WinSyslog 3.7 SP1

# User Manual

By Adiscon

# Contents

# About Adiscon WinSyslog 3.7

*WinSyslog is the enhanced Syslog Server for the Windows Platform.*

Syslog is a standard protocol for centralized reporting of system events. Its roots are in the UNIX environment, but most modern devices (e. g. Cisco routers) use the syslog protocol. They report important events, operating parameters and even debug messages via syslog. Unfortunately Microsoft Windows does not include a syslog server (a syslog server is called "syslog daemon" or - short - syslogd und UNIX).

Adiscon's WinSyslog fills this gap. Prior to version 3.0, WinSyslog was known under the name of "NTSLog". WinSyslog is the first and original syslog server available on the Windows platform. Its initial version was created in 1996 just to receive Cisco router status messages. The product has been continuously developed during the past years. Version 3 represented a major stepping stone. That was the main reason we decided to rename the product.

WinSyslog can also be used in conjunction with Adiscon's MonitorWare Agent, EventReporter and ActiveLogger products to build a totally centralized Windows event log monitoring tool. More in formation on centrally monitoring Windows NT/2000/XP/2002 can be found at www.monitorware.com.

Most customers use WinSyslog to gather events reported from syslog enabled devices (routers, switches, firewalls and printers to name a view) and store them persistently on their Windows system. WinSyslog can display syslog messages interactively on-screen but also store them in flat ASCII files, ODBC databases or the Windows event log. The product runs as a reliable background service and needs no operator intervention once it is configured and running. As a service, it can start up automatically during Windows boot.

The rule/action engine introduced in version 3.3 allows very flexible configuration of WinSyslog. WinSyslog detects conditions like string matches in the incoming messages and can actively act on them. For example, an email message can be send if a high priority message is detected.

## Features

### Centralized Logging

This is the key feature. WinSyslog gathers all syslog messages send from different sources and stores them locally on the Windows system. Event source can be any

syslog enabled device. Today, virtually all devices can use syslog. Prominent examples are Cisco routers.

## Ease of Use

Using the new WinSyslog client interface, the product is very easy to setup and customize. We also support full documentation and support for large-scale unattended installations.

## Powerful Actions

Each message received is processed by WinSyslog's powerful and extremely flexible rule engine. Each rule defines which actions to carry out (e. g. email message or store to a database) when the message matches the rule's criteria. Among others, criteria are string matches inside the message or syslog facility or priority. There are an unlimited number of criteria and actions per rule available.

## Interactive Message Display

Use the WinSyslog client to interactively display messages as they arrive. Message buffer size is configurable and only limited by the amount of memory installed in the machine.

## Freeware Mode

We care for the home user! WinSyslog can operate as freeware in so-called "freeware mode" without a valid license. It supports a scrolling interactive display of the 60 most current messages for an unlimited time. This feature is most commonly requested for home environments. And: even our free copies come with Adiscon's great support!

## View Syslog Messages via the Web

Never need to look at plain text files! WinSyslog comes with a fully functional sample ASP application that will display the contents of WinSyslog generated database entries.

The  web interface is not included in the core product and needs to be downloaded separately at

www.winsyslog.com/en/FAQ/How-can-I-view-syslog-messages-via-web.asp

It is just a few kilobytes in size.

## Syslog Hierarchy

WinSyslog supports cascaded configurations most commonly found in larger organizations. In a cascaded configuration, there are local WinSyslog instances running at department or site level which report important events to a central WinSyslog in the headquarter. There is no limit on the number of levels in a cascaded system.

## Email Notifications

WinSyslog emails received events based on the user defined rule set. Email notifications can be sent to any standard Internet email address, which allows forwarding not only to typical email clients but also pager and cellular phones. The email subject line is fully customizable and can be set to include the original message. That way, pagers can receive full event information.

## Store Messages Persistently

The WinSyslog server process stores all messages persistently. So later auditing and review of important system events is possible without effort. Messages can be written to flat ASCII files,  ODBC data sources and the Windows event log.

## Full Logging

WinSyslog logs the received syslog message together with it's priority and facility code as well as the sender's system IP address and date. It is also able to log abnormally formatted packages (without or with invalid priority/facility), so no message will be lost.

## Full Windows 2000 and XP Support

We have full Windows 2000 support since Windows 2000 ships! WinSyslog versions 3.6 and above are specifically designed for Windows XP and support advanced features like the new themes and fast user switching.

## Robustness

WinSyslog is written to perform robust even under unusual circumstances. Its reliability has been proven at customers sites since 1996.

## Minimal Resource Usage

WinSyslog has no noticeable impact on system resources. It was specifically written with minimal resource usage in mind. In typical scenarios, it's footprint is barely traceable. This ensures it can also be installed on heavily loaded servers.

## Firewall Support

Does your security policy enforce you to use a non-standard syslog port? WinSyslog can be configured to listen on any TCP/IP port for syslog messages.

## NT Service

The WinSyslog service is implemented as a native multithreaded Windows NT service. It can be controlled via the control panel services applet or the computer management MMC (Windows 2000).

### Runs on large Variety of NT Systems

NT 3.5(1), 4.0 or 2000; Workstation or Server - WinSyslog does run on all of them. We also have Compaq (Digital) ALPHA processor versions on platforms supporting this processor (service only, available on request).

### Double Byte Character Set Support (e. g. Japanese)

WinSyslog supports characters encoded in double byte character sets (DBCS). This is mostly used with Asian languages like Japanese or Chinese. All DBCS strings are correctly displayed and written to the log targets (database or flat file). However, the sending side must also be able to process DBCS correctly. As an example, Adiscon's event monitor for Windows, EventReporter, does so. For details on EventReporter please visit www.eventreporter.com.

### Multi-Language Client

The WinSyslog client comes with multiple languages ready to go. Out of the box, English, German, Japanese and Spanish are supported. Languages can be switched instantly. Language settings are specific to a user.

Additional languages can be easily integrated using Adiscon's brand new XML based localization technology. We ask customers interested in an additional language for a little help with the translation work (roughly 1 hour of work). Adiscon will than happily create a new version. This service is free!

## Components

### WinSyslog Client

The WinSyslog Client is used to configure all components and features of WinSyslog. The client can also be used to create a configuration profile on a base system. That profile can later be distributed to a large number of target systems.

The WinSyslog Client is also used to interactively display syslog messages.

The client can also operate in "freeware mode". In this mode, no license is necessary. A scrolling display of the most current 60 messages is available in freeware mode.

### WinSyslog Service

The WinSyslog Service runs as an NT Service and coordinates all message processing and storage.

The service is the only component that needs to be installed on a system that is acting as a syslog server. The WinSyslog service is called the product "engine". As such, we call systems with only the service installed "engine-only" installations.

The WinSyslog service runs in the background without any user intervention. It can be controlled via the control panel "services" applet or the "Computer Management" MMC under Windows 2000.

Due to its optimized structure, WinSyslog uses only very minimal system resources. How much it uses mainly depends on how many syslog messages are to be processed.

# System Requirements

WinSyslog has minimal requirements.

The WinSyslog client needs roughly 10 MB of disk space. The WinSyslog client is optional and needs not to be present on a production system.

Engine-only installations require roughly 400 KB of disk space and 4 MB of virtual memory. Please note that this is not actually used RAM - RAM usage is roughly 2 MB.

Please note that WinSyslog is developed under Windows 2000. It is tested both under Windows 2000 as well as NT 4.0. It has been tested and developed to meet the "Designed for Windows XP" logo requirements. The client does not work under Windows NT 3.5(1). However, although not tested under NT 3.5(1), we do not see any reason why the service shouldn't perform well in this environment. WinSyslog runs on top of Windows NT/2000/XP server and Windows NT Workstation / Windows 2000 Professional. It also runs under both Windows XP professional and home edition.

As Windows 9x and Windows Me do not support services, the service features are not available under these operating systems. File logging is supported via the client, only in this environment.

The default install set (most probably the one you found this documentation in) contains the executable for the Intel platform. However, there is an ALPHA version available on request. As ALPHA is not supported for Windows 2000 and above, there is no version for these platforms available.

# Getting Started

## Setup

I

nstallation is quick and easy. Typical users just need to run the setup program and follow on-screen instructions. Besides that, WinSyslog is enterprise-enabled and provides features to facilitate mass rollouts. Thus it has two setup modes:

- Full Install
- Engine-Only Install

***Attention Home Users***

*If you are a home user, you most probably want to setup WinSyslog with the default settings in Full Install mode. To do so, simply run the supplied setup program and follow on-screen instructions. There is no need to use the "engine only" install set.*

The full install includes both the WinSyslog client and service. In large environments, this is typically installed on a "master machine" being used to create the configuration parameters. The Engine-Only install includes the WinSyslog service only. In large environments, that is the install process used primarily on a larger number of target machines.

All users are highly encouraged to use the full install. It is the default install set downloadable from the WinSyslog web site.

Adiscon uses the Microsoft Windows Installer service for it's software installations. This is the new standard highly recommended by Microsoft. Using Windows Installer also enables software distribution via the Active Directory. Please note that for simplicity reasons our download sets include a copy of the Windows Installer service for those systems that do not have it already installed. As such, WinSyslog can be installed on any Windows system without problems. If you plan to do a mass rollout on systems that already have installed the Windows installer service, you can also request the pure MSI file from Adiscon. Please direct inquiries to support@adiscon.com.

### Full Install

The install set (the ZIP file you downloaded) contains a standard setup pro gram and it's necessary helper files. Please unzip the archive to any directory you like. This can be a local drive, a removable one or a remote share on a file server. A Win32 Unzip program can be found at www.winzip.com.

After unzipping, simply double-click "setup.exe" and follow the onscreen in structions.

There are also self extracting exe files available for download. If you downloaded these versions, there is no need to separately unzip the program. The self extracting version might also start the setup process automatically.

Setup.exe will install the WinSyslog client and copy the Service process to disk. However, it will not install the service itself. In order to do that, start the client and select "File"/"Install Service". This will install and enable the back ground process. Interactive viewing of syslog messages is possible without installing the WinSyslog service.

If you have Windows Installer already present on the target system, you can also setup the product by simply double clicking the .MSI file. Windows Installer is present on all Windows 2000 / XP systems.

## Engine-Only Install

There is no GUI setup program for an engine-only installation. The main purpose of this install mode is to roll out the product to a large number of machines. We encourage users performing a single or a few installations to use the "Full Install" set as the engine only install requires in depth knowledge of Windows, mass rollout methodologies and the WinSyslog product.

Actual installation, however, is straightforward

1. Copy WinSyslg.exe to any location you like (on the machines local hard drive)
2. Install it as a service by running "WinSyslg -i"
3. Use REGEDIT to customize its settings - or import a registry file (*.reg)

***Important***

*Please be sure to copy WinSyslg.exe to a directory on a* ***local*** *drive. The install process (WinSyslg -i) will install the service to run from the current working directory. If that is not on the local drive, you need to have access privileges to the file server WinSyslg.exe is stored on. The default service account - local system - does not have such privileges. Thus service startup will fail. If you need this setup, be sure to set the service account to someone with sufficient privileges (via control panel services applet).*

Customization of the WinSyslog service is via the registry. Modifications can be made directly via REGEDIT (see documentation on how to do that) or via the WinSyslog client (which must then be installed). Please note that the registry "Parameters" key

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AdisconWinSyslog\Parameters

can be exported to a .reg file and re-imported by calling REGEDIT. As such, a mass rollout can be fully scripted by the following batch file:

```
copy \\server\share\winsyslg.exe c:\some-local-dir
cd \some-local-dir
winsyslg –i
regedit \\server\share\configParms.reg
```

Users of any prior NT service versions of WinSyslog should uninstall the old version via "ntslog -u" before installing the new one. This is important as no two versions of the product can be running at the same time. If the automated setup process is used, there is no need to uninstall a previous version.

# Creating an Initial Configuration

Do you want results fast? If you know about computers and networking services, these steps will bring quick results:

- run setup.exe if not already done so (follow the on-screen instructions)
- if you just want to view syslog messages interactively, start the WinSyslog client and click the start button - that's all you need to do
- If you would like to use the enhanced features (like database or file logging), you need to configure the service. Do **not** start the interactive display! Follow these simple steps:
    1. Start the WinSyslog client and then the rule wizard - it should automatically start. If it doesn't start it via the "Rulebase" menu. Be sure to complete the wizard - if you don't do so, WinSyslog will not take any useful actions!
    2. Configure the service settings via the appropriate tabs in the client. You need to configure only the settings that you have selected rules for (e.g. if you just selected ODBC logging, you do to supply the ODBC parameters only - not the SMTP, file or any other ones.
    3. Start the WinSyslog service (if not already running). You can do so via the client or with the "Services MMC" (Control Panel in Windows NT). Once again: make sure you did not start the interactive display!

That's all you need to do to get a basic configuration working. However, we do strongly recommend that you read about the rule engine if you are interested in the advanced features. The reason is simple: the rule engine is WinSyslog's workhorse. It allows extremely flexible and advanced configuration. However, you need to know how it works in order to fully utilize it's potential.

# The WinSyslog Client

*The WinSyslog clients both allows interactive viewing of Syslog Messages and configuring the service parameters.*

The WinSyslog Client is used to customize the product. It doesn't need to be installed in order to process syslog messages. In fact, we recommend so-called "engine only installations" if a large number of WinSyslog servers is to be installed in a cascaded environment.

The client loads the configuration parameters upon startup. Modifications are saved by clicking the "OK" button. This will also terminate the application. If you just want to apply the changes, click the "Apply" button. Clicking the "Cancel" button will close the WinSyslog Client without saving any modifications.

**Important**: The WinSyslog services itself reads configuration information only at service startup. So you need to stop and re-start the service to activate a new configuration. Keep this in mind especially when modifying the rule base. The service can be restarted from the client.

## Launching the WinSyslog Client

To run the WinSyslog Client, click the "WinSyslog Client" icon present in the WinSyslog program folder located in the Start menu.

The WinSyslog Client can also be launched from the command prompt:

- Open a Command Prompt window
- Change to the drive and directory where the WinSyslog software is installed (default: "\Program Files\WinSyslog")
- Type "WINSyslogClient.exe" and hit enter.

## Windows XP Limited Users

Windows XP limited users can use the WinSyslog client real-time logging features to view syslog messages. However, they are not allowed to change any service configuration settings or start or stop the service. You need to be a full user to perform these tasks. The same is true for non-administrative users under Windows NT or 2000.

This behavior is by design and meant to protect the configuration set up by the machine administrator.

# The Real-time Logging Tab

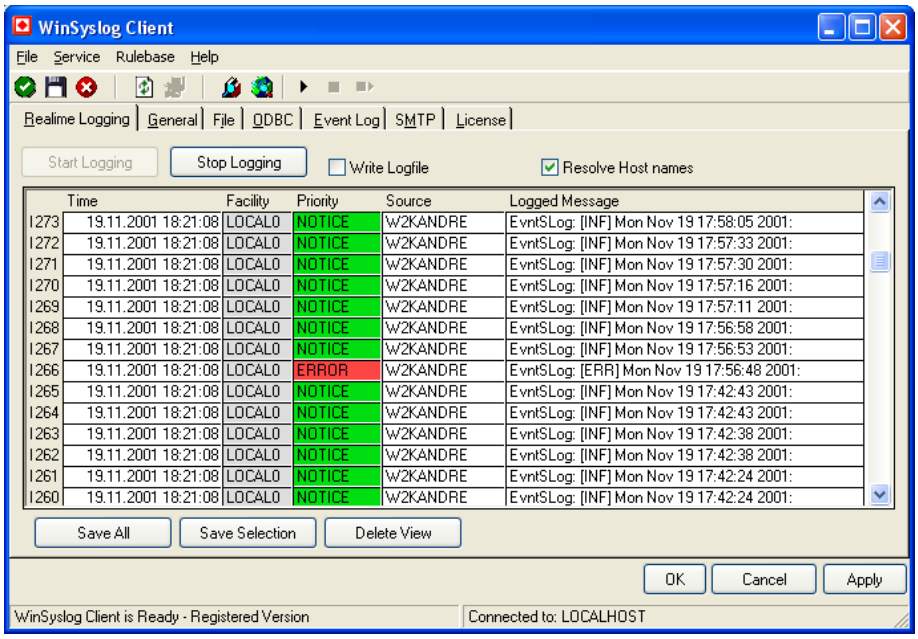
Real-time logging enables the client to log syslog messages itself (without the help of the service). Real-time logging is an excellent option for interactive debugging and product setup. For background logging, we strongly recommend using the WinSyslog service.

Real-time logging is also supported under Windows 9x and Windows Me systems.

There is also an online seminar available on WinSyslog's real-time logging. To view it, please visit our Seminar's Online Site

www.winsyslog.com/Common/en/SeminarsOnline/WinSyslog-Seminars.asp

and select "WinSyslog real-time logging Explained".



WinSyslog Client - Realtime logging Tab

## Start / Stop Logging Buttons

These buttons start and stop real-time logging. Once started, the client will log all incoming messages until logging is stopped by the user. Messages are written to a circular buffer. That means if the maximum buffer size is reached, new messages will be stored, but older messages will be removed from the buffer. This allows the client to run for extended periods of time without taking up to much system memory. The buffer size is configurable. New messages are always displayed on top of the list. Older ones are towards the bottom.

## Write Logfile

If checked, all messages are written to a log file in addition to the interactive display. Please note that this option influences the client only. If you would like to provide a reliable long term log, we strongly suggest to use the service. It's file logging parameters are customized under the "file tab".

## Resolve Host Names

If checked, the sender is displayed as a host name instead of the IP address. This is often useful to quickly see the system that sent the message. Please keep in mind, though, that the host name resolution takes a little bit of time (especially if a host can not be resolved) and as such should not be used on a loaded system.

## Save All

Used to save the current buffer contents to a comma-delimited file (so called CSV format). All entries dis played in the grid are written.

## Save Selection

Also saves a comma-delimited file. However, only messages selected (highlighted) will be written to the file.

## Delete View

Erases all messages from real-time display.

# Rules

Rules are the workhorse of WinSyslog. Except for the interactive display, all actions and processing carried out is configured by the rules defined. Rules are configured by the client and processed by the so-called "rule engine" inside the WinSyslog service.

There is also an online seminar available on WinSyslog's rule engine. To view it, please visit our Seminar's Online Site at

www.winsyslog.com/Common/en/SeminarsOnline/WinSyslog-Seminars.asp

and select "WinSyslog Rule Engine Processing Explained".

You might already know something similar to the WinSyslog rule engine. Rule engines and rule bases are an extremely powerful tool and in widespread use in the industry. Examples of rule bases can be found at Checkpoint's Firewall One Firewall Rule Base or Cisco Routing filter - just to name a few.

The rule base consist of the rules as configured in the client. The rule engine is the process carrying out the rules. A rule base can contain no, one or an unlimited number or rules. However, if there is no rule at all defined, no action will ever be carried out by WinSyslog. Consequently, the client will issue a warning message in this case.

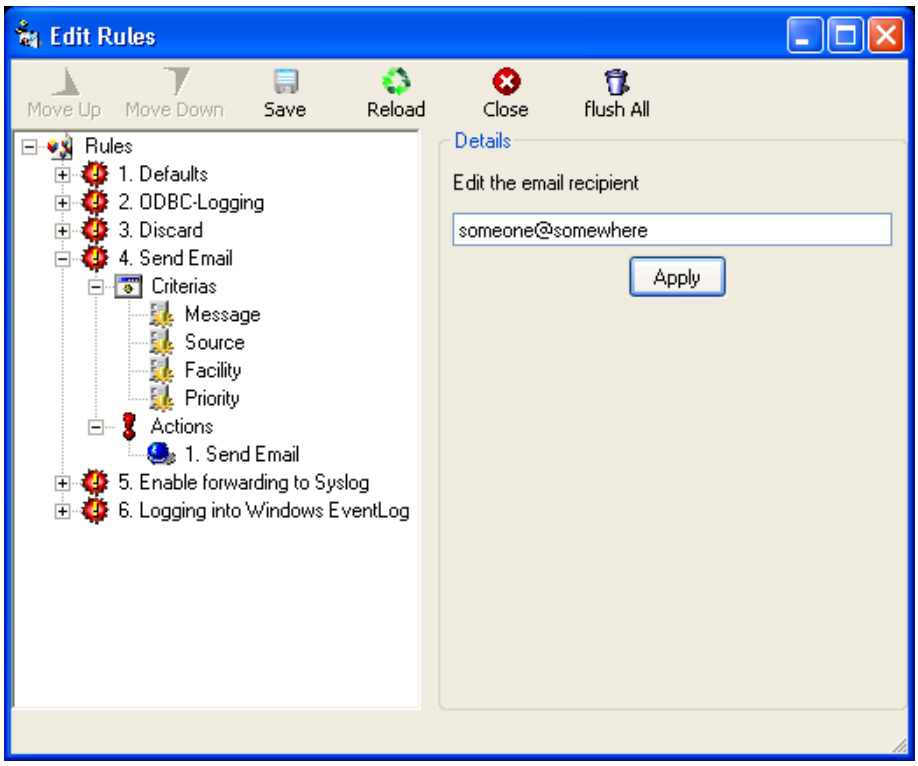
A rule has a description and associated match conditions and actions. The match conditions are called "criterias". These specify, when a rule is to be carried out. Again, there can be no, one or many criterias for a single rule. If there is no criteria, the rule will always match. This is useful in many cases. If there is more than one criteria, all criterias need to match in order for the rule to match (logical AND).

Actions associated with a rule specify what to do when the associated rule matches (and only the associated rule). Actions carry out the actual processing of a messages. For example, actions include logging a message to a flat file or database, sending it via email or forwarding it to another syslog daemon. There can be no, one or an unlimited number of actions associated with a rule. However, if no action is

associated, the rule will not have any effect. Consequently, the client will issue a warning when writing the rule base. Rules without actions can be useful to temporarily disable a rule with complex criterias. If there are multiple actions, they are not guaranteed to be carried out in any specific order. If you definitely need an action to be carried out before another one, you currently need to define two rules.

Actions can be modified with action modifiers. These are the strings attached to a specific action. Action modifiers allow to customize a specific behavior of this action. It modifies only this action and only this one, other actions of the same type are not affected - regardless if the appear in the same rule or a totally different one. The use of the action modifier depends on the type of action. For example, with syslog forwarding it is the host the syslog message is to be forwarded to. With ODBC database logging it is the DSN and so on. If there is no action modifier, the values configured in the client's configuration tabs will be used. They are also used for all values that can not be modified via the action modifier (e.g. the SMTP server address for email forwarding).

Below find a screenshot of a rule base with a number of rules, criteria and action modifier:




## Sample Rule Base

But now that we know the elements, how are rules being processed? It's easy. Rules are strictly processed from top to bottom, or from number 1 to the last one (number 6 in our sample). Each rule is checked to see if it matches. If it does, all associated actions are carried out. Then, the rule engine advances to the next configured rule. Once again, it checks if it matches and - if it does - carries out the actions associated with that rule. Then come the next rule and so on. The rule engine stops when there are no more rules to be evaluated. It also stops if a rule contains a "discard" action.

The "discard action" is a very special and powerful action. It does not actually carry out any processing. In fact, it disables all further processing for a message as soon as

it is found by the rule engine. Have a look at rule number 3 above. It contains the discard action. If a message matches that rule, actions 4, 5 and 6 will not be evaluated. even if there were a match in these rules, their actions won't be carried out. So what is the discard action good for? It is used to handle common situation where a number of well know messages - unimportant messages - should be filtered out so that the other rules do not need to take care of these messages. In many other products using rules bases, this is called the "block rule". Please note that with Adiscon's rule engine, there can be multiple block rules at multiple layers of the rule base giving you additional flexibility.

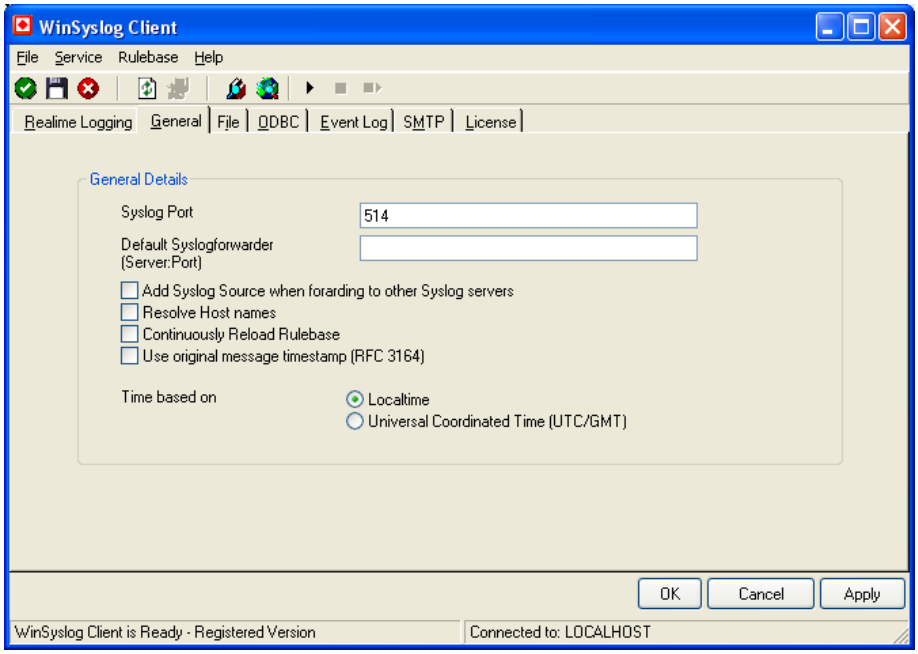
One last thing to mention: the rule base is applied to each and every message arriving at WinSyslog. By design, there is no way to modify the behavior of the rule base for the next message to be arrived. This ensures an always consistent processing of incoming messages.

While building and testing your rule base, please keep in mind that the WinSyslog service by default needs to be restarted to load a modified rule base. The reason is that the services does not re-read the rule base to save system resources. However, if you would like to have it always obtain a fresh copy of the rule base, you can do so via the "General" tab. There is a setting "Continuously Reload Rulebase" that will force the service to check if there is a new rule base and, if so, load it. The check will be made for every message received. This option is very useful when testing a new rule base. However, for performance reasons we recommend turning it off during production use. Please note that even if it is turned on, the rule base is only reloaded if needed. We check first to see if there are any changes. So it is an overall quick process - but one that typically needs not to be done once the final rule base has been created.

**Important note to WinSyslog 3.0, 3.1 and 3.2 users:** the rule engine supersedes the functionality of the action specific enabled/disable actions on the file, ODBC, etc. tabs of the client. Please note that actions can only be carried out by rules. So it is absolutely vital to configure rules in order to let WinSyslog do any useful work. The Rule wizard imports any pre 3.3 actions and converts them to rules if found.

# The General Tab

This tab contains general configuration parameters.




WinSyslog Client - General Tab

## Syslog Port

Port the WinSyslog service listens to. If left at 0, the default port from the system services database is used. This is the best value for most installations. If an different port is required by the reporting devices, enter the decimal port number. All syslog communication is via UDP.

## Default Syslog Forwarder

The default syslog server forwarded messages should be send to. Can be either a resolvable computer name or IP address. Forwarders are contacted via port 514/UDP by default. If you would like to forward to a different port, specify the port number after a colon (e.g. 127.0.0.1:10514 for the localhost).

The syslog forwarder can be overwritten with an action modifier in the rule base. Action modifiers can include also a port number in the format "server**:**port" (e. g. "10.1.1.1:10514" to send to port 10514/UDP).

## Add Syslog Source when forwarding to other Syslog servers

This option can be used to include the original Syslog source when forwarding a message to another Syslog server. This option is very useful for large scale solutions. For example if you have some Syslog servers that are forwarding all messages to a central Syslog server, you would not lost the original source.

## Time based on

Time can be expressed either in Universal Coordinated Time (UTC, formerly know as Greenwich Mean Time - GMT) or local time. Local time represents the time of you time zone (as set in the Windows international properties). UTC is a standard

time format that is the same all around the world. Based on your timezone, UTC will be some hours different from your local time. We recommend using UTC only if you need to have log information consistent across different time zones.

### Resolve Host Names

If checked, the message source IP address will be resolved to a host name. Standard DNS lookup processes are used to perform this task, so the success of this option is dependent on correct reverse DNS setup. If you check this option and host names do not resolve, please see your DNS administrator.

Resolving host names is a big plus if you monitor a large number of systems. With host name resolution, you will see the actual host names instead of the IP addresses.

### Continuously Load Rule Base

If checked, the service will continuously check for changes to the rule base. Otherwise it will only load the rule base on startup. A more thorough description can be found in the "Rules" section.

### Use the message timestamp

If checked, WinSyslog will use the timestamp inside the syslog message instead of the time of message receipt. This is compliant to the syslog RFC. Using the timestamp included in the message has a number of drawbacks, most notably there is no time zone information in it. So if you monitor devices in multiple time zones, the times logged by WinSyslog will be mixed up. As such, we recommend using the timestamp of message reception.

## The File Tab

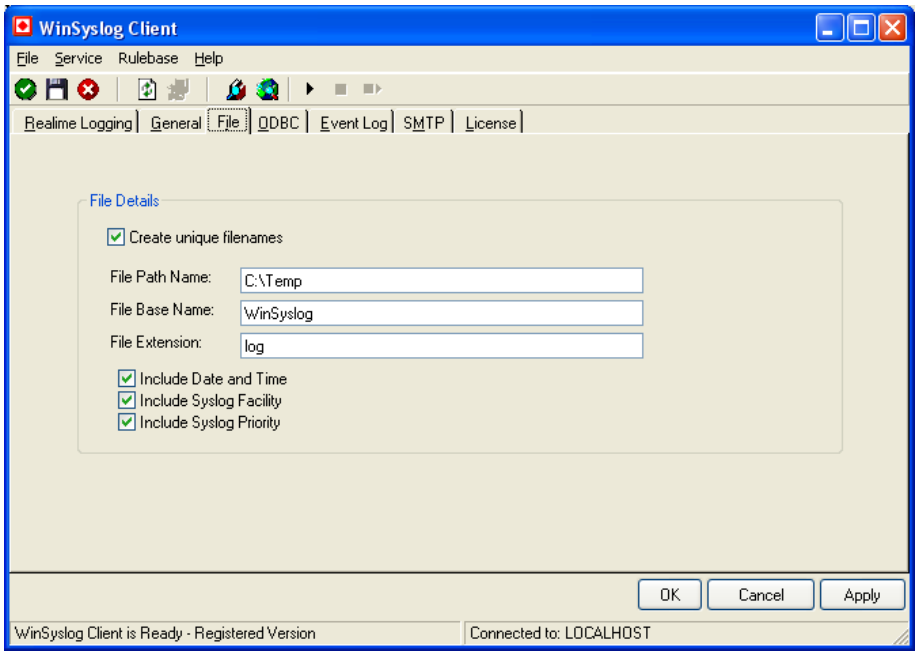
Configuration parameters for file logging. These parameters are written by the WinSyslog service. File logging is used to write a flat ASCII file of received event entries. One file per day is written. New entries are appended to the end of the file.

File locks are released when currently no data is written. So other applications can access the files while the service is running. However, please be sure that the other applications do not place a file-lock onto it. Popular WordPad does so. In this case, the service will not be able to log any further messages (an error event is written to the NT event log in this case). We recommend copying the file when accessing it at runtime - or use notepad.exe, which does not place file-locks on the files it opens.

**The filename is build as follows**:

<FilePathName><FileBaseName>-year-month-day.<FileExtension>

with the parameters in brackets being configured via the dialog.




WinSyslog Client - File Tab

## Create unique filenames

If checked, unique file names as described above are created for each day. If unchecked, WinSyslog does not create a new file each day. The date specific part is simply dropped, as such all data is written to a single file. The user is responsible for cleaning up this file from time to time. This setup is typically used when a third party file monitor monitors the WinSyslog log files.

## File Path Name

The base path (directory) of the file. Please see above for exact placement. Default is "".

## File Base Name

The base name of the file. This is the part before the date specific information. Please see above for exact placement. Default is "".

The file base name can be overwritten for a particular action. Use a corres ponding action modifier.

## File Extension

The extension to be used when writing the file. Please see above for exact placement. Default is ".log".

### Include Date and Time

If checked, the timestamp is included in the log file. If unchecked, there will be no such information (but the timestamp is most probably part of the logged message, too).

### Include syslog facility

If checked, the syslog facility is included as a separate field in the log file. If unchecked, the information is discarded. There is no way to reconstruct it later on.

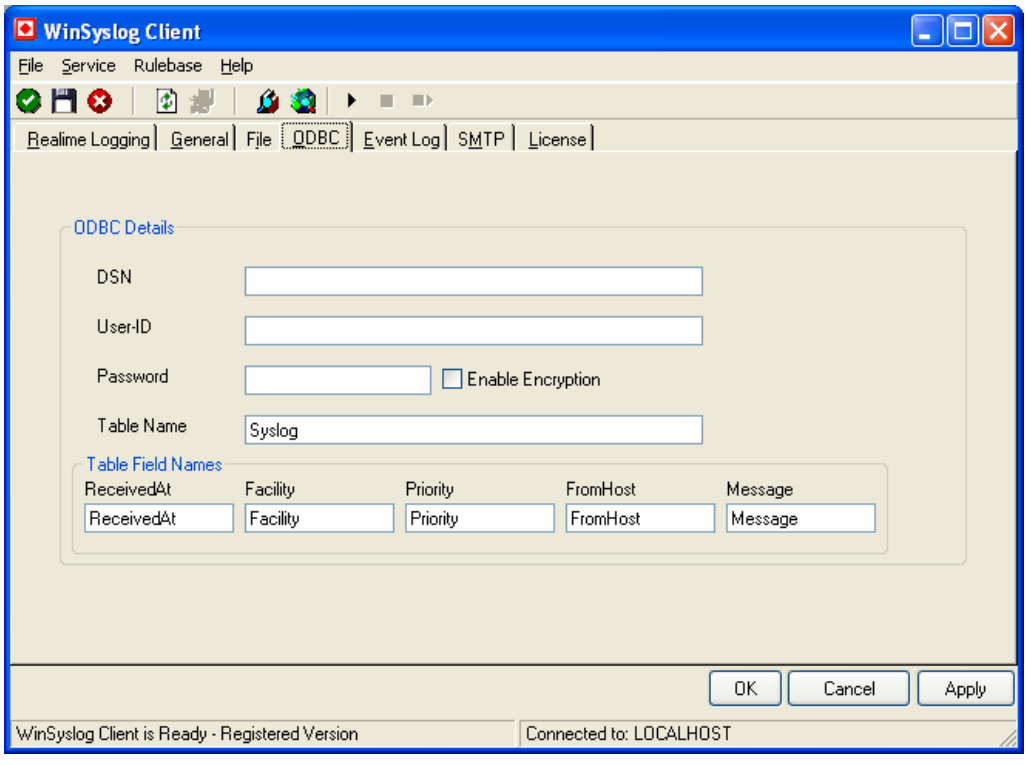
### Include syslog priority

If checked, the syslog priority is included as a separate field in the log file. If unchecked, the information is discarded. There is no way to reconstruct it later on.

## The ODBC Tab

Configuration parameters for the WinSyslog service. This tab controls database logging.

Database logging allows to write incoming events directly to any ODBC-compliant database (virtually any database system currently available for the Windows operating system supports ODBC).




WinSyslog Client - ODBC Tab

The name of the system data source (DSN - data source name) to be used when connecting to the database. Create this in ODBC manager (can be found in control panel under Windows NT). Important: it must be a system DSN, not a user or file

DSN. The DSN must be configured to have the correct connection parameters (for example database type and name, server name, authentication mode, etc.).

The DSN to use can be overwritten on a per-action basis. To select a different one, select the correct action modifier when defining the rule base.

## User-ID

The user id used to connect to the database. It is dependant on the database system used if it must be specified (e. g. Microsoft Access does not need one, while Microsoft SQL Server can force you to use one). If in doubt, please see your database administrator.

## Password

The password used to connect to the database. Must match the "User ID". Like the user id, it is dependant on the database system if a password is needed. Passwords can be stored either encrypted or unencrypted. We highly recommend storing them encrypted.

## Enable Encryption

Check to store the ODBC password encrypted. If left unchecked, the password is stored unencrypted. We strongly recommend checking this box.

If you store the password unencrypted for some reason, please be aware of the security implications. In this case, we recommend using an account with limited access privileges, only.

## Table

The name of the table to log to. This name is used to create the SQL insert statement and must match the database definition. Default is "syslog".

## Table Field Names

These 5 settings allow you to override the default field names to be used when storing data into the syslog table. You can change as many fields as you like.

***Important***

*The default name for the message field - "Message" is a reserved name on Sybase database systems. If you would like to log to a Sybase database, you must change that field name. Otherwise you will receive an ODBC error (visible in NT Event Viewer). We are unfortunately not able to change the default, as this would break many existing logging environments.*

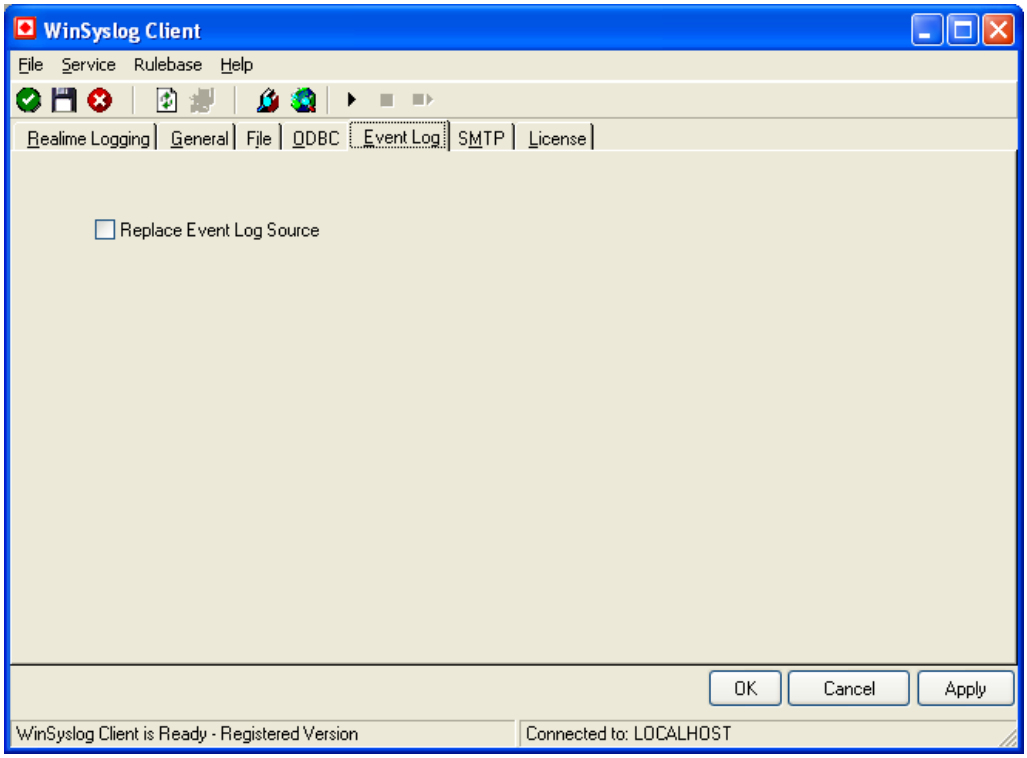
A sample jet (Microsoft Access) database file is included in the WinSyslog install set. If you would like to create the default database on SQL server, please use the following script:

```
CREATE TABLE [dbo].[Syslog] (
[ID] [int] IDENTITY (1, 1) NOT NULL ,
[ReceivedAt] [datetime] NULL ,
[Facility] [smallint] NULL ,
[Priority] [smallint] NULL ,
[FromHost] [nvarchar] (60) NULL ,
```

[Message] [text] NULL
) ON [PRIMARY] TEXTIMAGE_ON [PRIMARY]
GO

# The Event Log Tab

This tab is used to configure the WinSyslog service's logging to the Windows NT / 2000 or XP event log.




WinSyslog Client – Event Log Tab

## Replace Event Log Source

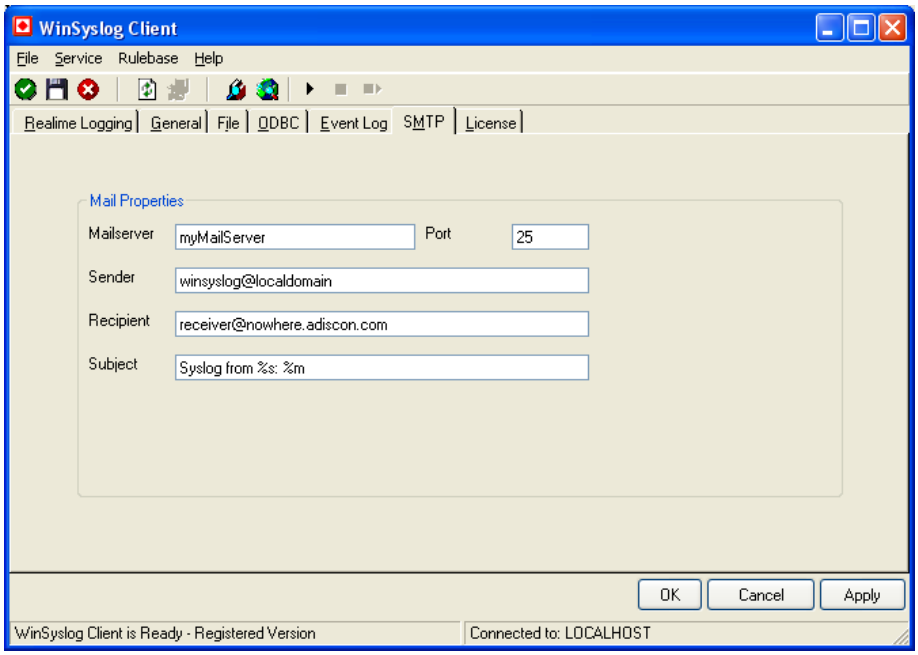
If checked, a special mapping mechanism is activated. In this mode, the Windows event source is set to the IP address of the system sending the syslog message. Also, the ID is set to syslog facility. This mode helps to quickly gather information about the system state in Windows event viewer.

**However, this mode has its drawbacks.** Effectively, we are writing invalid event source information to the event log. This does not harm any application, but Windows event viewer will try to locate the matching message libraries. Of course, this is impossible. As such, event viewer will warn the user that the message library could not be found. Nevertheless, it will display the whole logged message. This happens only in detail view.

Users should fully understand the implications of this mapping mechanism for their environment before turning this option on.

# The Mail Tab

This tab is used to configure the WinSyslog service's mail (SMTP) parameter. These here are the basic parameters for email forwarding. You need to configure them if you would like to forward messages via email.




WinSyslog Client - File Tab

## Mailserver

Name or IP address of the mail server to be used for forwarding the messages. Please note that this server must be able to relay messages if the recipient is not hosted at this server. Be sure to contact your mail server's administrator if in doubt on this issue.

WinSyslog expects to talk to a standard SMTP mail server.

## Port

Port the mail server is to be contacted at. Usually, this is 25. It might, however, be changed by in your system. Then, specify the port your mail server uses. If in doubt, try the default of 25 - or contact your mail server administrator.

## Sender

Email address used as the sender address for outgoing messages.

## Recipient

The recipient emails are addressed to. The recipient can be overridden with an action modifier for each specific rule and action.

## Subject

Subject line to be used for outgoing emails. The subject line being is used for each message sent. It can contain replacement characters to customize it with event details. This is especially useful when sending email to cellular phones or pagers, which often display only the subject line and not the actual message body. The subject line – after expansion of the replacement characters – can hold a maximum of 255 characters. Characters beyond this will be truncated. Please note that some email systems do impose a stricter limit and truncation as such might occur before the 255 character limit.

The following replacement characters can be used inside the subject line:

**%s** IP address or name (depending on the "resolve hostnames" setting) of the source system that sent the message.

**%f** numeric facility code of the received message

**%p** numeric priority code of the received message

**%m** the message itself. Please note: this is the complete message text and can be rather lengthy. As such, it is most probably subject to truncation. If that occurs, all other information after the %m replacement character is also truncated. As such, we strongly recommend using the %m replacement at the end of the subject line only.

**%%** represents a single % sign.

In the example above, replacement characters are being used. If a message "This is a test" was received from "172.16.0.1", the resulting email subject would read:

Syslog from 172.16.0.1: This is a test

The mail body will also include full event information, including the source system, facility, priority and actual message text. As there is no size limitation for message bodies, the body always contains the full message received.

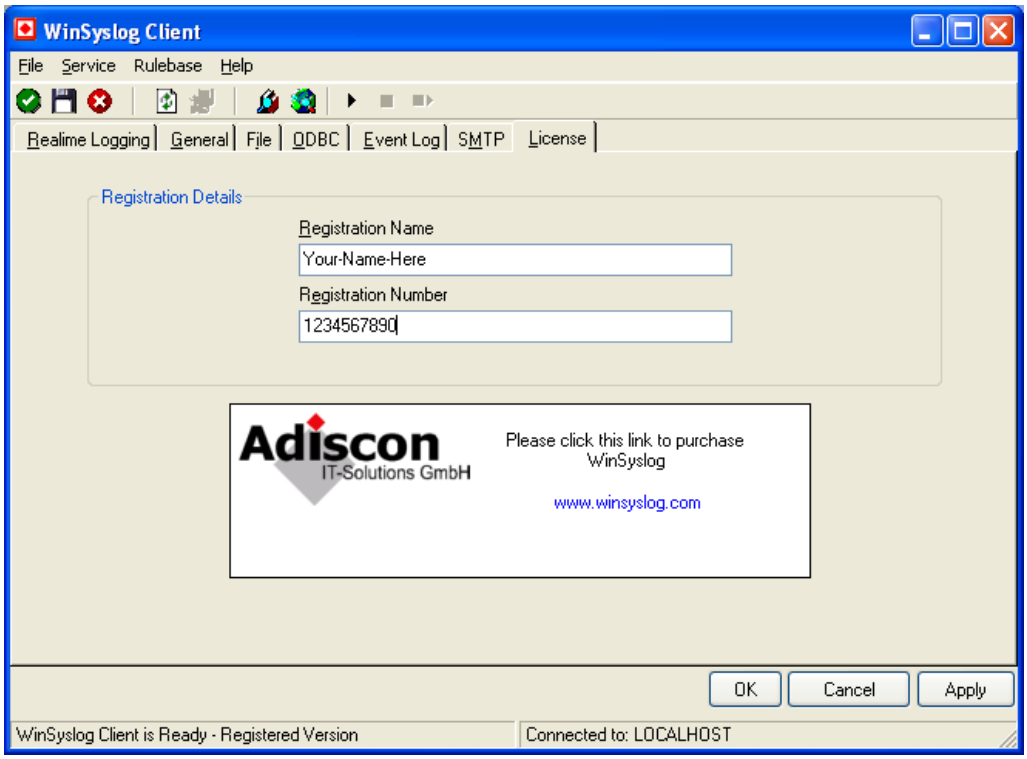
There will be one email for each received message. Email delivery is meant for urgent notifications and actions (e. g. calling pagers and such). It is not meant to provide an email report.

# The License Tab

The license tab is used to activate your WinSyslog installation after purchase.

After evaluation, WinSyslog can be activated just by entering a correct registration name and number. There is no need to reinstall. The activation information is provided by Adiscon after purchasing.

An expired trial version will be fully reactivated by entering a valid license key.




WinSyslog Client - License Tab

## Registration Name

The registration name is chosen by the user. It should correspond to your organization name, e.g. a company called "AA Carpenters, Inc." should not choose "AA" as registration name. This can easily be mistaken and most probably will be rejected by Adiscon for that reason. With the above scenario, we recommend using the full company name "AA Carpenters, Inc.".

Please note: the registration name is case sensitive. It must be entered exactly as given. Leading and trailing spaces are also part of the registration name, so be sure to enter none.

## Registration Number

This number is provided by Adiscon. It is valid for a specific registration name. Be sure to enter the correct registration number. The WinSyslog Client will detect invalid registration numbers and report an corresponding error.

# The Menu

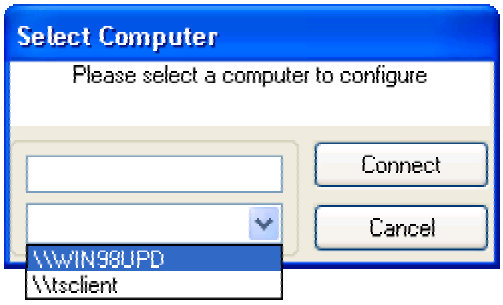
The menu bar offers some basic functions.

There are 4 main menu entries. The “Service” entry is basically used to control the service and to maintenance it. You can start, stop and restart the service from the Service menu. You can also (Only for expert users) install and reinstall the WinSyslog Service from the menu. Be careful with this two options. If you uninstall the service, all your settings will be lost.

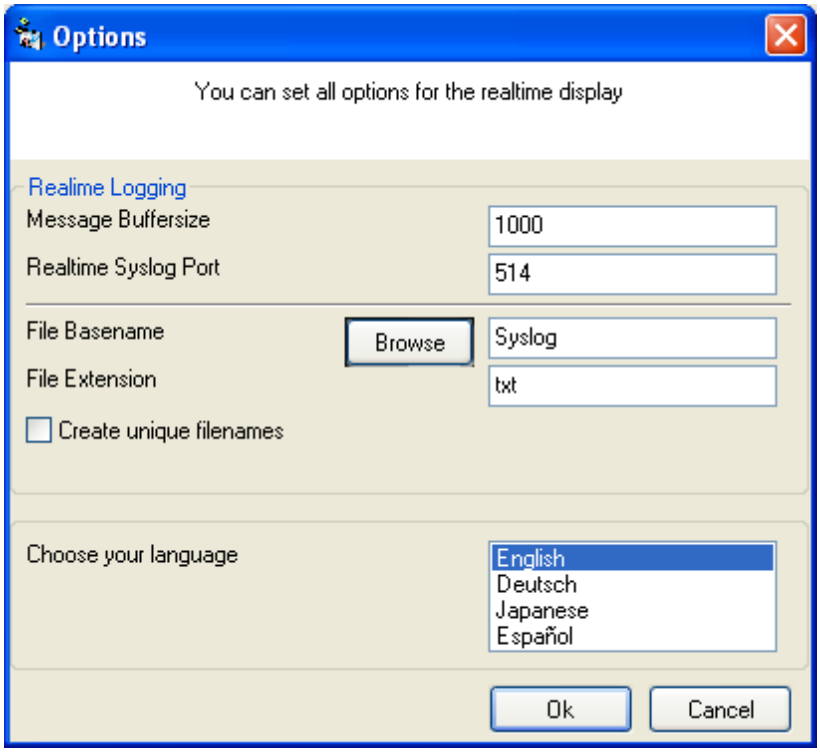
The “RuleBase” entry contains two child entries. One to call the Rulebase Wizard (which can be used to install a basic rule set) and one entry to open the RuleBase Editor.

The menu offers a dialog to check the WinSyslog version numbers. Please select "Help"/"About" to receive the "About" dialog shown below. The "About" dialog displays the WinSyslog version number as well as the version and build ID of the WinSyslog client.


"File" / "Select Computer" gives you the possibility to connect the WinSyslog Client to other computers to configure them. You can either use the select box as shown below, or you can type the name/IP-Address of the computer you want to connect to.




Finally, "File"/"Options" allows you to specify settings for the real-time display as well as the language settings:




## Message Buffersize

The message buffer size (in number of messages) to be used for real-time display. This is the maximum number of messages to be stored in memory. If this number is reached and a new message arrives, the oldest one is deleted from memory.

## Real-time Syslog Port

The UDP port the real-time display listens to. 0 is default from system services database. Most installations can leave it at 514.

## Language

The WinSyslog client is multilingual. Currently, English, German, Japanese and Spanish messages are implemented. Languages are set on a per user basis. They can be switched instantly without the need to restart WinSyslog.

If you are interested in other languages and volunteer to provide translation services, please email info@adiscon.com. We will gladly help.

# The WinSyslog Service

*The Service operates in the background while your computer is running.*

The WinSyslog service is available under Windows NT, 2000 and XP. Due to missing operating system features, it is not present under Windows 95, 98 and Millennium Edition.

The WinSyslog Service is the component that runs on the target machine (the one receiving syslog messages). The service is also called the "engine" of WinSyslog. It needs to be installed on every machine that should receive syslog messages.

WinSyslog can be "engine only" installed. In this case, only the service is installed onto a machine. It can be customized either by directly editing the registry or copying a registry snapshot from a machine with installed client. Please note that "Engine Only" installs need a full WinSyslog license.

The WinSyslog service program is called "winsyslg.exe". It is the sole executable that needs to be distributed for mass rollouts.

## The Service Account

NT Services must utilize an NT logon account in order to perform their intended tasks. The WinSyslog Service is no different. The account initially used by the service is "local system". We recommend to retain this setting.

If for any reason you would like to change the service account, you can do so via the control panel "services" applet (or the "Computer Management" MMC under Windows 2000). However, you need to make sure that the new account has sufficient permissions.

Please note that the WinSyslog startup type is "manual" right after installation. If you would like to start the service automatically at system startup, be sure to switch it to "automatic".

## Command Line Switches

The WinSyslog supports a limited set of command line switches. These are primarily used for unattended installations or "engine only" installs. These are:

| | |
|---|---|
| winsyslg –h | Help, displays a short usage notice. |
| winsyslg –I | Installs the service |

| | |
|---|---|
| winsyslg –u | Removes (uninstalls) the service |
| winsyslg –v | Displays version information as well as whether or not the service is installed. |

# Getting Help

*The WinSyslog Service is very reliable. In the event you experience problems, find here how to solve them.*

Do you need help with the WinSyslog Service or WinSyslog in general? Do you need an important question answered? No problem, there is lots of help available!

Please note that all options (except priority support) are also open to evaluating customers. So do not hesitate to try them. Help is available in English and German language. Our local resellers may provide local language support. Please check with them.

## WinSyslog Web Site

Visit the support area at

www.winsyslog.com/en/support

for further information. If for any reason that URL will ever become invalid, please visit www.adiscon.com for general information.

## Support Newsgroups

Share questions and answers with your peers! These groups are also monitored by Adiscon support staff.

The are available either via NNTP (Newsreader, for example Microsoft Outlook Express) at

news://news.adiscon.com/adiscon.products.winsyslog

They can also be viewed via a web browser at

http://erftstadt.adiscon.com/exchange/root.asp?acs=anon

## Email

Please adress all support request to

**support@adiscon.com**

An appropriate subject line is highly appreciated.

# Online Seminars

Adiscon offers a selection of online seminars. This selection is continously being expanded. All available seminars can be found at:

http://www.adiscon.com/Common/SeminarsOnline/

When viewing the seminar selection, please keep in mind that WinSyslog is a member of the MonitorWare line of products. As such, seminars related to the common reporting engine are relevant to WinSyslog, too.

***Please note:*** *Windows Media Player is required to view the seminars.*

# Phone

**+49-2235-985004** (with "+" being the international dialing prefix, for example 011 in the US).

**Phone technical support is limited to UpgradeInsurance customers.**

Please note that we are in the Central European Time zone (CET). That is 1 hour east of Greenwich Time. If it is 12pm in New York, it is 9pm at our office location. Our office hours are from 9am to 4pm. So we generally advise US customers to call in early mornings and Asian customers to call in late afternoon.

For best customer service, we highly recommend limiting phone calls to emergencies. We are checking our other support options regularly. Email support is available also during non office hours, typically until 10pm CET.

# Fax

Please direct your faxes to

**+49-2235-985032**

with "+" being the international dialing prefix, e.g. 011 in the US and 00 in most other countries.

# Software Maintenance

Adiscon's software maintenance plan is called UpgradeInsurance. It offers unlimited free upgrades and priority support during its duration. It can be purchased for a period between 1 and 5 years.

To learn more about UpgradeInsurance, please visit

http://www.adiscon.com/Common/en/products/upgrade-insurance-details.asp

# Non-Technical Questions

Please address all non-technical questions to

**info@adiscon.com**

This email alias will answer all non-technical questions like pricing, licensing or volume orders.

# Product Updates

The WinSyslog line of products is being developed since 1997. New versions and enhancements will be made available continuously.

Please visit

www.winsyslog.com

for information about new and updated products.

# Frequently asked Questions

For a current list of Frequently Asked Questions (FAQ), please visit

http://www.winsyslog.com/en/FAQ/

# Purchasing WinSyslog

*If you would like to use WinSyslog's advanced features, you can purchase your own copy. Here is how to do it easily.*

Advanced Features are available in the professional version. They can be used for 30 days after installation without a license. However, after this period a valid license must be purchased. The process is very easy and straightforward.

## The License

Please see license.txt for full license information. This file can be found in the ZIP file and is also displayed during installation.

## Differences between the Free and Professional Version

The free version includes the Realtime Syslog Server, an interactive Windows GUI program. It can be used to log messages in real-time for instant review. The message buffer is limited to the last 60 lines, which is more than enough in typical network troubleshooting situations.

The professional version offers all features described in this document. Most importantly, it includes the full rule engine including all services, criteria and actions. That engine is not available in the Realtime Syslog Server. The professional version can operate in the background as a system service. We strongly recommend this mode for continous monitoring of important devices.

Right after installation, WinSyslog is in so-called "trial mode" for 30 days. In this mode, it offers all features of the professional version. After 30 days, it reverts to "freeware mode" and the enhanced features – including the system service – are disabled. They can be renabled by simply entering the registration key after purchase. No new installation or configuration is necessary.

## Pricing

The license fee is US$ 49.

For customers in the "Euro Zone" (European countries using the EURO as official currency), the license fee is EURO 69 including 16% VAT. European Community residents with VAT identification number should state this number in order to receive tax exemption. If not stated, full VAT will be charged. All European

Community orders will be processed in EURO. US$ payment is available for international customers, only.

Please email Adiscon at sales@adiscon.com if you are interested in a volume order.

## How to order

The most convenient way is via our online order processing system found at

https://secure.adiscon.com/WinSyslog/en/

If you do not like to order online, registration is still as simple as 1-2-3:

4. Print out the registration form on the order web site
5. Please fill it in. Remember to include number of licenses requested and payment information as well as your email id.
6. Mail or fax the registration form to Adiscon.

We accept all major credit cards. If you would like to place a purchase order, please see

http://www.adiscon.com/Common/en/OrderByPO.asp

for details.

If you need any additional payment options, please contact us at Info@Adiscon.com or the below given addresses.

**Direct your orders to:**

Adiscon GmbH
Franz-Marc-Strasse 144
50374 Erftstadt
Germany

Fax: +49-2235-985032
Phone +49-2235-985004

email: order@Adiscon.com

All credit card orders need to be processed in Euro. US$ payments will be converted to Euro according to current exchange rate. There might be a slight difference in the converted value due to exchange rate differences.

## Order Form

Your order can be placed using the following form. The most current online order form is available at

https://secure.adiscon.com/WinSyslog/en/

If you'd like to order by mail or fax, please print out the order form and sign it.

# Miscellaneous

## Configuring via the Registry

*This Chapter is targeted towards System Administrators interested in large scale deployments. There is no need for typical users to read it.*

WinSyslog is configurable via the registry. All parameters can be changed dynamically. Parameters are read when the WinSyslog service starts. So when parameters are changed, WinSyslog needs to be stopped and restarted.

Starting with version 3.0, WinSyslog has a graphical configuration program, the WinSyslog Client. All options are customizable via it. So there is no need to modify the registry directly. However, we still document all registry keys in order to facilitate mass rollouts and unattended installs.

If you need to customize the product without the WinSyslog client available, you can do so via Windows REGEDIT. Please see "How to use REGEDIT" if you are new to direct registry editing.

### Registry Key Reference

All WinSyslog registry keys are stored under

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AdisconWinSyslog\Parameters

Please note that this is **one** key, even though it is broken onto multiple lines in this manual.

All parameters are documented in the following sections.

#### *szLicensee*

Type: string value

This is the name of the licensed user. The trial version does not have a licensee name string. It specifies "unregistered". If you register your copy of WinSyslog, you specify the license string of your choice. If it is not already used by another user, you will receive a matching license number (next parameter, nLicenseKey) from Adiscon. Enter both the license name and key into the registry. This will turn off the trial version warning. If it doesn't turn them off, be sure to check if both the name and number are correctly entered.

Please note: This parameter is case-sensitive!

### *nLicenseKey*

Type: DWORD value.

This is the license key issued by Adiscon. It must match the license name (szLicensee, see directly above). If it does not match, the WinSyslog service will not recognize your installation as licensed.

### *nSyslogPort*

Type: DWORD value.

The port number used for syslog messages. Can be either a valid IP port in the range of 1 to 65535 or 0. In case of 0, a Windows sockets lookup is used to get the system default syslog port (using etc/services). The default value is 0. We highly recommend using this default if there isn't a specific reason for changing it.

A different port is most often used in firewall setups.

### *nTimeMode*

Type: DWORD value.

This defines how WinSyslog gets the time. If set to 0, localtime is used. If set to 1 then Universal Coordinated Time (UTC/GMT) is used.

### *bWriteToLogFile*

bType: DWORD value (Boolean).

Controls, whether or not WinSyslog logs to a log file. If set to 1, it will write messages to the log file. If 0, no log files will be written.

### *szBaseLogFilePath*

Type: string value.

This is the base path (directory) for log files created by WinSyslog. The default value is "C:\TEMP".

### *szBaseLogFileName*

Type: string value

The first part of the log file name created by WinSyslog. The service appends the current date to this base part (there is one separate log file for each day). The default value is "WINSyslog".

### *szBaseLogFileExtension*

Type: string value

The file name extension used when creating the WinSyslog log file name. Default value is "log".

### *szODBCReceivedAt*

Type: string value

Used for ODBC logging. Specifies the field name inside the syslog table to hold the date and time of message reception. The default is "ReceivedAt".

### *szODBCFacility*

Type: string value

Used for ODBC logging. Specifies the field name inside the syslog table to hold the syslog facility of the message received. The default is "Facility".

### *szODBCPriority*

Type: string value

Used for ODBC logging. Specifies the field name inside the syslog table to hold the syslog priority of the message received. The default is "Priority".

### *szODBCFromHost*

Type: string value

Used for ODBC logging. Specifies the field name inside the syslog table to hold the address from the host that send the syslog message received. The default is "FromHost".

### *szODBCMessage*

Type: string value

Used for ODBC logging. Specifies the field name inside the syslog table to hold the actual syslog message received. The default is "Message". Please note that this default conflicts with a reserved name in sybase databases and as such needs to be changed.

### *bWriteToODBC*

Type: DWORD value (Boolean).

Controls, whether or not WinSyslog logs to an ODBC data source. If set to 1, it will write messages to ODBC. If 0, no ODBC logging occurs.

Default is 0.

### *szODBCDsn*

Type: string value

The data source name to be used for ODBC logging. This must be a system data source. There is no default value. Must be set, if ODBC logging is enabled.

### *szODBCUid*

Type: string value

The userid to be used for ODBC logging. There is no default value. It is depending on the data source if an userid is needed.

### *szODBCPwd*

Type: string value

The password to be used for ODBC logging. There is no default value. It is depending on the data source if a password is needed. This value is either encrypted or unencrypted (see parameter nODBCEncryption). For security reasons, we recommend storing it en crypted.

If you would like to do a mass-rollout, please use the client to create an en crypted value first time. Then roll out this value via a registry file or similar mechanism.

### *nODBCEnCryption*

Type: DWORD

A flag to indicate if the value in szODBCPwd (pass word) is encrypted. If set to 0, the password is stored unencrypted. If set to 1, the password is encrypted.

Default is 0.

### *szTableName*

Type: string value

The table to be used for ODBC logging. The default value is "syslog".

bWriteToEventLog

Type: DWORD value (Boolean).

Controls, whether or not WinSyslog logs to the Windows event log. If set to 1, it will write messages to the event log. All messages will be written to the application log. If 0, messages will not be written to the Windows event log.

Default is 0.

### *bReplaceEventLogSource*

Type: DWORD value (Boolean).

If set to 1, WinSyslog will use the IP address of the system that send the syslog message as the Windows event log source. It will also write the syslog facility and priority into the category and event ID.

If set to 0, these fields will not be touched. Instead, the source system's IP address, facility and priority are written comma-delimited into the message part of the Windows event log. This is the default.

We recommend to leave the default value (0) unless there is a strong reason not to do so.

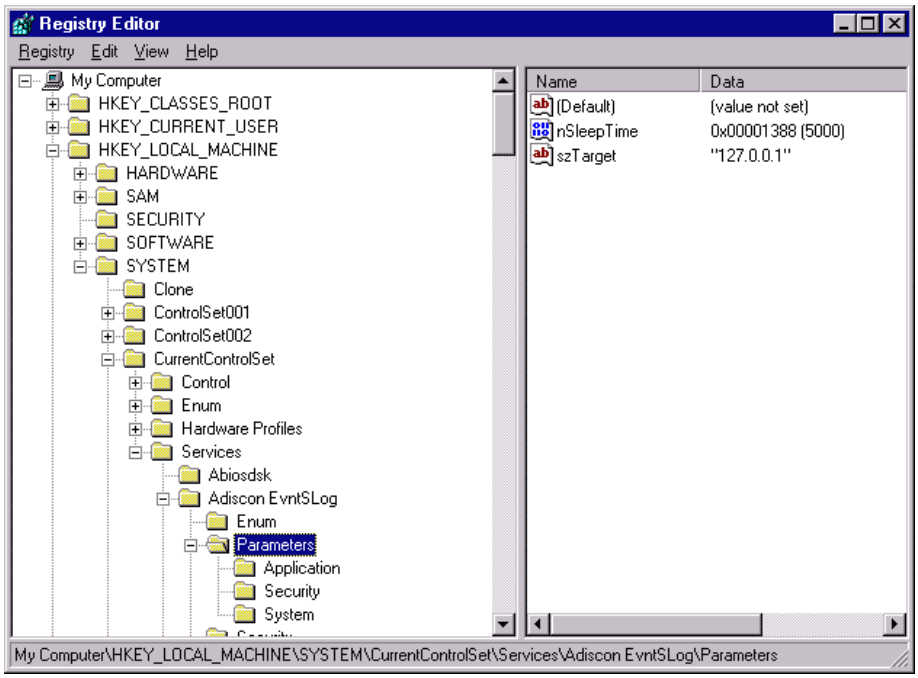
## How to use REGEDIT

Use the Windows NT run command and type "REGEDIT" (NT 3.5 users please type "regedt32") as the program to run. Once REGEDIT has started, you see several configuration settings. Please navigate the tree structure by clicking the elements. Navigate to

"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Adiscon WinSyslog\Parameters"

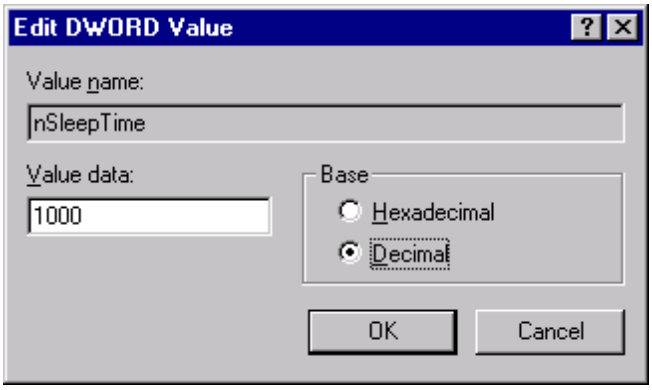
Please note that this is all on a single line.

The following screenshot displays a sample configuration.




Screenshot of regedit

Please note the parameters on the right side. Double-click the ones you would like to modify. The following picture shows the dialog appearing after double-clicking nSleepTime:




nSleepTime double-clicked

Please not the "Base" setting on the right side. The default is hexadecimal, which usually is not very user friendly. Change this to "Decimal" as show above. The "Value Data" holds the value you would like to set.

After modifying the value, click "OK" and the registry will be updated. The WinSyslog service will accept the new parameters after the next re-start.

# Version History

*Interested how the WinSyslog Service evolved and which features are new to this build? Read it here!*

This short history provides some background information about the versions available as well as their pros and cons.

This is user driven software.

**Please provide us with your feedback. Many features have become reality with the help of envisioning users!**

## 1.0

This is the initial release. It provides all the basic functionality, has some restrictions:

- there is no configuration program
- logging to stdout only
- does not run as a service

## 2.0

This is the feature-upgraded release. This release is available as shareware. It contains the following enhancements:

- runs as true multithreaded Win32 service process
- controllable via the control panel "services" applet
- supports logging to the Windows NT Event log
- extended log entries

## 3.0 beta 1

This version has been released to the public on October, 6th 2000.

- This version is much improved. It contains the following enhancements:
- WinSyslog client added
- interactive display of syslog messages
- easy service configuration
- logging to flat ASCII files
- logging to ODBC data sources
- Licensing via licensee name and license key. There is only a single executable for both the trial and the licensed version. This way, a trial installation can become a fully licensed one with even less effort.

## 3.0 Final Release

This version has been released to the public on October, 16th 2000. It is a production build of 3.0 beta 1. It contains the following enhancements:

- some bug fixes (Client & Service)
- minor user interface enhancements in the WinSyslog Client
- multilingual interface for WinSyslog Client

## 3.1 Beta 1

This version has been released to the public on October, 31st 2000. It contains the following enhancements:

- Japanese-language support
- XML based internationalization system
- increased message logging size
- fixed some minor bugs

## 3.1 Final Release

This version has been released to the public on December, 4th 2000. It contains the 3.1 Beta 1 enhancements plus:

- Password encryption for ODBC connection settings
- fixed a bug that caused a maximum of 256 bytes to be written to the ODBC data source (other event targets were reported correctly)
- enhanced setup program based on the Microsoft Windows Installer Service, the new standard for software installation in the Windows environment

## 3.2 Final Release (Build 111)

This version has been released to the public on January, 30th 2001. It contains new enhancements and some bugfixes:

- time zone used can now be configured (Localtime or UTC)
- fixed a bug in the WinSyslog Client that occurs only on Mutlimonitorsystems.
- fixed a bug that caused the client to hang when the user had insufficient access privileges to the system registry (client now displays an error message and quits gracefully)

## 3.3 Preview Release (Beta 1, Build 113)

This version has been released to the public on 2001-03-14. It offers major enhancements over the previous versions.

- Flexible Rule Engine - the big, big plus! Messages received are now run through rules. Each rule is associated with actions (like sending mail or writing to ODBC databases) that are carried out when the rule matches. There is an unlimited number of rules and actions.
- EMail Support - received syslog messages can now be forwarded to email recipients.
- Syslog Forwarding Support - allows to cascade syslog servers. Messages received by WinSyslog can be forwarded by syslog protocol to syslog servers on other systems.
- Remote Administration - the client can now connect to remote systems and configure them.

- Clients supports integrated Version checking via Adiscon's online eSupport site.
- Unicode based - results in faster execution under Windows NT/2000/XP and also eases internationalization.
- Web interface to syslog database - available as a separate free download. The web interface enables viewíng syslog messages from any web browser in real time.

## 3.3 Beta 2 (Build 114)

This version has been released to the public on 2001-03-23. It offers fixes and enhancements over the preview release.

- Added a new Registrykey bReloadRuleBase. If this value is set to 1, the WinSyslog Service reloads the Ruleset everytime when receiving a Syslog-message. This is very useful for testing and debugging a complex rule base.
- Enhanced the Client with the Rulebase Wizard, which helps all users to build a basic Ruleset. The Wizard also can Import older settings from WinSyslog 3.2 (And lower).
- Added a new Toolbar into the Client, where all function like Save or Reload ... can be called.
- Added more support for controlling the Service. The Client can now secure Start, Stop and Restart the service. If an error occurs while these actions, a detailed error message occurs
- Added more Support for Remote Configuring. That means you can configure and maintain a WinSyslog Service on other machines. This is very useful, you don't need a physical access to the machine running the WinSyslog Service.

## 3.3 Beta 3 (Build 115)

This version has been released to the public on 2001-04-02. It offers important fixes and enhancements over the beta 2 release.

- Fix for immediate expiration - a bug in beta 2 made enhanced features unavailable (see related news release at

  www.winsyslog.com/Common/en/News/WinSyslog-2001-04-02.asp
- Memory leak removed - beta 2 had a memory leak if ODBC errors occurred. This has been fixed.
- • More descriptive ODBC error messages - if ODBC connections fail, more detailed information is logged to the NT application event log.
- New, enhanced installation system - based on Windows Installer service and InstallShield. Now has complete repair options as well as custom setup options.

## 3.3 Final (Build 117/Client 3.3.31)

This version has been released to the public on 2001-04-12. It contains all features of the previous beta versions plus small changes. It is a fully supported final release meant to be used in production environments.

- Configurable syslog forwarder port - the IP port to be used when forwarding syslog messages can now be specified both globally and on a per action basis,
- bug fix in real-time logging display - priority and facility were mixed up
- some minor (cosmetic) bugs fixed

## 3.31 Final (Build 118/Client 3.31.40)

- bug fixed with DBCS-Encoding (WinSyslog Service) - A message encoded with DBCS-characters caused the Service to stop working. This is now fixed. All dbcs-encoded messages are right processed.
- RuleBase editing on Remote machine (WinSyslog Client) - While managing a remote machine, the RuleBase-Menu was always disabled. Now, you can also edit the RuleBase on a remote machine. Its also possible to run the Client on Windows9x and to maintaince a remote machine running Windows NT/2000.

## 3.32 Final (Build 119/Client 3.32.47)

- Fixed a bug in the "Send Email" function (WinSyslog Service). - When sending an email, the date was false in some timezones. This is now corrected.
- Enhanced the "Edit Rules" Window (WinSyslog Client).

## 3.4 Final (Build 120/Client 3.4.52)

- Windows 9x/Me file logging support - The client itself does now support logging to a flat file. This feature allows file logging under Windows 9x and Windows Me.
- Improved client display - Facilities are now displayed color coded and with full name (e.g. LOCAL0 instead of 16).
- 3.5 Final (Build 121/Client 3.5.75)
- Spanish language user interface - the WinSyslog client now supports a Spanish language user interface.
- ODBC logging enhancements - it is now possible to overwrite the default field names. This provides additional flexibility for enhanced solutions.
- Fixed a bug that could cause the WinSyslog service to stop unexpectedly if the mail server used for email delivery did refuse connection. Now, these event is properly reported and processing continues. Bug seen very seldom in reality.
- some minor bug fixes in the client application

## 3.6 (Build 122/ Client 3.6.112)

This version has been released to the public on 2001-09-06. The main new feature is support for Microsoft's new Windows XP operating system. It detects the operating environment automatically and adjusts accordingly.

- Enhanced the WinSyslog Client with the new Windows XP Look and Feel.
- The WinSyslog Client now fully supports the new Windows XP Fast User Switching feature. It checks if another user in another session is using the WinSyslog Client Realtime logging on the same port.
- New manual available in PDF Format.
- New option available for Syslog forwarding. It is now possible the add the original source of a message when forwarding to another syslog server.
- Fixed some minor bugs in the WinSyslog Client.
- WinSyslog has a new enhanced installer now. Users can now download a smaller install set which will download the Windows Installer only if necessary (it typically is not necessary under Windows 2000, Windows XP and systems with Office 2000 or above installed). In most cases this will reduce the download time.
- some minor bug fixes in the client application

## 3.7 (Build 124/ Client 3.7.126)

This version has been released to the public on 2001-12-06. It contains a number of user requested small enhancements as well as some bug fixes.

- Customizable email subject line. We do now have support for replacement characters. So the event source, facility, priority and message content can be included into the email subject. Great for pagers and cellular phones, which often only display the subject line of a message sent to them.
- RFC3164 compatible date and time parsing. If enabled, the receive time stamp is taken from the syslog message rather than from the local system time.
- Unique file name generation (based on system date) can now be turned off. This was requested by customers monitoring syslog files with external file monitor processes.
- File Logging data fields are now configurable. Date/Time, Facility and Priority fields can now be turned off. If so, they won't be written to the log file.
- Solved a usability issue. When using the rule wizard with standard settings, a syslog forward to local host was often accidentally created. This in turn lead to a loop where each message received was forwarded to WinSyslog itself, starting an endless iteration. Now, even when forwarding is enabled it is disabled by the product if no syslog forwarder address is specified (we formerly used a default of 127.0.0.1).
- Fixed a bug that occurred when ODBC logging was used with Oracle.

- Improved the WinSyslog Client speed. Especially slow machines with Windows XP should see a faster WinSyslog realtime log display.

# Other Products of Interest

You might be interested in Adiscon EventReporter. This tool can extract the Windows NT event logs and forward them either via email or to a syslog server like WinSyslog. EventReporter is available at http://www.eventreporter.com. To create consolidated reports out of the stored data, use MoniLog, available at www.monilog.com. If you would like to generate syslog messages from your Windows scripts, you might also be interested in ActiveLogger www.activelogger.com. With it, sending syslog messages requires just 2 lines of code! EventReporter, ActiveLogger and WinSyslog can be teamed together to provide a centralized management solution.

If your primary intention is Windows NT/2000/XP/2002 event monitoring, you might be interested in visiting www.monitorware.com

# Copyrights

# Glossary of Terms

## EventReporter

EventReporter is Adiscon's solution to forward Windows NT/2000/XP event log entries to central system. These central systems can be either WinSyslog's, other syslog daemons (e.g. on UNIX) or MonitorWare Agents. EventReporter is part of Adiscon's MonitorWare line of products.

## Millisecond

A millisecond is a thousand of a second. It is abbreviated as "ms". As such, 500ms mean half a second.

Inside the MonitorWare line of products, many timers are expressed in milliseconds as a fine control over the services and actions is provided to the administrator.

## MonitorWare Line of Products

Adiscon's MonitorWare line of products is a suite of monitoring and operations management tools. If consist of several components, each of which can be used either individually or as a complete solution. As of this writing, the following products are available:

- ActiveLogger (www.activelogger.com)
- EventReporter (www.eventreporter.com)
- MoniLog (www.monilog.com)
- MonitorWare Agent (www.monitorware.com)
- WinSyslog (www.winsyslog.com)

New products are continously being added – please be sure to check www.monitorware.com from time to time for updates.

## SETP

SETP is the "Simple Event Transfer Protocol". SETP allows reliable delivery of events between SETP supporting systems. All members of the MonitorWare line of

products support SETP. WinSyslog and EventReporter operate as SETP clients. As such, they can forward events generated and gathered by them to central or intermediary SETP servers. The MonitorWare Agent can operate both as a SETP server and client and as such also as a relay. It plays a vital role in a complex, distributed environment.

SETP was developed for MonitorWare. It allows synchronous communication between SETP clients and servers. With SETP, an event can be forwarded exactly as it was on the original event generating system. For example, if a syslog message is received on a remote system, that exact syslog message can be forwarded via as many SETP relays as is configured. During that relaying, no information from the original message is altered or lost. As such, each of the relays as well as the final SETP server will see the original source address, time stamps and message.

Furthermore, SETP guarantees reliable delivery. It is based on TCP, so each of the SETP peers know exactly that the communication partner can successfully receive and process the message. SETP guarantees that new events are only forwarded after the previous ones were successfully received and processed. SETP also checks for on the wire errors. Due to its characteristics, SETP can successfully be used in barely or occasionally connected environments like radio connected systems.

The SETP design is influenced by many industry standard movements, most notably the BEEP protocol and XML. However, SETP is optimized to have a very lightweight footprint. As such, it can be implemented even in low powered devices with little overhead.

# SMTP

The “Simple Mail Transfer Protocol”. This is an Internet standard for sending email messages. Virtually all major email systems are either based on SMTP or at least offer gateways to SMTP capable systems.

SMTP is used for sending email. It can not be used to pick up email messages. For this purpose, protocols like POP3 or IMAP4 are required.

SMTP is highly standardized. As such, a standard email client can work with all SMTP compliant servers. In the public Internet, almost all providers offer SMTP compliant mail servers for their customer’s use.

# TCP

A reliable IP transport protocol. TCP communication ensures that no packets are lost in transit. As such, it is most useful in low-bandwidth or unreliable environments. Examples are slow WANs or packet radio networks.

# UDP

A non-reliable IP transport protocol. It provides best effort delivery. Typically, in LAN environments UDP packets are never lost. However, in WAN scenarios or with heavily loaded LANs, UDP packets might be lost.

# UpgradeInsurance

UpgradeInsurance is Adiscon's software maintenance plan. It offers free major upgrades as well as priority support. UpgradeInsurance is available for all Adiscon products and can be purchased for a period between 1 and 5 years.

To learn more about UpgradeInsurance, please visit

http://www.adiscon.com/Common/en/products/upgrade-insurance-details.asp

# UTC

UTC is the so-called "universal coordinated time". UTC was formerly referred to as "GMT" (Greenwich Mean Time) and is the basis of the international time zone system. For example, New York, USA is 5 hours behind UTC. So if it is 12 noon in New York, the UTC time is 5pm.

The MonitorWare line of products often uses UTC. UTC has the fast advantage of providing one consistent time notation, even if devices are across multiple time zones. This is extremely valuable if a centrel location is to consolidate events from senders in multiple time zones.

Using UTC might not be appropriate if a whole system is contained within a single time zone. As such, most time parameters inside the MonitorWare line of products can be configured to work with local time instead of UTC.

# Index

## R



## S



## T



## U



## V



## W



## X