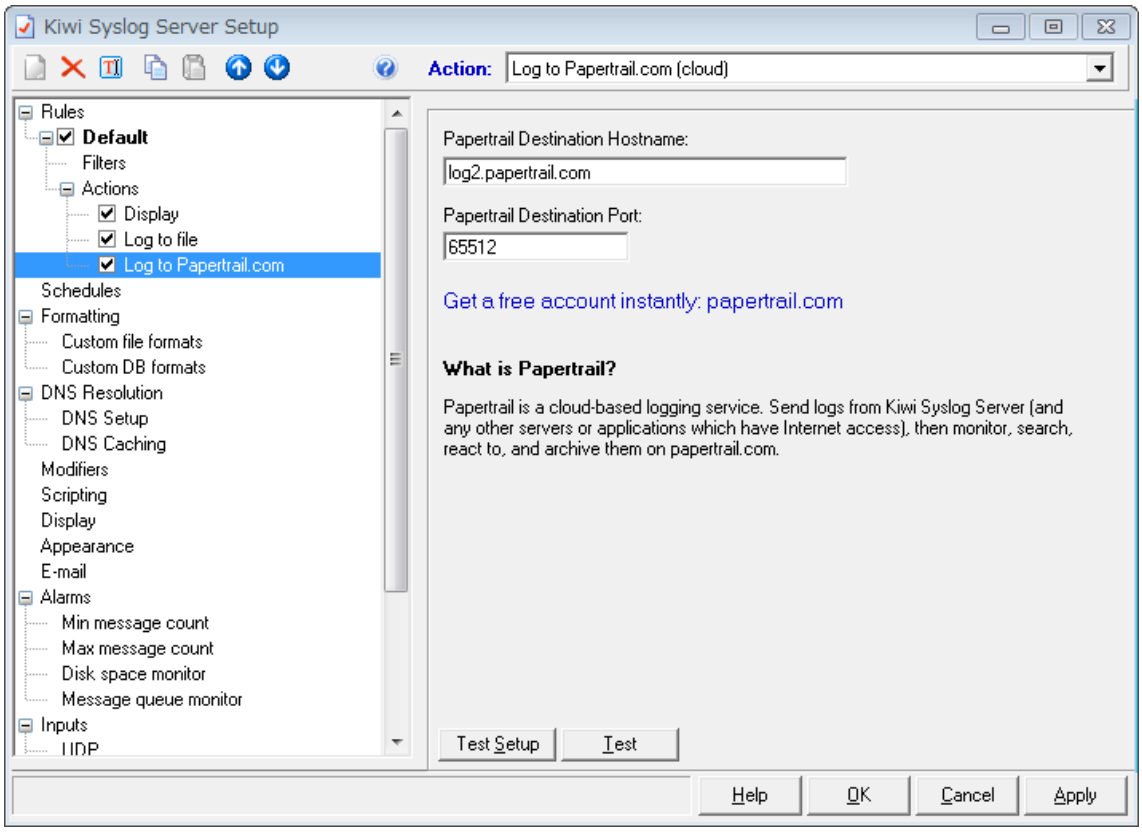
上図の場合、IPv6 アドレスが 2001:10:100:112:cd8a:6cf5:2843:7d3c ～ 2001:10:100:112:cd8e:6cf5:2843:7d3c の範囲内にあり、2001:10:100:112:4cf9:9855:54e6:e0da ～ 2001:10:100:112:4cf9:9855:54e6:e0dd の範囲内でなければ結果は真となります。

例 2：

上図は除外する IP アドレス範囲を指定する例です。

IPv6 アドレスが 2001:10:100:112:4cf9:9855:54e6:e0da～
2001:10:100:112:4cf9:9855:54e6:e0dd の範囲内になければ結果は真となります。

2.1.2 新しいアクションを追加：Log to Papertrail.com (cloud)（クラウドベースのサーバー Papertrail に Syslog メッセージを記録）



Papertrail は、クラウドベースの記録サービスです。 Kiwi Syslog Server（またはインターネットに接続することができる任意の他のサーバーやアプリケーション）からログを送信すると、Papertrail では、モニター、検索、アクション（重要なログ受信時のアラート等）や、Papertrail.com にログをアーカイブします。

Papertrail Destination Hostname（送信先の Papertrail のホスト名）：
送信先のホスト名には、syslog サーバーからログを送信する場所を設定します。Papertrail によって宛先ホストが提供されます。
例：logs2.papertrailapp.com

Papertrail Destination Port（Papertrail 宛先ポート）：

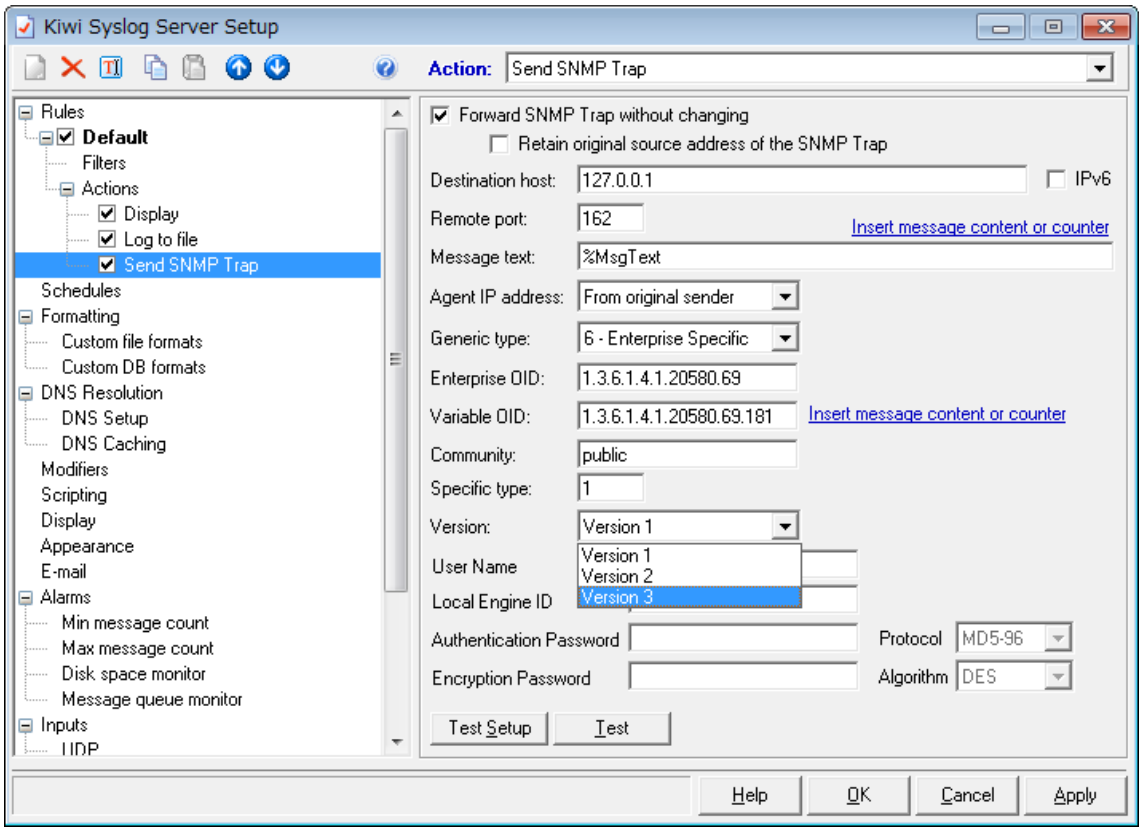
Papertrail を使用してログインアカウントを作成後、システム(ログ送信先)を作成すると Papertrail は、特定のポート番号を提供します。syslog メッセージを送信するために同じポート番号を使用してください。
例:58612

Get a free acount instantly: papertail.com
のクリックで Papertrail のサイトへアクセス可能です。

Papertrail の機能のヘルプについては、こちらをクリックしてください。

2.1.3 SNMP v1、v2、および v3 トラップの転送をサポート

v9.4.2 までは、SNMP v1, v2 の転送をサポートしていましたが、v9.5.0 からは v3 のトラップ転送もサポートします。



Action: Send SNMP Trap 設定で、v9.5.0 で新しく追加、変更された設定について説明します。

Forward SNMP Trap without changing（変更なしで SNMP Trap を転送）
このオプションをチェックすると、宛先ホストに元の SNMP トラップを転送します。
SNMP トラップの元の送信 IP アドレスを保持したい場合は、
□Retain original source address of the SNMP Trap（SNMP トラップのオリジナルの送信アドレスの保持）をチェックし有効にします。（注意：WinPcap がインストールされることで選択可能となります）

通常、syslog のプロトコルは、SNMP トラップを転送するとき、本来の送信元 IP アドレスを保持することができません。元の IP アドレスを保持するには、WinPcap バージョン 4.1 以上がインストールされていなければなりません。
WinPcap (Windows Packet Capture library)は、WinPcap, The Packet Capture and Network Monitoring Library for Windows からダウンロード可能です。

注意：WinPcap をインストール後、Kiwi Syslog Server のサービスを再起動する必要があります。

Destination host （宛先ホスト）
SNMP メッセージ送信先の IP アドレスまたはホスト名を入力します。

IPv6
IPv6 で IP アドレスを指定する場合はチェックします。

Remote port （リモートポート）←v9.5.0 から表示位置が Destination host の下に変更になりました。
SNMP トラップを送信するポートを指定します。デフォルトでは 162 に指定されています。
この設定を変更する場合、SNMP トラップ受信デバイスの受信待機ポートもこれと同じ番号にする変更する必要があります。

Version （バージョン）←v9.5.0 から表示位置が Specific type の下に変更になりました。
SNMP トラップを受信するシステムがサポートする SNMP バージョン(Version 1, Version 2, Version 3)を選択します。
つまり、Kiwi Syslog Server から他のシスログサーバーへどの SNMP バージョンタイプ(Version 1, Version 2, Version 3)で、SNMP トラップを送信するかを指定します。

バージョン 3 を選択した場合、User Name(ユーザー名)、Local Engine ID(ローカルエンジン

ID)、Authentication Password(認証パスワード)、Encryption Password(暗号化パスワード)、Protocol(プロトコル: None/MD5-96/SHA-96)、
Algorithm(アルゴリズム: None/DES/AES/3DES/AES192/AES256)を入力する必要があります。

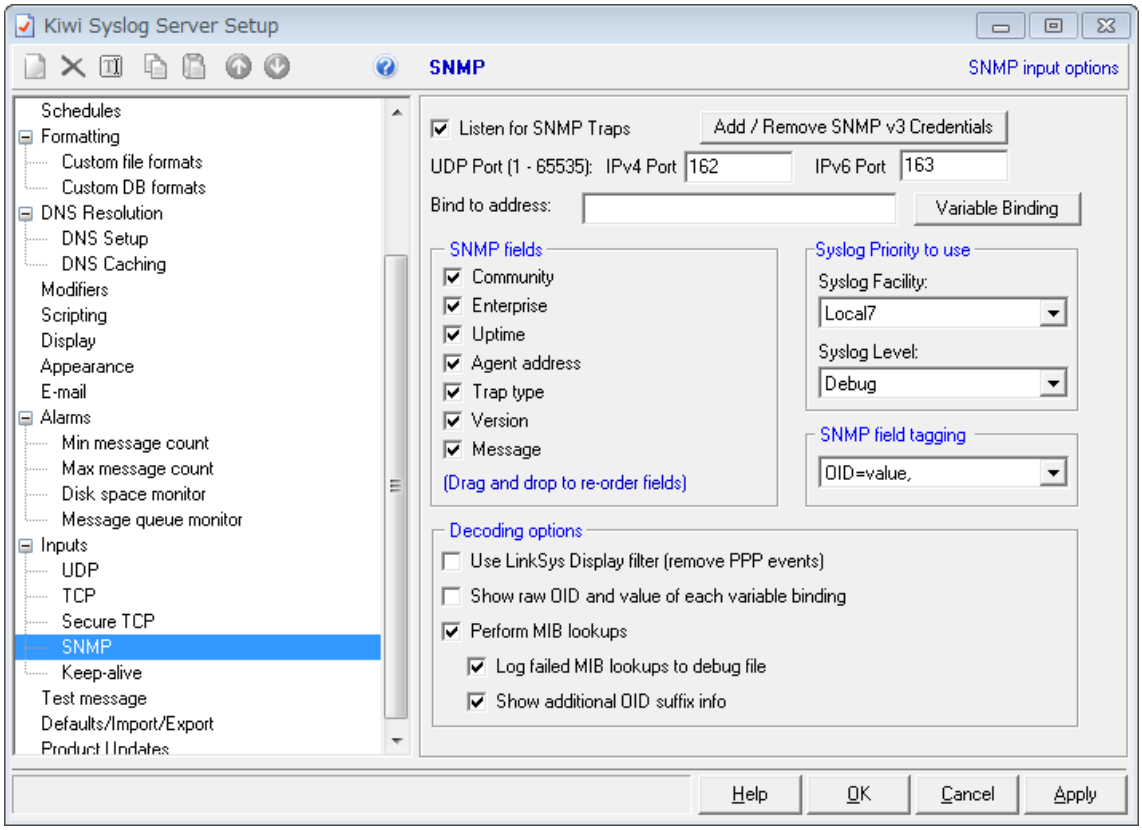
例えば、ユーザーが暗号化パスワードとアルゴリズムを設定すると、『認証』だけのセキュリティレベルとして作動します。

注意:v3 のトラップを送信／転送するには、SNMP credentials (SNMP 証明書)が受信側および送信側で必要です。

2.1.4 SNMP v3 トラップの送信／受信をサポート

SNMP v3 トラップの送信については、「2.1.3 SNMP v1、v2、および v3 トラップの転送をサポート」を参照してください。

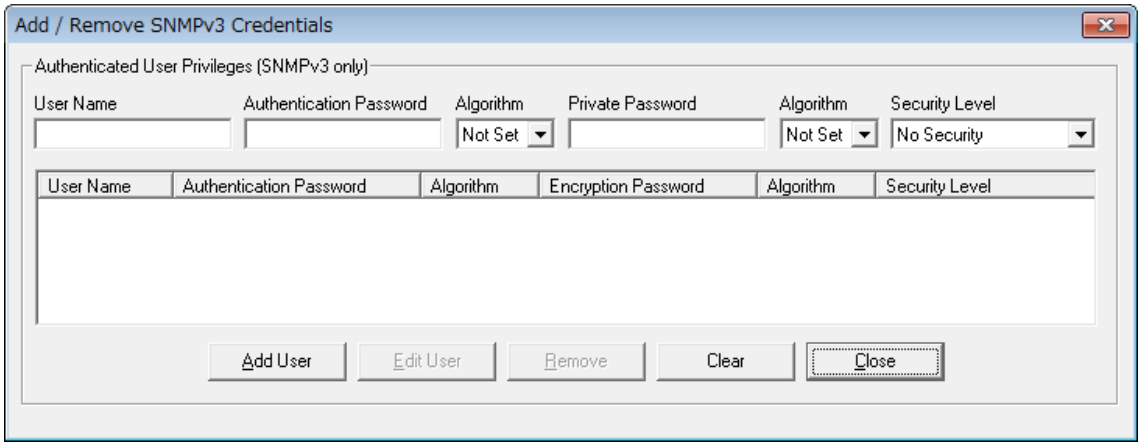
Kiwi Syslog Server は、SNMP version1/2c トラップに加え、v9.5.0 で、v3 トラップも受信できるようになりました。受信したトラップはデコードされ syslog メッセージと同様に処理されます。SNMP トラップの受信は、
Inputs>SNMP で、
☑ Listen for SNMP Traps
にチェックし有効にします。デフォルトは、無効です。



v9.5.0 で追加された設定について説明します。

Add/Remove SNMP v3 Credentials（SNMP v3 証明書の追加/削除）:

SNMP トラップ v3 を受信する場合、セキュリティとリモート設定の入力を行います。 SNMP トラップ v3 を処理するために、証明書の詳細を Kiwi Syslog Server に追加してください。



User name（ユーザー名）:

送信元デバイスに指定されているユーザー名を指定します。ユニークな値である必要があります。

Authentication Password と Algorithm（認証パスワードとアルゴリズム）:
有効な送信元を認証するために、認証パスワードとアルゴリズム（MD5 または SHA のいずれか）を設定します。

Private Password & Algorithm（プライベートパスワードとアルゴリズム）:
プライバシーのためのデータ暗号化は、プライベートパスワードとアルゴリズム（AES/DES/3DES のいずれか）を使って実行されていますので、その情報を入力します。

Security Level:
セキュリティレベルは、以下に示す通信メカニズムのいずれかを選択します。
・*No security（セキュリティなし）*: 認証もユーザーのための暗号化もなし。
・*Authentication only（認証のみ）*: 送信されたデータの暗号化なしで認証する。
・*Authentication and Privacy（認証とプライバシー）*: 認証とデータの暗号化の両方。

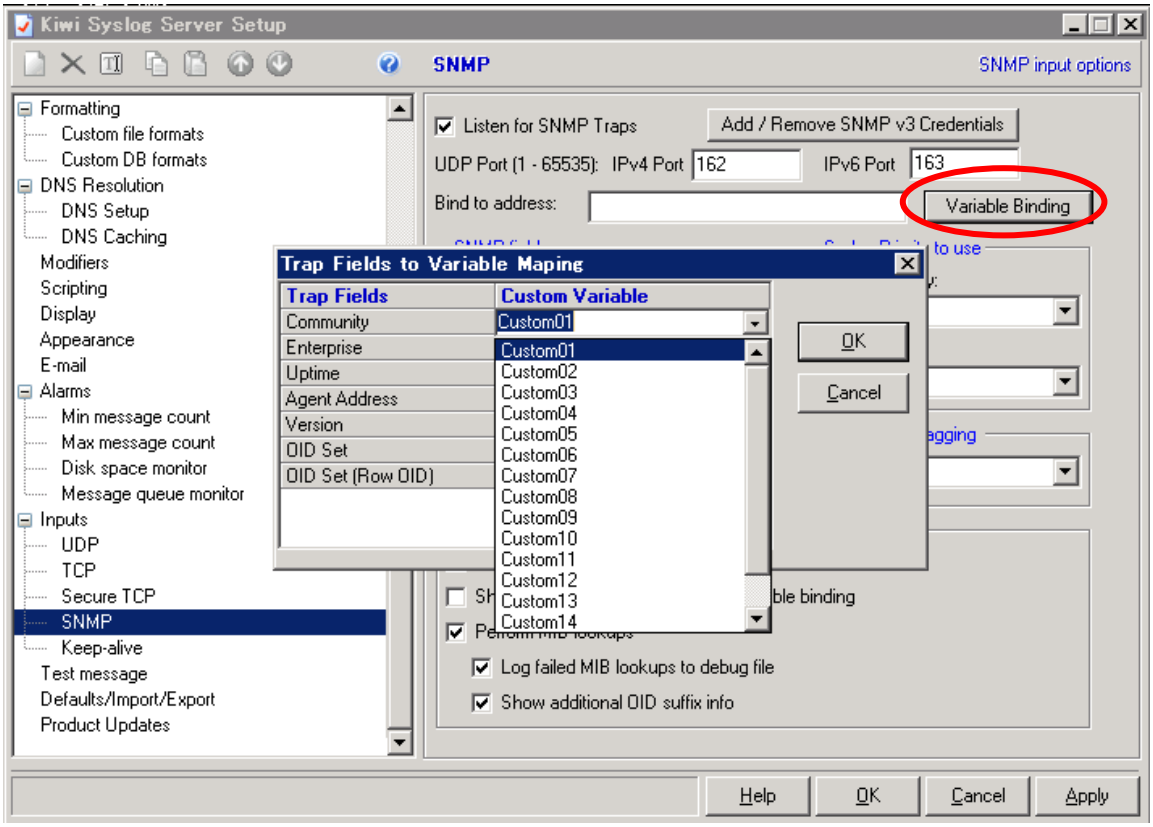
UDP port (1 - 65535)（UDP ポート (1 - 65535) ）:
SNMP トラップを受信する UDP ポートを指定します。通常、IPv4 のトラップは、162 ポートに IPv6 トラップは 163 ポートに送信されますが、受信する SNMP トラップのポートを変更することができます（1～65535 までの値）。デフォルトの 162 または 163 以外の値を選択した場合は、トラップを送信するデバイス側でも指定されたポートに送信していることを確認してください。

注：SNMP トラップの受信で、IPv4 と IPv6 のポート番号は、同じあってはいけません。

2.1.5 出力時に TrapVarBinds エレメントを許可

SNMP トラップの受信時に各トラップフィールドにカスタム変数を割り当てることで、アクションにおいて関連付けたカスタム変数＝VarCustom 変数（VarCustom01、VarCustom02... VarCustom16）として、共に出力することが可能となります。

Inputs>SNMP
Variable Binding （変数バインディング）:
SNMP トラップのフィールドに、Custom Variable(カスタム変数)を関連付けることができます。以下のように、各 Trap Field(トラップフィールド)に、Custom01、Custom02... Custom16 などの Custom Variable(カスタム変数)を割り当てます。



Trap Fields(トラップフィールド)には、以下があります。

1. Community
2. Enterprise
3. Uptime
4. Agent Address
5. Version
6. OID set
7. OID set (Row OID)

アクション設定で、**Insert message content or counters**（メッセージ内容またはカウンターの挿入）リンクから、Custom fields(カスタムフィールド)として、VarCustom 変数(VarCustom01、VarCustom02... VarCustom16)が選択できます。

Custom fields(カスタムフィールド)が選択できるアクションには以下があります。

・Log to file (ファイル記録)

・Run external program (外部プログラム実行)

・E-mail message (E メールメッセージ送信)

・Send Syslog message (Syslog メッセージ送信)

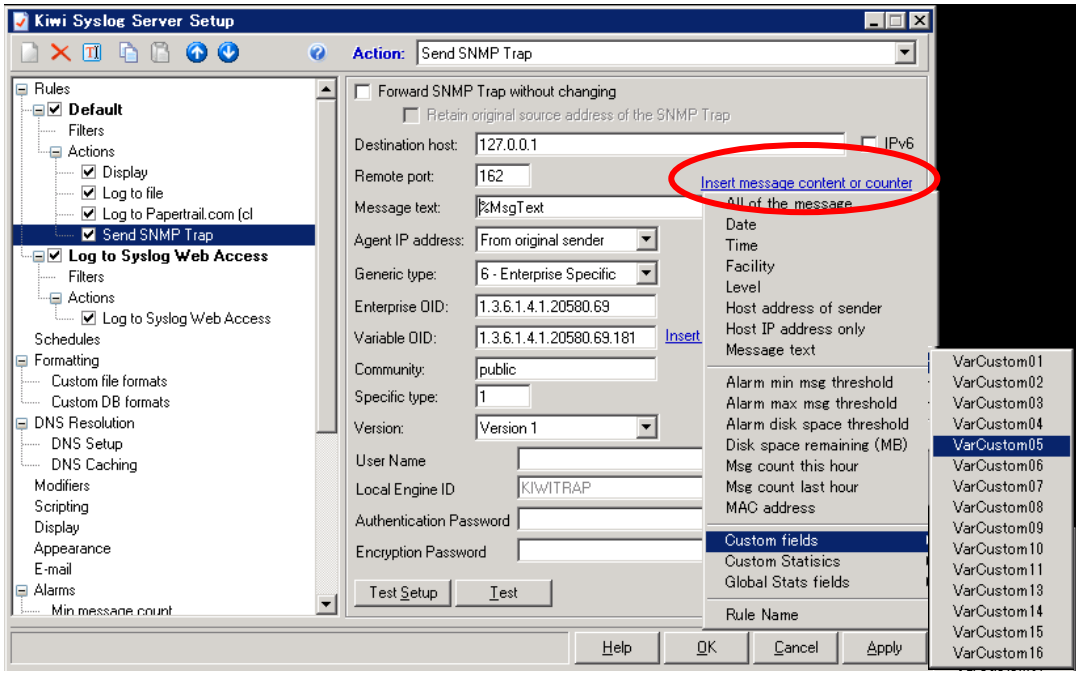
・Send SNMP Trap (SNMP トラップ送信)

・Send message via NotePage Pro (NotePage Pro 経由でメッセージ送信)

例:

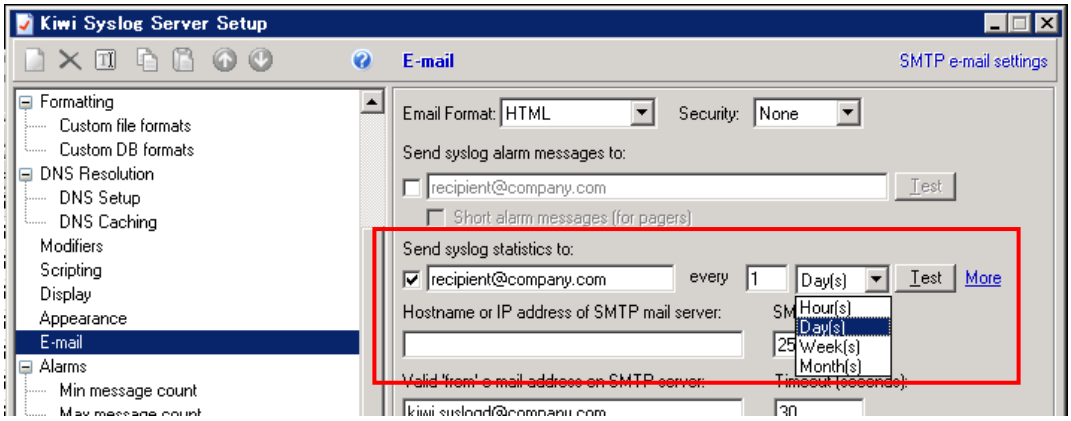
Action:Send SNMP Trap(SNMP トラップの送信)の Message text 欄に、カスタム変数を追加するために、**Insert message content or counters** (メッセージ内容またはカウンターの挿入)をクリックします。

以下の画面のように、Custom fields として、VarCustom 変数(VarCustom01, VarCustom02... VarCustom16)が選択できます。



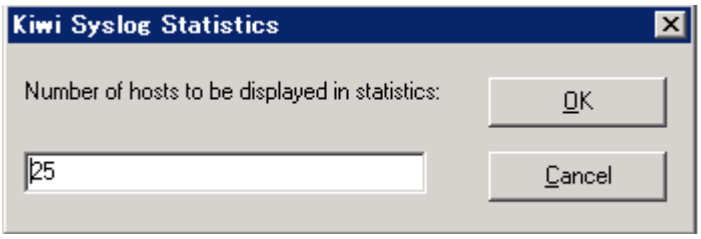
2.1.6 統計レポートのメール送信機能に毎週/毎月が追加され、レポート期間を明記。(毎時/毎日/毎週/毎月を選択可能)

E-mail 設定の **Send syslog statistics to**: (syslog 統計の送信先)を有効にすると、設定した E-mail アドレスへ統計レポートが選択した間隔(時間/日/週/月)で、電子メールとして送信されます。



統計レポートには、ログファイルのサイズ、アーカイブドライブの空き容量、メッセージ総数、メッセージ送信元の概要、ファシリティとレベルなどが記載されます。
この統計情報は、全てのカラムが並ぶように、Courier new などの固定フォントで表示することをお勧めします。これは安全に送信することができます。

More: このオプションで、統計レポートのメールに表示するホストの最大数を変更することができます。v9.5.0 からの機能です。デフォルトは 25 です。



Hours: 時間での指定は 24 の倍数と、1、2、3、4、6、8、12 の値を指定することが可能で、指定した時間間隔で統計レポートを電子メールで送信することができます。
Days: Day での統計レポートは、設定された日数に基づき、深夜 00:00 に電子メールで送信されます。
Weeks: Week での統計レポートは、設定された週の数に基づき、デフォルトでは、日曜日の 00:00 に電子メールで送信されます。
Months: Month での統計レポートは、デフォルトでは、毎月 1 日の 00:00 に、または設定した数ヶ月間隔で 1 日の 00:00 に電子メールで送信されます。

日次統計レポートの E-mail メッセージのサンプルは以下になります。
例:

```
件名:Syslog statistics for 1 Day(s) period ending on: Fri, 02 Oct 2015 00:00:03
///          Kiwi Syslog Server Statistics          ///
------------------------------------------------------------
1 Day(s) period started on:       Thu, 01 Oct 2015 00:00:04
```

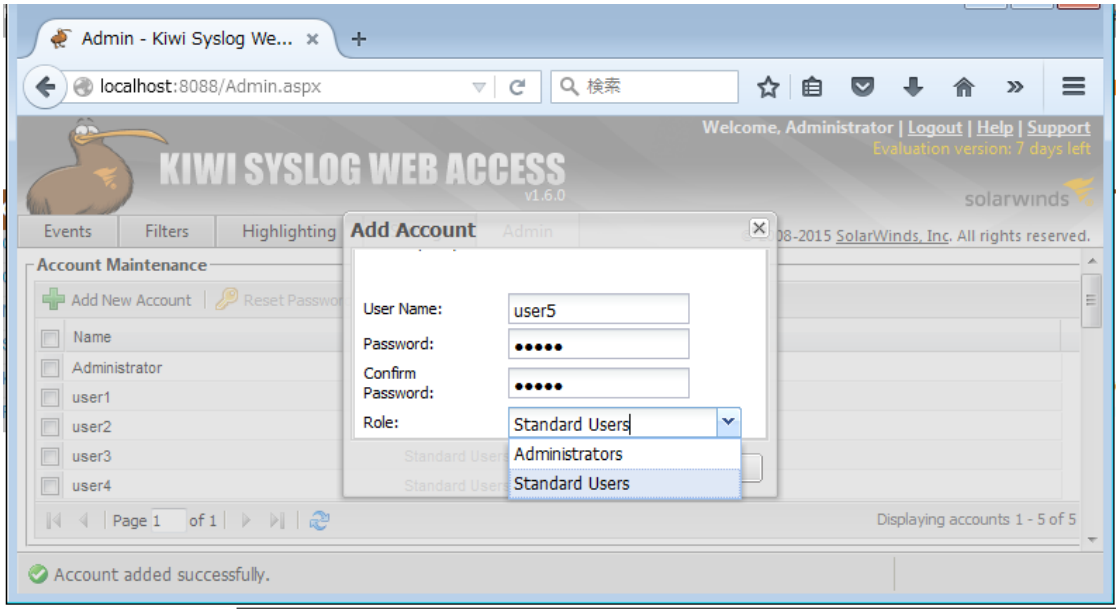
```
1 Day(s) period ending on:           Fri, 02 Oct 2015 00:00:03
Syslog Server started on:            Tue, 08 Sep 2015 17:31:26
Syslog Server uptime:                23 days, 6 hours, 28 minutes
--------------------------------------------------------

+ Messages received - Total:                        1355008
+ Messages received - Last 1 Day(s):                31605
+ Messages received - Last 24 hours:                33140
+ Messages received - Since Midnight:               31605
+ Messages received - Last hour:                    1464
+ Message queue overflow - Last hour:               0
+ Messages received - This hour:                    1393
+ Message queue overflow - This hour:               0
+ Messages per hour - Average Last 1 Day(s):        1317
+ Messages per hour - Average Last 24 hours:        1343

+ Messages forwarded:                               0
+ Messages logged to disk:                          31605

+ Errors - Logging to disk:                         0
+ Errors - Invalid priority tag:                    0
+ Errors - No priority tag:                         0
+ Errors - Oversize message:                        0

+ Disk space remaining on drive C:                  29909 MB

--------------------------------------------------------


    Breakdown of Syslog messages by sending host
+----------------------------------------+------------+--------------+
|       Top  25 Hosts                    |  Messages  |  Percentage  |
+----------------------------------------+------------+--------------+
| 192.168.30.1                           |     31605  |     100.00%  |
|                                        |         0  |       0.00%  |
|                                        |         0  |       0.00%  |
|                                        |         0  |       0.00%  |
|                                        |         0  |       0.00%  |
|                                        |         0  |       0.00%  |
|                                        |         0  |       0.00%  |
|                                        |         0  |       0.00%  |
|                                        |         0  |       0.00%  |
|                                        |         0  |       0.00%  |
|                                        |         0  |       0.00%  |
|                                        |         0  |       0.00%  |
|                                        |         0  |       0.00%  |
|                                        |         0  |       0.00%  |
|                                        |         0  |       0.00%  |
|                                        |         0  |       0.00%  |
|                                        |         0  |       0.00%  |
|                                        |         0  |       0.00%  |
|                                        |         0  |       0.00%  |
|                                        |         0  |       0.00%  |
|                                        |         0  |       0.00%  |
```

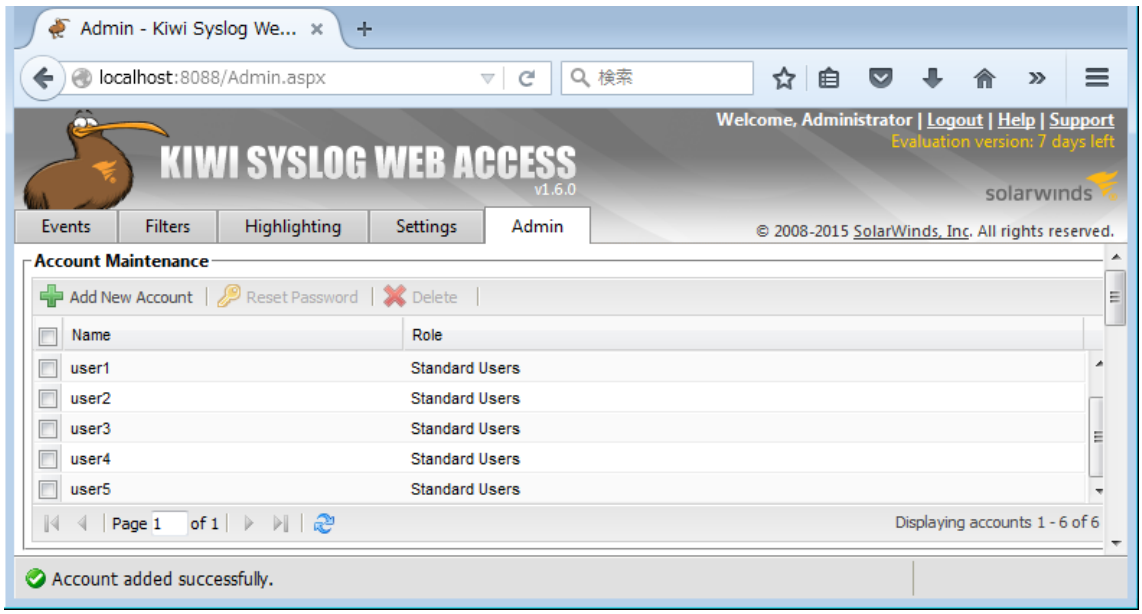
```
|                                          |         0  |        0.00% |
|                                          |         0  |        0.00% |
|                                          |         0  |        0.00% |
|                                          |         0  |        0.00% |
+------------------------------------------+------------+--------------+


    Breakdown of Syslog messages by severity
+--------------------+------------+------------+
| Message Level      |  Messages  | Percentage |
+--------------------+------------+------------+
| 0 - Emerg          |         0  |      0.00% |
| 1 - Alert          |         0  |      0.00% |
| 2 - Critical       |         0  |      0.00% |
| 3 - Error          |        10  |      0.03% |
| 4 - Warning        |     27985  |     88.55% |
| 5 - Notice         |      2393  |      7.57% |
| 6 - Info           |      1217  |      3.85% |
| 7 - Debug          |         0  |      0.00% |
+--------------------+------------+------------+

Custom statistics
-----------------
CustomStats01: 0
CustomStats02: 0
CustomStats03: 0
CustomStats04: 0
CustomStats05: 0
CustomStats06: 0
CustomStats07: 0
CustomStats08: 0
CustomStats09: 0
CustomStats10: 0
CustomStats11: 0
CustomStats12: 0
CustomStats13: 0
CustomStats14: 0
CustomStats15: 0
CustomStats16: 0

End of Report.
```

2.1.7 Kiwi Web Access のユーザーアカウントが 5 人までの制限解除

複数の管理者(Administrator)および標準(Standard)ユーザーアカウントの設定が可能となりました。

例：Administrator と user1 から user4 までの 5 つのアカウント登録がある状態で、6 つ目の user5 を追加。


Admin - Kiwi Syslog We...
localhost:8088/Admin.aspx
検索
KIWI SYSLOG WEB ACCESS
v1.6.0
Welcome, Administrator | Logout | Help | Support
Evaluation version: 7 days left
solarwinds
Events
Filters
Highlighting
Add Account
Admin
08-2015 SolarWinds, Inc. All rights reserved.
Account Maintenance
Add New Account
Reset Passwor
Name
Administrator
user1
user2
user3
user4
User Name:
user5
Password:
Confirm Password:
Role:
Standard Users
Administrators
Standard Users
Page 1 of 1
Displaying accounts 1 - 5 of 5
Account added successfully.


Admin - Kiwi Syslog We...
localhost:8088/Admin.aspx
検索
KIWI SYSLOG WEB ACCESS
v1.6.0
Welcome, Administrator | Logout | Help | Support
Evaluation version: 7 days left
solarwinds
Events
Filters
Highlighting
Settings
Admin
© 2008-2015 SolarWinds, Inc. All rights reserved.
Account Maintenance
Add New Account
Reset Password
Delete
Name
Role
user1
Standard Users
user2
Standard Users
user3
Standard Users
user4
Standard Users
user5
Standard Users
Page 1 of 1
Displaying accounts 1 - 6 of 6
Account added successfully.

2.2 修正

2.2.1 Kiwi Syslog Server v9.4.2 から v9.5 RC1 への Web Access アップグレードの問題を修正

2.2.2 Kiwi Syslog Server - 統計レポート内で同一サーバーが重複してエントリ表示される問題を修正

2.2.3 Kiwi Syslog Server - 統計レポート内のメッセージカウントが適切に午前 0 時にリセットされていなかった問題を修正

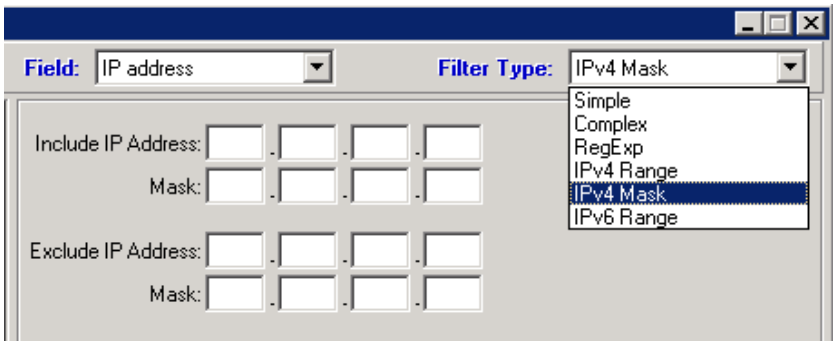
2.2.4 Kiwi Syslog Server – 統計レポートに表示されるホスト数をカスタマイズ可能

この修正について詳しくは、E-mail 設定の「More:」をご参照ください。

2.3 既知の問題

2.3.1 2003 オペレーティングシステム上での Kiwi Syslog Server で Log to Database アクションを問題なく使用するには、Microsoft のパッチ(Windows Server 2003-KB983246)が必要です。

2.3.2 Kiwi Syslog Server - IP フィルタマスク設定は、IPv4 でのみ使用可能です。



IPv6 でのフィルタマスク設定はありません。

2.3.3 IPv6 形式を使用して別のホストにトラップを転送時、送信元アドレスを保持することはできません。

3 よくあるご質問

Kiwi Syslog Server に関するよくあるご質問を以下 URL にまとめています。
疑問点、ご不明な点がある場合は、1度 FAQ をご確認ください。

http://www.jtc-i.co.jp/faq/faq_kiwisyslog.html

4 問い合わせ窓口について

正規版を弊社よりご購入された場合のお問合せは、下記の弊社カスタマーポータル
『製品サポートお問合せ』で受付けております。

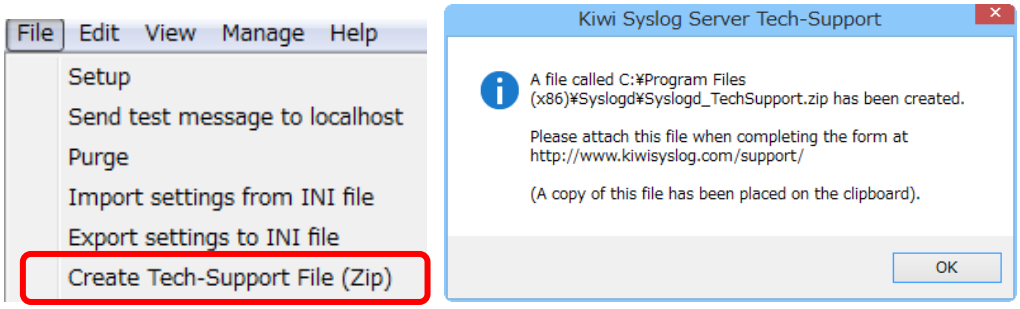
カスタマーポータル： https://www.jtc-i.co.jp/support/customerportal/index.php
使い方ガイド： https://www.jtc-i.co.jp/support/customerportal/csportalstartguide.html

「初めてご利用の方へ」から
「ご契約中のユーザー様以外の方」をクリックしていただきますと、ライセンス所有ユーザー様以外の方もお問い合わせ可能です。
（ライセンス証書に記載の K から始まる弊社管理番号が必要です）

障害時の調査が必要な場合は、次のファイルを取得し、弊社カスタマーポータルよりご送付ください。

調査ファイルの取得

1. コンソール画面で、File＞Create Tech-Support File (ZIP) を選択すると、インストールフォルダ直下に Syslogd_TechSupport.zip という調査用ファイルが作成されますので、これを取得します。



※その他障害切り分けのため、Windows イベントログの取得が必要な場合があります。

2. カスタマーポータルにログインし、『製品サポートお問合せ』で質問事項を記入し、「参照」ボタンをクリックして、Syslogd_TechSupport.zip を指定後、「送信」ボタンをクリックします。

発行日 2015 年 10 月 6 日

ジュピターテクノロジー株式会社 技術課