

Hot Links

Trouble Report

Site Specialists

Knowledge Base

Webmail

Contact Us

Information For...

Faculty & Staff

Students

New Users

ECN Staff

Print-Friendly: Share this Page: 

Shortcut URL:

<http://eng.purdue.edu/jump/8d520>

Eventlog to Syslog Utility

by [Curtis Smith](#)

The *Eventlog to Syslog* utility is a program that runs on Microsoft Windows NT, Microsoft Windows 2000, Microsoft Windows 2003 server, and Microsoft Windows Vista, in either 32-bit or 64-bit mode, monitoring eventlog messages. When a new message appears in the eventlog, it is read, formatted, and forwarded to a UNIX syslog server. Depending on the facility and priority of the message and the configuration of the syslog server, the message will be logged to a message file or displayed on the console. The most useful situation is to log **ERROR** or **WARNING** messages on a console that will alert the administrative staff when unusual conditions exist on the Windows server. The console ought to be one that the administrative staff monitor regularly.

This document contains a link to the source files and executables and instructs how to install the service.

Executables

Compilation

Extract a copy of the [source code](#) to a Windows machine that has Visual Studio 8 (or Visual Studio 2005) with a C/C++ compiler. Bring up a command prompt window. Start a command window (usually Visual Studio Tools folder with the title **Visual Studio Command Prompt**). Build from the source code by executing **nmake**. Copy the files **evtsys.exe** and **evtsys.dll** into the System32 directory (usually `%systemroot%\system32`).

Pre-built Executables

Optionally, download either [32-bit pre-build executables](#) or [64-bit pre-build executables](#), and place the **evtsys.exe** and **evtsys.dll** files in the System32 directory `%systemroot%\system32` the same as above.

Configuration

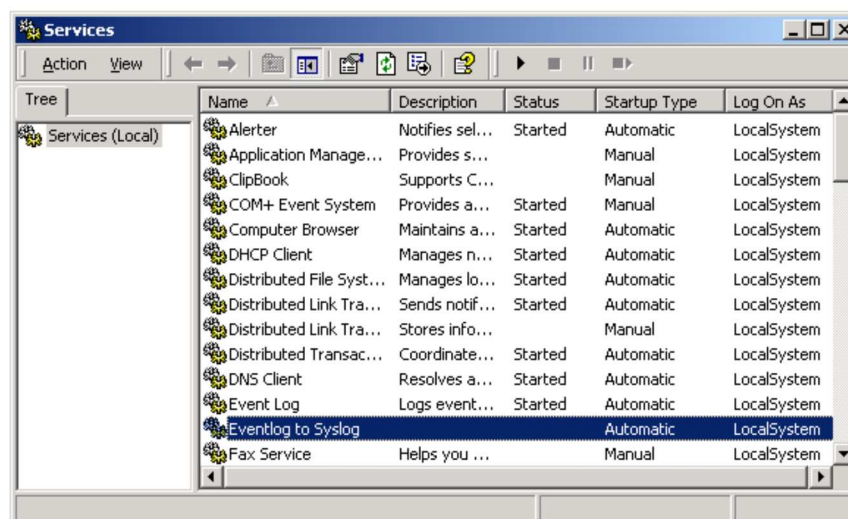
Basic configuration

Once the executables are in place in the `%systemroot%\system32` directory, a service entry will need adding to the Windows registry. To do that, bring up a command prompt windows (using **Run As Administrator**) and execute the following command:

```
evtsys -i -h hostname
```

Where **-i** indicates to install the service. The **-h hostname** switch indicates the hostname or IP address of the UNIX syslog server that will receive eventlog messages. Note that if a hostname is given, it will be converted to an IP address and stored in the registry. This might cause problems if the IP address changes for the host as evtsys will continue to use the same IP address.

If the command indicates success, the service is now installed and Windows will show a new service in the service control program. Bring up the service control program by using the menu **Administrative Tools -> Services**.



Scroll down to the entry *Eventlog to Syslog*. Adjust the entry from *Automatic* to *Manual* if you're not interested in running this service every time the server boots. Start the service by pressing the *Start* button. Watch the console (as indicated above with the *-h* switch) to see if the start message appears. The *Eventlog to Syslog* utility will send out the message *Eventlog to Syslog Service Started* if the service starts and communication to the syslog server is working.

The *Eventlog to Syslog* service forwards messages to the syslog server with a facility of **DAEMON** and priority of **ERR**, **WARNING**, or **NOTICE**. It is possible to use a different syslog facility than **DAEMON** by specifying a **-f** switch during the installation.

Uninstalling

Remove the service and the executable files in three steps. First, stop or make sure the service is stopped by running the service control program and checking the status column. If the status is *Started*, press the *Stop* button. Once the service is stopped, uninstall the service by bringing up a command prompt window and running the command **evtsys -u**. Finally, remove the two files, **evtsys.exe** and **evtsys.dll** from the **%systemroot%\system32** directory.

Note: Sometimes the **evtsys.dll** file is in use by the Eventlog service. Either wait a while, do a reboot of the server, or wait and remove the file after the next reboot. Leaving the file won't cause a lot of problems.

Changing Parameters

Changing the parameters of the Eventlog to Syslog Service will require an uninstall and reinstall. But this is a fairly quick process. Stop the service, uninstall the software, install the software with the new parameters, then start the service. Perform the following commands in a command window:

```
net stop evtsys
evtsys -u
evtsys -i -h newhostname
net start evtsys
```

Note: Uninstalling the service loses all of the original parameters. Be sure to install again with new parameters, remembering to set all the parameters. For example, to change the facility, you'll need to reinstall with the original host as well:

```
evtsys -i -h samehostname -f newfacility
```

Version 3.6

May 31, 2007

Version 3.6 contains a whole bunch of fixes:

1. The code is now operating in 64-bit mode (by popular request), requiring a few changes to C types to avoid compiler warnings, but the original code generally worked once it was compiled into native 64-bit code.
2. The EventID is now part of the message (by popular request).
3. The output messages were reworked to better handle exceptional conditions.
4. Oddly named Microsoft C compiler functions were hidden by use of macros.
5. The version and number of bits is now part of the start message.
6. A facility may be set to override to previous default of DAEMON. This added the **-f** flag to the command line.
7. The syslog.h file was updated with new facility codes.
8. A version information file was added to identify the program, especially useful to Windows Defender.

Be sure to uninstall and install the new evtsys program due to changes in registry.

Note: While this program works on Windows Vista (both 32-bit and 64-bit), it does not handle the use of logging messages via the **Windows Event** API. A lot of messages in the form **Cannot find key value** will appear when logging from Windows Vista. The fix to this will have to be the aptly named **Windows Events to Syslog** service, which I probably won't get to for a while.

Download

Download the source or executable by clicking below.

- [evtsys_exe_32.zip](#) (Last updated Thursday, May 31, 2007, Size 57,383 bytes)
- [evtsys_exe_64.zip](#) (Last updated Thursday, May 31, 2007, Size 64,023 bytes)
- [evtsys_src.zip](#) (Last updated Thursday, May 31, 2007, Size 34,618 bytes)
- [evtsys_exe_32.zip.sig](#) (Last updated Thursday, May 31, 2007, Size 65 bytes)
- [evtsys_exe_64.zip.sig](#) (Last updated Thursday, May 31, 2007, Size 65 bytes)
- [evtsys_src.zip.sig](#) (Last updated Thursday, May 31, 2007, Size 65 bytes)

Engineering

[COLLEGE OF ENGINEERING](#)

[FIRST YEAR ENGINEERING](#)

[SCHOOLS & PROGRAMS](#)

Information Technology

[ENGINEERING COMPUTER NETWORK](#)

[INFORMATION TECHNOLOGY AT PURDUE](#)

[WHY SECURE WEB SERVICES?](#)

Admissions

[OFFICE OF ADMISSIONS](#)

Follow Us

[FACEBOOK](#)

[TWITTER](#)

[YOUTUBE](#)

Purdue Links

[PURDUE HOMEPAGE](#)

[PURDUE SEARCH](#)

[CAMPUS MAP](#)

[PURDUE DIRECTORY](#)

Contact Us

WEBMASTER@ECN.PURDUE.EDU

Copyright © 2009, Purdue University, all rights reserved.

An equal access/equal opportunity university