White Paper

Introduction
To
Console Management
And
SRENA

Secure Remote
Enterprise Network Management
Introduction to Console Management & SRENA

Market Overview ............................ 3
What SRENA Solutions are about! ....... 3
Meeting the Needs .......................... 4
Console Management ........................ 4
KVM Switches ............................... 5
Remote Control ............................. 5
Serial Consoles—Universal Management . 6
Remote Console Management (RCM) ...... 8
What is SRENA? ............................. 9
Problem-Solving with SRENA .............. 9
SRENA Required Features ................. 11
Selecting Your SRENA Solution .......... 13
Total Cost of Ownership Consideration 13
OutPost Sentinel Solutions .............. 15
The Emergency Network Specialist (ENS-8) 15
Port Commander ........................... 16
Secure Sentinel ............................ 17
Life Signs Sentinel (LSS) ................. 18
Power Control ............................. 19
Cycle Power ............................... 19
Summary .................................... 20
Market Overview

There has been a recent explosion in growth and demand for very large data centers and telecom collocation facilities. The centers provide much needed data storage, high-speed Internet access and web hosting facilities for businesses and Internet Service Providers (ISPs). These centers provide safe and redundant computer facilities, which require remote network management of equipment.

Companies need a way to access and manage networks and intelligent devices both locally and remotely. While being there is a preferred method of managing a network, it is not always possible. There is a shortage of trained MIS professionals, making it difficult or financially impossible for many businesses and remote branch locations to have onsite the technical expertise their businesses require. In addition, there are sites, such as high availability data centers, where it is not possible to have an MIS professional physically located at the site.

Secure Remote Emergency Console Administration (SRENA), like that provided by OutPost Sentinel, enables safe, secure and economical management of computing devices both locally and remotely.

Improving Data Integrity & Reliability

What OutPost Sentinel SRENA Solutions are about!

- REDUCE IT COSTS
  Lower Total Cost of Enterprise Network Management

- ELIMINATE DOWNTIME
  Immediate Access to down Network Devices

- MAXIMIZE IT COVERAGE
  Reduce Manpower and perpetually monitor all mission critical devices

- IMPROVE SERVICE
  Resolve problems instantly without waiting for onsite dispatch or traveling to down equipment

- INCREASE PRODUCTIVITY and MAXIMIZE PROFITS
Introduction to Console Management & SRENA

Meeting the Needs

Console Management

In-band Network Access

There are primarily two ways to manage a network: in-band network management and out-of-band management (OBM). In-band is managing locally through the network itself, using a telnet connection to a router or by using SNMP-based tools (such as HP’s Open View). In-band is the most common way to manage a network. However, for large or business-critical networks, in-band network management alone is not enough. If the network is down, you cannot use the network to reach the affected devices and resolve the problem. You need an alternate or secondary access path to get around the problem or to access the source of the problem—that is essentially what Out-of-Band Management (OBM) provides.

Out-of-Band Management

If there is a problem with a device such a server or a router, and traffic cannot flow through the network, you need an alternate path to reach the network nodes even when the network is down. Management using independent dedicated channels is called OBM.

OBM provides accessibility when an alternate path is needed to access the network nodes. In addition, OBM can provide coverage to many pieces of manageable equipment or intelligent devices that may not have a direct network connection to the data network, such as uninterruptible power supplies, PBX phone systems and intelligent thermal controls. For some of these intelligent devices that are not networked OBM may provide the only support and management tool.

For mission-critical networks, in-band management tools are not enough. You need a secure remote emergency network access path to manage and troubleshoot when the device is not on the network, the device is not network manageable or the data network is down. That is the benefit of OBM console management.

OutPost Sentinel’s Emergency Network Specialist (ENS-8) and Cyber Command Center offer a suite of both in-band and OBM tools.
KVM Switches

KVM (keyboard-video-mouse) and KVM Switching is one method of providing OBM. You may have seen the old “Crash Carts” that were carts with a keyboard, a monitor and a mouse on them. The administrator would push the heavy cart over to the failed system and plug the KVM devices directly into the unit to repair that station. This was a slow, labor-intensive solution. KVM switches were then developed, which can connect to multiple servers through their I/O ports and enable centralized local access from a single workstation. KVM switches provide a good local OBM solution because they use the same interface (keyboard-video-mouse) which we are already most familiar. However, KVM solutions are generally for local management only and remote access to the servers is usually not possible.

There are now some products that do offer KVM over IP, but these require very high bandwidth and do not work over dial-up lines. In addition, KVM switches generally require software specific to particular operating systems and may not support all platforms. KVM switches are also limited to managing only specific servers and cannot manage other intelligent devices such as routers, switches or PBXs.

The OutPost Sentinel ENS-8 does allow limited KVM system management and configuration.

Remote Control

Remote control programs can be used as an OBM management tool, as well. The remote control software is installed in the server to be managed. From a client PC (with remote control client software), you can connect to the server remotely using the network (in-band) or using a dial-up modem connection (out-of-band) and take control of the server, as if you were local to the machine.

Server-based remote control software is a limited solution because, like KVM solutions, it works for servers only and not for other
equipment. Even for servers, the remote control software may be limited to specific operating systems and platforms. It is also not a scalable solution and suffers from many of the same in-band network constraints. It is generally a one-to-one connection and would require considerable processing power, space, network bandwidth and telephone lines to manage multiple servers remotely.

Serial Consoles—Universal Management

The serial console is the only universal out-of-band management (OBM) medium. It provides both in-band and OBM management tools. It will manage any intelligent devices found on a network or in a data center and it can manage the devices locally or provide secure reliable remote network management.

A management solution may include many of the tools previously discussed, but it will not be complete unless it supports local and remote access to console ports. Look at the back panel of any desktop or laptop computer, server, modem, switch, power control, UPS, or PBX system and you will find a connector labeled “COM”, “AUX” or “Console”. This is what makes the serial console universal.

Network Servers

Originally the first computers had serial consoles as their only mechanism for external communication and interaction. Today, all computers, from the smallest desktop to the largest server has a serial console or a “COM” port that can be used as direct interface to manage the computer equipment and intelligent devices.

UNIX systems provide much of the backbone for the Internet and much of the enterprise level compute power. All UNIX servers running on RISC platforms (Sun Solaris on Sparc, HP HP/UK, IBM AIX on RS/6000, Compaq True64 on Alpha, etc.) use serial consoles for monitoring and management. The console ports also provide access to low-level system configuration (BIOS “monitor mode”) and allow remote power-on/off even before the OS is loaded.

PC-based servers such as Free BSD, Linux and Microsoft Windows NT can also use serial console ports for console management. These PC-based servers have built-in support for management using a serial console. As the price for PC servers continues to fall and the computing power and clustering abilities continue to increase, the need to control these servers in a headless environment through their console parts becomes increasingly important.

For some regular PC motherboards, console monitoring is possible only after the Operating System is active. Low-level monitoring and BIOS configuration cannot be done through a serial console. However, these PC’s may still be managed through their serial console or Com ports once the operating system is active. To activate or “Cold Start” one of these PCs the OutPost Sentinel ENS-8 should be used.
in conjunction with an OutPost Sentinel recommended intelligent power supply. This intelligent power supply allows power to be managed and cycled on or off through the OutPost Sentinel ENS-8 or Cyber Command Center units. Using the OutPost Sentinel intelligent power option enables controlled shut down and remote reboots. Once the operating system is engaged the OutPost Sentinel unit can manage and control these devices both in-band and out-of-band. It should also be noted that, new motherboards, adopted by every major server appliance vendor, specifically designed for use in rack-mounted servers and data centers come with a special console port for out-of-band management.

Clustering

Clusters or server farms are a collection of two or more computers working together to execute a task. To increase computing power, more computers or nodes are added to the cluster. Clustering is not new, but has gained momentum with the development of better clustering software, a significant increase in computing power in PCs, and by an increase in the demand for applications which require larger amounts of computing horsepower.

The clustering software allows a cluster or group of computers to be seen as a single large computer. Clustering software can immediately detect a node failure and re-assign the tasks to another node, thus yielding “high availability,” and with much less expensive hardware than mainframes. Unlike mainframes, clustering allows you to add power by adding to your computer instead of discarding it and getting a larger one. It allows you to leverage your existing hardware investment and incrementally scale computing power by adding another node (PC). OBM products like the ENS-8 provide clustering solutions with the redundancy and high availability they require.

Other Intelligent Devices

In addition to the physical network interfaces, almost every piece of intelligent network equipment (routers, switches, and access servers) has an additional OBM and configuration port, called a console or auxiliary port. Most other manageable devices have serial console, as well: UPS, PBX, ventilation systems, power control, temperature monitoring, data collection, etc. Some of those devices do not have direct network connections and the serial console is the only way to access the device remotely for management. Serial console management is the
only truly universal tool for all types of intelligent devices and network management.

Remote Console Management (RCM)

Remote console management gives you direct access to network devices regardless of network issues or your physical location. For example, when your router at a remote location is down you cannot communicate with it through the WAN. In-band management is impossible. You must find an MIS expert to send onsite.

Out-of-band management (OBM) provides a secondary path to the network devices. It allows the administrator to gain access to the remote device regardless of network issues. The administrator can dial into a remote console management device such as the OutPost Sentinel ENS-8 and connect directly up to the network element or intelligent device that is causing the failure. That device can then be restarted, reconfigured, or taken offline enabling your network to function with minimum downtime.

In addition, OutPost Sentinel products complement in-band management solutions, such as HP’s OpenView, NetCool or Tivoli. OutPost’s SRENA products pick up where these in-band or in network tools leave off. They provide local and remote network management even when the network is impaired. Again, you can not use the network to fix a device on the network when the network is “broken” and there is no network traffic. OutPost Sentinel’s SRENA products integrate well with these SNMP in network tools and compliment them by providing many of these same in network tools and by adding to them a much needed out of band or out of network solution — all at a fraction of the cost of in-band-only solutions.
What is SRENA?

SRENA, Secure Remote Emergency Network Administration, is a standard for new class of products specifically designed to monitor and manage servers and intelligent devices both locally (through TCP/IP) and remotely out of network, also known as out of band management (OBM). If your network were a building SRENA would be the building code which requires your building (network) to have a smoke detector, fire alarm, fire-escape and some fire prevention and fire fighting tools.

OutPost Sentinel is the leader in SRENA technology and has designed the first suite of products exclusively tailored to provide secure remote emergency network access through a comprehensive set of administration, management and diagnostic tools.

Problem-Solving with SRENA

People who have just been introduced to the concept of out-of-band management by reading this document may be wondering what kind of practical situations would benefit from console management. Having access to all the console ports without the need to switch cables or to move to another workstation is great, but problems that completely disable the network cannot rely solely on in-band management tools.

Here are some scenarios where having a SRENA solution is the difference between being able to diagnose and solve a problem quickly and having to go onsite or be out of operation for a long time.

**A server crashed and the Data Center is unattended.**

One of the servers in the cluster running the e-commerce application crashes and sends a panic message to the console port.

Life Sign Sentinel (LSS) or the clustering software monitors the alarms generated by the SRENA and sends periodic pings to the servers in the cluster. When it detects that one of the servers is not responding properly, it pages you and sends an email with the panic message captured by the unit.

You connect to the ENS-8 SRENA system over the Internet using the link sent to you in the e-mail. You review the console messages prior to the OS panic/crash and find that there is no specific event causing it. It was probably an OS crash caused by some software error. You send a reboot sequence to the console port; the server reboots and resumes operation. In this example, the SRENA solution enabled you to set trigger events and generate alarms to warn you about the problem and then allowed you to locate the troubled device with pager message or link to the ENS8 and the failed device. The ENS8 then enabled you to remotely reboot a server to restore operation.
**Router is malfunctioning and the site is down.**

Someone at your POS (Point of Sale) retail outlet reports that the entire site is down. In-band management tools such as HP Open View or telnet are useless because the remote network is inaccessible. Using a modem and a phone line, you remotely connect to the SRENA unit at the affected site and look for the problem. LSS tells you the entire site is down, and that there is something wrong with one of the backbone routers.

By using the link provided by LSS to the failed device, you quickly find the LAN interface that is not working. You temporarily reconfigure other routers so that the traffic takes an alternate path, restoring the site’s connectivity. Or you gain root access to the router through your SRENA unit and reconfigure the affected router. In this example, the ENS-8 technology allowed you to access the equipment at the remote location even when the site had lost its network connection.
SRENA Required Features

The following features make up a comprehensive SRENA solution

<table>
<thead>
<tr>
<th>Feature</th>
<th>ENS-8</th>
<th>CCC-16/32</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SECURITY</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSH v3+</td>
<td>X</td>
<td>X</td>
<td>Must include the latest in security</td>
</tr>
<tr>
<td>IP Packet Filtering</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Remote Shell</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>RADIUS</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Remote Shell</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Dial Back</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>PAP &amp; CHAP</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Security Global Repository</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Remote Dial-In</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>In Rack Login Screen</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Control at the Rack</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td><strong>Networking &amp; Local Management</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Telnet</td>
<td>X</td>
<td>X</td>
<td>Terminal</td>
</tr>
<tr>
<td>Reverse Telnet</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>RSH Routing</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>KVM Connections</td>
<td>X</td>
<td>X</td>
<td>Local KVM Support</td>
</tr>
<tr>
<td>10Base-T &amp; 100 Base-T</td>
<td>X</td>
<td>X</td>
<td>10Base-T &amp; 100 Base-T</td>
</tr>
<tr>
<td>10/100 Ethernet (2nd Port)</td>
<td>NA</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>SNMP</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>NAT</td>
<td>X</td>
<td>X</td>
<td>High Speed Private Network routing via 2nd WAN Ethernet or USB</td>
</tr>
<tr>
<td>PPP</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>TFTP</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td><strong>Remote Console Management</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dial Up Modem Support</td>
<td>X</td>
<td>X</td>
<td>Supports all major modems</td>
</tr>
<tr>
<td>ADSL</td>
<td>X</td>
<td>X</td>
<td>Provides DSL connectivity and 1.5 Megabyte downloads</td>
</tr>
<tr>
<td>DHCP Client</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>PPTP</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td><strong>Emergency OBM Access</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dedicated Console</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>KVM Access</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Network access</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Max Ports</td>
<td>8</td>
<td>32</td>
<td></td>
</tr>
<tr>
<td>Feature</td>
<td>ENS-8</td>
<td>CCC-16/32</td>
<td></td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------</td>
<td>-----------</td>
<td></td>
</tr>
<tr>
<td><strong>Management Tools</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tab Commands</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Graphical Configuration</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Console Syslog</td>
<td>X</td>
<td>X</td>
<td>System Event Log</td>
</tr>
<tr>
<td>AUDIT Trail &amp; Large Port Buffering</td>
<td>X</td>
<td>X</td>
<td>User-configurable buffer up to 256K per port</td>
</tr>
<tr>
<td><strong>Heart Beat Monitoring</strong></td>
<td></td>
<td></td>
<td>LSS – Life Signs Software</td>
</tr>
<tr>
<td><strong>E-mail Notification</strong></td>
<td></td>
<td></td>
<td>LSS – Life Signs Software</td>
</tr>
<tr>
<td><strong>Paging Notification</strong></td>
<td></td>
<td></td>
<td>LSS – Life Signs Software</td>
</tr>
<tr>
<td>Windows Ctrl</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td><strong>Graphical Control</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stored Configuration</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Port Numbering</td>
<td>X</td>
<td>X</td>
<td>Port Commander</td>
</tr>
<tr>
<td>Port Naming</td>
<td>X</td>
<td>X</td>
<td>Port Commander</td>
</tr>
<tr>
<td>Device Locator</td>
<td>X</td>
<td>X</td>
<td>Port Commander</td>
</tr>
<tr>
<td>Flash Upgrade</td>
<td>X</td>
<td>X</td>
<td>Secure in field upgrades</td>
</tr>
<tr>
<td><strong>Database Authentication</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Headless NT</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td><strong>Accessories</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Redundant Power supply</td>
<td>NA</td>
<td>X</td>
<td>* Optional</td>
</tr>
<tr>
<td>DC Power Supply</td>
<td>NA</td>
<td>X</td>
<td>* Optional</td>
</tr>
<tr>
<td>DB –9 Cable connection</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>RJ-45 Cable Connection</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>DB-25 Cable Connection</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Manages Power</td>
<td>X</td>
<td>X</td>
<td>Intelligent Power Supply Options available</td>
</tr>
<tr>
<td>Rack Usage</td>
<td>NA</td>
<td>1U</td>
<td></td>
</tr>
</tbody>
</table>
Selecting Your SRENA Solution

Most remote console management servers are actually modified terminal servers designed in the pre-Internet era, to physically connect terminals to UNIX servers. They are generally hardware-intensive products with complex designs and unnecessary overhead. They have poor security features; slower connect speeds, and inadequate administration and management tools. They are generally difficult to use and provide little flexibility.

Total Cost of Ownership Consideration

The network management market is evolving fast. We need to take great care in selecting products. Total Cost of Ownership (TCO) is vital in making technology-purchasing decisions. SRENA has a tremendous value proposition and often a 1-day payback. However, even such an obvious decision merits additional investigation to make sure you have the right product and the right tools to get the best results from your environment and the fully utilize your technical resources. The differences between a state-of-the-art SRENA product and an older adapted terminal server product are tremendous. Below, some information has been provided to help you make a more educated decision for your remote network access.

- When selecting a remote console management solution, make sure it has the functionality you require, and that it is also secure and reliable.

- For larger installations, the unit should integrate well with your rack and cable management systems. Most data centers today use Category 5 cabling and patch panels. Ideally, the unit would provide serial connections and cabling connections, which plug directly into the console ports you wish to manage.

- Security is Key – Multiple levels of security and a vendor committed to provide the latest and best technologies available are essential. Critical components include 128-bit encryption, SSHV3+, IP Packet Filtering, Dial-back capable and supporting centralized authentication.

- The power supply and power management should be integrated into the box. In a Microsoft NT environment your solution may also require additional power management capabilities, which include intelligent power supplies. Cycle power to specified individual devices.

- In a Sun Solaris environment you may wish to incorporate a solution to address the Sun "break" issue. You want to make sure the console server is "break-safe" (does not send unintentional break signals) and is capable of sending intentional breaks (using RFC2217).

- It should be flexible, and support direct telnet, reverse telnet,
SSH (v2 and v3), multiple port addressing methods (IP address, TCP port number, or manual selection in a menu). It should allow local or server-based authentication.

- It should allow you to proactively monitor and manage your networks and to set customizable event triggers and provide emergency notification about potential problems.

- It should allow you to proactively monitor and manage your networks and to set customizable event triggers and provide emergency notification about potential problems.

- It should allow you to proactively monitor and manage your networks and to set customizable event triggers and provide emergency notification about potential problems.

- It should allow more than a megabyte of port buffering of console messages even when nobody is connected or logging messages. It also needs to provide trouble shooting tools including port replay and keyword searches.

Port Buffering allows you to review what happened before failure occurred.
OutPost Sentinel Solutions

The Emergency Network Specialist (ENS-8)

Improving Productivity while Reducing Costs—The ENS-8 from OutPost Sentinel (OPS)

Businesses increasingly rely on computers and when the network is down business is down. OutPost Sentinel’s ENS-8 is a Secure Remote Emergency Network Administration (SRENA) solution designed for improving network uptime and business productivity. The Emergency Network Specialist (ENS-8) gives your business or branch offices access to a dedicated network specialist, monitoring your network equipment twenty-four by seven.

- Monitors your network around the clock and immediately notifies you of potential computer-related issues.
- Provides remote network access even when the network is down.
- Reduces guesswork by identifying the problem device and directing you to it.
- Provides management of multiple networks and locations from single access point.
- Ensures secure access with full SSHv3 128-bit encryption, dial-back, and IP packet filtering.
- Maintains audit trail for faster troubleshooting.

The ENS-8 is ideal for smaller network installations with eight mission critical devices per location.

For very large rack solutions, the 1U rack Cyber Command Center (CCC) provides 16- or 32-port unit solutions.
Port Commander

The ENS-8 Port Commander allows easy configuration and administration of ports and devices. OutPost Sentinel’s powerful but easy-to-use scripting and tab completion commands enable you to quickly set up the unit and to easily run pre-set tasks. A web browser interface is very nice and enhances ease of use greatly. However, be careful that your web browser does not compromise the security of your network and that it provides secure SSL http access.

- Port Commander enhances manageability with port numbering and device naming.
- Troubleshooting has never been easier with non-connect port buffering providing a complete audit history featuring actual port replay and a keyword search.
- Unit status information and device statistics provide an instant view of activities and hardware for quick repairs.
- Easily save and restore settings and e-mail configurations by using the EAdmin features.
- Use Port Commander to configure devices and enable “in-rack” flash upgrades and customization.
Secure Sentinel

OutPost Sentinel’s Secure Sentinel ensures secure management of network devices.

- Secure Shell (SSHv3) protocol with 128 bit encryption
- NAT firewall services
- RSH remote shell administration
- User authentication—local, remote and native
- IP packet filtering
- Dial-back communications
- Authorizations and permissions
- Custom key lengths to make it virtually impossible to decipher data packets.

Secure Sentinel defines Security Levels
Life Signs Sentinel (LSS)

OutPost Sentinel’s Life Signs Sentinel (LSS) provides perpetual monitoring of critical devices. When changes are detected within selected network equipment, LSS event triggers will notify you using a built-in audio alarm, or by pager or e-mail.

- Constant pulse and heart beat monitoring of all critical network devices
- Immediate notification including: audio alarm, pager calls and e-mail messaging
- EAdmin E-mail Utilities allow you to e-mail yourself system and event logs and configurations, as well as emergency e-mail notifications for specified events

Configuring System Monitoring
Power Control

The ENS features external power management tools allowing managed devices to be power recycled at the click of a mouse. With this option, monitored devices will be powered on and off with no onsite human intervention required. The ENS provides tools to easily manage other industry power strips should an enterprise have a power strip standard. The tip command can be used to control such user-defined units.

Cycle Power

*Cycling power on power port 1*
Summary

**Businesses can’t afford to be down.** Having your network up to code is the best insurance to provide safe and secure emergency network management. Selecting the right SRENA solution means selecting the best solution with the best Total Cost of Ownership for your network.

**Preventing a single network crash or eliminating an onsite visit will often more than pay for a SRENA solution.** However, selecting the right solution means being able to further reduce your IT budget requiring fewer IT resources while improving IT coverage and up time. Perpetually monitor all network devices every minute of every day and gaining secure access to all network devices from anywhere even if the network were to fail.

**Reduce Your IT Costs** – eliminate response time and unnecessary onsite visits while maximizing the utilization of your scarce technical resources to effectively and efficiently monitor and manage more networks and more types of devices than previously believed possible.

**Maximize IT Coverage** – 24/7 continual monitoring of all devices. Gain direct access and control to all devices even if the network fails. Get the right IT expert to the potential problem area instantly from anywhere. Manage all your various network devices with one safe, simple and secure solution.

**Eliminate Down Time** – set emergency event triggers notifications and alarms. Take the guesswork out and identify problem areas with monitoring and notification providing device names and a direct link to the device and error messages.

Installing smoke detectors fire escapes and fire prevention and fire-fighting equipment for your networks providing safe and secure emergency access and management of your entire network will maximize business potential and profits.

---

**Having a Specialist on your Networks gets**

**The Right Expert,**

**To the Right Location,**

**Right Now!**
How can we help you?

*OutPost Sentinel is passionate about helping you*
*Improve your business and the services you provide.*

**OutPost Sentinel, LLC**
PO Box 2153
Alpharetta, GA 30023
(678) 867-9957
www.outpostsentinel.com

**ANY TIME! ANY WHERE!**