

Log Forwarder for Windows

© 2009 SolarWinds, Inc.



Table of Contents

Part I Welcome	1
1 What is Log Forwarder for Windows?	1
2 Configuration	2
3 Deployment	2
Log Forwarder Configuration File	2
Event Log Subscriptions.....	4
Syslog Facilites	5
Syslog Servers.....	6
Part II Subscriptions	7
1 Overview	7
2 Add	8
3 Rename	10
4 Edit Properties	10
5 Remove	11
Part III Syslog Servers	11
1 Overview	12
2 Add	13
3 Rename	13
4 Edit Properties	14
5 Remove	14
Part IV Test	15
1 Overview	15
Part V Troubleshooting	16
1 Windows Firewall	16
Index	0

1 Welcome

Welcome to the Log Forwarder for Windows help file documentation.

Hopefully you will find the necessary help or assistance you require within these pages. If however you do not find what you are looking for, then please search the SolarWinds **Thwack** forums.

The following topics can be found in this chapter :

- See **What is Log Forwarder for Windows** for a general overview of the product.
- See **Configuration** for information on how and where your configuration settings are stored.
- See **Deployment** for instructions on how to run the MSI version of the installer.

1.1 What is Log Forwarder for Windows?

Log Forwarder for Windows is a service which runs on a Windows system, forwarding event log records to a Syslog Server via **UDP** (User Datagram Protocol).

Log Forwarder for Windows can be run on the following Windows operating system versions:

- Windows 2000
- Windows Server 2003 *
- Windows XP *
- Windows Vista *
- Windows Server 2008 *

* x86 and x64 editions supported.

Log Forwarder for Windows comprises of 2 standard application executables (.exe).

- the **Service** (*LogForwarder.exe*), and
- the **User Interface** (*LogForwarderClient.exe*)

The Log Forwarder for Windows Service is named "*SolarWinds Log Forwarder for Windows*" and is installed and started during the installation process.

Management of the Log Forwarder for Windows Service (starting, stopping, etc.) is via the Windows Services manager or Windows command prompt; for example: Net Start "*ServiceName*".

The Log Forwarder for Windows User Interface (UI) which allows you to configure the Service, can (depending on which options were selected during installation) be opened using the *SolarWinds Log Forwarder for Windows* desktop shortcut item, the Quicklaunch item, or from the *SolarWinds Log Forwarder for Windows* Program group accessible from the Windows Start button.

Log Forwarder for Windows supports forwarding of both Windows Eventing 5 & 6 event records.

- Windows eventing 5 **Event Log** records - > Windows O/S versions prior to Windows Vista and Windows Server 2008
- Windows eventing 6 ("*Crimson*") **Windows Event Log** records - > versions of Windows based on the Windows NT 6.0 kernel (Windows Vista and Windows Server 2008)

1.2 Configuration

The Log Forwarder for Windows **Subscriptions** and **Syslog Server** settings are stored in the configuration file *LogForwarderSettings.cfg* located in the product installation directory. When a change is saved within the UI, the configuration file is updated and the Service reinitializes to pickup the changes immediately.

- See **Deployment** for information on how to deploy the configuration to a target machine.

1.3 Deployment

The Log Forwarder for Windows program installer is provided as a Standard application executable file (.exe) and as a Windows Installer Package file (MSI).

- The Standard application executable file (.exe) is installed simply by double-clicking on the file.
- The Windows Installer Package file (MSI) is provided for 'silent' deployment using the */quiet* switch.

To run the MSI on the target machine, use the following command syntax:

```
SolarWinds_LogForwarder_Version_Setup.msi /quiet
```

Note:

The MSI installer package for Log Forwarder for Windows does not include the prerequisites installer, which automatically downloads and installs required prerequisite software, such as the .Net Framework 2.0 from Microsoft. As a consequence, in order to successfully deploy Log Forwarder for Windows, you will need to first ensure that the required prerequisites are already installed.

MSI Prerequisite install requirements:

Microsoft .Net Framework 2.0 (or above).

Deployment of the configuration file

To deploy the configuration file to a target machine, copy the *LogForwarderSettings.cfg* file to the Log Forwarder for Windows installation directory after the MSI has been installed successfully.

For example: (<Program files>/SolarWinds/Log Forwarder for Windows/...).

1.3.1 Log Forwarder Configuration File

Configuration information for Log Forwarder for Windows is contained in a file named *LogForwarderSettings.cfg*.

The configuration file, located in the installation directory of Log Forwarder for Windows (usually C:\Programs Files\SolarWinds\Log Forwarder for Windows), contains a nested heirarchy of XML tags and subtags that specify the configuration settings.

All configuration information resides between the **<LogForwarderSettings>** and **</LogForwarderSettings>** root XML tags. Configuration information between the tags is grouped into two main sections: **<EventLogSubscriptions>** and **<SyslogServers>** both of which are required.

```
<?xml version="1.0" encoding="utf-8"?>
<LogForwarderSettings xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:
xsd="http://www.w3.org/2001/XMLSchema">
  <EventLogSubscriptions>
    ...
  </EventLogSubscriptions>
  <SyslogServers>
    ...
  </SyslogServers>
```

```
</LogForwarderSettings>
```

For Event Log Subscriptions, each Event Log Subscription is declared with an **<EventLogSubscription>** tag. The following LogForwarderSettings.cfg file declares two Event Log Subscriptions.

```
<?xml version="1.0" encoding="utf-8"?>
<LogForwarderSettings xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:
xsd="http://www.w3.org/2001/XMLSchema">
  <EventLogSubscriptions>
    <EventLogSubscription>
      <channels>
        <string>Security</string>
      </channels>
      <types>
        <int>1</int>
        <int>2</int>
        <int>4</int>
        <int>8</int>
        <int>16</int>
      </types>
      <sources />
      <eventIDs />
      <categories />
      <keywords />
      <users />
      <computers />
      <facility>4</facility>
      <enabled>true</enabled>
      <name>New Security Event Log Subscription</name>
      <description>Security Event Log - All Event Types (Error,
Warning, Information, Audit Success, Audit Failure)</description>
    </EventLogSubscription>
    <EventLogSubscription>
      <channels>
        <string>System</string>
      </channels>
      <types>
        <int>1</int>
        <int>2</int>
        <int>4</int>
      </types>
      <sources />
      <eventIDs />
      <categories />
      <keywords />
      <users />
      <computers />
      <facility>10</facility>
      <enabled>true</enabled>
      <name>New System Event Log Subscription</name>
      <description>Security Event Log - Error, Warning and
Information Event Types</description>
    </EventLogSubscription>
  </EventLogSubscriptions>
  <SyslogServers>
    ...
  </SyslogServers>
</LogForwarderSettings>
```

For Syslog Servers, each Syslog Server is declared with an **<SyslogServer>** tag. The following LogForwarderSettings.cfg file declares two Syslog Servers.

```
<?xml version="1.0" encoding="utf-8"?>
```

```
<LogForwarderSettings xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:
xsd="http://www.w3.org/2001/XMLSchema">
  <EventLogSubscriptions>
    . . .
  </EventLogSubscriptions>
  <SyslogServers>
    <SyslogServer>
      <serverName>Syslog Server A</serverName>
      <IPAddress>10.190.2.243</IPAddress>
      <Port>514</Port>
      <enabled>true</enabled>
    </SyslogServer>
    <SyslogServer>
      <serverName>Syslog Server B</serverName>
      <IPAddress>192.168.1.10</IPAddress>
      <Port>514</Port>
      <enabled>true</enabled>
    </SyslogServer>
  </SyslogServers>
</LogForwarderSettings>
```

1.3.1.1 Event Log Subscriptions

Each Event Log Subscription must include the following tag declarations:

<channels>

A list of valid event log channels (eg. Application, System, Security) that are subscribed to. Each subtag of type **<string>**.

<types>

A list of valid event log types. Each subtag of type **<int>**. Valid values are 1 (Error), 2 (Warning), 4 (Information), 8 (Audit Success), 16 (Audit Failure).

<sources>

A list of valid event log sources. Each subtag of type **<string>**.

<eventIDs>

A list of event ID's or event ID ranges. Each subtag of type **<string>**.

<categories>

A list of valid event log task categories. Each subtag of type **<string>**.

<keywords>

A list of event keywords. Each subtag of type **<string>**.

<users>

A list of users. Each subtag of type **<string>**.

<computers>

A list of computers. Each subtag of type **<string>**.

<facility>

The default syslog facility number to use when generating a syslog message to send. See syslog facilities.

<enabled>

true/false. If set to true the event log subscription is active. Events collected when the event log subscription is enabled will be forwarded to the configured syslog servers.

<name>

The name of the Event Log Subscription.

<description>

The description of the Event Log Subscription.

```
<?xml version="1.0" encoding="utf-8"?>
<LogForwarderSettings xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:
xsd="http://www.w3.org/2001/XMLSchema">
  <EventLogSubscriptions>
    <EventLogSubscription>
      <channels>
        <string>Application</string>
      </channels>
      <types>
        <int>1</int>
        <int>2</int>
        <int>4</int>
      </types>
      <sources>
        <string>SolarWindsAlertingEngine</string>
        <string>SolarWindsEventSysLogger</string>
        <string>SolarWindsSyslogService</string>
        <string>SolarWindsTrapService</string>
      </sources>
      <eventIDs>
        <string>0</string>
        <string>1003 - 1006</string>
      </eventIDs>
      <categories>
        <string>(0)</string>
        <string>(100)</string>
        <string>(101)</string>
      </categories>
      <keywords />
      <users>
        <string>System</string>
        <string>Administrator</string>
      </users>
      <computers>
        <string>SERVER-A</string>
        <string>SERVER-B</string>
      </computers>
      <facility>0</facility>
      <enabled>true</enabled>
      <name>New Application Event Log Subscription</name>
      <description>Application</description>
    </EventLogSubscription>
  </EventLogSubscriptions>
  <SyslogServers>
    ...
  </SyslogServers>
</LogForwarderSettings>
```

1.3.1.1.1 Syslog Facilites

0 kernel messages
1 user-level messages

2 mail system
3 system daemons
4 security/authorization messages
5 messages generated internally by syslogd
6 line printer subsystem
7 network news subsystem
8 UUCP subsystem
9 clock daemon
10 security/authorization messages
11 FTP daemon
12 NTP subsystem
13 log audit
14 log alert
15 clock daemon
16 local use 0 (local0)
17 local use 1 (local1)
18 local use 2 (local2)
19 local use 3 (local3)
20 local use 4 (local4)
21 local use 5 (local5)
22 local use 6 (local6)
23 local use 7 (local7)

1.3.1.2 Syslog Servers

Each Syslog Server must include the following tag declarations:

<serverName>

The name of the Syslog Server.

<IPAddress>

A valid Syslog Server IP address (IPv4 or IPv6), hostname or FQDN.

<Port>

The Syslog Server port (default is 514).

<enabled>

true/false. If set to true the Syslog Server is active. Events collected will only be forwarded to the syslog servers which are enabled.

```
<?xml version="1.0" encoding="utf-8"?>
<LogForwarderSettings xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:
xsd="http://www.w3.org/2001/XMLSchema">
  <EventLogSubscriptions>
    ...
  </EventLogSubscriptions>
  <SyslogServers>
    <SyslogServer>
      <serverName>Syslog Server A</serverName>
      <IPAddress>10.190.2.243</IPAddress>
      <Port>514</Port>
      <enabled>true</enabled>
    </SyslogServer>
    <SyslogServer>
      <serverName>Syslog Server B</serverName>
      <IPAddress>192.168.1.10</IPAddress>
      <Port>514</Port>
```

```
<enabled>>true</enabled>
  </SyslogServer>
</SyslogServers>
</LogForwarderSettings>
```

2 Subscriptions

This chapter provides information and guidance relating to the **Subscriptions** screens in Log Forwarder for Windows.

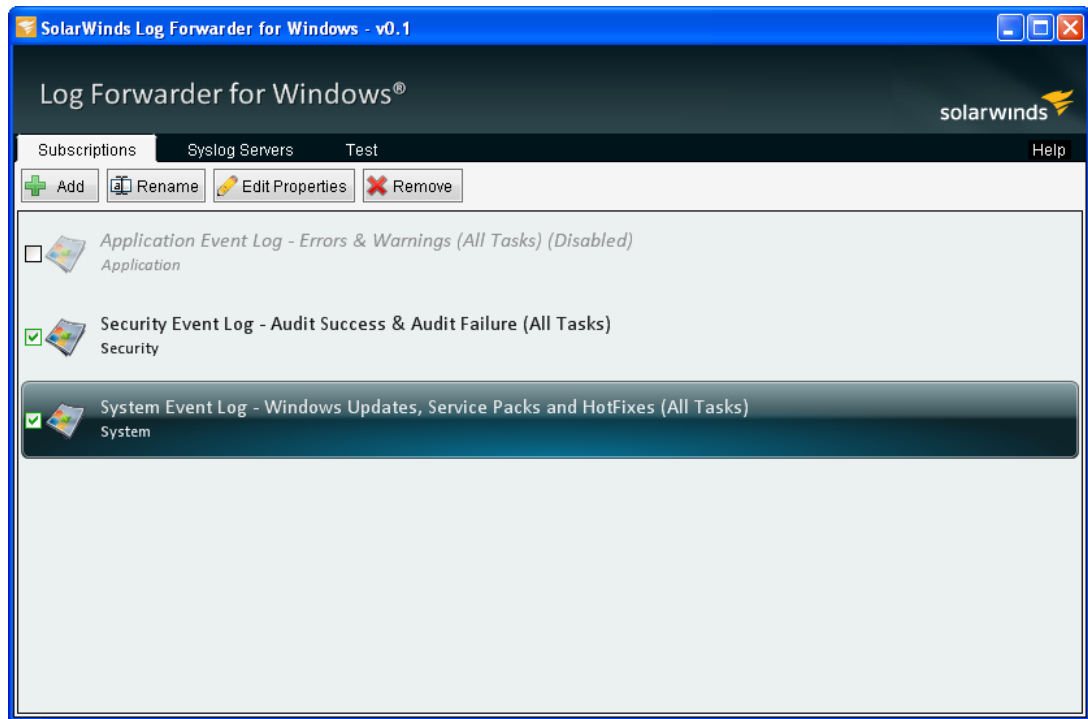
The following topics can be found in this chapter :

- See **Overview** for a general overview of the **Subscriptions** screen.
- See **Add** for information on adding a new Subscription item to the list.
- See **Rename** for information on renaming an existing Subscription item.
- See **Edit Properties** for information on editing the properties of an existing Subscription item.
- See **Remove** for information on deleting an existing Subscription item from the list.

2.1 Overview

The **Subscriptions** screen allows you to add or maintain the subscriptions you have created for the Log Forwarder for Windows program.

Below is a sample screenshot of the Subscriptions screen with three example subscriptions setup.



- **Application Event Log - Errors & Warning (All Tasks)**. This subscription has been *disabled*, by unticking the item tick-box therefore the associated log records will not be

forwarded.

- **Security Event Log - Audit Success & Audit Failure (All Tasks).**
- **System Event Log - Windows Updates, Service Packs and HotFixes (All Tasks).**

The screen also contains four command buttons:

The **Add** button (always enabled)

The **Rename** button

The **Edit Properties** button

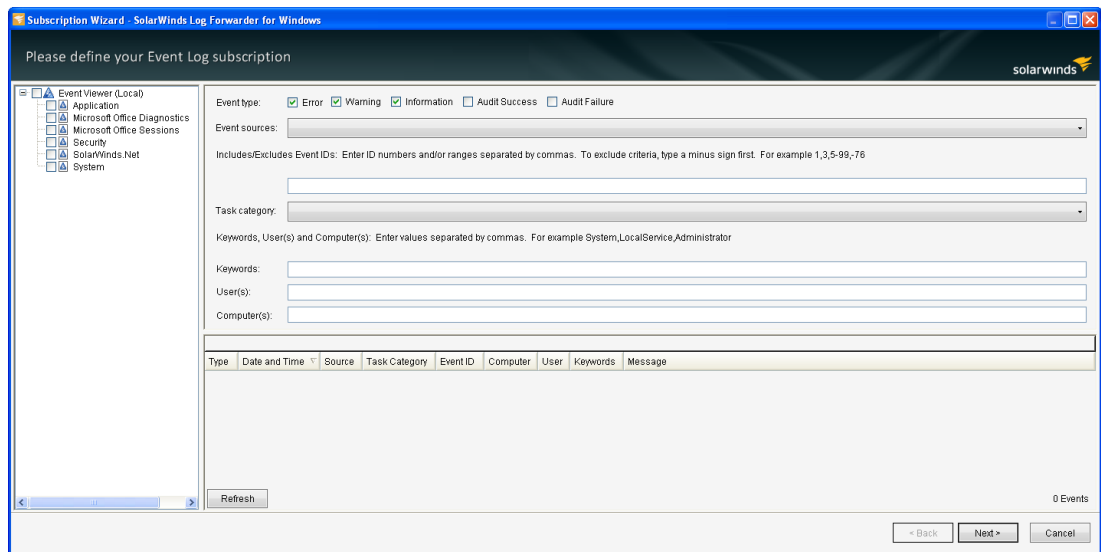
The **Remove** button

Note: The **Rename**, **Edit Properties** and **Remove** buttons are ONLY enabled when a subscription item has been selected.

2.2 Add

To add a new subscription within the **Subscriptions** screen, click on the **Add** button.

On clicking the **Add** button, the *Subscriptions Wizard* window will appear.



1. Select the event log (or event logs) you wish to subscribe to from the left column treeview control.

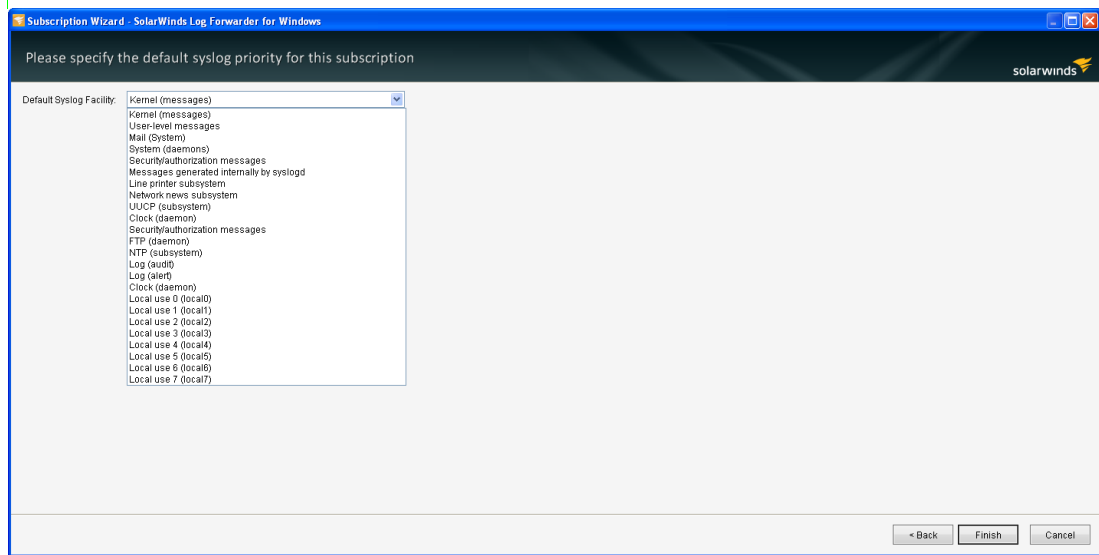
2. Configure the event type, event sources, task category and filtering options:

Field	Value
-------	-------

Event type	Filter event records by one or more of the <i>Error</i> , <i>Warning</i> , <i>Information</i> , <i>Audit Success</i> and <i>Audit Failure</i> event types
Event sources	Filter event records by one or more event sources. Event sources field is populated depending on the chosen event log(s).
Includes/Excludes Event IDs	Filter event records by including and/or excluding event IDs. (for example: you can apply a filter to only show records with event ID's 1, 3 or within the range of 5-99, but excluding events with ID's of 76 by typing: 1,3,5-99,-76)
Task category	Filter event records by one or more task categories. Task categories field is populated depending on the chosen event log (s).
Keywords	Filter event records by keywords (<i>not available for Windows eventing 5 versions of Windows</i>)
User(s)	Filter event records by user(s)
Computer(s)	Filter event records by computer(s)

3. Click the **Refresh** button to preview the event records currently found in your event log(s) which match your subscription configuration settings.

4. Click the **Next >** button to navigate to the next Subscription Wizard screen.



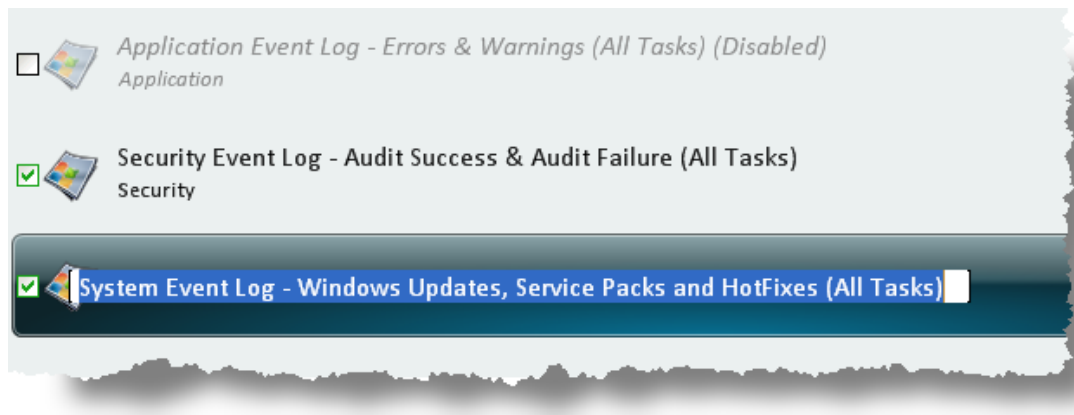
5. Select the **Default Syslog Facility** that the event records will be forwarded to the syslog server(s) with. The *Default Syslog Facility* is combined with the record *Event type*, to form the message *Priority* column data within the Syslog Server display window.

6. Click the **Finish** button to save your subscription configuration settings and return to the Subscriptions listing screen.

2.3 Rename

To rename an existing subscription within the **Subscriptions** screen, select a subscription item then click on the **Rename** button.

The subscription item name will then be made editable for you to make changes.

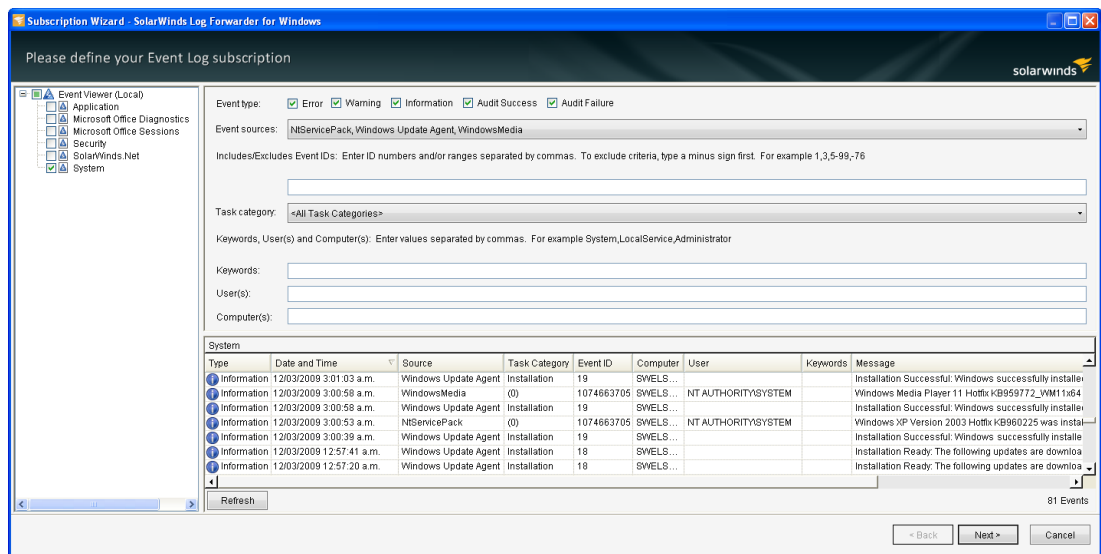


Once you have completed renaming, click out of the subscription item to save the changes.

2.4 Edit Properties

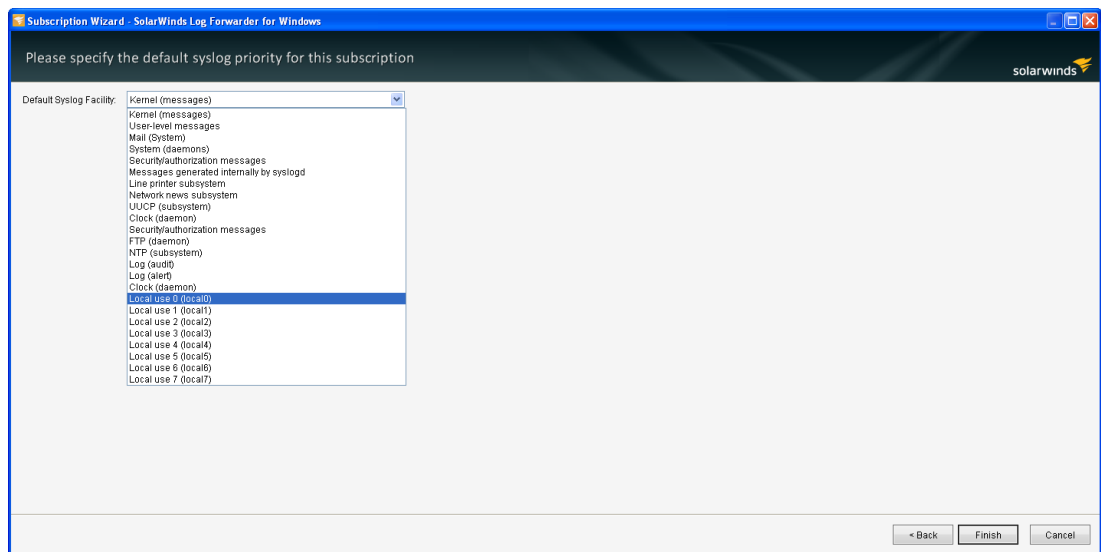
To edit the properties of an existing subscription within the **Subscriptions** screen, select a subscription item then click on the **Edit Properties** button.

On clicking the **Edit Properties** button, the *Subscriptions Wizard* window will appear with the existing fields values displayed.



1. Make your changes to the existing field values accordingly, then click the **Refresh** button to preview the effects of your filtering changes on the event log records.

2. Click the **Next >** button to navigate to the next Subscription Wizard screen to check or change your **Default Syslog Facility** selection.

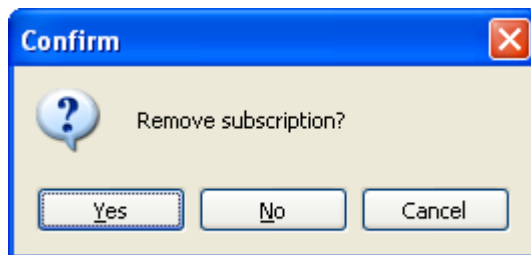


3. Click the **Finish** button to save your subscription configuration settings and return to the Subscriptions listing screen.

2.5 Remove

To remove an existing subscription item from within the **Subscriptions** screen, select a subscription item then click on the **Remove** button.

On clicking the **Remove** button, a confirmation message-box will appear.



Click the **Yes** button to continue with removing the selected subscription item.

3 Syslog Servers

This chapter provides information and guidance relating to the **Syslog Servers** screen in Log Forwarder for Windows.

The following topics can be found in this chapter :

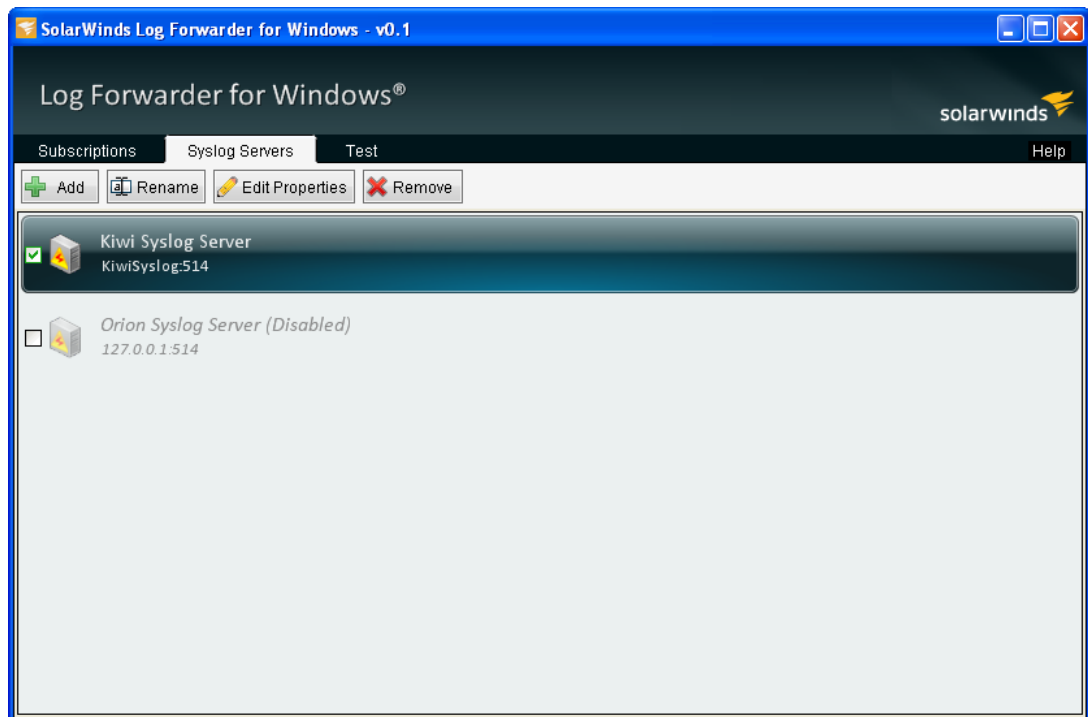
- See **Overview** for a general overview of the **Syslog Servers** screen functionality.
- See **Add** for information on adding a new Syslog Server item to the list.

- See **Rename** for information on renaming an existing Syslog Server item.
- See **Edit Properties** for information on editing the properties of an existing Syslog Server item.
- See **Remove** for information on deleting an existing Syslog Server item from the list.

3.1 Overview

The **Syslog Servers** screen allows you to add or maintain the syslog servers that the Log Forwarder for Windows program forwards the log messages to.

Below is a sample screenshot of the Syslog Servers screen with two syslog servers setup.



- The **Kiwi Syslog Server** has been added using its Hostname and UDP port 514.
- The **Orion Syslog Server** is using the LocalHost IP Address and UDP port 514. This syslog server item has been currently *disabled* by unchecking the item tick-box therefore will not receive forwarded records.

The screen also contains four command buttons:

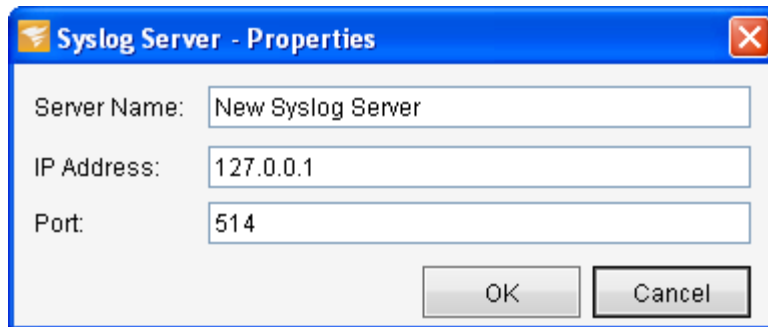
- The **Add** button (always enabled)
- The **Rename** button
- The **Edit Properties** button
- The **Remove** button

Note: The **Rename**, **Edit Properties** and **Remove** buttons are ONLY enabled when a syslog server item has been selected.

3.2 Add

To add a new syslog server within the **Syslog Servers** screen, click on the **Add** button.

On clicking the **Add** button, the *Syslog Server - Properties* window will appear with pre-populated field default values.



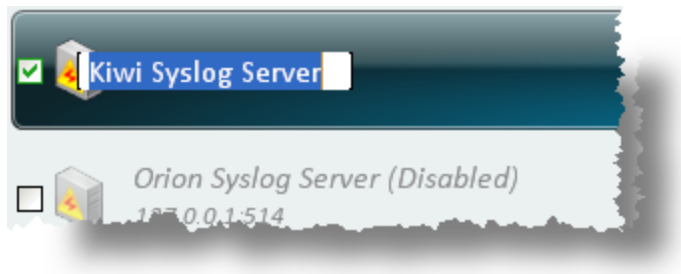
Over-type the default field values accordingly, then click the **OK** button to save your settings.

Field	Value
Server Name	Display name for the syslog server
IP Address	IPv4 or IPv6 Address, Hostname, or a fully qualified domain name of the syslog server
Port	UDP port to send event log messages via

3.3 Rename

To rename an existing syslog server within the **Syslog Servers** screen, select a syslog server item then click on the **Rename** button.

The syslog server item name will then be made editable for you to make changes.

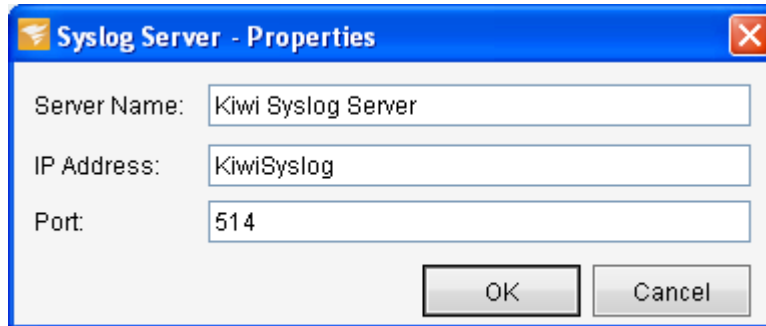


Once you have completed renaming, click out of the syslog server item to save the changes.

3.4 Edit Properties

To edit the properties of an existing syslog server within the **Syslog Servers** screen, select a syslog server item then click on the **Edit Properties** button.

On clicking the **Edit Properties** button, the *Syslog Server - Properties* window will appear with the existing fields values displayed.



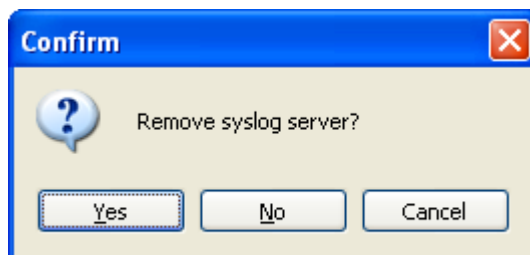
Make your changes to the existing field values accordingly, then click the **OK** button to save your settings.

Field	Value
Server Name	Display name for the Syslog Server
IP Address	IPv4 or IPv6 Address, Hostname, or a fully qualified domain name of the Syslog Server
Port	UDP port to send event log messages via

3.5 Remove

To remove an existing syslog server item from within the **Syslog Servers** screen, select a syslog server item then click on the **Remove** button.

On clicking the **Remove** button, a confirmation message-box will appear.



Click the **Yes** button to continue with removing the selected syslog server item.

4 Test

This chapter provides information and guidance relating to the **Test** screen in Log Forwarder for Windows.

The following topics can be found in this chapter :

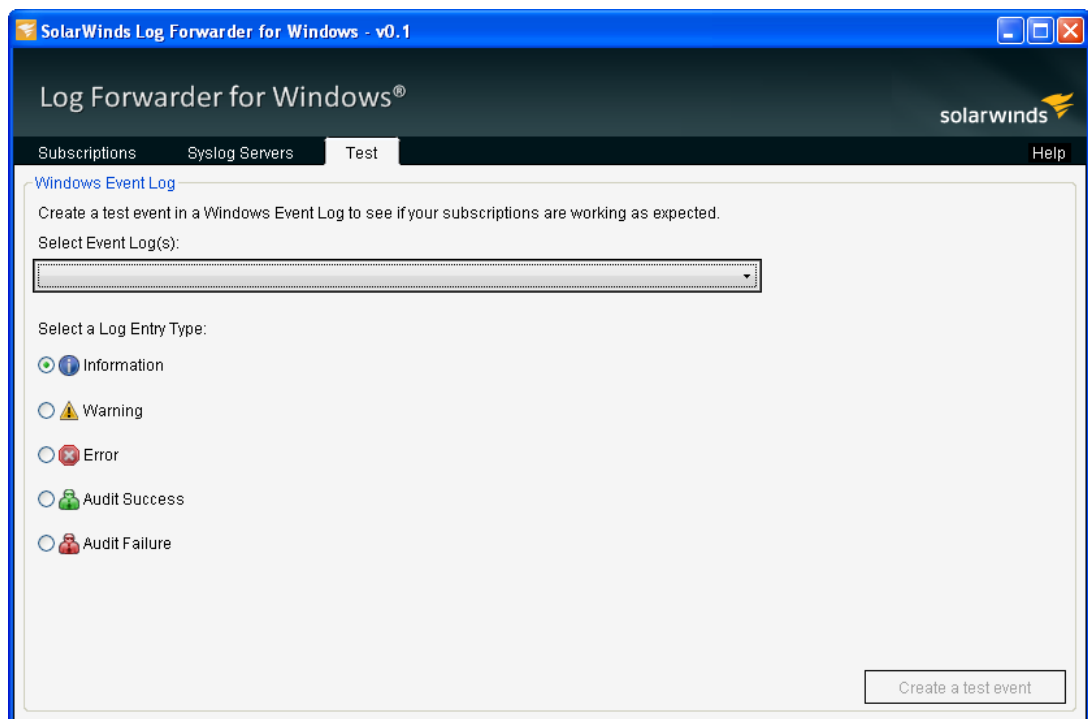
- See **Overview** for a general overview of the **Test** screen functionality.

4.1 Overview

The **Test** screen allows you to add a test event into one of the available Event Logs.

Provided that the Event Log you are adding a test event into is included within one of your **Subscriptions**, and also that you have set-up a **Syslog Server** to forward the messages to; the Test screen could then be used to test the Log Forwarder for Windows functionality and ensure that events are being forwarded.

Below is a screenshot of the **Test** screen.



- Click the **Select Event Log** drop-down field to select an Event Log you wish to add a test event to.
- Next, from the **Select a Log Entry Type** radio field item group, choose the event message type you wish to add to the Event Log.
- Finally, click on the **Create a test event** button to add the test event to the Event Log.

If Log Forwarder for Windows is unsuccessful in creating a test event, a message-box will be displayed. (Below is a common message you may receive if trying to create a test event within the Security Event Log.)



5 Troubleshooting

This chapter contains useful information on troubleshooting issues with the Log Forwarder for Windows.

The following topics can be found in this chapter :

- See **Windows Firewall** for information regarding the Windows Firewall exception.

5.1 Windows Firewall

If turned on, the **Windows Firewall** may block programs or program functionality from being executed on the system.

To prevent blocking of the Log Forwarder for Windows program, the Log Forwarder for Windows product installer will automatically add an **exception** for the program to prevent the Windows Firewall from blocking, when the Windows Firewall is turned on.

If log messages appear not to be forwarding to your designated Syslog Server, please check the Windows Firewall to ensure that the program exception exists

The Windows Firewall exception is *removed* automatically when the product is uninstalled using the Log Forwarder for Windows uninstaller.