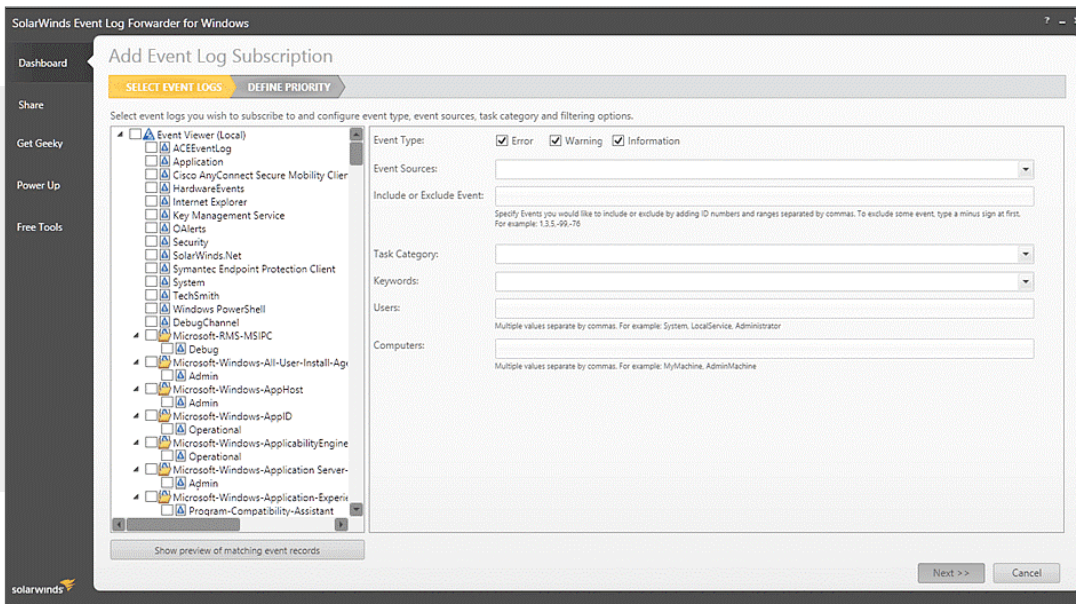


How to Send Windows Event Logs to Log Manager for Orion



MONITOR AND MANAGE YOUR WINDOWS EVENTS LOGS WITH EASE

[TRY IT FREE](#)

Your infrastructure is continuously generating log data to provide network performance insight. Whether it is syslog, SNMP traps, or Windows® events, they often provide crucial bits of insight to help with troubleshooting. With Log Manager for Orion®, you can collect, consolidate, and analyze log information with one tool to help you find the root cause faster.

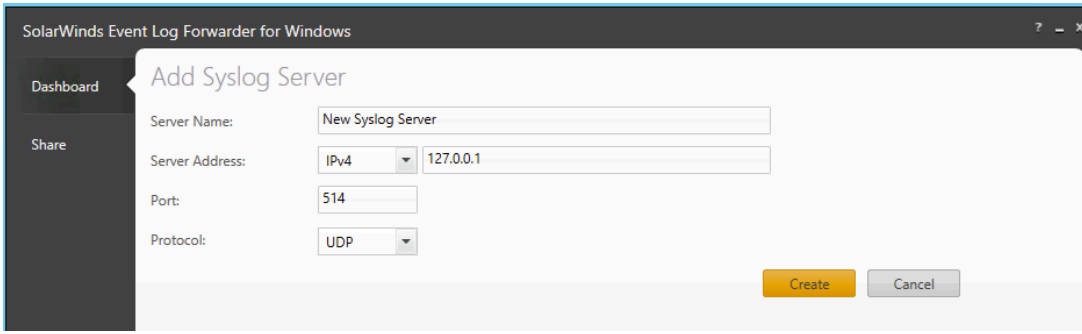
To forward your Windows events to Log Manager, you must first download SolarWinds® FREE [Event Log Forwarder for Windows](#). Using this free tool, you can forward Windows events based on events source, event IDs, computers, and keywords in the event to Log Manager for Orion.

Follow these steps to forward your Windows events to Log Manager for Orion.

1. Configure your Event Log Forwarder

Configure Event Log Forwarder for Windows to send log data to Log Manager. Go to 'Syslog Servers' and add your Log Manager/Orion server details (default port 514/UDP is fine). If you need to forward the logs to multiple servers, you can list additional servers in [LogForwarderSettings.cfg](#).

TRY IT FREE

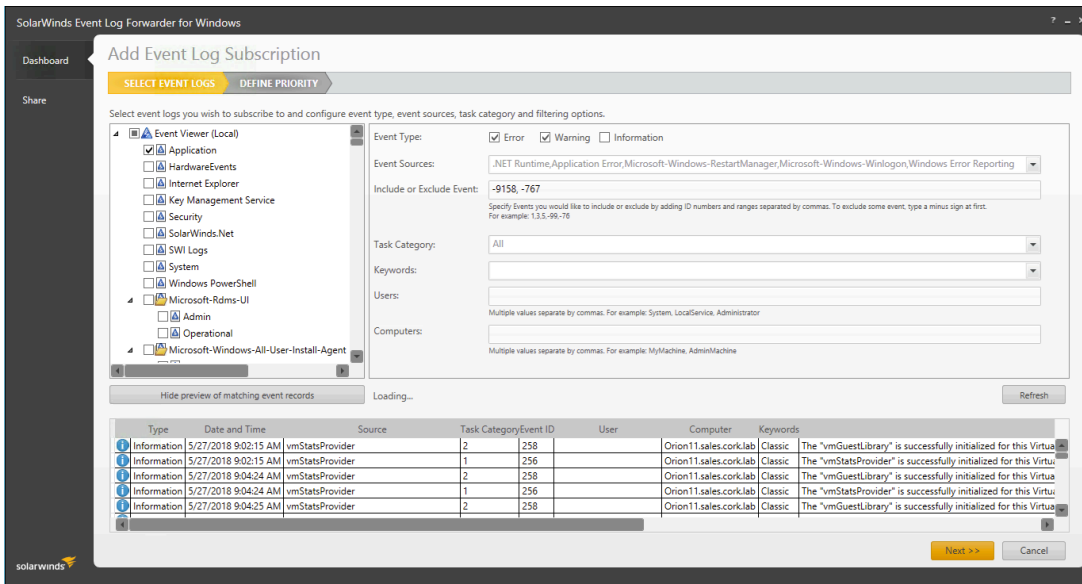


2. Configure logs you want to transmit

Configure which logs you want to transmit to Log Manager. In addition to the Application, System, and Security logs, Windows Event Viewer includes a vast array of other categories. The Log Forwarder also allows you to customize exactly which logs are sent to Log Manager to ensure that only certain events are forwarded and you are not bombarded with noise.

You could configure Log Forwarder to only send error and warning logs from systems and applications while excluding certain event IDs such as Windows Filtering Platform events (which are notoriously noisy).

In this example, error and warning logs have been configured to be sent from a number of application logs, excluding two event IDs. You can use the 'Show preview of matching event records' option to get a sneak peek at logs that match your conditions.

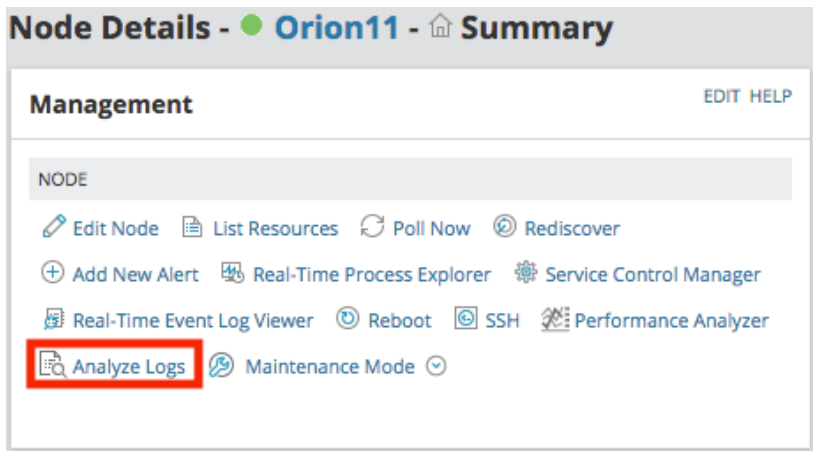


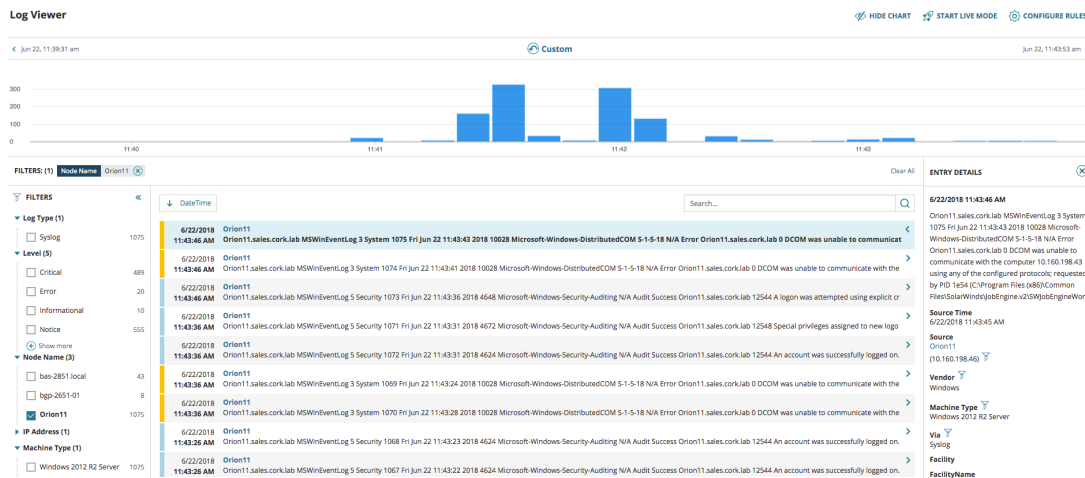
3. Ensure that you have added the node to Orion

Now that logs are being sent to Log Manager, you need to ensure you have added the node to Orion. If not, you'll get a notification in Orion to let you know that log data from an unknown node is being received.

When you browse to the Node Details page you'll notice the 'Analyze Logs' button, which will take you directly to the Log Viewer and display the Windows Events for that node. This additional layer of visibility and immediate access to log data can be especially useful when troubleshooting a server or application issue in Server & Application Monitor (SAM).

TRY IT FREE





TRY IT FREE

4. Get ready to view, filter, search, and chart Windows events like syslog and traps!

At this point you can now view, filter, search, and chart your Windows Events in the same way as your syslog and traps.

LEARN MORE

AMERICAS

Phone: 866.530.8100
 Fax: 512.682.9301
 Email: sales@solarwinds.com

EMEA

Phone: +353 21 5002900
 Fax: +353 212 380 232
 Email: emeasales@solarwinds.com

APAC

Tel : +65 6593 7600
 Fax : +65 6593 7601
 Email: sales@solarwinds.com

For product information about SolarWinds products, visit solarwinds.com, call, or email.
 7171 Southwest Parkway | Building 400 | Austin, Texas 78735



For additional information, please contact SolarWinds at 866.530.8100 or email sales@solarwinds.com.
 To locate an international reseller near you, visit http://www.solarwinds.com/partners/reseller_locator.aspx

© 2018 SolarWinds Worldwide, LLC. All rights reserved.

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.