smartzone™

Technical Reference 050-SZ

Published: **7/25/18**

Configuring the Syslog Feature

Applies to:	Syslog setup in SmartZone
Objective:	If you desire to set up a syslog in the SmartZone™ Software as an optional feature, the following technical reference will walk you through the setup of a syslog and syslog daemon using Kiwi as an example.

Description

Syslogs are typically used for computer system management and security audits and are supported by a wide variety of devices and receivers across multiple platforms. Because of this, a syslog can be used to consolidate log data output and events from many different types of systems into a central repository.

Performing the Procedure

1. Obtain the Kiwi Syslog Daemon 9.2 file download, and a file download screen will appear.

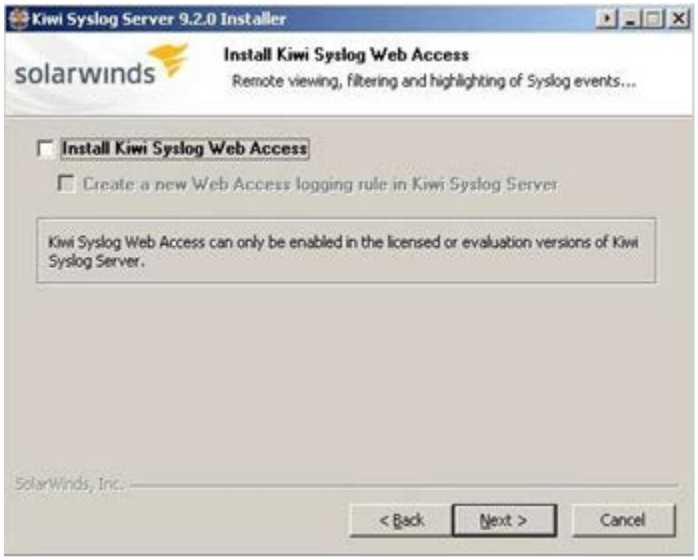
2. Choose **Save** to save the SyslogServer-v9.zip file to your system, and the file will download to your local computer. Extract the **Kiwi_Syslog_Server_9.2.0.setup.exe** file from the compressed file and double click to execute.

3. After reading the license agreement, choose **I Agree** to begin the installation.

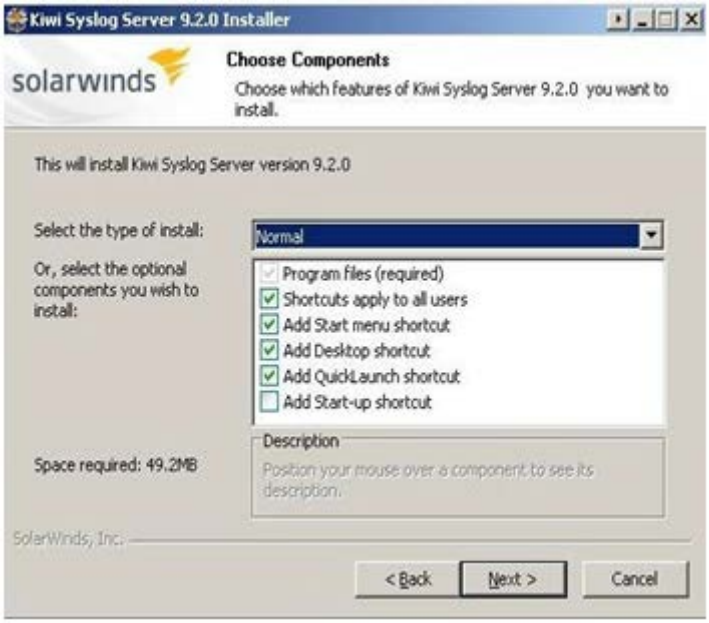
4. Choose whether to install the syslog daemon as a service or as an application and choose **Next** to bring up the service installation screen.

5. Choose the account in which the daemon will be installed and choose the **Next** button to bring up the Web Access screen.

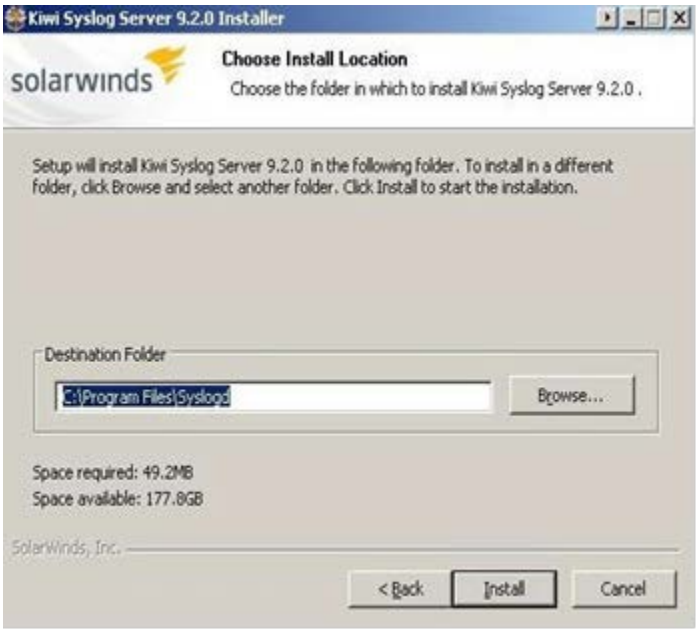
6. Uncheck “Install Kiwi Syslog Web Access” and choose the **Next** button to bring up the Components screen.



7. Choose the syslog daemon components you want to install and choose **Next** to bring up the Install Location screen.



8. Choose the location in which the software should be installed and select the **Install** button begin the installer.



9. Once the installation is complete, you will be prompted with a final installation wizard screen.

10. Select the **Finish** button to complete the installation.

Configuring the Syslog File

1. Configure the syslog configuration file on the SmartZone™ server to point to the location of the syslog daemon by updating the SYSLOG.properties file in c:\Program Files\PANDUIT Physical Infrastructure Manager\jboss\server\ pvng\conf folder as below:

LOG_SERVER= 192.168.0.37 <**ip_address where syslog daemon is running**>

DEST_PORT=514 **(default port for UDP)**

FACILITY=23

TAG=PanView iQ

Information listed in red will be dependent upon your own system configuration.

//Trap Severity mapping to Syslog severity

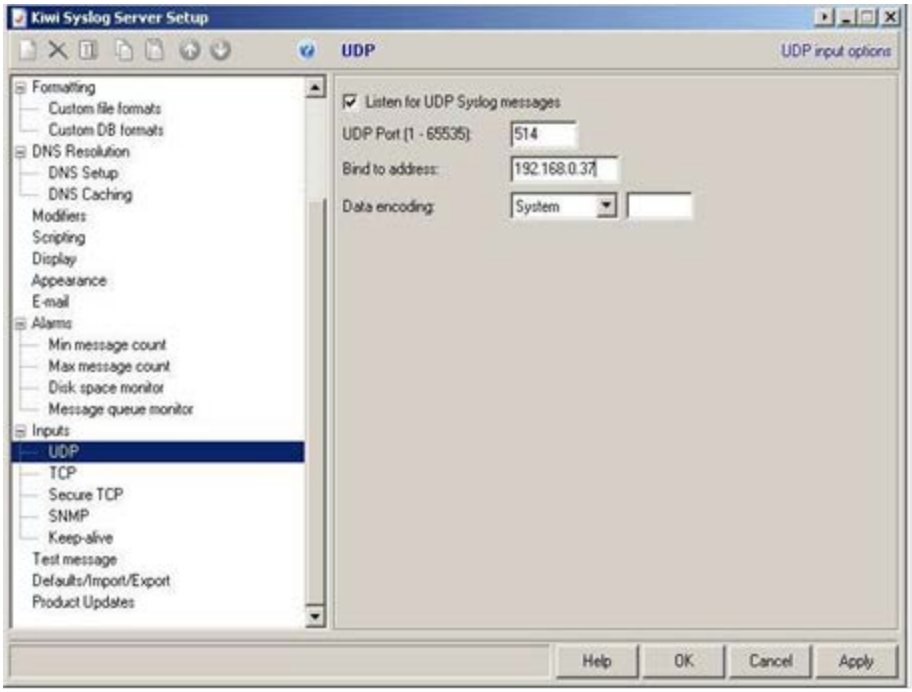
//Syslog severity Emergency=0, Alert=1, Critical=2, Error=3, Warning=4, Notice=5, Info=6, Debug=7

CRITICAL_TRAP=4 MAJOR_TRAP=4
NORMAL_TRAP=6 MINOR_TRAP=6

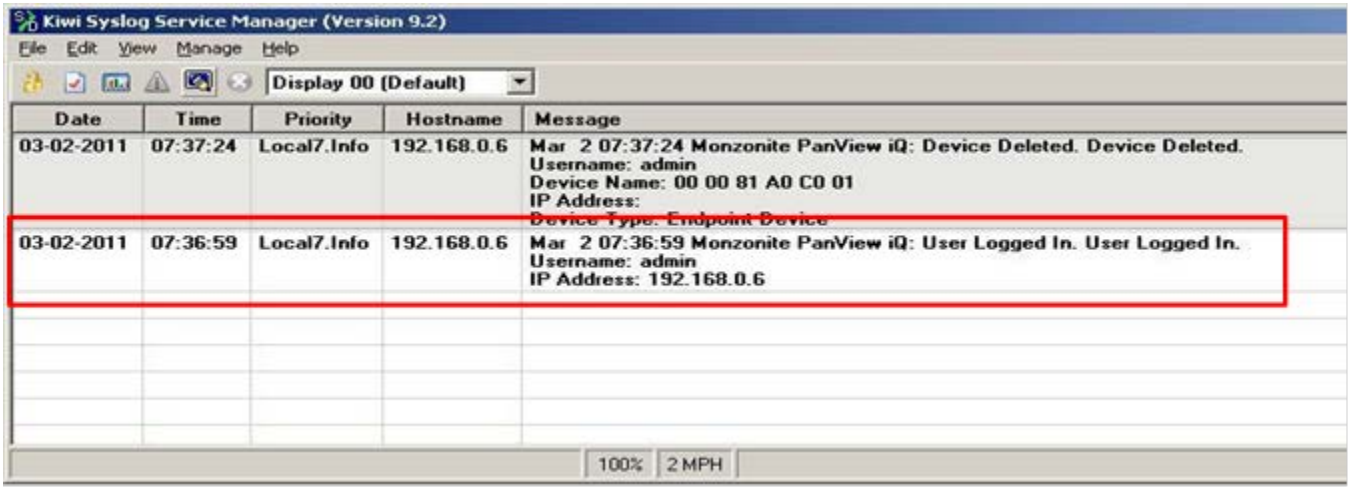
DEFAULT=6

Note: The numbers above correlate to the severity/priority the event will be assigned in the syslog daemon. For example, when a Critical alarm is generated (CRITICAL_TRAP=4 and Syslog Severity Warning=4) the alarm will be reported in the syslog as a Warning.

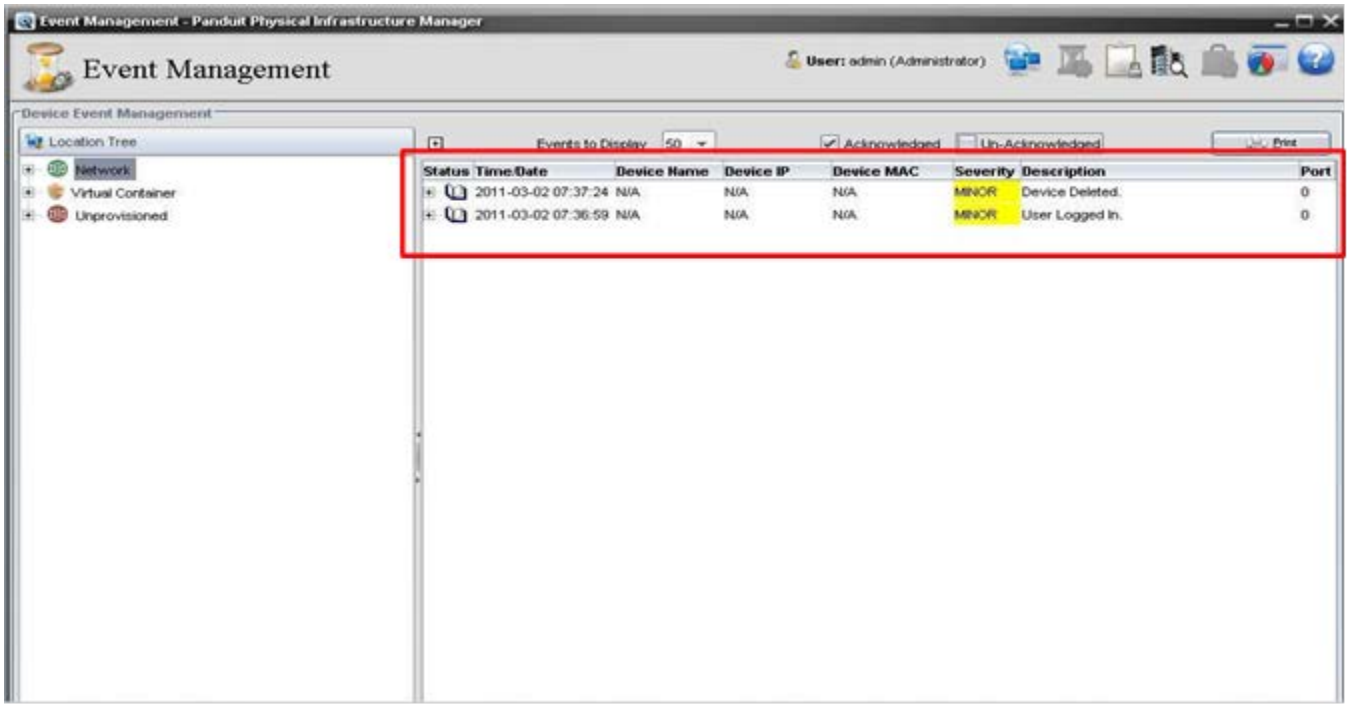
2. Make sure the port number in the syslog.properties file matches the port number in the syslog Daemon Setup.



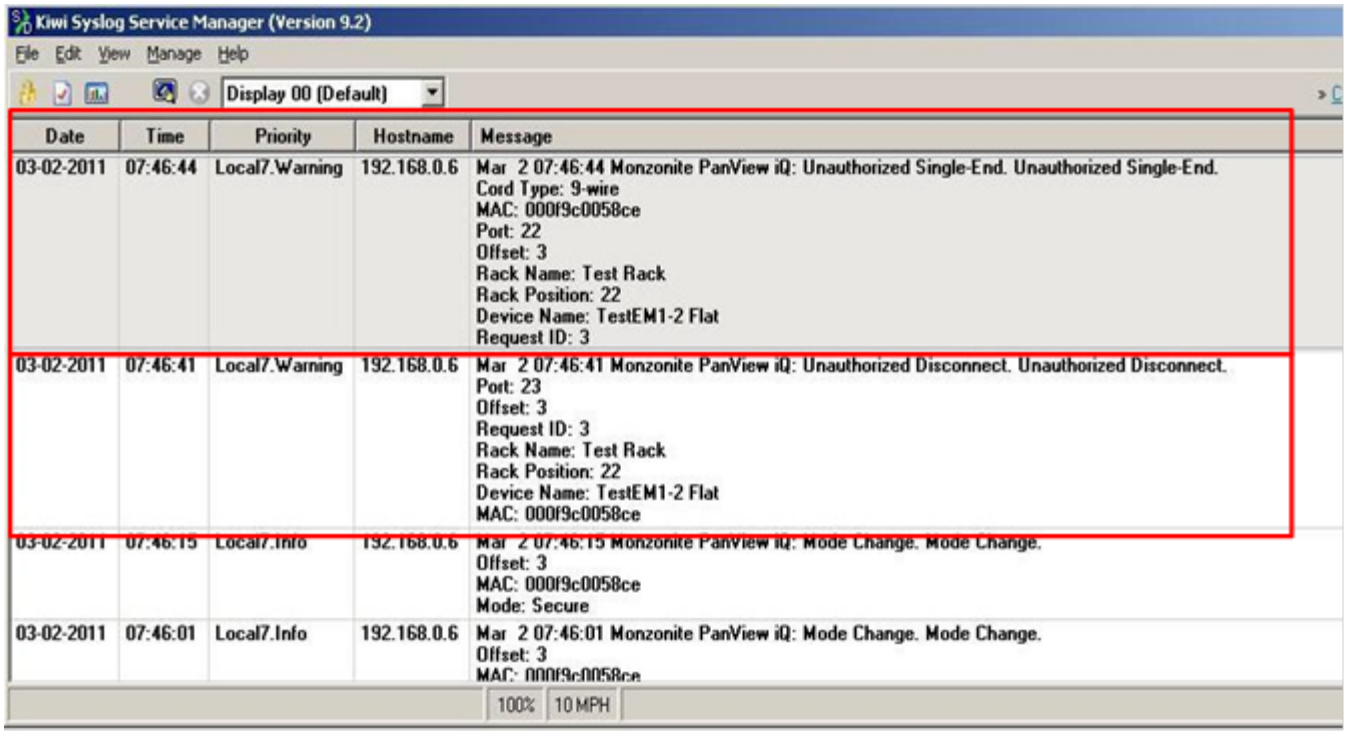
3. After the syslog configurations have been saved, restart the jboss server.
4. Invoke the SmartZone™ client and perform a successful login.
5. Monitor the Syslog Service Manager and verify that the events are reported.

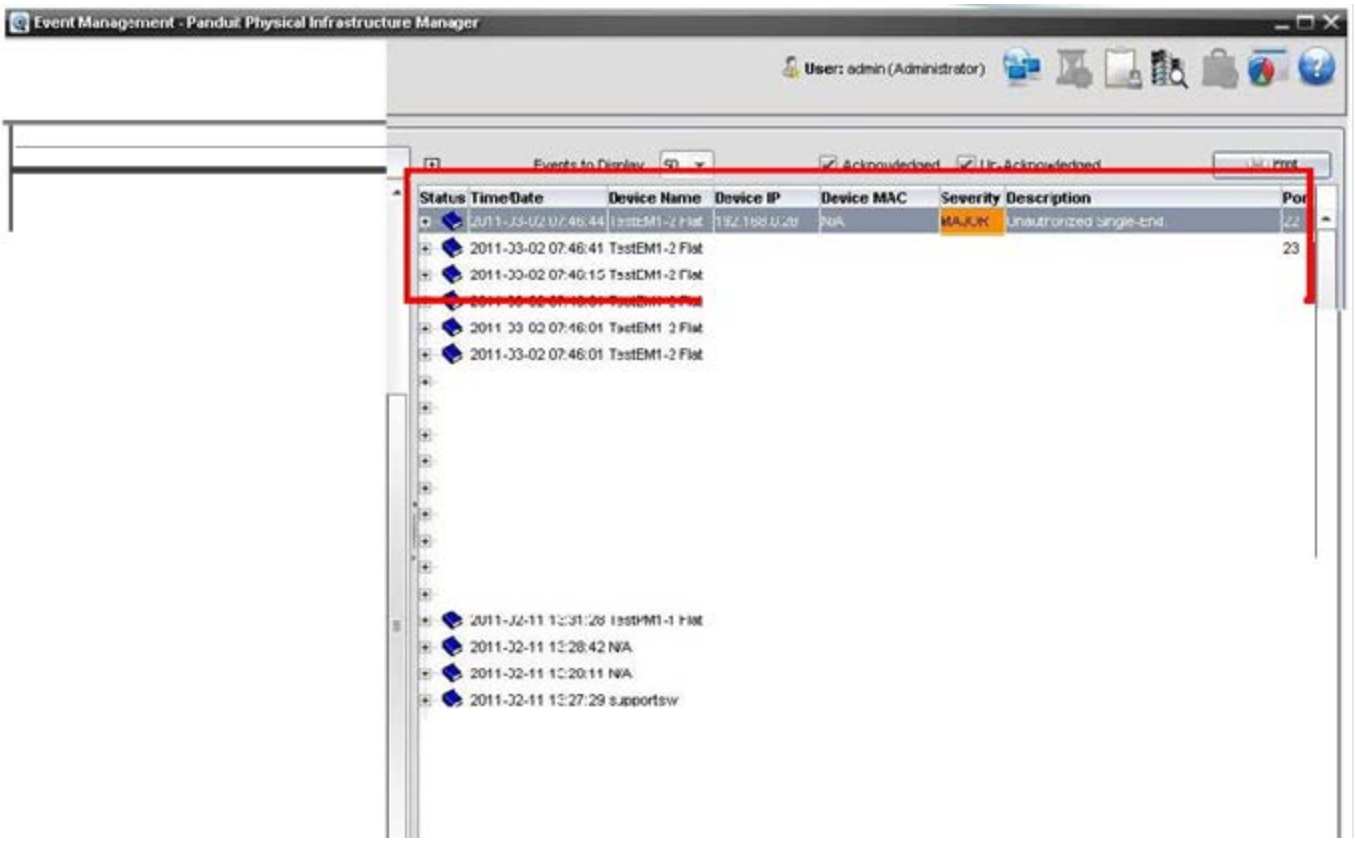


As they are reported in the SmartZone™ Event Management window:



As more severe events are generated, you will see the change in priority in the syslog daemon. You will also see all details of the event reported in the syslog daemon.


Kiwi Syslog Service Manager (Version 9.2)
File Edit View Manage Help
Display 00 (Default)
Date Time Priority Hostname Message
03-02-2011 07:46:44 Local7.Warning 192.168.0.6 Mar 2 07:46:44 Monzonite PanView iQ: Unauthorized Single-End. Unauthorized Single-End.
Cord Type: 9-wire
MAC: 000f9c0058ce
Port: 22
Offset: 3
Rack Name: Test Rack
Rack Position: 22
Device Name: TestEM1-2 Flat
Request ID: 3
03-02-2011 07:46:41 Local7.Warning 192.168.0.6 Mar 2 07:46:41 Monzonite PanView iQ: Unauthorized Disconnect. Unauthorized Disconnect.
Port: 23
Offset: 3
Request ID: 3
Rack Name: Test Rack
Rack Position: 22
Device Name: TestEM1-2 Flat
MAC: 000f9c0058ce
03-02-2011 07:46:15 Local7.Info 192.168.0.6 Mar 2 07:46:15 Monzonite PanView iQ: Mode Change. Mode Change.
Offset: 3
MAC: 000f9c0058ce
Mode: Secure
03-02-2011 07:46:01 Local7.Info 192.168.0.6 Mar 2 07:46:01 Monzonite PanView iQ: Mode Change. Mode Change.
Offset: 3
100% 10 MPH


Event Management - Panduit Physical Infrastructure Manager
User: admin (Administrator)
Status TimeDate Device Name Device IP Device MAC Severity Description
2011-33-02 07:46:41 TestEM1-2 Flat
2011-33-02 07:46:01 TestEM1-2 Flat
2011-33-02 07:46:01 TestEM1-2 Flat
2011-32-11 11:28:42 N/A
2011-32-11 11:20:11 N/A
2011-32-11 11:27:29 supportsw

End State

You have successfully set up a syslog feature in SmartZone.