Event Log Forwarder for Windows

Version 1.2
© 2019 SolarWinds Worldwide, LLC. All rights reserved.

This document may not be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the prior written consent of SolarWinds. All right, title, and interest in and to the software, services, and documentation are and shall remain the exclusive property of SolarWinds, its affiliates, and/or its respective licensors.

SOLARWINDS DISCLAIMS ALL WARRANTIES, CONDITIONS, OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON THE DOCUMENTATION, INCLUDING WITHOUT LIMITATION NONINFRINGEMENT, ACCURACY, COMPLETENESS, OR USEFULNESS OF ANY INFORMATION CONTAINED HEREIN. IN NO EVENT SHALL SOLARWINDS, ITS SUPPLIERS, NOR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY, EVEN IF SOLARWINDS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

The SolarWinds, SolarWinds & Design, Orion, and THWACK trademarks are the exclusive property of SolarWinds Worldwide, LLC or its affiliates, are registered with the U.S. Patent and Trademark Office, and may be registered or pending registration in other countries. All other SolarWinds trademarks, service marks, and logos may be common law marks or are registered or pending registration. All other trademarks mentioned herein are used for identification purposes only and are trademarks of (and may be registered trademarks) of their respective companies.
# Table of Contents

- Event Log Forwarder Administrator Guide ................................................................. 5
  - Event Log Forwarder Features .................................................................................. 5
- About the Event Log Forwarder ..................................................................................... 6
  - Key Features .............................................................................................................. 6
  - Supported Operating Systems ................................................................................. 6
- Event Log Forwarder Service vs User Interface ............................................................. 7
- System requirements for Event Log Forwarder ............................................................. 8
  - Hardware and software requirements ....................................................................... 8
- Install Event Log Forwarder ......................................................................................... 9
  - Prepare the server to install Event Log Forwarder ....................................................... 9
  - Installation steps for Event Log Forwarder ............................................................... 10
- Configure Log Forwarder settings .............................................................................. 11
  - EventLogSubscriptions ............................................................................................. 11
  - SyslogServers ............................................................................................................ 13
- Deploy the program installer ....................................................................................... 14
  - Event Log Forwarder configuration file ..................................................................... 14
  - Event log subscriptions ............................................................................................ 17
  - Syslog server subscription ....................................................................................... 18
- Subscriptions .................................................................................................................. 21
- Add an event log subscription .................................................................................... 22
  - Enable or disable a subscription ............................................................................... 23
- Rename an event log subscription .............................................................................. 25
- Edit event log subscription properties ...................................................................... 26
- Delete an event log subscription ................................................................................ 28
- Syslog Servers .............................................................................................................. 29
- Add a syslog server ..................................................................................................... 30
- Edit syslog server properties ..................................................................................... 31
- Delete a syslog server ............................................................................................... 32
Event Log Forwarder Administrator Guide

The purpose of this guide is to assist you in installing, configuring, and using the Kiwi Syslog Server Event Log Forwarder (ELF). Use the information in this guide to prepare your environment and begin using Event Log Forwarder.

Event Log Forwarder Features
About the Event Log Forwarder

SolarWinds Event Log Forwarder for Windows (Log Forwarder) is a tool that runs on a Windows® operating system and automatically forwards event log records to a syslog server via User Datagram Protocols (UDP) or Transmission Control Protocols (TCP). It sends events - based on the event source, event ID, users, computers, and keywords in the event - to your syslog server and allows you to take further action against the event. Log Forwarder can be used to send syslog messages to a configured NPM server or Kiwi Syslog Server.

Event Log Forwarder for Windows supports forwarding of both Windows Eventing 5 and 6 event records:


Key Features

Log Forwarder provides the following features for monitoring and send Windows events:

- Quickly specify and automatically send events from workstations and servers to your syslog server.
- Export event data from Windows servers and workstations.
- Filter events to forward by source, type ID, and specific keywords.
- Forward events to external systems to alert, store, and audit activity.
- Send events to multiple servers over UDP or TCP.

Supported Operating Systems

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

Both x86 and x64 editions of Windows are supported.

- Windows 10
- Windows 8 | Windows 8.1
- Windows 7 | Windows 7 SP1
- Windows Server 2016
- Windows Server 2012 | 2012 R2
- Windows Server 2008 | 2008 SP2 | 2008 R2 | 2008 R2 SP1
- Windows Server 2003 R2 SP2

For more information on supported software, see Windows Server Support.
Event Log Forwarder Service vs User Interface

After you have downloaded and extract the Log Forwarder files, you can use one of two options to set up your program: the application or the Windows installer. Event Log Forwarder for Windows is comprised of two standard application executables (.exe):

- The Service (LogForwarder.exe)
- The User Interface (LogForwarderClient.exe)

Log Forwarder User Interface

The Event Log Forwarder for Windows user interface allows you to configure the Service. It can - depending on which options were selected during installation - be opened using the SolarWinds Event Log Forwarder for Windows desktop shortcut item, the Quicklaunch item, or from the SolarWinds Event Log Forwarder for Windows Program group accessible from the Windows Start button.

Log Forwarder Service

Event Log Forwarder for Windows Service is named SolarWinds Event Log Forwarder for Windows and is installed and started during the installation process. The Service allows you to check or manage the Event Log Forwarder for Windows Service (start, stop, restart etc.) from the Windows Services manager. You can also run the Windows command prompt: `Net Start "ServiceName"`. 
System requirements for Event Log Forwarder

Before you install Event Log Forwarder, verify that your server meets the following minimum hardware and software requirements.

**Hardware and software requirements**

<table>
<thead>
<tr>
<th>Hardware and software</th>
<th>Requirements</th>
</tr>
</thead>
</table>
| Operating System       | - Windows® 10  
|                        | - Windows 8 | Windows 8.1  
|                        | - Windows 7 | Windows 7 SP1  
|                        | - Windows Server 2016  
|                        | - Windows Server 2012 | 2012 R2  
|                        | - Windows Server 2008 | 2008 SP2 | 2008 R2 | 2008 R2 SP1  
|                        | - Windows Server 2003 R2 SP2  
|                        | For more information on supported software, see [Windows Server Support](#).  
|                        | ![Both x86 and x64 editions of Windows are supported.](#)  
| Hard drive space       | 20 MB  
| CPU                    | 1.2 GHz  
| RAM                    | 256 MB  

For more information on supported software, see [Windows Server Support](#).
# Install Event Log Forwarder

Use the following information to prepare the environment and install Log Forwarder.

## Prepare the server to install Event Log Forwarder

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review system requirements</td>
<td>Verify that your environment meets the <a href="#">hardware and software requirements</a>.</td>
</tr>
<tr>
<td>Run all Windows updates</td>
<td>Check for and <strong>run all Microsoft Windows Updates</strong> on the server. If a Windows update runs, your system might reboot.</td>
</tr>
</tbody>
</table>
| Check for antivirus software              | Determine if any antivirus software is installed on the server where you plan to install Event Log Forwarder. Exclude the SolarWinds directory. For example, on Windows Server 2016, exclude the directory:  
                                       | **C:\ProgramData\SolarWinds\**  
                                       | For a full list of antivirus exclusions, see [Files and directories to exclude from antivirus scanning](#). |

*Note:* Do not exclude executable files. SolarWinds assumes that **C:\** is the default volume.
### Installation steps for Event Log Forwarder

<table>
<thead>
<tr>
<th>Task</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Download the installation file</td>
<td>Complete the following steps for new and existing users. If you have purchased another Kiwi product, such as Kiwi Syslog Server or Kiwi CatTools:</td>
</tr>
<tr>
<td></td>
<td>1. Log in to the SolarWinds Customer Portal. If you do not have a SolarWinds account, see <a href="#">Access the Customer Portal</a> to create an account.</td>
</tr>
<tr>
<td></td>
<td>2. Navigate to Downloads &gt; Download Product.</td>
</tr>
<tr>
<td></td>
<td>3. Select &quot;Kiwi (CatTools, Syslog Viewer, Log Viewer)&quot; from the Products drop-down field.</td>
</tr>
<tr>
<td></td>
<td>If you do not have a previously purchased Kiwi product:</td>
</tr>
<tr>
<td></td>
<td>3. Enter your contact information. All fields are required to download Event Log Forwarder.</td>
</tr>
<tr>
<td></td>
<td>4. Click Proceed to Free Download.</td>
</tr>
<tr>
<td>Run the installation file</td>
<td>1. Log in to your server as an administrator.</td>
</tr>
<tr>
<td></td>
<td>2. Extract the contents of the downloaded installation ZIP file to the server.</td>
</tr>
<tr>
<td></td>
<td>3. Run the application version of <code>SolarWinds_Event_LogForwarder_Setup.exe</code>. If .NET framework 4.0 is not installed, you are prompted to install it. Click Download and install this feature. Then restart <code>SolarWinds_Event_LogForwarder_Setup.exe</code>.</td>
</tr>
<tr>
<td>Complete the Event Log Forwarder setup wizard</td>
<td>1. If you agree with the license agreement, click Next.</td>
</tr>
<tr>
<td></td>
<td>2. Select the shortcuts to create, and click Next.</td>
</tr>
<tr>
<td></td>
<td>3. Specify the installation location, and click Next. The installer displays status messages as it installs Event Log Forwarder.</td>
</tr>
<tr>
<td>Close the wizard</td>
<td>Click Finish to close the Event Log Forwarder setup wizard and open Event Log Forwarder.</td>
</tr>
</tbody>
</table>
Configure Log Forwarder settings

The Event Log Forwarder for Windows Subscriptions and Syslog Server settings are stored in the LogForwarderSettings.cfg configuration file, located in the product installation directory: \Program Files (x86)\SolarWinds\SolarWinds Event Log Forwarder for Windows. The configuration file uses XML markup language.

You can make changes to Subscription or Syslog Server settings from this configuration file, or from the Log Forwarder user interface. When a change is saved within the user interface, the configuration file is updated and the Service re-initializes to pick up the changes immediately.

EventLogSubscriptions

Edit the details of an event log subscription used by Log Forwarder. Each subscription is contained under an individual <EventLogSubscription> element. You can configure the event type, event sources, event IDs, tasks, and so on, for specific subscriptions.

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
</table>
| <channels> | • Channels monitored by the subscription, for example, System or Windows PowerShell.  
               • Each channel type must be entered on an individual <string> child-element. |
| <types>    | • The event type logged by the subscription.  
               • The event type is indicated by an integer. Each type must be entered on an individual <int> child-element.  
               • 1 = Error  
               • 2 = Warning  
               • 3 = Information |
| <sources>  | • Source device of the event.  
               • The source must be entered on an individual <string> child-element.  
               • To indicate that all device sources should be used, leave the <source> element empty. |
| <eventIDs> | • Events to include, or exclude. For excluded events, type a minus sign before the ID: 1, -3, 5  
               • Each eventID must be entered on an individual <string> child-element. |
| <categories>| • Task category of the event.  
               • Each task category must be entered on an individual <string> child-element.  
               • To indicate that all task categories should be used, leave the <source> element empty. |
### Keywords
- Keywords used by the event subscription filter. Event Log Forwarder has specific pre-configured keywords that must be used.
- Each keyword must be entered on an individual `<string>` child-element.
- To indicate that all keywords should be used, leave the `<source>` element empty.

### Users
- User types used by the event subscription filter. For example: Admin, System, Local
- Each user must be entered on an individual `<string>` child-element.

### Computers
- Name of the device the event subscription filters by. For example: AdminMachine, Workstation05
- Each computer must be entered on an individual `<string>` child-element.

### Facility
- Default syslog facility priority for the event subscription.
- The facility is determined by an integer. Use the appropriate facility ID:
  - 1 = Kernel (messages)
  - 2 = User-level messages
  - 3 = Mail (System)
  - 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)

### Enabled
- True/false boolean that determines if the configured event subscription is active.
- This triggers the Enable/Disable button on the Subscriptions tab.

### Name
- Name of the configured event subscription.
Activates the "preview of matching events" window in the event subscription configuration window.

When shown, the preview window displays the records that matches the event subscription criteria.

**SyslogServers**

Edit the details of a syslog server used by Log Forwarder. Each syslog server is contained under an individual `<SyslogServer>` element. You can configure the server name, IP address, port, and so on, for specific syslog servers.

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;enabled&gt;</code></td>
<td>• True/false boolean that determines if the configured syslog server is active.</td>
</tr>
<tr>
<td></td>
<td>• This triggers the Enable/Disable button on the Syslog Server tab in Log Forwarder.</td>
</tr>
<tr>
<td><code>&lt;SendMode&gt;</code></td>
<td>• Protocol used for sending messages from the syslog server</td>
</tr>
<tr>
<td></td>
<td>• The protocol is indicated by an integer.</td>
</tr>
<tr>
<td></td>
<td>○ 0 = UDP</td>
</tr>
<tr>
<td></td>
<td>○ 1 = TCP</td>
</tr>
<tr>
<td><code>&lt;SourceFormat&gt;</code></td>
<td>• Server address system type of the syslog server.</td>
</tr>
<tr>
<td></td>
<td>• The source format is indicated by an integer.</td>
</tr>
<tr>
<td></td>
<td>○ 0 = IPv4</td>
</tr>
<tr>
<td></td>
<td>○ 1 = IPv6</td>
</tr>
<tr>
<td></td>
<td>○ 2 = FQDN</td>
</tr>
<tr>
<td></td>
<td>○ 3 = Host name</td>
</tr>
</tbody>
</table>
Deploy the program installer

The Event Log Forwarder for Windows installer is provided as a standard application executable file (.exe) and as a Windows Installer Package file (.msi). The Windows Installer Package file is provided for "silent" deployments using the /quiet switch.

To run the .msi file on the target machine, use the following command syntax: SolarWinds_Event_LogForwarder_<Version>_Setup.msi /quiet

ℹ️ The .msi installer package for Event Log Forwarder for Windows does not include the prerequisites installer, which automatically downloads and installs any required prerequisite software, such as .NET Framework 4.0 from Microsoft. In order to successfully deploy Event Log Forwarder, first ensure that the required software is already installed on your server.

Event Log Forwarder configuration file

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

The configuration file contains a nest hierarchy of XML tags and subtags that specify the configuration settings. It is located in the installation directory of Event Log Forwarder, usually C:\Program Files (x86)\SolarWinds\SolarWinds Event Log Forwarder for Windows. To deploy the configuration file to a target machine, copy the LogForwarderSettings.cfg file to the Event Log Forwarder for Windows installation directory after the .msi file has been successfully installed.

All configuration information resides between the <LogForwarderSettings> and </LogForwarderSettings> root XML tags. Configuration information between the tags is grouped into two main sections:

- <EventLogSubscriptions>
- <SyslogServers>

Both of the above groups are required.

```xml
<?xml version="1.0" encoding="utf-8"?>
   <EventLogSubscriptions> ...
   </EventLogSubscriptions>
   <SyslogServers> ...
   </SyslogServers>
</LogForwarderSettings>
```
Example: Declare Event Log Subscriptions

For Event Log Subscriptions, each subscription is declared with an `<EventLogSubscription>` tag. The following LogForwarder.cfg code snippet declares to Event Log Subscriptions:

```xml
<?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/>
        </EventLogSubscription>
    </EventLogSubscriptions>
</LogForwarderSettings>
```
Example: Declare syslog servers

For syslog servers, each syslog server is declared with an <Syslog Server> tag. The following LogForwarderSettings.cfg file declares two syslog servers in Log Forwarder.

```xml
<?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>
      <SendMode>0</SendMode>
      <SourceFormat>0</SourceFormat>
    </SyslogServer>
    <SyslogServer>
      <serverName>Syslog Server B</serverName>
      <IPAddress>192.168.1.10</IPAddress>
      <Port>514</Port>
      <enabled>true</enabled>
      <SendMode>0</SendMode>
      <SourceFormat>0</SourceFormat>
    </SyslogServer>
  </SyslogServers>
</LogForwarderSettings>
```
Event log subscriptions

Each configured event log subscription must include the following tag declarations:

<table>
<thead>
<tr>
<th>Tag</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;channels&gt;</td>
<td>A list of valid event log channels (e.g. Application, System, Security) that are subscribed to. Each is a subtag of type &lt;string&gt;.</td>
</tr>
<tr>
<td>&lt;types&gt;</td>
<td>A list of valid event log types. Each is a subtag of type &lt;int&gt;. Valid values are:</td>
</tr>
<tr>
<td></td>
<td>• 1 - Error</td>
</tr>
<tr>
<td></td>
<td>• 2 - Warning</td>
</tr>
<tr>
<td></td>
<td>• 4 - Information</td>
</tr>
<tr>
<td></td>
<td>• 8 - Audit Success</td>
</tr>
<tr>
<td></td>
<td>• 16 - Audit Failure</td>
</tr>
<tr>
<td>&lt;sources&gt;</td>
<td>A list of valid event log sources. Each is a subtag of type &lt;string&gt;.</td>
</tr>
<tr>
<td>&lt;eventIDs&gt;</td>
<td>A list of valid event IDs or event ID ranges. Each is a subtag of type &lt;string&gt;.</td>
</tr>
<tr>
<td>&lt;categories&gt;</td>
<td>A list of valid event log task categories. Each is a subtag of type &lt;string&gt;.</td>
</tr>
<tr>
<td>&lt;keywords&gt;</td>
<td>A list of event keywords. Each is a subtag of type &lt;string&gt;.</td>
</tr>
<tr>
<td>&lt;users&gt;</td>
<td>A list of users on the syslog server. Each is a subtag of type &lt;string&gt;.</td>
</tr>
<tr>
<td>&lt;computers&gt;</td>
<td>A list of computers monitored by the syslog server. Each is a subtag of type &lt;string&gt;.</td>
</tr>
<tr>
<td>&lt;facility&gt;</td>
<td>The default syslog facility number to use when generating a syslog message to send. For more information, see Syslog facility numbers.</td>
</tr>
<tr>
<td>&lt;enabled&gt;</td>
<td>Enables the event log subscription. Uses TRUE/FALSE syntax.</td>
</tr>
<tr>
<td></td>
<td>• TRUE: the event log subscription is active in Log Forwarder.</td>
</tr>
<tr>
<td></td>
<td>• FALSE: the event log subscription is inactive in Log Forwarder.</td>
</tr>
<tr>
<td>&lt;name&gt;</td>
<td>The name of event log subscription.</td>
</tr>
<tr>
<td>&lt;description&gt;</td>
<td>The description of the event log subscription.</td>
</tr>
</tbody>
</table>

Syslog facility numbers

A facility number (code) is used to specify the program type logging the syslog message. The list below identifies the default syslog facility numbers to use when generating a syslog message to send to a syslog server.
<table>
<thead>
<tr>
<th>Facility</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kernal (messages)</td>
<td>0</td>
</tr>
<tr>
<td>User-level messages</td>
<td>1</td>
</tr>
<tr>
<td>Mail system</td>
<td>2</td>
</tr>
<tr>
<td>System (daemons)</td>
<td>3</td>
</tr>
<tr>
<td>Security / authorization messages</td>
<td>4</td>
</tr>
<tr>
<td>Messages generated internally by syslogd</td>
<td>5</td>
</tr>
<tr>
<td>Line printer subsystem</td>
<td>6</td>
</tr>
<tr>
<td>Network news subsystem</td>
<td>7</td>
</tr>
<tr>
<td>Unix-to-Unix Copy Protocol (UUCP) (subsystem)</td>
<td>8</td>
</tr>
<tr>
<td>Clock (daemon)</td>
<td>9</td>
</tr>
<tr>
<td>Security / authorization messages</td>
<td>10</td>
</tr>
<tr>
<td>File Transfer Protocol (FTP) (daemon)</td>
<td>11</td>
</tr>
<tr>
<td>Network Time Protocol (NTP) (subsystem)</td>
<td>12</td>
</tr>
<tr>
<td>Log (audit)</td>
<td>13</td>
</tr>
<tr>
<td>Log (alert)</td>
<td>14</td>
</tr>
<tr>
<td>Clock (daemon)</td>
<td>15</td>
</tr>
<tr>
<td>Local use 0 (local0)</td>
<td>16</td>
</tr>
<tr>
<td>Local use 1 (local1)</td>
<td>17</td>
</tr>
<tr>
<td>Local use 2 (local2)</td>
<td>18</td>
</tr>
<tr>
<td>Local use 3 (local3)</td>
<td>19</td>
</tr>
<tr>
<td>Local use 4 (local4)</td>
<td>20</td>
</tr>
<tr>
<td>Local use 5 (local5)</td>
<td>21</td>
</tr>
<tr>
<td>Local use 6 (local6)</td>
<td>22</td>
</tr>
<tr>
<td>Local use 7 (local7)</td>
<td>23</td>
</tr>
</tbody>
</table>

**Syslog server subscription**

Each syslog server must include the following tag declarations.
<table>
<thead>
<tr>
<th>Tag</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;serverName&gt;</code></td>
<td>The name of the syslog server you are subscribing.</td>
</tr>
<tr>
<td><code>&lt;IPAddress&gt;</code></td>
<td>A valid syslog server IP address, host name, or FQDN. IP address must be IPv4 or IPv6.</td>
</tr>
<tr>
<td><code>&lt;Port&gt;</code></td>
<td>The syslog server port number. Default is 514.</td>
</tr>
<tr>
<td><code>&lt;enabled&gt;</code></td>
<td>Enables the syslog server. Uses TRUE/FALSE syntax.</td>
</tr>
<tr>
<td></td>
<td>- TRUE: the syslog server is active in Log Forwarder.</td>
</tr>
<tr>
<td></td>
<td>- FALSE: the syslog server is inactive in Log Forwarder.</td>
</tr>
<tr>
<td></td>
<td>Events collected are only forwarded to syslog servers that are enabled.</td>
</tr>
<tr>
<td><code>&lt;SendMode&gt;</code></td>
<td>Decides which protocol to use when sending logs:</td>
</tr>
<tr>
<td></td>
<td>- TCP</td>
</tr>
<tr>
<td></td>
<td>- UDP</td>
</tr>
<tr>
<td></td>
<td>- 1-TCP</td>
</tr>
<tr>
<td></td>
<td>- 0-UDP</td>
</tr>
<tr>
<td><code>&lt;SourceFormat&gt;</code></td>
<td>Decides the server address format as IPv4 or IPv6.</td>
</tr>
</tbody>
</table>

**Sample syslog server subscription**

```xml
<?xml version="1.0" encoding="utf-8"?>
<LogForwarderSettings xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xs="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>
      <SendMode>0</SendMode>
      <SourceFormat>0</SourceFormat>
    </SyslogServer>
    <SyslogServer>
      <serverName>Syslog Server B</serverName>
      <IPAddress>192.168.1.10</IPAddress>
      <Port>514</Port>
    </SyslogServer>
  </SyslogServers>
</LogForwarderSettings>
```
<enabled>true</enabled>
<SendMode>0</SendMode>
<SourceFormat>0</SourceFormat>
</SyslogServer>
</SyslogServers>
</LogForwarderSettings>
Subscriptions

Creating event log subscriptions defines which event log records are forwarded to your syslog servers. The Subscriptions screen allows you to add or maintain the subscriptions you have created for the Event Log Forwarder program.

![Event Log Forwarder Dashboard](image)

The command buttons Edit, Rename, Enable/Disable, and Remove are only available when a subscription item has been selected.

This chapter provides information relating to the Subscriptions screens in Event Log Forwarder for Windows. The following topics are covered:

- Add an event log subscription
- Rename an event log subscription
- Edit event log subscription properties
- Remove an event log subscription
Add an event log subscription

In the Add window, you can configure the event type and filtering options.

1. From the Subscriptions tab, click Add.
2. Select the event log (or event logs) you wish to subscribe to from the left column tree.
3. Configure the Event type, Event sources, and Task category, and filtering options:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Type</td>
<td>Filters the event records by the event type selected.</td>
</tr>
<tr>
<td>Event Sources</td>
<td>Filters the event records by one or more event source.</td>
</tr>
<tr>
<td></td>
<td>The Event Sources field is populated based on the selected event log.</td>
</tr>
</tbody>
</table>
Include or Exclude Event

Enter the relevant event IDs. Event records containing an specified event ID are excluded or included in the event filter. Event IDs with a minus sign are excluded.

For example, to apply a filter that only shows records with event ID 1, 3, are within the range of IDs 5–99, and excludes event ID 76, enter: 1, 3, 5–99, –76.

Task Category

Filter event records by one or more selected task categories.
The Task Category field is populated based on the selected event log.

Keywords

Filter the event records by specified keywords.
Not available for Windows Eventing 5 versions of Windows.

Users

Filter event records by the user logged in to the device at the time of the event.
Multiple users must be separated by commas.

Computers

Filter event records by devices the event occurs on.

4. By default, you are provided a grid view of the event from the selected subscriptions. To hide or show this preview, click Hide / Show preview of matching records.

5. Click Refresh to preview the event records currently found in your event logs, based on configured subscription settings.

6. Click Next to continue to the Define Priority screen.

7. Select the default syslog facility number that the event records when forwarding messages to the syslog server.

   The default syslog facility number is combined with the record event type to form the message Priority column data within the syslog server display window.

8. Click Finish.

Enable or disable a subscription

You can enable or disable an existing subscription from the Subscriptions screen. Only one subscription can be enabled or disabled at a time. Any disabled subscription is greyed out on the subscriptions tab.
1. From the Subscriptions tab, select a subscription item.
2. Hover your pointer over Enable/Disable.
3. From the drop-down field, select Enable or Disable.
Rename an event log subscription

To rename an existing subscription within the Subscriptions screen:

1. From the Subscriptions tab, select the subscription item to edit.
2. Click Rename.
3. Enter a new subscription name.
4. Click Update to save your changes.
**Edit event log subscription properties**

To edit the properties of an existing subscription:

1. From the Subscriptions tab, select the subscription to edit.
2. Click Edit.
3. Make your changes to the existing subscription fields accordingly.
4. Click Refresh to preview selected filtering changes on the event log records.
5. Click Next.
6. Confirm or update your default syslog facility settings.

7. Click Finish to save your changes.
Delete an event log subscription

To delete an existing subscription from Event Log Forwarder:

1. From the Subscriptions tab, select the subscription to be deleted.
2. Click Remove.
3. In the confirmation message box, click Yes to continue removing the selected subscription item.
Syslog Servers

The Syslog Servers tab allows you to add or maintain syslog servers that the Event Log Forwarder program forwards log messages to.

For example, the following image displays the setup of two syslog servers in Event Log Forwarder:

- The Alpha Syslog Server has been added using a local host IP address and UDP port 468.
- The Beta Syslog Server has been added using the host name and TCP port 514. Notice that the Beta Syslog Server has been disabled in Event Log Forwarder and therefore does not receive forwarded log records.

This chapter provides information relating to the Syslog Servers tab in Event Log Forwarder. The following topics are covered:

- Add a syslog server
- Edit syslog server properties
- Remove a syslog server
Add a syslog server

From the Add Syslog Server window, you can configure the syslog server details. Only syslog servers added to Event Log Forwarder receive configured log subscription reports.

1. From the Syslog Servers tab, click Add. The Add Syslog Server properties window opens with pre-populated field default values.

2. Enter values into the default fields accordingly.

   The Server Address field accepts IPv4, IPv6, host names, or fully qualified domain names of a syslog server.

3. Click Create to add the syslog server.
Edit syslog server properties

To edit the properties of an existing syslog server in Event Log Forwarder:

1. From the Syslog Servers tab, select the syslog server item to edit.
2. Click Edit.
3. To rename the syslog server, enter the new syslog server name. You cannot enter a name that already exists.

4. Edit existing values displayed in fields as necessary.
5. Click Update to save your changes.
Delete a syslog server

To remove an existing syslog server from Event Log Forwarder:

1. From the Syslog Server tab, select the syslog server to be deleted.
2. Click Remove.
3. In the confirmation message box, click Yes to continue removing the selected syslog server.
Testing

The Test tab allows you to add a test event to an available event log subscription. You can only perform a test event on subscriptions that are configured with a syslog server configured in Event Log Forwarder to receive messages from that subscription.

Both the subscription and the syslog server must be configured to test the Event Log Forwarder’s functionality and ensure that events are correctly forwarding.

Test an event log subscription

1. From the Test tab, select which event log subscriptions you want to test from the drop-down field.

2. Under Type of test event, select the event message type to add to the event log subscription.

3. Click Create a test event to add the test event to the event log subscription.
A test that has been created successfully is validated with a confirmation message "Test event successfully created":

If the test event does not execute, the validation message instead states: "Creation of test event was unsuccessful".
Troubleshooting

You can find discussion topics and solutions to common issues in Event Log Forwarder on the Success Center or on THWACK.

Event Log Forwarder is a free tool and is not supported by SolarWinds technical support.

Windows Firewall

When the Windows Firewall is enabled, the firewall may block programs or program functionality from executing on your system.

To prevent blocking of the Event Log Forwarder, the product installer automatically adds an exception for the program to prevent the Windows Firewall from blocking Event Log Forwarder functions.

- If log messages are not forwarding to your designated syslog server, check your Windows Firewall settings to ensure that a program exception exists.
- The Windows Firewall exception is automatically removed when Event Log Forwarder is uninstalled using the program's uninstaller. Re-installation of Event Log Forwarder requires adding the exception back into your system's Windows Firewall.