Logging HP FutureSmart Printer Embedded Security Features to HP ArcSight or Standard Syslog Servers

Contents

Overview

This document describes how to configure HP printing devices to send Syslog messages for security events to an HP ArcSight environment or a standard Syslog server. Also described are instructions on how to install and configure a freeware Syslog server, "Kiwi Syslog Server", for testing purposes and proof of concept.

Configure the Printing Device for Sending Syslog Security Events

1. Using Internet Explorer, Browse to the Printer IP address

2. Select the "Networking Tab", then Select the "Advanced Tab" in TCP/IP Settings

3. Enter the Syslog server parameters as shown:

Hop Limit/WSD	32
TTL/SLP:	4
Syslog Server:	<Syslog server IP Addr>
Syslog Protocol	UDP
Syslog Port	514
Syslog Maximum Messages:	100
Syslog Priority:	7 (Use '8' to disable.)
☑ Enable CCC Logging	

4. Select "Apply"

Configure HP Printing Devices for HP ArcSight notifications

HP FutureSmart printing devices can be configured to provide security event notification to existing HP ArcSight environments. The printer's Syslog security messages are sent to the HP ArcSight SmartConnector, which converts standard Syslog messages to HP ArcSight Common Event Format.

Steps to configure HP FutureSmart printers for HP ArcSight logging:

1. Ensure the customer has installed the HP Printing SmartConnector in the HP ArcSight networking environment.

   Note: The HP Printing SmartConnector is included at no cost and bundled with HP ArcSight.

2. Request the IP address of the HP ArcSight SmartConnector and Syslog Port from the customer ArcSight administrator.

3. Configure the printers Syslog Server address with the IP address of the SmartConnector

4. Configure the printers Syslog Port if different from the default value of 512

5. Select the "Enable CCC Logging" checkbox to enable security logging events

6. Select Apply

Kiwi Syslog Server installation

The Kiwi Syslog server is available as a freeware syslog application for monitoring up to 5 devices. This software can be use d to demo HP printing device security event messaging or for proof of concept. Full versions are available for purchase that include advanced filtering and e-mail event notification.

1. Download the Kiwi Syslog Server from www.kiwisyslog.com/downloads

   Note: Select "Kiwi Syslog Server – Free Edition" from "Free Products" section

2. Run the Kiwi_Syslog_Server_Freeware.setup.exe file

3. Select "I Agree" to the Solarwinds license agreement

4. Select "Install Kiwi Syslog Server as an Application", then Select Next

5. If required, Enter administrative user credentials, then Select Next

6. Select preferred program shortcuts, then Select Next

7. Verify Destination Folder

8. Select Install

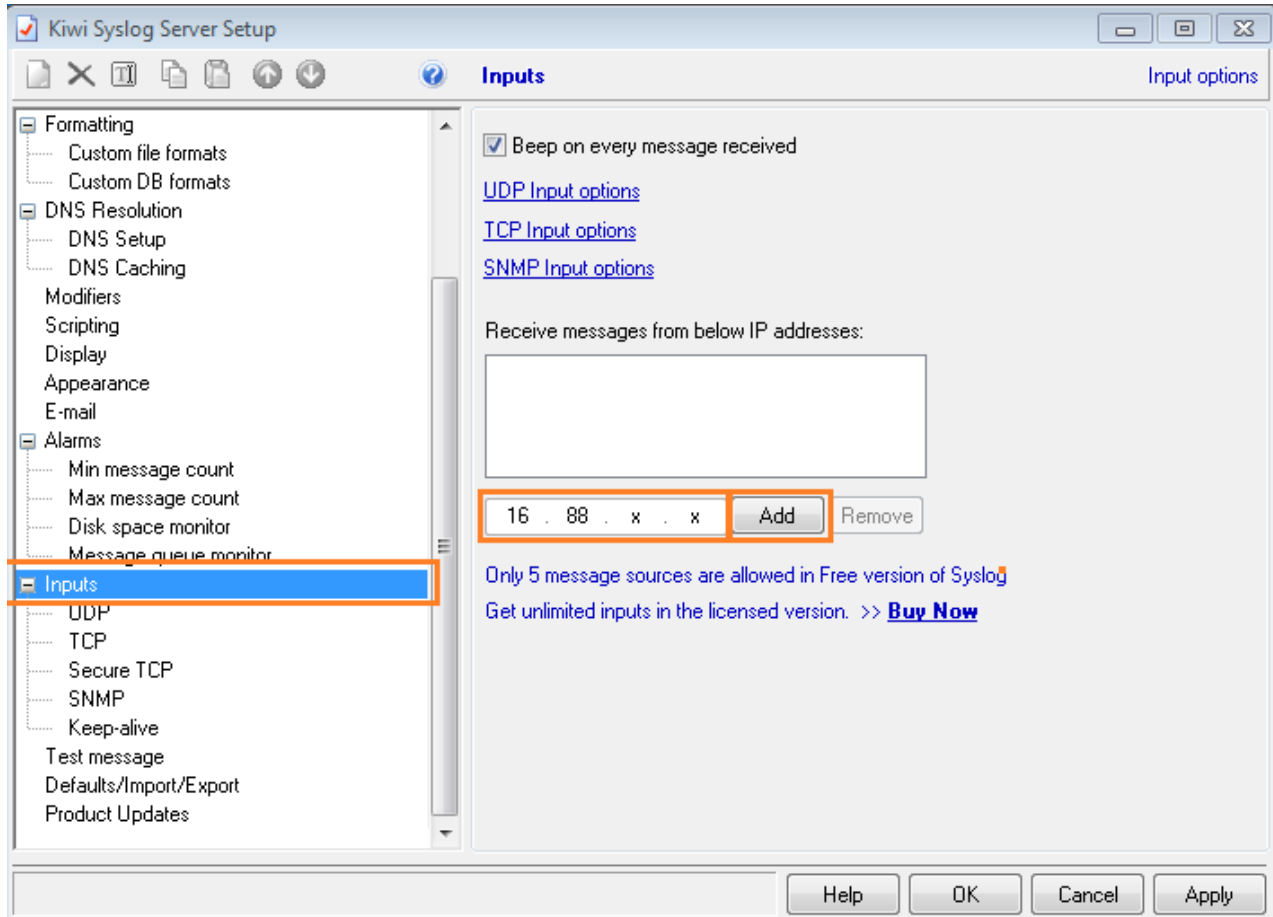## Configure the Kiwi Syslog Server to Monitor HP Printer Security Events

1. Open the Kiwi Syslog Server

2. Select "File", then "Setup"
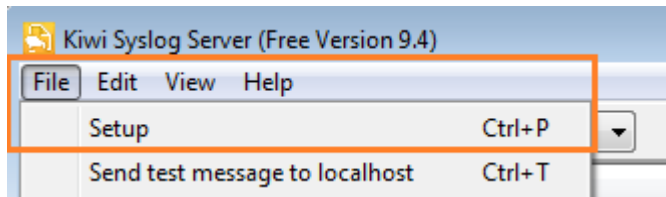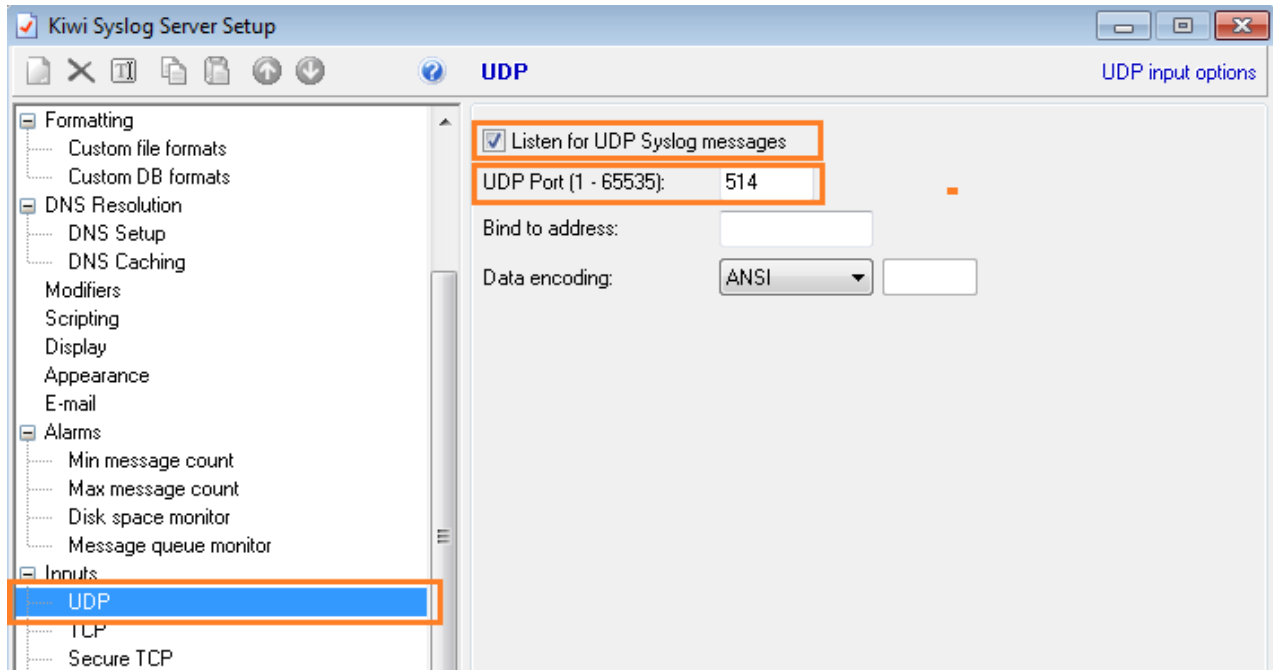

3. Click on "Inputs" in the left Menu Tree

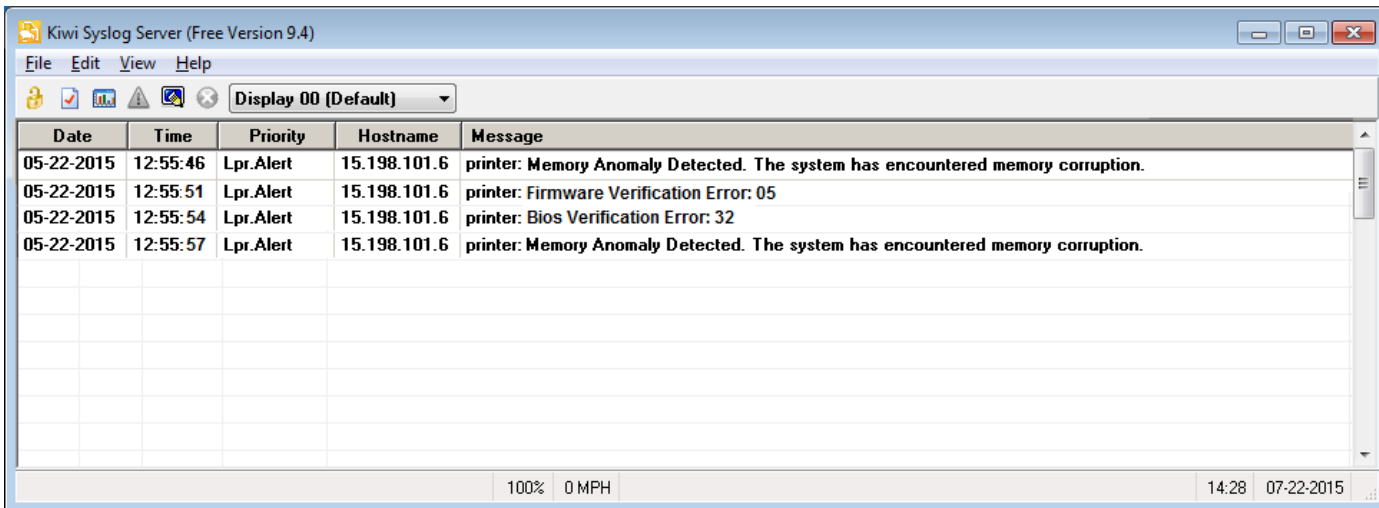4. Enter the Printer IP Address in the address field and Select the "Add" button

5. Click on "UDP" in the left Menu Tree

6. Select the "Listen for UDP Syslog messages" checkbox

7. Enter "514" in the UDP Port field

8. Select "OK"

Monitor Kiwi Syslog Server console for security events

Open the Kiwi Syslog Server console and review any captured security logging entries

These issues are only seen on full solution CD or Downloaded drivers packages with self-installing drivers