Stealth Labs ILF-100 User Manual

Internet Line Fault Monitor
© 2006 Stealth Laboratories, LLC
Patent Pending
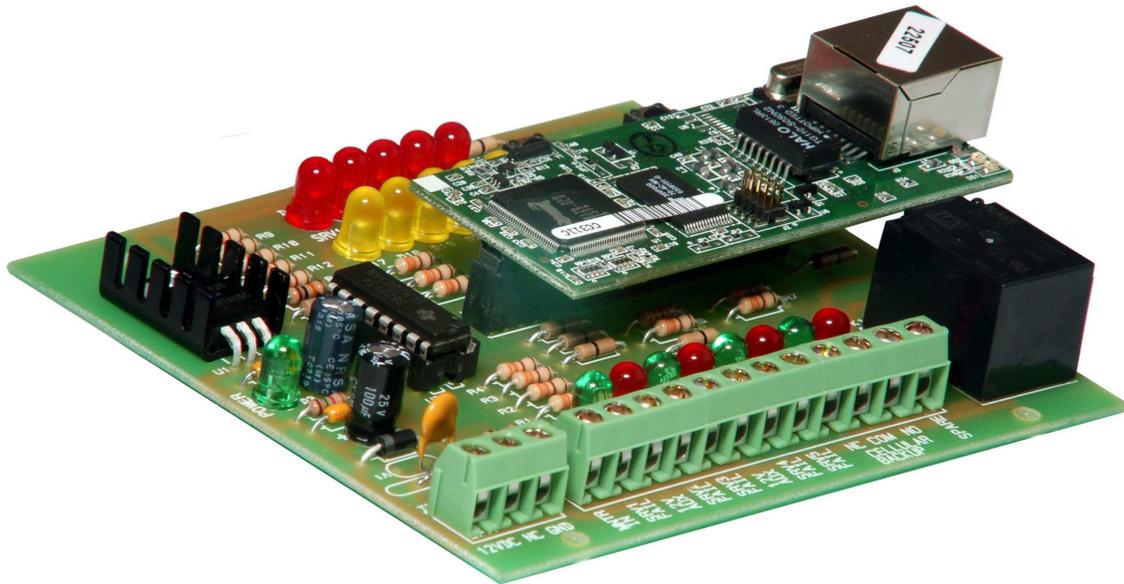
Table of Contents:

FAQ

Q: What is the ILF-100 and what does it do?

A: The ILF-100 is an *Internet Line Fault monitor*. Line fault monitors have been around for many years for telephone lines. They were designed to detect cut telephone lines and trigger some type of backup communication for burglar alarm transmission reports (typically a cellular dialer or radio link). The ILF-100 is the internet equivalent of the telephone line fault monitor. Instead of detecting a faulty telephone line, the ILF-100 detects a faulty broadband internet connection for customers using a Voice over Internet Protocol (VoIP) service for their alarm reports. If the internet connection is lost, the ILF-100 will trigger a relay output that can be used to switch over any burglar / fire alarm transmissions to a backup communications device. It obviously can't send an email notice if the internet connection fails, but the ILF-100 will send an email notice when the connection restores.

Q: What else does the ILF-100 do?

A: The ILF-100 has several secondary functions:

1. It can monitor a user input for any HIGH or LOW state changes and send email notices when this input changes states. This feature is very useful for monitoring an alarm system violation output, a freezer alarm or basement water alarm. It can even be used in conjunction with a telephone line fault monitor to send email notices if the premises telephone line is cut. These email notices can even be sent to a wireless phone as SMS text emails. All pertinent information is contained in the email subject line.
2. The ILF-100 also detects and compares the WAN IP address that is assigned to the broadband connection by the Internet Service Provider. If this IP address changes, the ILF-100 can be configured to send an email notice. This is a great feature for anyone who monitors remote internet devices (security cameras, etc.) that sometimes get new IP addresses assigned by the ISP.
3. Since the ILF-100 already polls five different servers (one each minute), an obvious use is to monitor one or more web servers. If you have an important web site and want to know if it is down, the ILF-100 can trigger an open collector output and send an email when any of the monitored servers fail to respond. There is a separate output for each of the five servers, useful for triggering a local buzzer or remote LED indicator. All five servers can be assigned by the user. Any given server will be polled once every five minutes.

Q: Who needs an internet line fault monitor?

A: More and more people are switching over to Voice over Internet Protocol services (VoIP) for their telecommunications needs. As this trend grows, the internet connection is becoming much more critical. The broadband connection is literally taking the place of the telephone line. Anyone who uses a VoIP service with a monitored burglar / fire alarm should have an internet line fault monitor.

Q: Does the ILF-100 work with DSL?

A: The ILF-100 works equally well with cable modem or DSL broadband internet connections. Dialup connections are not supported.

Q: How does the ILF-100 detect internet line faults? Does it measure voltage, current, or frequency?

A: Actually, none of the above. Instead of trying to detect some physical / electrical attribute of a valid connection, the ILF-100 polls one of five different web servers every minute to insure the internet connection is working. It is equivalent to a telephone line fault monitor actually making a phone call every minute to test the phone line. Not practical for your phone line, but highly practical for a broadband connection.

Q: What is an IP Address?

A: An IP address is a unique 32-bit number for each host on a network. This number is known as the Internet Protocol Address, the IP Address, or the Internet Address. These terms are interchangeable. The IP address is considered in two parts: the prefix which identifies the physical network, and the suffix which identifies a computer on the network. A unique prefix is needed for each network in an internet. A good analogy is to think of the IP address as a telephone number. The prefix is the area code and exchange. The suffix is the number that identifies your individual telephone. In a class C network, for example, if your IP address is **192.168.0.114**, the prefix portion of your IP is **192.168.0**. The suffix is **114,** which is the unique number that differentiates your computer from all the other computers connected to the same local area network.

For a computer connected to a network with internet access, there are actually two IP addresses to be concerned with: a local private IP address that is only visible to your local area network (LAN), and a public IP address that is assigned to your router by your ISP. This is your Wide Area Network (WAN) IP address, and is the address that is used when you connect to servers on the internet.

Q: What is a Router?

A: A router is a hardware device that connects two or more networks. Routers are the primary backbone device of the Internet, connecting different network technologies into a seamless whole. Each router is assigned two or more IP addresses because each IP address contains a prefix that specifies a physical network. Most routers act as a firewall and DHCP server, as well as provide the means for sharing a single broadband internet connection with all the computers connected to its LAN.

Q: What is DHCP?

A: **DHCP** stands for **D**ynamic **H**ost **C**onfiguration **P**rotocol. DHCP is the means for automatically assigning an IP address to a computer when it connects to a network. Since DHCP is dynamic, there is no guarantee which IP address will be assigned to the computer (although some routers do allow static IP addresses to be assigned with DHCP).

Installation and Configuration

Server Status LEDs. Yellow = Test in progress; Red = Fail

To network

Cellular back-up relay activates for total internet failure.

Power Terminal Block

Main Terminal Block

Internet Status LEDs. Green = Pass, Red = Fail

Internet   Email   Ping   HTTP

5 open collector outputs for individual server failures

12V DC NC GND   MNTR SRVR 12V SRVR SRVR 12V SRVR SRVR NC COM NO SPARE
                 IN   1   AUX 2   3   AUX 4   5

To cellular or other back-up

+
-
12V DC Power Supply 500mA or greater

+
-

Optional 12V piezo buzzer, wired to sound if server fails

Control Panel Open collector output (requires external pull-up resistor)

+12V

4.7K

Optional user input. Monitors high/low state of a 12V output, e.g. a security system's violation output. Be sure to connect a common ground to the device being monitored.

Figure 1: ILF-100 Wiring

Electrical Connections (see Figure 1)

- Connect the ILF-100 to a 12V (500mA or greater) regulated DC power supply.
- Connect the relay terminals to a cellular backup dialer. The relay terminals are labeled NC (Normally Closed), COM (Common) and NO (Normally Open). Since cellular dialers vary, you will need to refer to your cellular backup dialer's hookup instructions for details on the proper hookup.
- To use the optional User Input (MNTR IN), connect a common ground wire between the device being monitored and the ILF-100. Connect MNTR IN terminal to the device's output. The MNTR IN can accept any DC voltage between 5V and 24V. If the device uses open-collector outputs, a user-supplied pull-up resistor must be connected (see lower left detail in Figure 1). See **User Inpu**t in the **ILF-100 Configuration** section for details on enabling email notices for User Input state changes.
- One or more Server Fail outputs may be used to trigger visual or audible indicators for individual servers that may fail. The total current drawn by these outputs must not exceed 400mA. Note that these are open-collector outputs, which means they must be connected to the "-" terminal of the device being switched. The 12V AUX terminals may be used for powering the "+" terminal of the device. See Figure 1 for an example hookup.
- Connect the ILF-100's Ethernet controller board to an open port on a router or Ethernet switch using the supplied network cable.

Network Configuration

The ILF-100 is designed to be connected to a network router. It must initially be configured using a web browser on a computer that is connected to the same router (i.e., on the same local area network). In order to connect to the ILF-100, its IP address must be known. There are a couple of methods for determining the IP address. **The recommended method is to simply plug the ILF-100 into an existing network router that uses Dynamic Host Configuration Protocol (DHCP).** When connected to a DHCP-enabled router, the ILF-100 will send an email to a mailing list maintained by Stealth Labs (see the section entitled, "**DHCP Method"** for details). Even if a static IP address is going to be assigned to the ILF-100, the network configuration will go much smoother if DHCP is initially used. The other (more difficult) method is to connect the ILF-100 directly to a computer using a crossover cable. See the section entitled, "**Fallback Method Using a Crossover Cable"** for details on using this method.

Hint: If you are only concerned with detecting a failed internet connection and do not need any of the email notification features, you may simply plug the ILF-100 into a DHCP-enabled router and connect the relay terminals to your alarm system's backup communication device. No further configuration is needed!

DHCP Method

1. Power up the ILF-100 and observe the LEDs on the Ethernet control module (very small surface mount LEDs located next to the RJ-45 connector). The green LED should be steadily illuminated and the yellow LED should occasionally blink to indicate network activity.
2. The green E-MAIL LED (located on the main circuit board) should illuminate after a few seconds, indicating that the "sign-on" email was successfully sent.

3. Using a computer connected to the internet, type **http://archives.ILF100.com** into the address bar of a web browser.
4. Click on the archive for today's date by clicking the **View by: [Thread]** link.
5. Press **<Ctrl> F** to open the search dialog box in your web browser.
6. Type in the serial number of your ILF-100. The serial number is printed on the bar code label that is affixed to the chips on the top side of the Ethernet controller board.
7. Click the **Find** button of the dialog box.
8. The browser should highlight the subject line of the email that your ILF-100 just sent.
    a. Note: if you powered your board up more than once, you may need to refresh your browser window to see the latest email.
9. Click on the message link to view the email body.
10. Click the link after **IP Addr:** to access your ILF-100's configuration page. **Security Note: this link will only work for users connected to the same LAN as your ILF-100**.
11. You should see a password dialog box similar to Figure 2.
12. Enter **admin** for the User Name and **pass** for the password. Both are case sensitive.
13. If you were successful, you should see the ILF-100 configuration screen, illustrated in Figures 5 - 9.
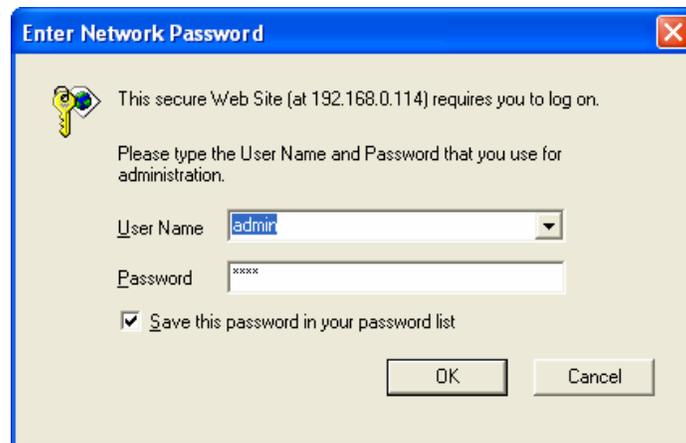14. Proceed to the **ILF-100 Configuration Web Page** section of this document.

Figure 2: Network Logon Dialog Box

Fallback Method Using a Crossover Cable

Skip this section if you are using the DHCP Method.

1. Connect the ILF-100 directly to a computer using a CAT5 network crossover cable (this is a cable that is specially wired to allow two computers to connect directly to each other – it is not the same as a normal network patch cable).
2. If a crossover cable is not available, connect the ILF-100 and a computer to an Ethernet switch *that is not connected to a network*. The only two devices connected to the switch should be the ILF-100 and the computer.
3. The ILF-100 will "fallback" to a static IP address of **192.168.1.10** if no DHCP server is detected. If your local network is already configured with a prefix of **192.168.1** (and if no other computer is using IP address **192.168.1.10**), then the ILF-100 may simply be connected to your network (go directly to **Step 5**). Otherwise, your computer must be configured to use an IP address in this range before it can connect to the ILF-100. **Be**

sure to make a note of your computer's network settings before following these steps. You will need the original settings to return your computer to its normal network settings.

4. In Windows XP, do the following:
    a. Click the **Start** button, then select **Control Panel**.
    b. Click **Network Connections** (be sure the computer is already connected to the ILF-100 via the crossover cable or Ethernet switch).
    c. Right-click on Local Area Connection and select Properties.
    d. Highlight **Internet Protocol (TCP/IP)** as shown in Figure 3.
    e. Click the **Properties** button.
    f. Click the **Use the following IP address:** button and enter **192.168.1.20** (see Figure 4).
    g. Leave the default **255.255.255.0** Subnet mask.
    h. Leave the Default gateway blank.
    i. Click **OK** to close the **TCP/IP Properties** box.
    j. Click **Close** to close the **Local Area Connection Properties** box.
5. Open a web browser and type **192.168.1.10** in the address bar. Click **Go** or press **Enter**.
6. You should see a password dialog box similar to Figure 2.
7. Enter **admin** for the User Name and **pass** for the password. Both are case sensitive.
8. If you were successful, you should see the ILF-100 configuration screen, as shown in Figures 5 – 9.
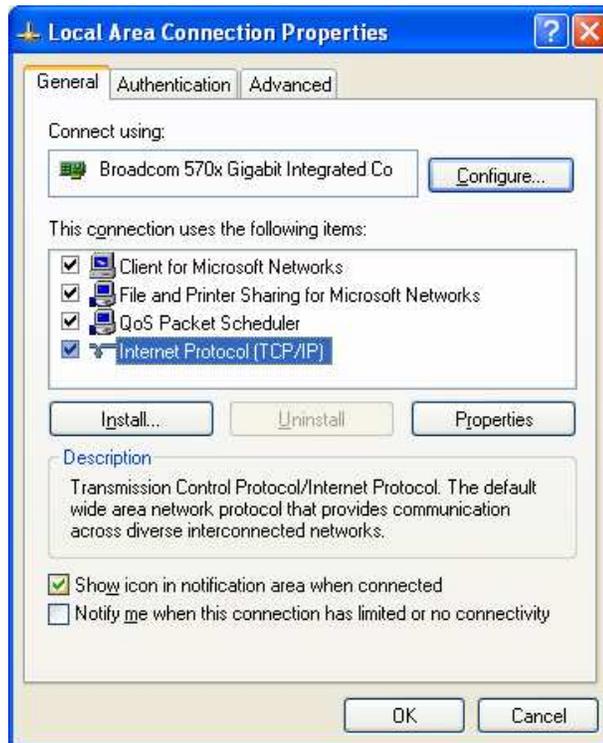9. Proceed to the **ILF-100 Configuration Web Page** section of this document.

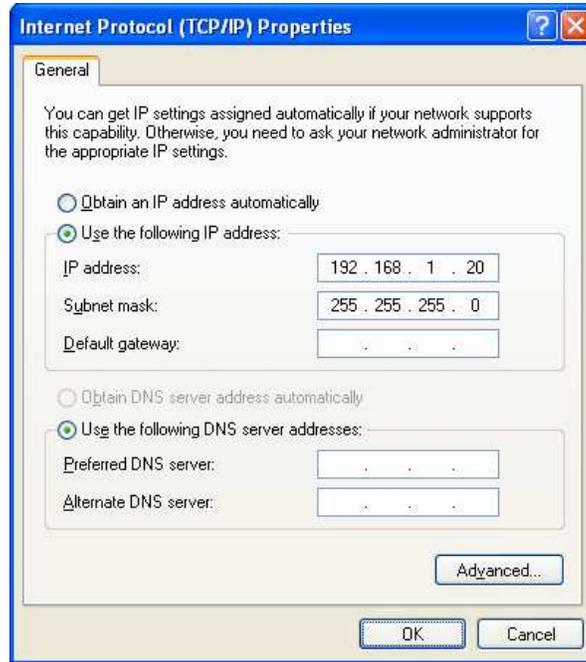**Figure 3: Local Area Connection Properties**

Figure 4: TCP/IP Properties

ILF-100 Configuration Web Page

The ILF-100 Configuration Web Page is divided into five sections:

1. Text To Identify This Unit
2. Network Settings
3. Email Settings
4. Internet Monitor Settings
5. ILF-100 Username & Password

Text To Identify This Unit

The first section is shown in Figure 5. This text field allows the user to describe / name the ILF-100 or the location in which it is installed. All emails sent by the ILF-100 will include this text in the body of the email to help clarify which unit sent the email. This text may be up to 25 characters in length.

🖹Text To Identify This Unit

This text will be displayed here and in the body of all emails:

My ILF-100   25 alpha-numeric characters max

Figure 5: Text To Identify This Unit

Network Settings

The Network Settings section is shown in Figure 6. The LAN and WAN IP addresses are displayed at the top of the section. If the ILF-100 has not yet connected to the internet, the WAN IP will be displayed as **0.0.0.0**, otherwise it will display the IP address that was assigned to the router by your broadband Internet Service Provider. If the ILF-100 was able to connect to a DHCP server, the LAN IP address will display the IP address that was assigned to it by the router. If no DHCP server was found, the fallback IP address of **192.168.1.10** will be displayed.

If DHCP is being used, there is no need to make any changes to this section. Just make sure the **Obtain IP address automatically** and **Obtain DNS server address automatically** buttons are selected. Proceed to **the Email Settings** section.

⛁Network Settings

ILF-100 public (WAN) IP address is: **24.123.456.789**
ILF-100 private (LAN) IP address is**: 192.168.0.114**

◉ Obtain IP address automatically

◯ Use the following IP address:

LAN IP address: | 192.168.0.114 |

Subnet mask: | 255.255.255.0 |

Default Gateway | |

◉ Obtain DNS server address automatically

◯ Use the following DNS server address:

First DNS server: | |

Second DNS server: | |

Figure 6: Network Settings

Manually Assigning an IP Address

If your network does not use DHCP, or if you plan on being able to access the ILF-100 from remote locations, you will need to manually assign an IP address. *Note that some routers allow static IP addresses to be assigned while still using DHCP*. If this is the case with your router, you can leave the **Obtain IP address automatically** button selected. Refer to your router's setup manual for more information on enabling static IP addresses.

If your router does not support static IP address assignments through DHCP, you must manually assign an IP address to the ILF-100. Click the **Use the following IP address** button. This instructs the ILF-100 not to use DHCP. A DHCP address suffix typically starts at 100, so you should use a suffix that is not located in the range being used by DHCP. If

your router uses addresses **192.168.1.100 – 192.168.1.199** for DHCP, you should use a suffix greater than 1 (which is usually assigned to the router) and less than 100, such as **192.168.1.10** or **192.168.1.15**, etc. You will also need to make sure that the IP address you select is not already in use by another computer on your network.

Once you have entered a valid IP address, press the **Tab** key to highlight the **Subnet mask** field. In most cases, this should be left set at **255.255.255.0**.

Tab to the next field, **Default Gateway**. Enter the IP address of your router. You can determine this address by running "**ipconfig**"from a Windows command prompt (click the **Start** button, then **Run** and type "**cmd**" in Windows XP or Windows 2000, or "**command**" for Windows 98). Use the same Default Gateway IP address shown by the **ipconfig** command.

Next, you must enter the IP address for at least one (preferably two) DNS server(s). You may need to contact your ISP for these addresses, or you may be able to find them listed on your router's status page. The **Obtain DNS server address automatically** button will not work if DHCP is not being used.

Remotely Accessing the ILF-100

For remote access, you will have to configure your router to allow outside access to the ILF-100's IP. This is usually done by enabling the router's **DMZ** (**D**e-**M**ilitarized **Z**one). You will need to enable the DMZ and enter the ILF-100's local LAN IP address. Once enabled, you will be able to access the ILF-100 configuration page from a remote computer by entering your router's public IP address in the remote computer's web browser address bar (this is the WAN IP address shown at the top of the ILF-100 configuration page). When the router sees the remote access request, it will connect the remote computer to the ILF-100. Refer to your router's setup manual for more information on enabling the DMZ.

Notes:

- **Both the LAN and WAN IP addresses must be static. A static LAN IP is set in your router; a static WAN IP must be set up by your ISP (charges may apply). With some ISPs, your IP address will not change unless you make changes to your equipment, such as replacing your cable or DSL modem. In this case, you may not have to pay extra for a static IP address – it should remain the same as long as you don't change equipment.**

- To prevent unauthorized remote access, be sure to change the ILF-100 default Username and Password!

⊠Email Settings

Instructions:

- Change **TO** to the email address you wish to use to receive notices.
- Change **FROM** to an email account that allows outgoing SMTP emails.
- Change **POP3 Server** to the incoming mail server (some servers require a POP3 read before SMTP send).
- Change **SMTP Server** to the outgoing mail server.
- Note: It is okay if **Email To** and **Email From** are the same.
- Change **Account Name** to username for the "FROM" account.

Emails will be sent TO:

> ilf100@ilf100.com

Emails will be sent FROM:

> ILF100@ilf100.com

Incoming Mail Server (POP3):

> mail.ilf100.com

Outgoing Mail Server (SMTP):

> mail.ilf100.com

Account (User) Name:

>

Password:

> ***************

Figure 7: Email Settings

Email Settings

If you wish to receive email notification of individual server failures, internet connection restorals, WAN IP changes, or User Input changes, you will need to make changes to this section. The Email Settings section is shown in Figure 7.

1. Enter a valid email address in the **Emails will be sent TO:** field. All outgoing emails will be sent to this email address.
2. Enter a valid email address in the **Emails will be sent FROM:** field. This is the email account that will be used to send the emails. It must be an account that allows SMTP outgoing emails. This will probably be an email address from your ISP or place of business. Free accounts such as Yahoo do not allow SMTP access. This account will also have to either allow relaying or POP3 before SMTP access (this means you can't send outgoing email until you have first checked your incoming email).

3. Enter the incoming POP3 mail server name for the **Incoming Mail Server (POP3):** field. This is typically something like **pop3.youremailprovider.com** or **pop.youremailprovider.com**. Consult your email provider for more information.
4. Enter the outgoing mail server name for the **Outgoing Mail Server (SMTP):** field. This is typically something like **mail.youremailprovider.com** or **smtp.youremailprovider.com**. Consult your email provider for more information.
5. Enter the Username for the **Account (User) Name:** field. This may be just the username or it may be your entire email address. Consult your email provider for more information.
6. Enter your password in the **Password:** field. Note: this is the password for your email account. The password for the ILF-100 configuration page is set in the last section.

☞Internet Monitor Settings

Domains / IP addresses to monitor:

Server 1 | ebay.com | ☐ Enable Server 1 fail / restore emails

Server 2 | stealthlabs.com | ☐ Enable Server 2 fail / restore emails

Server 3 | rr.com | ☐ Enable Server 3 fail / restore emails

Server 4 | vonage.com | ☐ Enable Server 4 fail / restore emails

Server 5 | charter.net | ☐ Enable Server 5 fail / restore emails

Locally monitored resources:

☐   Send email notice if WAN IP changes

☐   Send email if user input changes states

Last Input State: | LOW | Refresh |

Figure 8: Internet Monitor Settings

Internet Monitor Settings

The Internet Monitor Settings section is shown in Figure 8.

The ILF-100 includes five predefined servers, but the user is free to change any or all of them. There are a few things you must keep in mind, however:

1. You do not need to enter "www" or "http://" - just type in the domain name or IP address.
2. Do **not** include a trailing '/' or index.html, etc.
3. IP addresses can and do change. If a server has a domain name, it is always better to use that rather than the IP address. The ILF-100 will automatically resolve the domain names into IP addresses, assuming valid DNS servers were setup.

4. If you use IP addresses, be sure they resolve to external internet sites and not a computer on your local network. Otherwise, the ILF-100 will not be able to determine when your internet connection has failed (the local IP address will probably respond even if the internet connection is bad).
5. If you want to poll a server more often than once every five minutes, you may list the server multiple times. However, it is not recommended that the same server be listed for all five servers.
6. Finally, select the checkboxes for any email notices you wish to receive: server outages, WAN IP changes, and User Input state changes.

MNTR IN Terminal (User Input)

The user input allows you to monitor the state of an external device, such as a freezer / flood alarm or a security system violation output. The signal being monitored should be a voltage level in the range of **5V** to **24V** *DC*. Press the **Refresh** button to update the input state. If enabled, the ILF-100 will send emails anytime this input changes from high to low, or low to high. It is up to you to know the meaning of the high or low states. Keep in mind that the ILF-100 can quickly generate excessive emails which can cause them to be flagged as spam. If this happens, your emails may be blocked by your email provider. It is not recommended that this input be connected to an output that changes states often, such as a motion sensor in a high traffic area. To help prevent runaway emails, the ILF-100 has a built-in limiter. It will send no more than 3 emails every 5 minutes. Additional state changes are counted and this count will be emailed once the email limiter has timed out. **Even with the limiter, it is highly possible that your emails will be flagged as spam if your ILF-100's user input is connected to an output that changes states multiple times within a minute. USE THIS FEATURE WITH CAUTION**.

ILF-100 Username & Password

If you have enabled remote access to the ILF-100, it is very important that you change the default username and password. The password can be up to eight characters long and the password can be up to ten characters long. Both fields are case sensitive. Refer to Figure 9.

☞ILF-100 Username & Password

Change **Username** and **Password** to prevent unauthorized access of this page.

Username: admin 8 alpha-numeric characters max

Password: ********* 10 alpha-numeric characters max

Submit   Reset

Figure 9: Username & Password

Saving Your Changes

Once you have made all the necessary changes to the ILF-100 configuration page, press the **Submit** button. The web browser will be redirected to a page that displays the progress as the ILF-100 saves all parameters to flash memory. Once the configuration is complete, click the **Close Window** button to close the browser window. The ILF-100 will reboot itself in order to begin using the new settings.

Using the ILF-100

Restoring Factory Defaults

To return the ILF-100 to the factory default settings, press the INIT switch SW2 when powering up the ILF-100.

To restore factory defaults without removing power, press and hold the RESET switch SW1, then press and hold the INIT switch SW2. Release the RESET switch, then release the INIT switch when you see all the red / green LED pairs illuminate. The red / green LED pairs will blink once a second as an indication that factory defaults are being re-written to flash memory. When the blinking ceases, the initialization is complete.

Hard Reset

The ILF-100 can be reset by momentarily pressing the RESET switch SW1.

Re-sending the Sign-On Email

To prompt the ILF-100 to re-send its sign-on email (with serial number, IP address, and firmware version), momentarily press the INIT switch SW2.

Explanation of the INTERNET, EMAIL, PING, and HTTP Status LEDs

INTERNET

- Green: One or more of the monitored servers are responding.
- Red: No servers are responding; the internet connection is down.

EMAIL

- Green: An email was successfully sent.
- Red: The last email attempt failed.

PING

- Green: The server being tested replied to the ping test.
- Red: The ping test failed / timed out. **Note: some servers reject all pings. This is normal and can be ignored as long as the HTTP test passes.**

HTTP
- Green: The server replied to an HTTP request.
- Red: The server did not reply to an HTTP request and is not reachable.