APPLICATION NOTE

Using the Syslog Client to log System Security Events locally

This application note outlines how to use the **Envisalink**'s built-in Syslog client to log security events to a LAN connected Syslog server. It also explains how to install an open-source Syslog server on a Windows PC for those who don't have a Linux Syslog server. The Syslog client is only available on the **Envisalnk 4** and requires a firmware version of 1.01.108 or higher.

Overview

The **Envisalink's** Syslog client can not only log security events like alarms, arming and disarming, it can also log zone openings and closings in real-time. Honeywell users will be limited to zone information only when disarmed and will have a latency of up to 60 seconds on zone closures. This is a limitation of Honeywell panels and not of the **Envisalink.**

The type and format of events logged depends on whether the **Envisalink** is connected to a DSC or Honeywell panel.

DSC Panels	Honeywell and UNO
Zone Openings and Closings System Openings and Closings (Arm/Disarm) Zone Alarms Shutdown Requests	Zone Openings and Closings All Contact ID Events in Contact ID format Zone Alarms Shutdown Requests

Table 1: Syslog Events

The Syslog client is RFC3164 compliant and allows you to select from any of the 8 "Local" facility services. Severity is coded per the severity of the event, but in general they fall between WARNING, NOTICE, and INFO (i.e. zone openings and closings)

1. Setting up a local Syslog Server on Windows

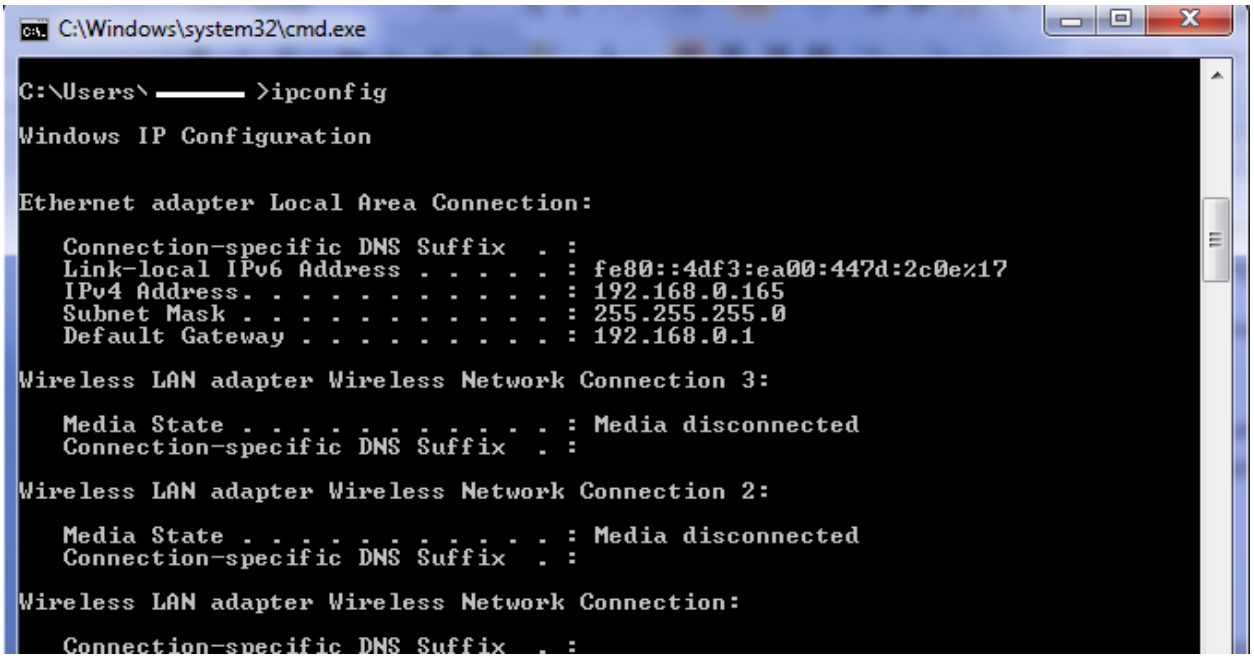
If you already have a Linux computer on your LAN, then you can skip this section and go directly to the "Setting up the Syslog Client".

For you to log the output of the Envisalink's Syslog client, you need a server. There are many free servers available but we'll use a popular Open-Source server called "Visual Syslog Server".

1) Download **Visual Syslog Server for Windows** from Sourceforge

https://sourceforge.net/projects/syslogserverwindows/

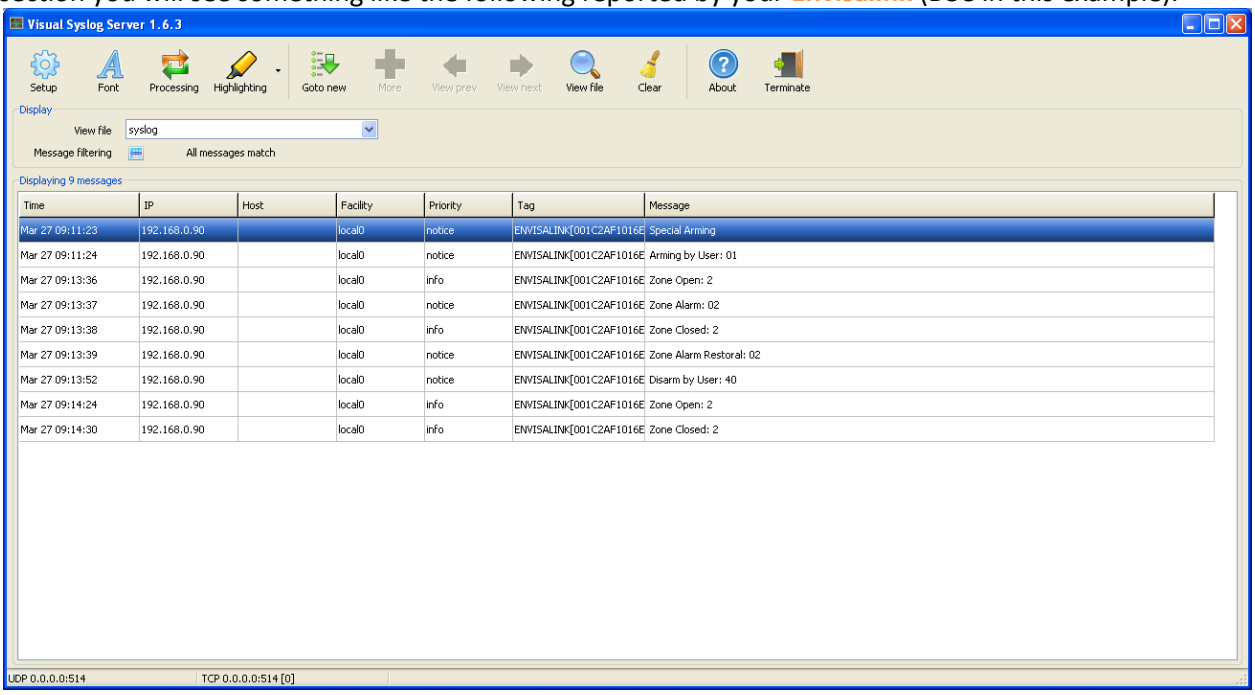
2) Install the Syslog server as per its instructions
3) Find out the IP address of your computer. You can do this by opening a command window and typing “ipconfig”. See below



In this example the IP address of the PC is 192.168.0.165.

Note: You should make a MAC reservation for your PC in your router’s DHCP table so that your IP address

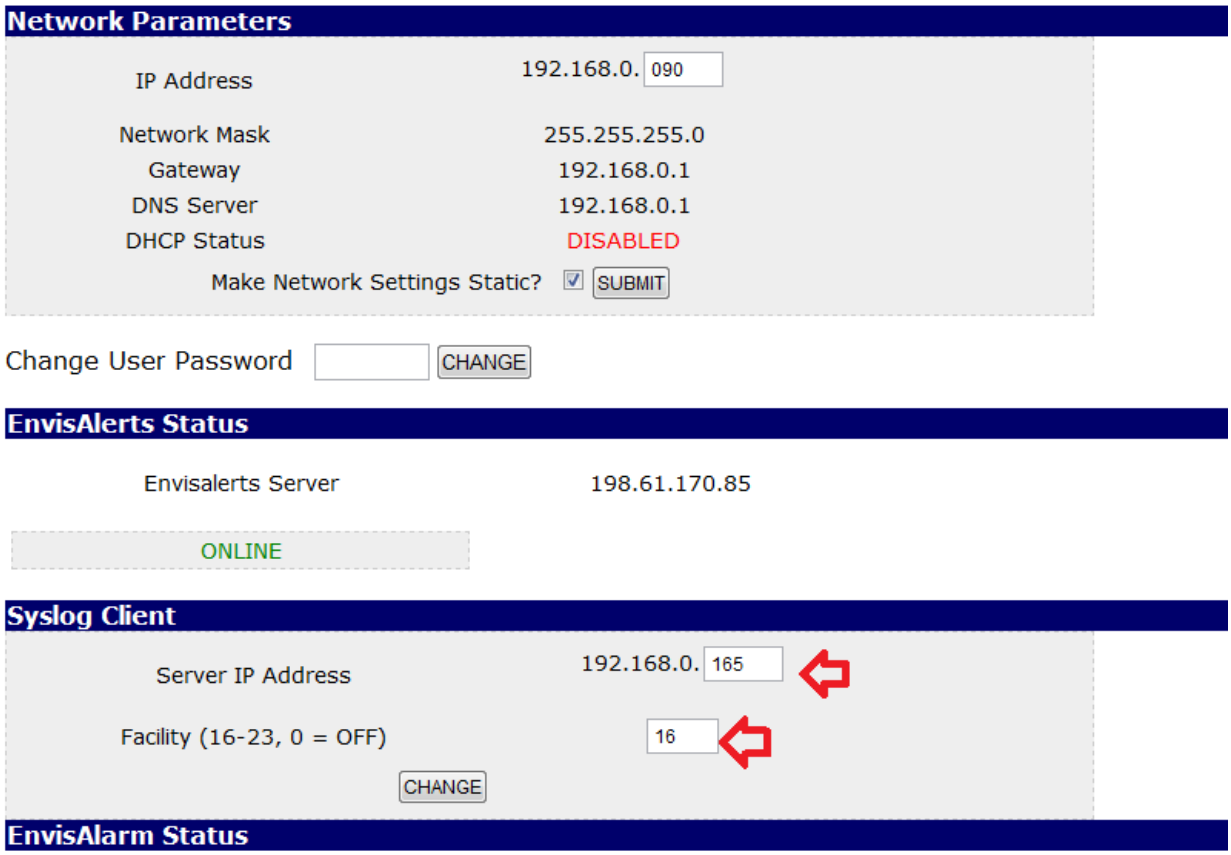
4) If you haven’t done already, start the Virtual Syslog Server for Windows. Once you have completed the steps in the next section you will see something like the following reported by your **Envisalink** (DSC in this example).



2. Setting up the Syslog Client

You configure the Syslog client by logging into your Envisalink directly so this requires that you be on the same LAN as your Envisalink.

1) Connect to the IP address of your Envisalink from a Web Browser. The default username is **user** and the default password is **user**. For more information on how to find your IP address, see the **"Connecting to your Envisalink Locally"** application note.
2) Go to the network page and look for the new section called "Syslog Client". See below.



3) The first arrow points to where you enter the last number of the IP address of your Windows server machine. In our example it is 165
4) The second arrow points to the "Facility". You can select anything from 16 to 23 which corresponds to LOCAL0-LOCAL7 (see RFC3164 for more information on facilities). Select anything from 16 to 23, it doesn't matter to the Windows client. On Debian/Ubuntu Linux, the LOCAL facilities will show up in **/var/log/messages.** Selecting 0 for the facility turns off the Syslog Client entirely.
5) Select the "Change" button to save your settings and then **reboot your** Envisalink for those changes to take effect.