



User Manual
SyslogAgent v3.3.5

Table of contents

Table of contents.....	1
Introduction.....	2
Installation.....	2
Upgrading.....	3
Configuration.....	4
Exporting your settings to a .reg file.....	4
Troubleshooting.....	6
Verify that the service is running.....	6
Common problems.....	6
Online help.....	6

Introduction

The op5 SyslogAgent are installed as a service on Microsoft Windows 2000/XP/2003 clients and servers to provide syslog compatibility. There are reports that it works for NT4 as well but this is not supported by op5.

The entries in the Event log are sent to the op5 Logserver or op5 Monitor server. Text based application logs are also supported.

The op5 SyslogAgent is a repackaged version of the Datagram SyslogAgent, which initially is a bug fixed version of Sabre Net's old NT_Syslog. The op5 SyslogAgent is licenced as GPL software.

Installation

The op5 SyslogAgent installation package consists of an msi installer. To install simply double-click the installation msi file and follow the on-screen instructions.



fig. 1.

By default the op5 SyslogAgent will be installed in an op5 subdirectory to the program files folder. Usually: `C:\Program Files\op5\SyslogAgent\`

During the installation you will have the opportunity to change where to install the application.

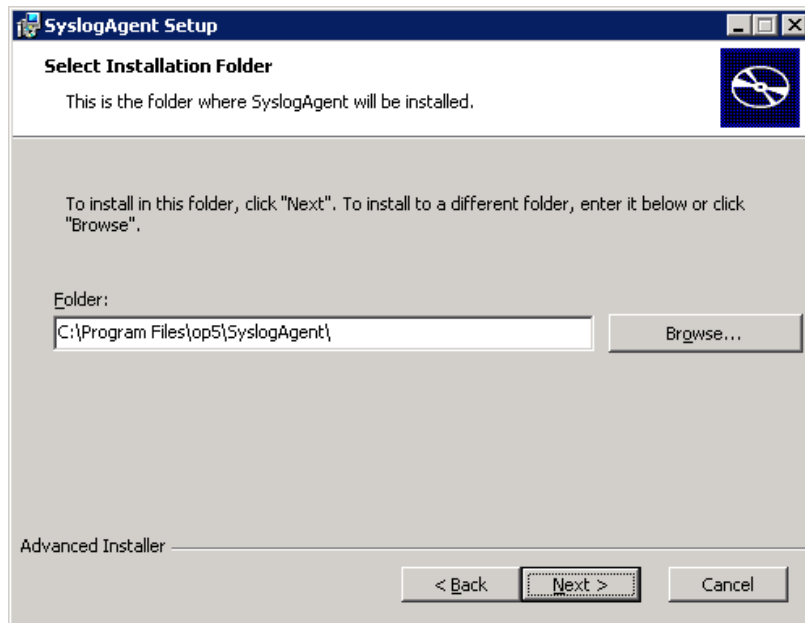


fig. 2.

You will also have the possibility to choose if you want to create start-menu, desktop and quick launch shortcuts to the SyslogAgent-configuration tool.

After the installation is completed you will be asked if you want to start SyslogAgentConfig. If you don't do this the agent won't be configured and cannot be started. If you choose to start the SyslogAgent configuration continue to the "Configuration" section.

Upgrading

If a prior version of the SyslogAgent is installed it should, to avoid problems, be stopped and uninstalled as a service and then uninstalled. Stopping and uninstalling the service can be done from the SyslogAgent Configuration tool. Follow these steps to stop and uninstall the SyslogAgent service:

1. Start the SyslogAgent Configuration tool
2. Press the "Stop"-button (see Fig 3. in the section Configuration)
3. Press the "Uninstall"-button

After the service have been stopped and uninstalled you should uninstall the previous version of the SyslogAgent from "Add/Remove software" on the windows control panel.

Now you can proceed with the installation of the new version as usual. Note that your previous settings will be used directly when the installation is complete.

Configuration

When the configuration tool is started the following window should be displayed:

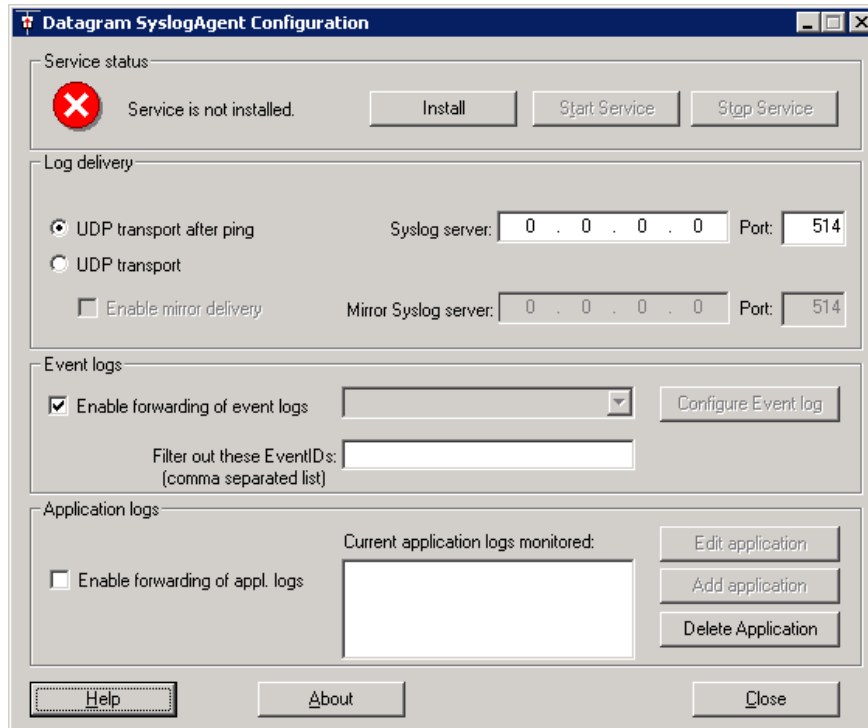


fig. 3.

To get the elementary functions configured and the SyslogAgent started follow the following steps:

1. Press the “Install”-button, this will install the SyslogAgent as a service.
2. Enter the IP address in the field “Syslog Server:”. This IP should be the one to your op5 Logserver or op5 Monitor server.
3. Control that the check box “Enable forwarding of event logs” is checked.
4. Press the “Start Service”-button.

Your SyslogAgent is now configured and should be sending logs to your op5 Logserver or op5 Monitor server.

Exporting your settings to a .reg file

All settings are stored in the registry, and can therefore be exported to a .reg file. This way the settings can be pushed out via a group policy, scripts etc. **Please observe** that in such an export the key 'LastRun' should be **deleted** before copied to another computer- it's the key that helps each computer to know which entries has already been sent. Not deleting this field can cause computers to not send syslog entries.

To create a .reg-file simply open the regedit-tool, i.e type regedit from the command-line and follow these steps.

1. Navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Datagram\SyslogAgent (see *fig. 4*)

2. Right-click the folder and choose export.
3. Save the file and open it by right-clicking the file and choosing edit. Remove the whole line corresponding to the keyword "LastRun"(if present). The line can be found under the section: "[HKEY_LOCAL_MACHINESOFTWARE\Datagram\SyslogAgent]"

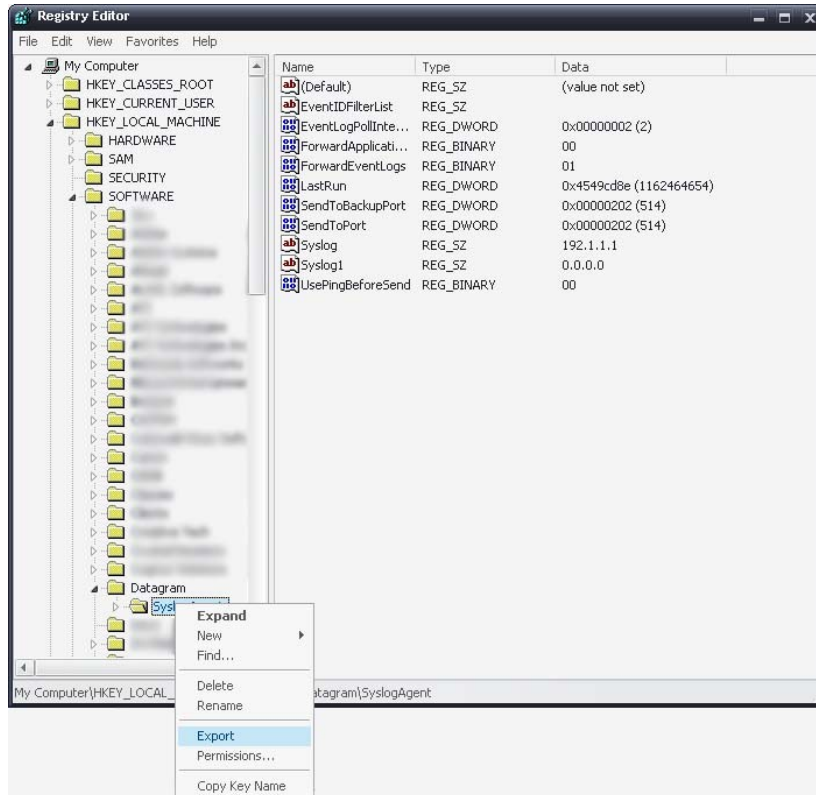


fig. 4

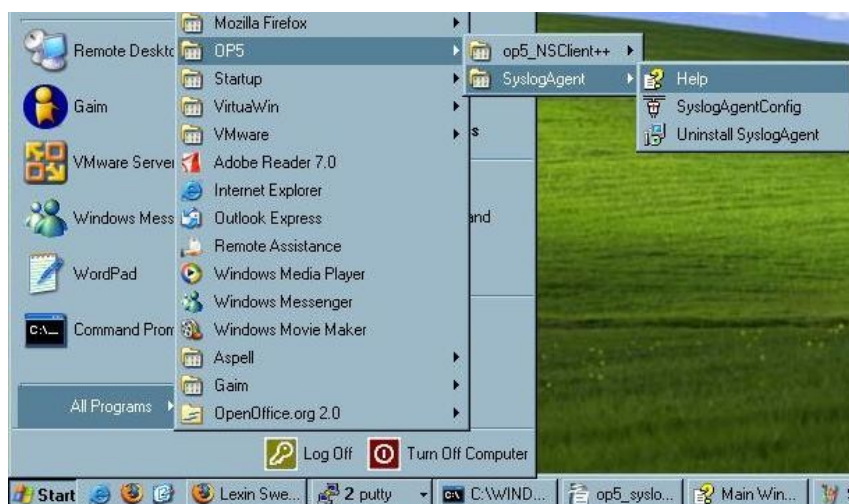


fig. 5

Troubleshooting

This section includes a number of troubleshooting tips to be used if SyslogAgent doesn't send eventlogs.

Verify that the service is running

Locate Syslog Agent in the list of services. How to navigate to the services list depends on operating system and control panel mode. It might, for example, be found in Control panel -> Administrative Tools -> Services.

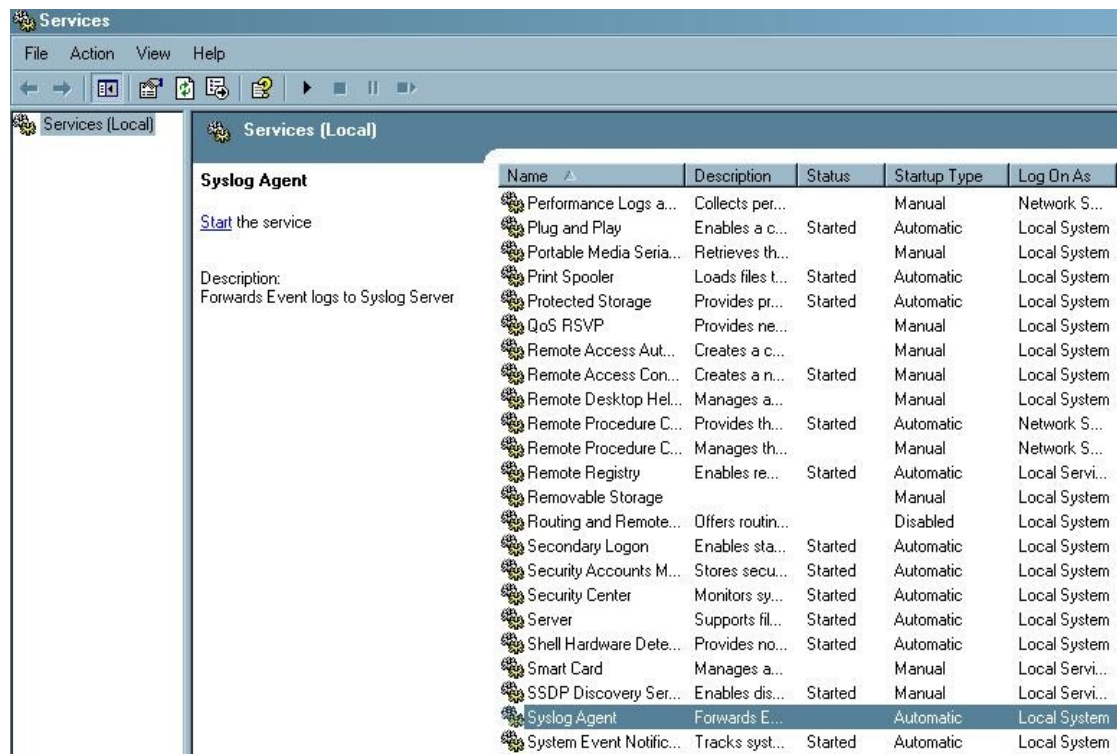


fig. 6

From this view it is also possible to start and stop the service.

Common problems

Firewalls blocking the traffic can be one cause of communication problems. Verify that the used ports are open between the op5 server and the logging windows server (default port 514udp).

Online help

On the op5 support web, <https://support.op5.se>, you will find additional documentation as well as information on how to contact the op5 support team.