Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Securing Your RILOE Cards

Compaq Remote Lights Out Edition (RILOE) Cards are a PCI based Board designed by Compaq intended to provide remote server manageability from any network client using a standard web browser. The RILOE board provides keyboard, mouse, network, power, and video capability for a server regardless of the state of the host operating system or host server. In order for one to completely understand RILOE's, I believe it's very important for me to cover all aspects of the card. In this paper I will outline the components of the ...

Copyright SANS Institute
Author Retains Full Rights

AD
CounterTack
Counter Tack Active Forensics for In-Progress Attacks
GET THE WHITE PAPER NOW >>>

Securing your RILOE cards

Abstract:

Early in 2001, I was tasked with qualifying and testing RILOE cards in our environment here.. Soon after product qualification, my company started ordering Compaq Remote Lights Out Edition Cards (RILOE) for our proliant family of servers. RILOE's are a PCI based Board designed by Compaq intended to provide remote server manageability from any network client using a standard web browser. The RILOE board provides keyboard, mouse, network, power, and video capability for a server regardless of the state of the host operating system or host server. In order for one to completely understand RILOE's, I believe it's very important for me to cover all aspects of the card. In this paper I will outline the components of the RILOE, detailed features and functionality of the card, pre installation tips, physical installation instructions, physical setup instructions, and initial setup configuration perameters. These sections prelude the most important part of this paper which is securing the RILOE card. I've found that knowing how to secure the card is just as, if not more important as any of the sections mentioned above. A misconfigured or unsecure RILOE could grant an attacker supreme dominance of your server and any other servers in which your host has access to. The capabilities of the RILOE are unparalleled by any other remote management solution. If a RILOE is a potential candidate for a remote managing solution in your environment, it is of utmost importance that the time is taken to secure it . First, lets look at the basics of the RILOE.

Functionality:

Some of the functions the RILOE offers remotely are:

*__Remote Reboot__ for resetting your server
*__Remote recycling__ for resetting your serve
*__Virtual Floppy__ for inserting a virtual 3.5 floppy image
*__Remote Firmware Update__ for updating your firmware on your server or RILOE.
*__Native graphical remote control__ for remote controlling your server
*__Down the wire disaster recovery, or OS rebuilds__ which provide the functionality of rebuilding your system from the ground up without touching your system.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

***External Power Backup** for access to your server if power is unavailable.
***Dedicated network interface** for network access if network connectivity is lost to your server

There are other companies that offer remote manageability devices such as DELL DRAC (Dell Remote Assistant Card). My focus in this paper will be specifically the RILOE card installed in a Compaq Proliant DL380 server. Proliant servers occupy a large portion of datacenters worldwide. RILOE's are compatible with a large amount of Proliant and Prosignia servers. The Proliant DL380 is a very common Compaq server which is why I decided to talk about RILOE cards in that specific server. For compatability, please see Compaq's Quickspecs @:
http://www.compaq.com/products/quickspecs/10452_div/10452_div.html#QuickSpecs [1]

Security should always be a primary concern to the owner of the server. Once a RILOE is installed in a server, it opens up a vast array of options for an attacker to use at will provided they have access to the subnet the RILOE is connected to. Once the RILOE is installed and connected, all the settings are default until changed by an administrator. This makes it extremely easy for a perpetrator to browse to the card, enter default login parameters, and instantly he/she has complete control of the server all the way down to the power. I will go over these issues in a bit, but before I do, I feel it is important to understand the physical aspects of the RILOE and proper installation. Before addressing security issues, its absolutely necessary that the RILOE card is correctly installed, configured, and tested. Only after these tasks are completed and validated can you configure a secure installation of the RILOE. I will talk about how to secure the RILOE in order to avoid this sort of situation..

First and foremost lets talk about physical installation, specifically in the Proliant DL380. DL 380's are a common Compaq server with 6 bays and typically Dual Processors. Note: In the DL380 ***G2*** model, RILOE boards come integrated thus not needing physical installation. Lets do a quick walkthrough of a RILOE installation in the DL380.

Physical Installation:

A basic checklist that I created for training site operation personel consisted of four of the most important components. Usually during typical installations, one of the 'basic six' components were overlooked.

PRE - CHECKLIST:
Having the right components:

[1] Quick Specs for the RILOE card. Compaq Computer Corp. DA-10452 World-Wide Version 6 Feb 22 2001

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

•Physical RILOE Card and appropriate connectors?
Remember- some models come pre-installed

•AC power supply?
not required in all models

•Network drop (Production Subnet)

•Network settings : Static IP ***NOT*** DHCP

•Secure IP addresses and DNS entry for Server ***and*** Riloe

•Compaq Agents installed/present.

Taking an Inventory of Parts:

First, take an inventory of the parts and insure that all the components are there. Here is what you should have:

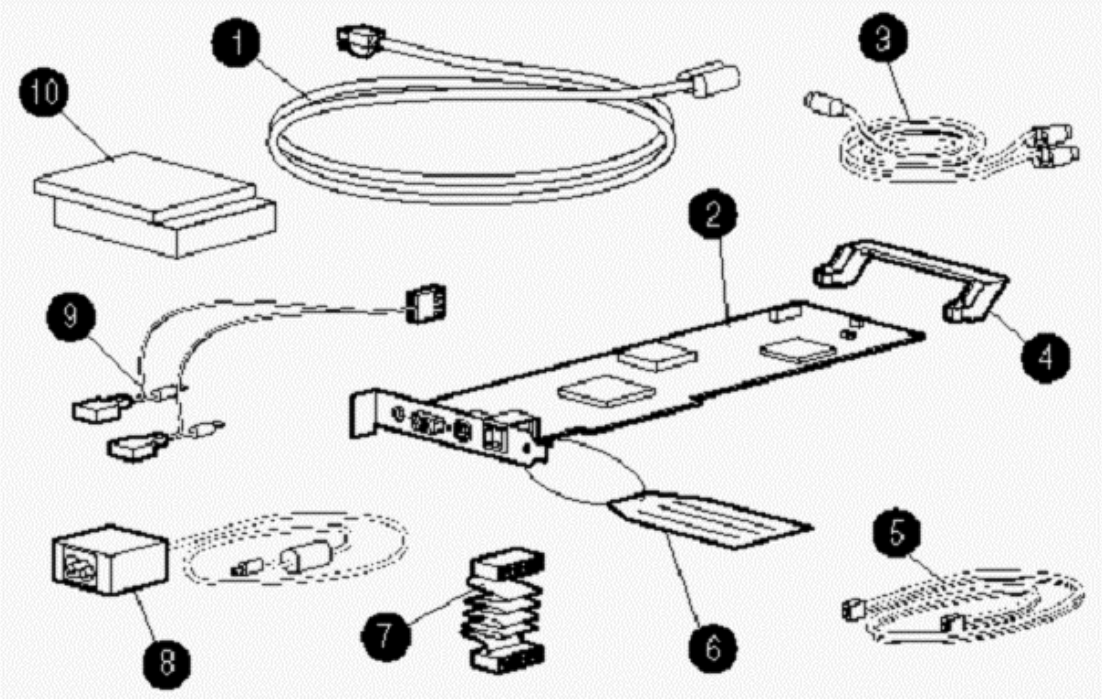


*Figure 1.1 from RILOE User Guide Section 2-2
ftp://ftp.compaq.com/pub/products/servers/management/159206-005bm.pdf[2]

[2] Compaq RILOE User Guide, fifth Edition July, 2001, Part # 159206-005

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

1. Power Cord
2. Remote Insight Lights Out Edition Board
3. Keyboard / Mouse adapter cable
4. PCI extender bracket
5. Virtual power button
6. Network Settings Tag
7. Internal virtual power button, keyboard, mouse, and power cable
8. AC power adapter
9. N/A
10. System documentation and support software CD

Now that we have validated that we have all the right hardware Lets go over installation steps for the RILOE in the DL380:

Installation Steps:

Step1: Power off the server and remove the power cord from the back of the server.
Step2: Remove the server access panel.
Step3: Insert the RILOE in PCI slot 1. Note: Compaq requires the RILOE to occupy this slot.
Step4: Connect the virtual power cable.
Step5: Replace server access panel
Step6: Replace power cord to the server.

Now that the card is physically installed in the server, we can setup the card.
This involves a few more steps. The below diagram explains the connectors on the card:

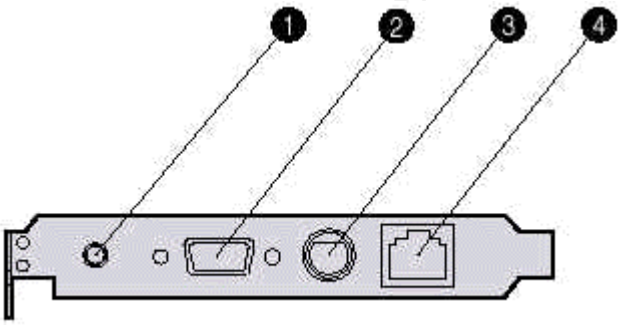


*Figure 2.2 Section 2-10 from RILOE User Guide
ftp://ftp.compaq.com/pub/products/servers/management/159206-005bm.pdf[2]

1. AC connector
2. Video port

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

3. Keyboard/Mouse port (K/M port)
4. RJ-45 connector

Physical Setup:

Lets go over the quick setup steps for the RILOE in the DL380:

Step1: Connect RILOE power cable to AC adapter
Step2: Plug power AC adapter cord to AC connector on the RILOE card.
Step3: Plug AC adapter into outlet
Step4: Referring to diagram below, connect K/M adapter cable to appropriate areas:

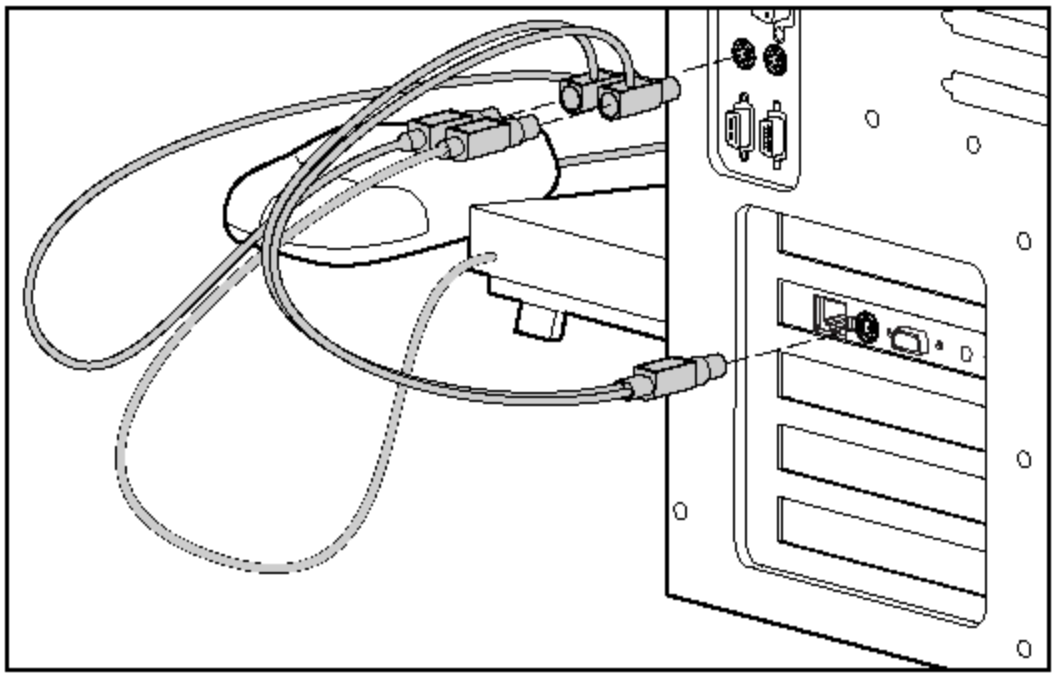
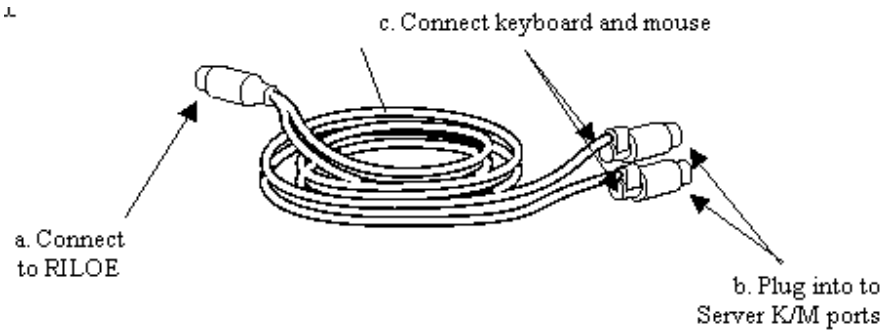


*Figure 2.3 Section 2-11 RILOE User Guide
ftp://ftp.compaq.com/pub/products/servers/management/159206-005bm.pdf

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.



A. Connect RILOE keyboard/mouse adapter to RILOE K/M port on card.
B. Connect the separate K/M adapter plugs to the appropriate ports on the server.
C. Connect keyboard and mouse to respective RILOE adapter cable plug.

Step5: Connect video cable from monitor to RILOE video port.
Step6: Connect your network drop to the RJ-45 connector
Step7: Power on the server

Understanding the Capabilities:

Now that the RILOE is installed, it is important to completely understand the key features of the card and what the capabilities of the card are. Let me briefly go over the key features and give an explanation of each:

Virtual Graphical Remote Console - This is a hardware based, OS independent graphical
remote console requiring only a browser. Once connected to the RILOE, you can start a remote console and even watch the server reboot from the console. Once in the console, you have full control over the machine as if you were standing right in front of it..

Virtual Floppy Drive – This feature allows the host server to remotely boot from a standard 1.44 MB floppy diskette. All that is needed is Compaq's diskette image utility to create a bootable image which is virtually inserted into the memory on the card acting as a real floppy in the server. This allows down-the –wire firmware updates, and flashing the systems BIOS.

Virtual Power Button – This feature allows you to remotely power up or down your server through a web console. You can simply start a browser from a remote machine, log onto the card and instantly power the machine up or down.

Dedicated LAN Network Connectivity - The RILOE has an onboard Ethernet chip (10/100Mb/s) that provides a dedicated network connection to the server or RILOE card itself.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Auto Configuration of IP Address via DNS/DHCP – This feature allows automatic network configuration which allows it to work right out of the box. (Very dangerous if not preconfigured)

External Power Backup__-- The RILOE has a external power connector assuring continuous power to the server even if it is powered off or the power is disconnected.

Initial Setup Parameters:

Now the RILOE is online and set to it's default initial settings. There are two ways we can set the card initially; with the setup prompt,
or the web interface. I recommend the setup prompt because it is the simplest and quickest way to disable the default settings and no agents
or web browsers are needed. The below are the areas to focus on changing IMEDIATELY. Not changing these settings leaves the biggest
security hole possible. Attackers always shoot for the 'default' target first counting on the administrator to overlook changing them.
Here are the key parameters needing changing:

****DHCP enabled***: This lets the DHCP server on this network chose an IP address for the RILOE
card itself. not changing this will make it difficult to track the IP of your card. This should be set to static
for accountability. Using DHCP for the card, you can never be sure which IP address the card is using. Changing
this will simplify finding the card on the network later and assure it follows the IP standards you set up for the card
especially if there are other RILOE's in your environment.

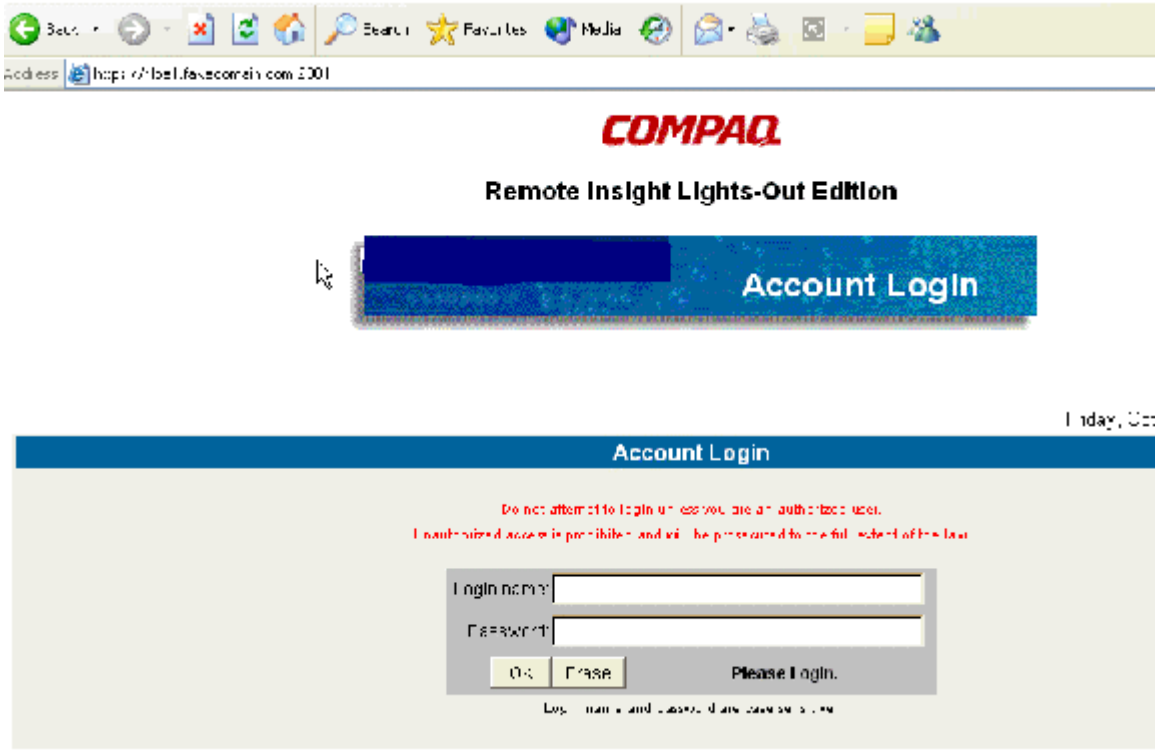
****DNS Name***: The default DNS name of the card will be a few characters followed by the serial number of the card itself.
The serial number is on the tag that is accompanied with the card once it is pulled out of the box. It could be very easy for someone
to find this tag, and instantly know the name of your card. It is important that you keep this tag somewhere safe and hidden if not
destroyed once you configure your RILOE.

****Administrator account on card:*** This account has the password set to the last four digits of the serial number of the RILOE card.
this can easily be obtained by running scripts against the card, specifically XML scripts that can be provided by Compaq.

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Because the RILOE is a card that enables Web Access to the card itself, Anyone can browse to the card, enter in the default
administrator username and last four digits of the serial number, and instantly, they have control of not only the card, but the server itself.
changing this is probably the most important step in securing your RILOE. Below is a screen capture of a web interface to the card. Notice
by default it connects using port 2301.



Now that I have gone over the basics of the initial configuration, lets walk through the pre-setup option that Compaq gives you before you take full control of your RILOE through a web interface:

<u>Preconfiguring the RILOE through the Setup Prompt:</u>

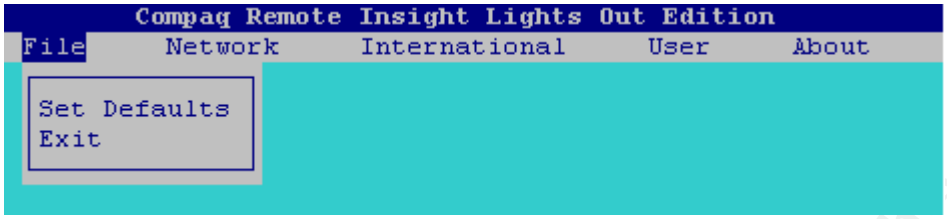
After installing the RILOE and reboot, an extra setup prompt will appear when booting. When prompted, press [F8] and this will bring you into the initial setup screen. This is what it will look like:

```
Compaq Remote Insight (Hit [F8] to configure)
```

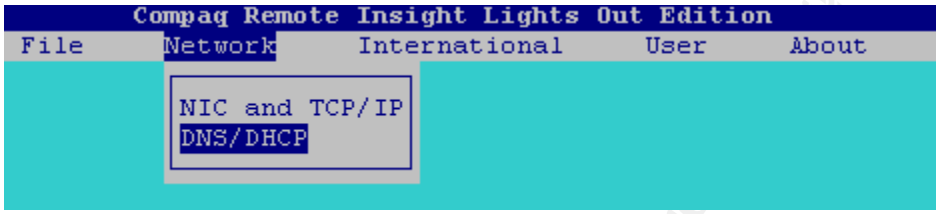
Here you will be able to configure some of the necessary options in order to start the security configuration ..

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

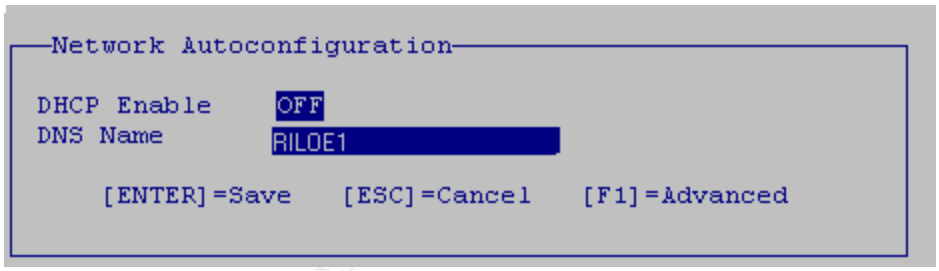
Once you push the [F8] button, this screen will appear. Here a few parameters should be set in order to set the IP to a static address and disable DHCP.



Here under Network, scroll down to DNS/DHCP and hit enter.



Once this screen is visible, [SPACEBAR] will toggle the 'ON' to 'OFF' DHCP has just been disabled and a static address can be entered under "NIC and TCP/IP" or the web configuration once logged onto the card through a web console.



Below, under network settings and "NIC and TCP/IP" you can configure the IP Address, Subnet Mask, Default Gateway. Enter these designated parameters for the RILOE. Note: You can also turn the network adapter on or off as well as transceiver Speed Auto select.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

```
Network Configuration

MAC Adress                          xx-xx-xx-xx-xx-xx
Network Interface Adapter           ON
Transceiver Speed Autoselect        ON

IP Adress                           X.X.X.X
Subnet Mask                         255.255.255.0
Default Gateway                     X.X.X.X

    [ENTER]=Save    [ESC]=Cancel    [F1]=Advanced
```

[ENTER] will save settings and the reboot the host machine.

Securing the RILOE:

Now that we've gone over proper installation and setup.. We can focus on securing the RILOE to minimize damage in the case of an attack.. This process is often overlooked by non- security minded administrators. That is why it is important to know of the security features that the RILOE has to offer. For a quick-spec security doc please see: http://www.compaq.com/manage/remote-lightsout-security.html. [3]

A non-secure RILOE connected to a server can introduce a much larger threat to the host server than if it had no RILOE installed at all. That is why it is CRITICAL that you tailor a security implementation that fits your network environment.. In the rest of the paper, I will provide a detailed description of most of the available options for implementing security on your RILOE or RILOE's. Below I will list the available security features and how to configure them after the RILOE is set up and online.

Security Recommendations:

This sections outlines the BKM (best known methods) for securing your RILOE card. The below recommendations are in my opinion the best way to start out your RILOE security configuration. I will outline my recommendations for key areas and expand on them in order to convey the process of fully securing your RILOE.

[3] Security Features of the RILOE, 2002 Compaq Info technologies group, L.P.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Setting up User accounts and assigning privileges: RILOE's currently are programmed with 12 user accounts all of which can be granted different privileges. I recommend setting up one account that has privileges to add, delete, or modify users. The rest should be set to your administrative needs. Here are the types of accounts you can create within the RILOE and a rundown of the user privileges:

Receive Host OS Generated SNMP Traps	○ Yes	⊙ No
Receive Compaq Remote Insight Board Alerts	○ Yes	⊙ No
Supervisor Access	⊙ Yes	○ No
Login Access	⊙ Yes	○ No
Remote Console Access	⊙ Yes	○ No
Remote Server Reset and Power Button Access	⊙ Yes	○ No

***Supervisor*:** With these privileges, the user can add, delete, or modify users privileges. It also inherits all of the privileges offered .

Login Access: With these privileges revoked, (provided the user does not have supervisory access) the user can not login in, but receive RILOE card alerts which I will talk about in a later section.

Remote Console Access: With these privileges revoked, (provided the user does not have supervisory access) the user can not access the remote console portion of the RILOE.

Remote Reset and Remote Power Button Access: With these privileges revoked, (provided the user does not have supervisory access), the user can not access the remote console portion of the RILOE which I will discuss in a later section.

Receive Host OS Generated SNMP Traps: Refer to the RILOE with CIM XE section.

Receive Compaq Remote Insight Board agents: Refer to the RILOE with CIM XE section.

Setting Strong Passwords: Setting Strong Passwords is one of the most basic but most important security methods used in today's network environments. For Strong Password According to the Administrative Information Service of Perdue University, a Good password is difficult to guess because of these attributes:

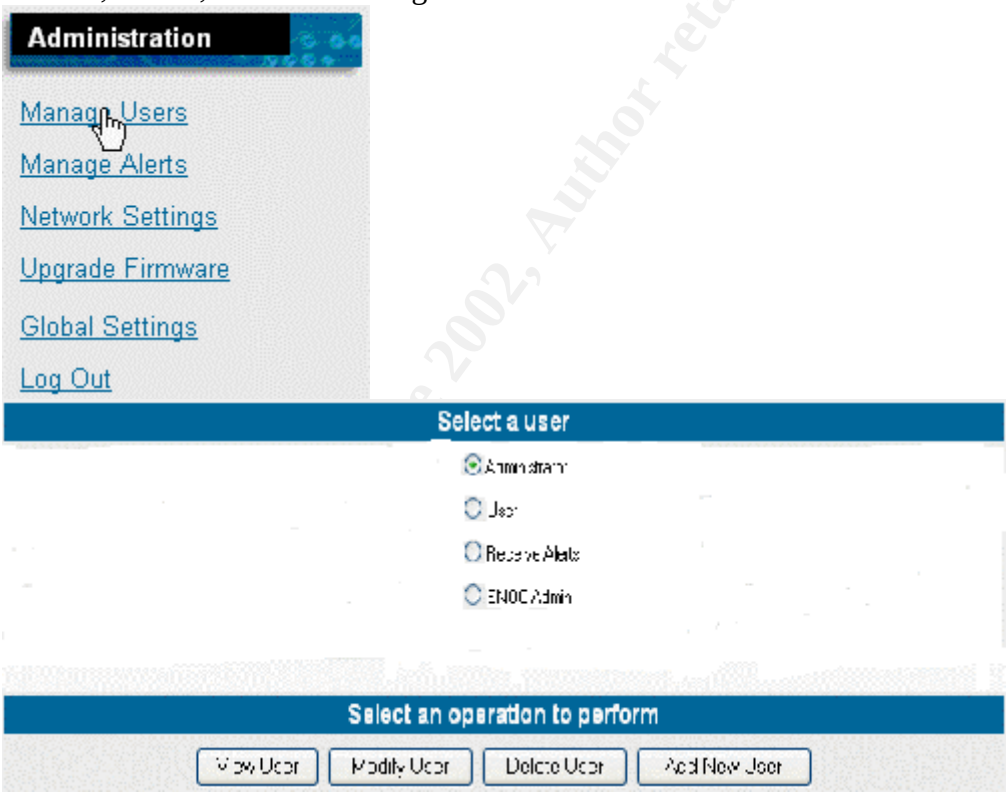
- Are easy to remember, so they do not have to be written down.
- Are seven or eight characters long (the longer the stronger).

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

- Can be typed quickly, so somebody cannot determine what you type by watching over your shoulder.
- May contain both uppercase and lowercase letters.
- May contain digits and/or punctuation characters as well as letters.
- May include some control characters and/or spaces."

Please see http://www.adpc.purdue.edu/BSC-Pete/TotalComp/passwrds.htm [4] for some good password creating recommendations and Best known Methods (BKM). Towards the end of this paper I included some code in XML to enforce a strong password on the RILOE.

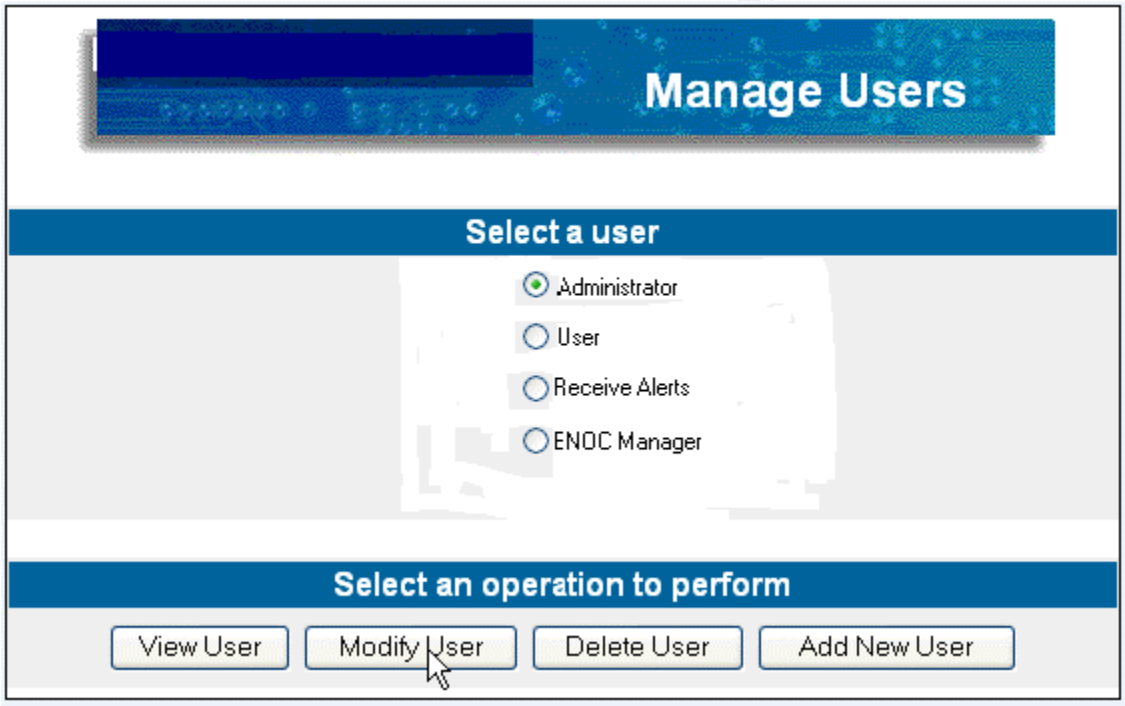
To set passwords click on the manage users link and chose the user you want. Click on Modify User button and the modify user screen will appear. Here you can set your User Name, Login Name and Passwords. The User Name and Login name differ in that the User Name is not used to login, but is displayed in the user list and on the home page. The Login name is what must be entered at login with a password. Users can be Created, Deleted, Edited, or Viewed using the buttons below the user names.

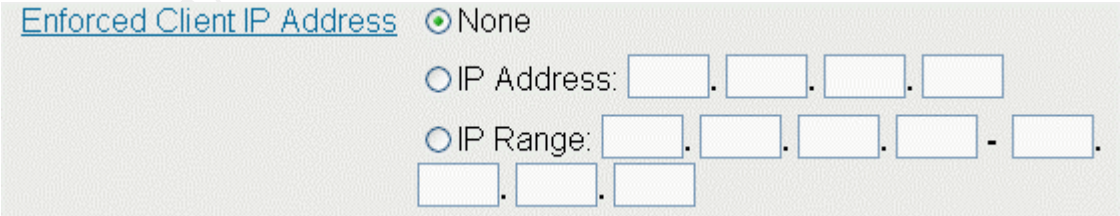


[4] Setting Strong Passwords, Perdue University, copyright 2000

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Enforcing Client IP address's: When editing a user account, the administrator can limit inbound login access to a specific IP address, range of IP's, or DNS name. This is a very good way to keep track of who is logging into your card and limiting the threat of outsiders gaining access to your RILOE.
To do this, follow the same steps to modify the user's account and click on the Enforce Client IP Address radio button and set the desired IP address or Range.



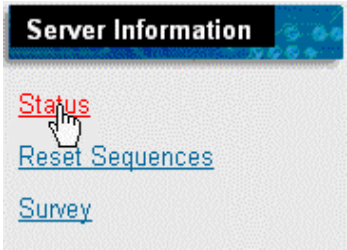


Upgrading the 40-bitSSL encryption to 128-bit SSL Encryption: RILOE's currently come with 40-bit SSL encryption. Compaq offers 128-bit encryption which can be

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

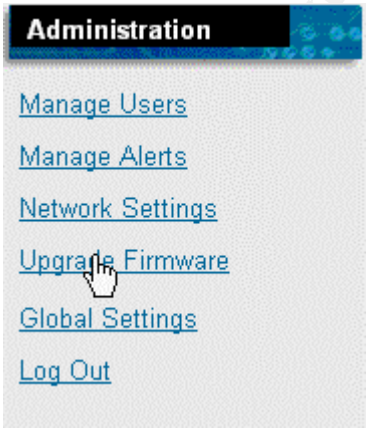
downloaded and loaded onto your RILOE card. Upgrading the firmware on the RILOE to the latest version will automatically install 128-bit SSL encryption. For more info on SSL please see: http://developer.netscape.com/tech/security/ssl/howitworks.html[5] for a good understanding of SSL concepts.

Before you upgrade the firmware, you should check the current version of the RILOE. To check the version, go to the Server Information section on the left, and click on the 'Status' Link. This will show you a variety of configuration options and settings. Specifically we are looking for the 'Remote Firmware Version' line which lists the current firmware version installed on the RILOE.



Our screen print reflects that the last version of firmware version upgrade to the RILOE was the 08/27/2001 version:.

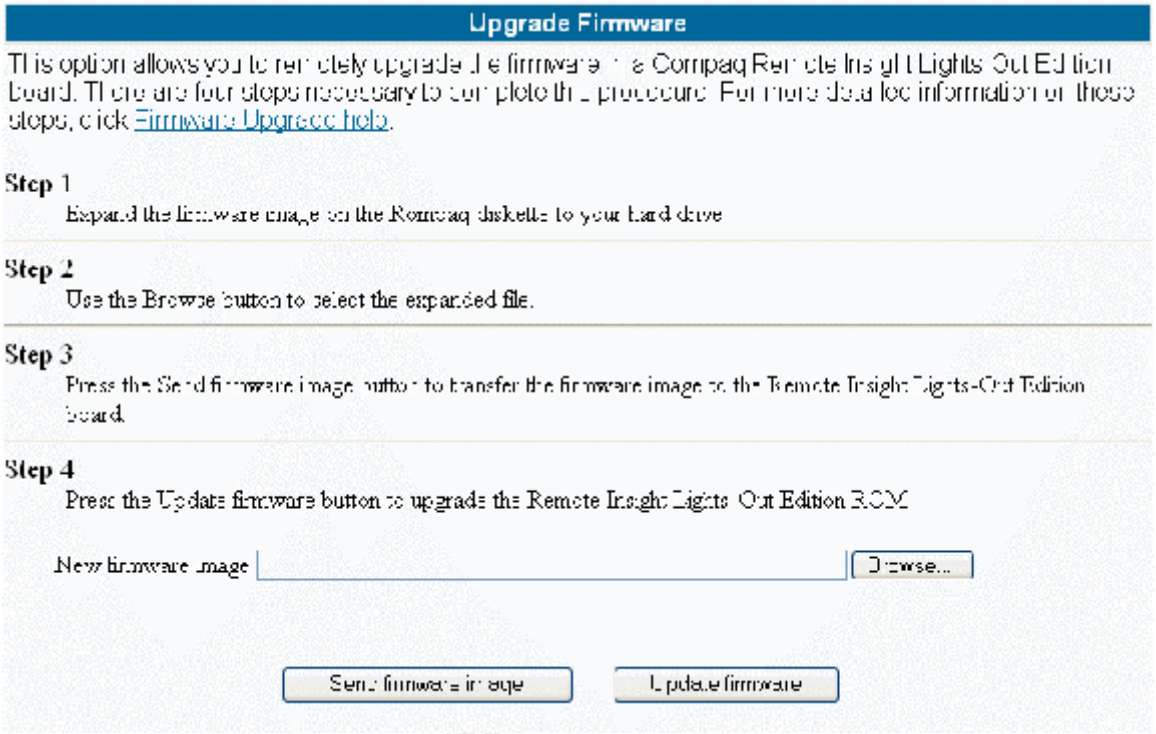
So now that we know the version, we can proceed with downloading the latest firmware version and upgrading it on the RILOE. To do this, I'll go over some quick steps in order to upgrade the firmware on the card. The RILOE has a specific firmware upgrading tool built into the software on the card. To update firmware using this tool, go to the Upgrade Firmware' area under 'Administration and click on the
link.



[5] How SSL works, Netscape Communications 1999

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Here, the Firmware Upgrade tool will give you step by step directions and walk you through the process. I have never seen an easier way to upgrade the firmware on any device. It is full proof and as long as you download the image from Compaq and are able to browse to it, it's as easy as a few clicks and you're done... There is also a 'Help' section if needed.

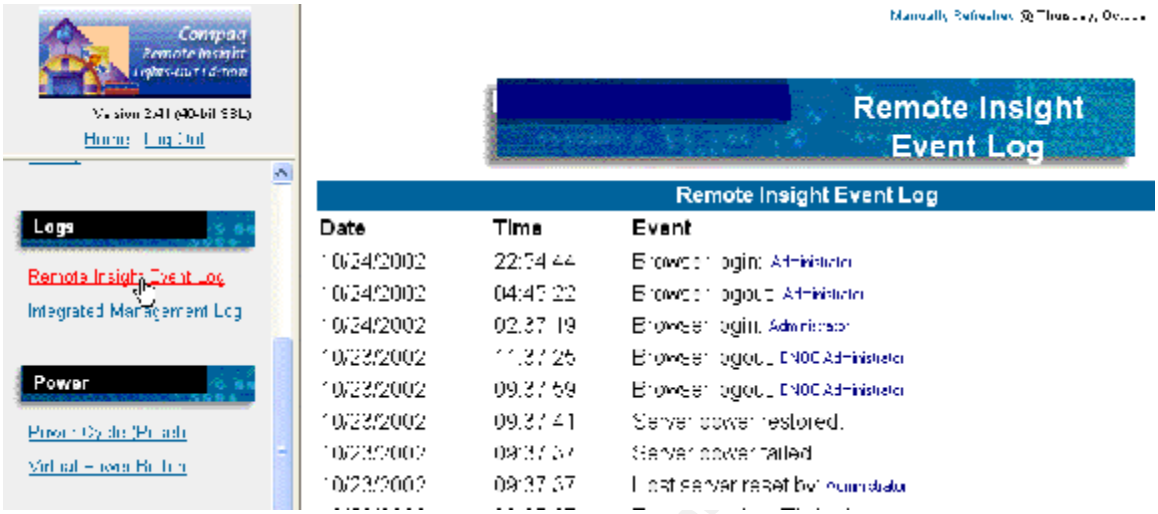


Remote Insight Event Logging: Event logging is a very good security tool that leaves a trail of events that occur on your system... "Event logging is the process of recording user-initiated activities and has been a practice software usability testing for decades" - http://www.netconversions.com/IP_EventLogging.pdf [6].. Event logging is available in many environments, from NT, Active Directory, to Linux, to Stand-Alone event logging apps such as S.E.L.M. (Security Event Logging Management)..It is available within most all operating systems and applications.. With Event Logging enabled, you have a comprehensive recollection of events that occurred on your Operating system or Application. Event logging can be set up for web pages and be as granular as recording points of a web page that users clicked. This information can be analyzed and used for future web design effectiveness... RILOE cards contain event logging called Remote Insight Event Logging which is independent of the operating system. The amount of information propagated depends drastically on how comprehensive event logging you set up.. To access the event log within the RILOE card, simply click on the Remote Insight Event Log link under the Logs section.

[6] Event Logging, Steven Kangas, PH.D technology officer, June 2001 "Learning from Event Logging"

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Here you will find most events that occur on your card and the user that initiated them. As stated in a further section of this paper, RILOE's can be set
up to forward events via traps to a central console such as CIM XE.



Alert Administration - Another feature of the RILOE card is alerting. using traps sent to a central console,
the RILOE can be configured to send an alert to the CIM XE console given the two are set up to communicate.
The RILOE can be configured to send an alert on various events such as a failed user login, server reset,
and others. From the CIM XE console, alerting can be set up to page a user when an alert is received. There
are several different implementations of this in different network environments. Mine specifically, was set up
by events occurring in this order:

1. CIM XE Server SNMP polls all Compaq servers.
2. CIM XE Server SNMP polls all RILOE cards.
3. Compaq Insight Agents send SNMP traps to CIM XE on error (these are agents that sit on individual boxes and RILOE cards.)
4. RILOE's send traps to CIM XE Server
5. CIM XE Server uses another service to send events to another alerting console which is passed to other services.

Properly Set up, alerting can be very helpful in managing servers and RILOE's but for me to go over a detailed configuration would
be useless considering the differences in implementations depending on your network environment. Let me attempt to convey a surface
understanding of CIM XE by covering the key aspects of CIM XE:

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

What is Compaq Insight Manager?

*A web based Enterprise Management Application (WBEM) enabling browser access to manage devices and groups of devices from any web browser.

CIM XE's Three Main Components*: *Management Services, Systems Management, and Cluster Manager

But the Component I will focus on here is the **Management Services** Component and the **Systems Management** Component. In the Management Services component you can collect data, perform event information, notifications, and access. In the System Manager, you can access web consoles on individual machines, perform event notification, and perform operations on groups of devices.

CIM XE Architecture:

CIM XE is a three-tiered client-server application. The following represents the three layers:

Management application (CIM XE)
User interface (Web Browser)
Agents (Compaq Management Agents that reside on the RILOE and Server)

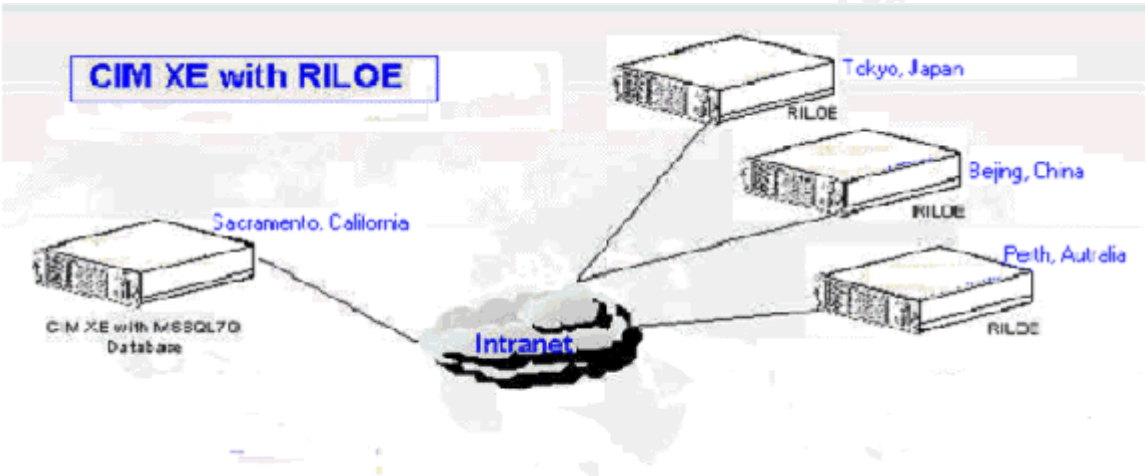
Since I am focusing on RILOE's in this paper I won't go very in depth into Compaq's CIM product. Instead I will give a general overview to demonstrate the functionality and integration of RILOE with CIM XE.

Below is a graphic of an implementation where RILOE's world wide are managed by the

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

CIM XE application. CIM XE runs on a SQL back-end with a Web interface to access the data.
Here RILOE's can be accessed from the CIM XE console, and management operations can be
performed on each individual server all from one central console. CIM XE makes managing RILOE's
simple and easy.

A typical CIM XE with RILOE implementation:



Managing your RILOE's with XML:

In addition to managing your RILOE's through a web console, or CIM XE console, Compaq
leaves the option to use scripts to accomplish this. RILOE's work off of a language called
Remote Insight Board Command Language (RIBCL). Compaq can provide XML scripts if this your management choice. Then you can modify these scripts in order to tailor them to your
network environment. Below I want to provide some scripts written by a friend of mine. These scripts use XML, PERL, and RIBCL to execute tasks such as: listing the firmware version of the card to listing user information on a card. Listed below is a sample code written in conjunction with the code Compaq provided in order to modify these functions to
our needs: It is my intent to provide this in hopes of saving you some time if this is an area of administration you'd like to concur. Please note that all environments differ from each other and I do not guarantee that this specific code will execute successfully in your environment. At the very least, this could be a good reference to pull from when writing your own scripts.

A brief explanation:

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

When an option is selected the XML script needed to perform the task is generated and put in the input.file text file which is passed to the cpqlocfg.exe program for execution.

When adding a user there is additional code to require that strong passwords are entered. This is a GREAT feature in the script that will not accept anything but a strong password with minimum characteristics including that the password be between 8 and 48 characters,
include characters, numbers, and special characters. This script uses a combination of RIBCL, XML, and PERL. Please use at your own risk.

CODE:

```
## COMPAQ RILOE CARD XML TOOL
## Author - Kirt Nystrom
## Last updated
##

print "Enter Servername or IP Address:";
SERVER: chomp($server=<STDIN>);
print "Enter User Name:";
USER: $user=<STDIN>;
chomp($user);
PASSWORD: print "Enter Password:";
$password=<STDIN>;
chomp($password);
while ($input ne "x") {
MENU:
print "\n\nRILOE Menu for $server - Username - $user\n\n";
print <<EOF;
1 - Get All Users
2 - Get Firmware Info
3 - Get Host Power Status
4 - Get User Info
5 - Get Virtual Floppy Status
6 - Get Virtual Power Button Cable Status
7 - Add User
8 - Remove User
9 - RESET Server
e - Exit

Enter Selection:
EOF

        $input=<STDIN>;
        $inputfile="input.file";
        $logfile="riloe.log";
        $xmlout="riloe.xml";

        open(LF, ">>$logfile") || die "Can't open $logfile($!)\n";
        open(XML, ">$xmlout") || die "Can't open $xmlout($!)\n";

        ## Write Header for input file
        open(INPUT, ">$inputfile") || die "Can't open $inputfile($!)\n";
        print INPUT "<RIBCL VERSION=\"1.2\">\n";
        print INPUT "<LOGIN USER_LOGIN=\"$user\" PASSWORD=\"$password\">\n";
        ##

        if ($input==1) {        ## All Users

                print INPUT "<USER_INFO MODE=\"read\">\n";
                print INPUT "<GET_ALL_USERS />\n";
```

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

```
                print INPUT "</USER_INFO>\n";

        }elsif ($input==2) {    ## Firmware Info

                print INPUT "<RIB_INFO MODE = \"read\">\n";
                print INPUT "<GET_FW_VERSION/>\n";
                print INPUT "</RIB_INFO>\n";

        }elsif ($input==3) {    ## Host Power Status

                print INPUT "<SERVER_INFO MODE = \"read\">\n";
                print INPUT "<GET_HOST_POWER_STATUS/>\n";
                print INPUT "</SERVER_INFO>\n";

        }elsif ($input==4) {    ## User Info
                print "Enter User name:";
                chomp($user_login=<STDIN>);

                print INPUT "<USER_INFO MODE=\"read\">\n";
                print INPUT "<GET_USER USER_LOGIN=\"$user_login\" />\n";
                print INPUT "</USER_INFO>\n";

        }elsif ($input==5) {    ## VF Status

                print INPUT "<RIB_INFO MODE=\"read\">\n";
                print INPUT "<GET_VF_STATUS/>\n";
                print INPUT "</RIB_INFO>\n";

        }elsif ($input==6) {    ## VPB Cable Status

                print INPUT "<SERVER_INFO MODE = \"read\">\n";
                print INPUT "<GET_VPB_CABLE_STATUS/>\n";
                print INPUT "</SERVER_INFO>\n";

        }elsif ($input==7) {    ## Add User
                print "Enter User Display Name:";
                chomp($user_name=<STDIN>);
                print "Enter Login:";
                chomp($user_login=<STDIN>);

#-------------------------------------------------------------------------------------------------------------------------------------------------------------#
# Strong Password Enforcement code
                PASSWORD:print "Enter Password:";
                chomp($user_pw=<STDIN>);
                $pwlength=length($user_pw);
                if ($pwlength <9) {
                        print "Invalid Password - Must be at least 8 characters in length\n";
                        goto PASSWORD;
                }
                if ($user_pw =~ /.{1,}\d+[~!@#\$%^&*()_+=`~]/) {
                        #print "Valid\n";
                } elsif ($user_pw =~ /[~!@#\$%^&*()_+=`~]+.{1,}\d/) {  ## Comment this item... and also check for length between 8 and 48
characters
                        #print "Valid\n";                                                ## Also check max allowed password length...

                } else {
                        print "$user_pw is not a valid Password - Must include characters,numbers and special characters\n";
                        goto PASSWORD;
                }
#-------------------------------------------------------------------------------------------------------------------------------------------------------------#
                print "*Enter SNMP Address:";
                chomp($snmp_addr=<STDIN>);
                print "*Enter SUPERVISOR_PRIV(Y/N):";
                chomp($SUPERVISOR_PRIV=<STDIN>);
                print "*Enter Client Range . value1:(xxx.xxx.xxx.xxx)";
                chomp($client_range1=<STDIN>);
                print "*Enter Client Range . value2:(xxx.xxx.xxx.xxx)";
                chomp($client_range2=<STDIN>);

                print INPUT "<USER_INFO MODE=\"write\">\n";
```

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

```
                print INPUT "<ADD_USER USER_NAME=\"$user_name\" USER_LOGIN=\"$user_login\" PASSWORD=\"$user_pw\">\n";
                if ($snmp_addr ne "") {print INPUT "<SNMP_ADDRESS value =\"$snmp_addr\"/>\n";}
                if ($SUPERVISOR_PRIV ne "") {print INPUT "<SUPERVISOR_PRIV value =\"$SUPERVISOR_PRIV\"/>\n";}
                print INPUT "<LOGIN_PRIV value =\"Y\"/>\n";
                print INPUT "<REMOTE_CONS_PRIV value =\"Y\"/>\n";
                print INPUT "<RESET_SERVER_PRIV value =\"N\"/>\n";
                print INPUT "<OS_TRAPS value =\"Y\"/>\n";
                print INPUT "<RIB_TRAPS value =\"N\"/>\n";
                if ($client_range1 ne "") {print INPUT "<CLIENT_RANGE value =\"$client_range1 - $client_range2\"/>\n";}

                print INPUT "</ADD_USER>\n";
                print INPUT "<GET_ALL_USERS />\n";
                print INPUT "</USER_INFO>\n";

        }elsif ($input==8) {    ## Remove User
                print "Enter User Name to Remove:";
                chomp($user_login=<STDIN>);

                print INPUT "<USER_INFO MODE=\"write\">\n";
                print INPUT "<DELETE_USER USER_LOGIN=\"$user_login\"/>\n";
                print INPUT "<GET_ALL_USERS />\n";
                print INPUT "</USER_INFO>\n";

        }elsif ($input==9) {    ## RESET SERVER
                print "Are you sure you want to reset $server?(Y/N)";
                $reboot=<STDIN>;
                if ($reboot=="Y") {
                        print INPUT "<SERVER_INFO MODE = \"write\">\n";
                        print INPUT "<RESET_SERVER/>\n";
                        print INPUT "</SERVER_INFO>\n";
                } else {
                        print "NOT RESETTING $server\n";
                        goto MENU;
                }

        }elsif ($input =~ /e/) {                ## Exit
                print "Goodbye...\n";
                exit;
        } else {
                print "Invalid Entry";
                goto MENU;
        }
        ## Write Footer for INPUT file
        print INPUT "</LOGIN>\n";
        print INPUT "</RIBCL>\n";

        close(INPUT);
        ## RUN XML INTERPRETER ON INPUT FILE
        print "Processing input...\n";
        if ($input<10) {$output=`cpqlocfg -s $server -l $logfile -f $inputfile`;}
        #exit;
        print $output;
        print XML $output;
        close(XML);
        goto MENU;
}
```

[7]

Conclusion:

[7] Compaq RILOE Card XML Tool, Kirt Nystrom, February 8th, 2002

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Remote Management solutions are constantly changing in an ever so quickly changing technical space. Which solution you chose to use in your environment will greatly depend on the type of your hardware and the manufacturer of the hardware you are using. RILOE's are probably the best solution if the majority of your hardware is Compaq. RILOE's would not be a good fit if the majority of your hardware is DELL. Without the Compaq agents present, the RILOE is not as functionally robust. In this situation the DELL DRAC (Dell Remote Access Card) might be a good option. Whatever solution you chose, I urge you to exhaustfully take into consideration these key factors; Cost, Functionality, Compatibility, and Usability. With this in mind, being open to new technology and solutions will give you the edge you need to chose a long lasting product that will make your corporation a return on investment and make you look good in your yearly review process. ☺

Bibliography:

1. "Quick Specs" for the RILOE card. Compaq Computer Corp. DA-10452 World-Wide Version 6 Feb 22 2001 (September 25 2002)
http://www.compaq.com/products/quickspecs/10452_div/10452_div.html#QuickSpecs

2. "Compaq RILOE User Guide", fifth Edition July 2001, Part # 159206-005 (September 25, 2002)
ftp://ftp.compaq.com/pub/products/servers/management/159206-005bm.pdf

3. "Security Features of the RILOE", 2002 Compaq Info technologies group, L.P. (September 27, 2002)
http://www.compaq.com/manage/remote-lightsout-security.html.

4. "Setting Strong Passwords", Perdue University, copyright 2000 (October 02, 2002)
http://www.adpc.purdue.edu/BSC-Pete/TotalComp/passwrds.htm

5. "How SSL works", Netscape Communications 1999 (September 22, 2002)
http://developer.netscape.com/tech/security/ssl/howitworks.html

6. "Learning from Event Logging", Steven Kangas, PH.D technology officer, June 2001 "Learning from Event Logging" (September 23, 2002)
http://www.netconversions.com/IP_EventLogging.pdf

7. "Compaq RILOE Card XML Tool", Kirt Nystrom, February, 9th, 2002

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: June 19th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**