WHITE PAPER

# UTILIZING SITEBOSS NETWORKING TOOLS

How Telecom Operators can use Telecom Site Automation Network Features to Improve Network Resilience and Efficiency

Asentria®

# Table of **Contents**

# Summary

There are a wide variety of networking challenges facing telecom network operators at their remote telecom sites. More and more systems (eg. Generators, HVAC, DC Rectifiers) at remote telecom sites have network based “smart” interfaces that could provide valuable data to help manage the network. The Asentria SiteBoss has a wide variety of both hardware and software based network functions that can help in the management of these sites.

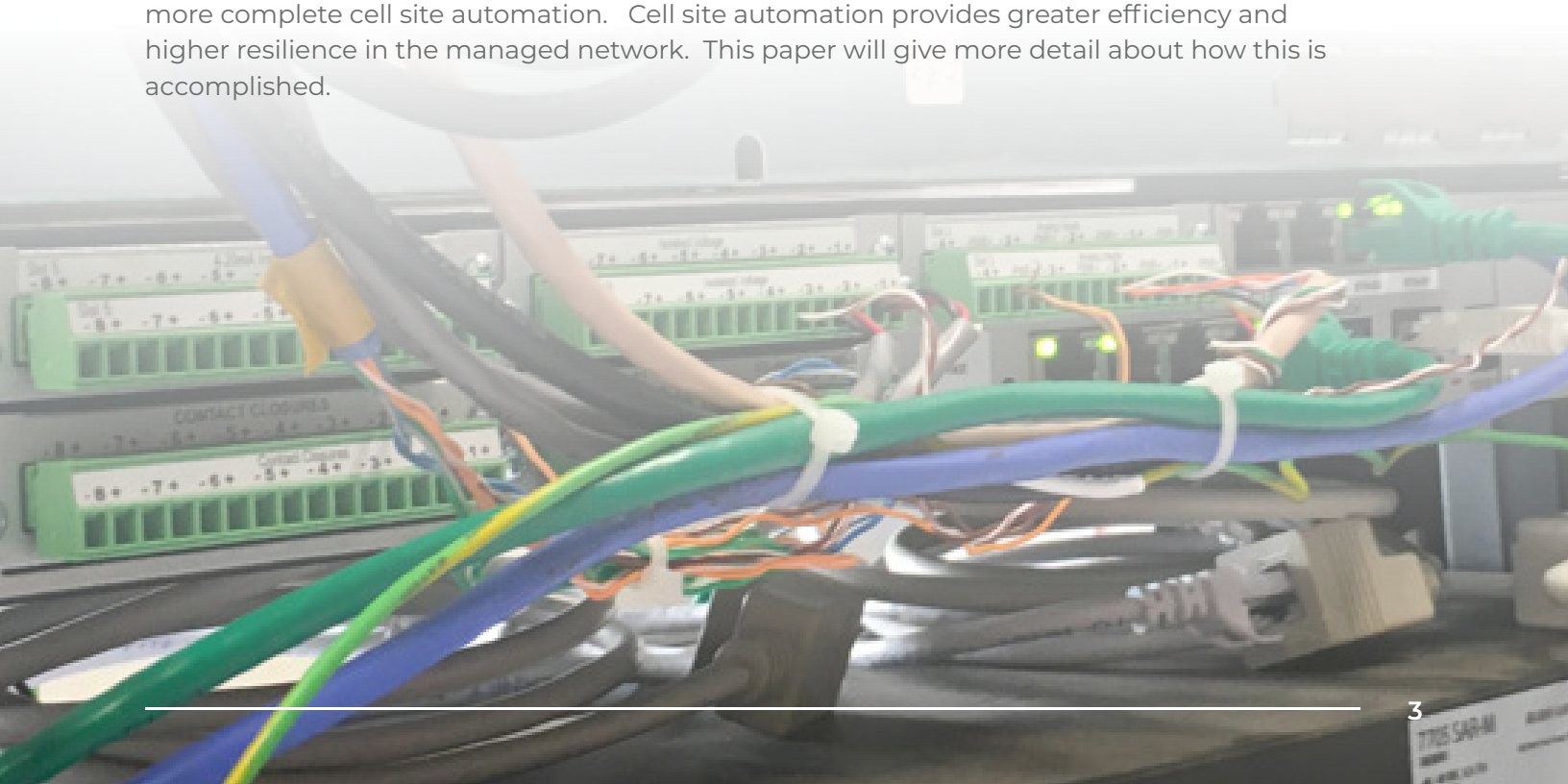
## Hardware

1. **“Northbound”** – The SiteBoss unit can include specific hardware for sending data northbound from the site. RJ45 Ethernet ports, SFP fiber connections, or a wide range of wireless modems.
2. **“Southbound”** – The SiteBoss can include specific hardware for communicating to devices southbound at the site. RJ45 Ethernet ports, RJ485/232 serial connections, and other various I/O connection points.

## Software

1. **Routing/Bridging** – Enables the SiteBoss to allow access to and from devices at the remote site.
2. **Security** – Security features to determine who can access underlying systems at a site.
3. **Protocol Conversions** – Converting either protocols from devices at the site, or sending specific protocols “northbound” from a site.

Using the SiteBoss an operator can “flatten” the data from underlying sub-systems, and enable more complete cell site automation. Cell site automation provides greater efficiency and higher resilience in the managed network. This paper will give more detail about how this is accomplished.



# Site Issues

## More network devices

More and more equipment at a cell site is becoming network enabled. DC power plant controllers, generator controllers, HVAC systems, UPS's, IP cameras, tower light controllers, environmental monitoring systems, and many other devices were not traditionally on the network. All of this equipment can provide valuable operational data and allow for remote troubleshooting and control when connected to an operator's network. Just as all this valuable data is coming online, IP addresses on customer networks are becoming more scarce. New technologies like 5G and expansions of existing LTE technologies are gobbling up IP address for customer traffic, making it difficult to justify using IPs for management and monitoring. This problem is especially prevalent in IPv4 networks. Even if more physical network ports could be added to site routers and switches there are simply not enough IP addresses on the network to connect everything an operator would want.

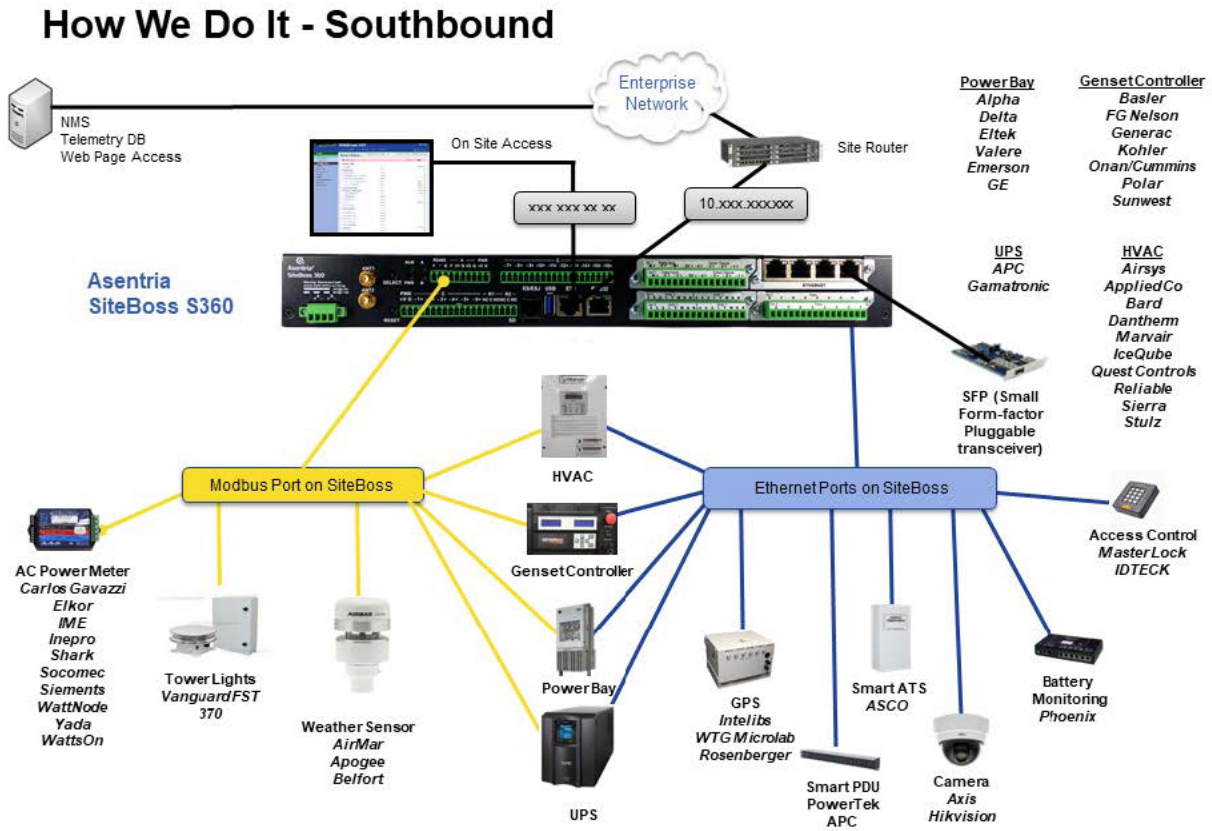
## Other network issues

Adding enough physical ports to cell site routers or switches can be expensive even if there are enough IP address available. There are other specialized issues to cell sites where specialized hardware can be helpful. Particularly for things like -48V powered POE injectors that are specialized for the telecom environment, or when a traditional RJ45 copper Ethernet connection to a cell site router is not an option. A SiteBoss can also act as the "approved" secure device for use on the network, keeping all the underlying "smart" devices on a separate network. This can reduce costs related to doing security audits on every smart controller that might be used on a network.

# The SiteBoss Solution

## "Northbound" and "Southbound" Interface

Asentria broadly divides networking issues into two categories. We refer to these as "Northbound" and "Southbound" traffic. With the SiteBoss itself as our point of reference, northbound data and connections are to anything on the main network that is not at the cell site. A northbound connection would be from the SiteBoss to the cell site router for example. This is because that connection provides access outside the site. This connection routes traffic to services outside the site such as NMS systems aggregating data from multiple sites. Southbound connections are to devices that sit "below" the SiteBoss at the site on the SiteBoss management subnet (eg. Generator controllers, IP cameras).




Understanding this distinction is important to understanding the rest of this document. Broadly speaking the SiteBoss networking hardware and software tools solve northbound and southbound networking problem at a site.

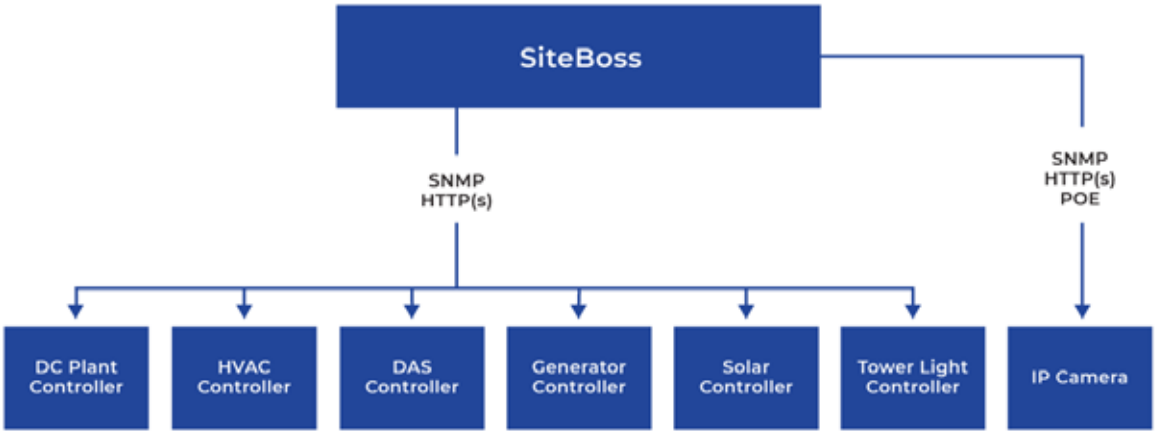
# SiteBoss Tools - Hardware Solutions

## Ethernet Expansion Cards

SiteBoss base units that support Ethernet expansion cards can easily scale the number of RJ45 Ethernet ports available on the site for management. The most basic form is the four port Ethernet expansion card. Regardless of the number of ports installed, all of the auxiliary Ethernet ports are on a single logical switch. Ethernet ports scale in blocks of four for non-POE, or two at time for POE. This allows an end user to only use the number of ports needed. This scalability keeps costs down and allows the local network to scale with the number of smart devices on the site.

Once an Ethernet expansion card is added to a base SiteBoss unit a local management network can be created to provide a network for all smart devices on site. This is the primary method southbound integration is facilitated for networked devices. These southbound devices can then all be accessed directly from the northbound network via routing (see the routing section of this document). With the management subnet the SiteBoss can also make a variety of queries or receive data from these devices to create alarms and telemetry from connected devices for analytics.

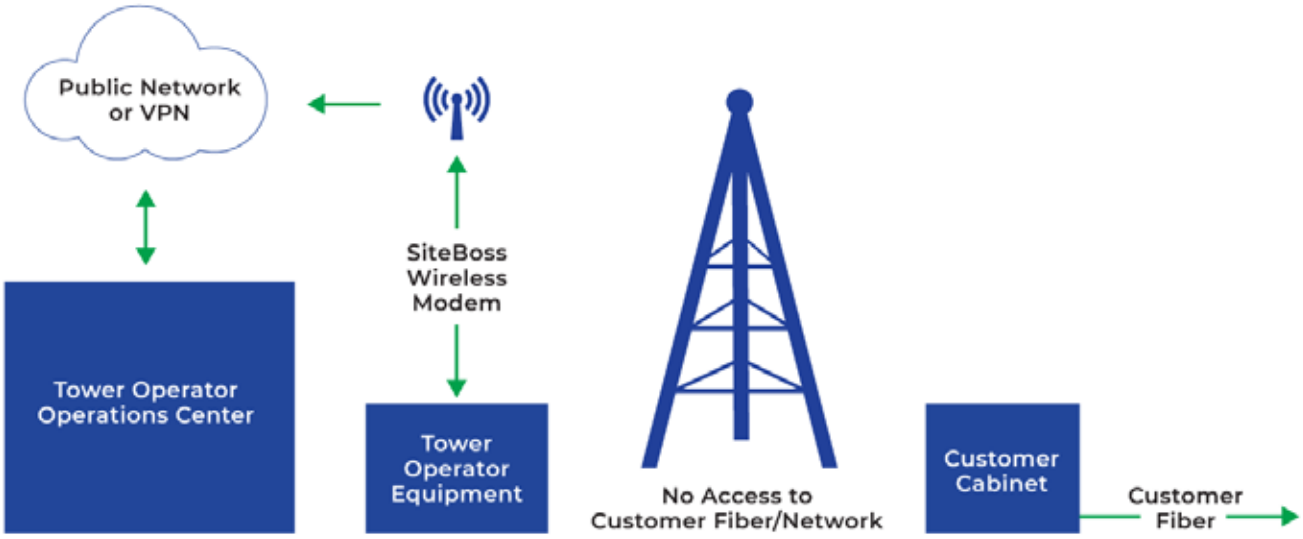
The SiteBoss auxiliary Ethernet cards can be setup with a DHCP server or used with statically addressed devices (or both at the same time as desired). This can serve IP addresses to most non-traffic carrying devices on site. The SiteBoss can be setup with port forwarding to access the web pages or SNMP interfaces of connected devices from the main network. If port forwarding is not allowed on the user network a more advanced feature can be setup like interface forwarding to allow access to these devices. All of these solutions only consume one IP address on the primary network. This functionality is accessed with the relatively low cost of SiteBoss hardware, compared to the cost of IP address and cell site router or switch capacity. Plus all the other integration advantages of the SiteBoss are gained.




The 4 Port Ethernet expansion card is the most widely used hardware tool and the primary “Southbound” interface for all Asentria networking solutions. This card enables many of site based solutions and is very important to any modern Asentria cell site automation solution.

## Using Cell Modems, SFP, and alternate interfaces

In the most common application of the SiteBoss hardware, the networking configuration is a standard RJ45 copper Ethernet connection from the primary Ethernet interface (ETH1 typically) to a northbound cell site router or switch. Then 4 port Ethernet cards are used to connect to all the southbound network devices. Access is provided to southbound devices from the copper northbound interface. However in some network or site type configurations there is no cell site router or switch onsite to make a copper northbound connection. So an alternate solution is needed. On a SiteBoss these alternate northbound connections are typically cell modems or SFP (direct fiber) interfaces.



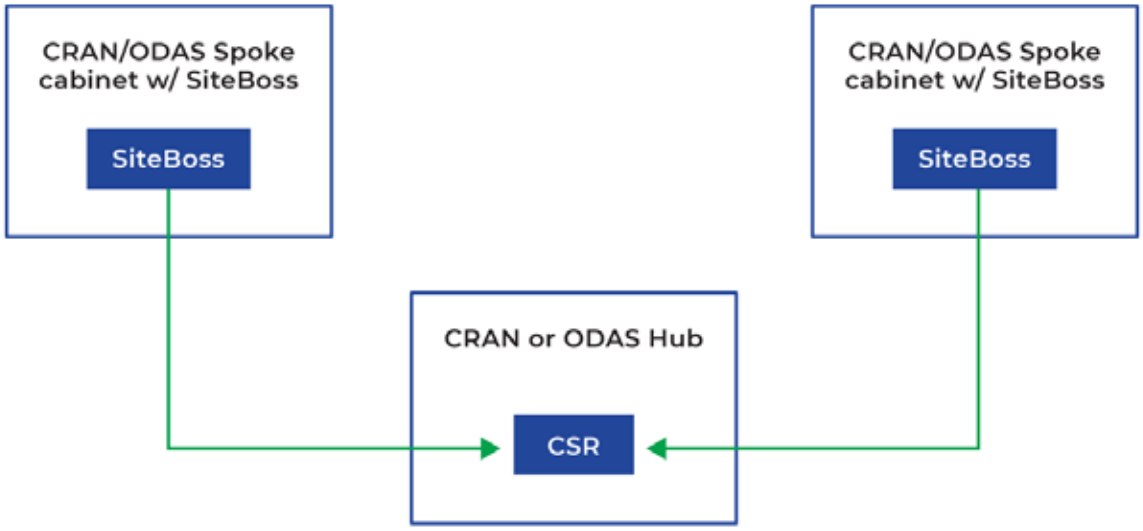

Using wireless modems as the primary method of access is particularly common with tower leasing companies. These types of customers often have infrastructure that needs to be monitored and controlled but do not have a widespread network like a mobile network operator does to connect to this infrastructure. The site infrastructure could include things like backup generators onsite, or AC power meters that provide billing data for lessees. As tower companies are traditionally not network operators there is not a usually a fiber or copper network they have access to for getting this data back to a central location, so a wireless modem is often used.

There are a variety of types and speeds of modems to meet many customer applications. For example full speed LTE modems can be used for access to SiteBoss web interfaces, or a CAT M or other IOT type modem can be used to limit data usage and lower costs if less data is needed. Additionally specialized dual SIM modems can be used for cases where redundant access is critical if one network fails.

All cell modems can route their traffic through built in VPN tools on the SiteBoss for additional security. The SiteBoss can be configured with a VPN client or as a VPN server (Open VPN for both) depending on the application.

## Using Cell Modems, SFP, and alternate interfaces (continued.)

Monitoring and control is needed in a cabinet but there is no cell site router or switch. A cell modem could be used in these sites, but if fiber pairs are available, fiber is more cost effective to connect the SiteBoss to network, as cell modems have a monthly cost of a data connection and some additional complexity to set up. If fiber is present, the operator likely already has a network available. In most SiteBoss systems the optional SFP northbound interface can be installed as a slot card option. Once the SFP card is installed it becomes a discrete network interface that functions like any other of the network interfaces.




## Other Cell Modem Applications

In some cases even if a traditional copper northbound interface or fiber connection is made a cell modem can still be used as a backup interface. All types of Asentria network hardware have discrete network interfaces so can be used concurrently. So if a particular site with a copper or fiber connection to a network is especially critical, a cell modem can be used as an alternate “out-of-band” path to the site if the main network connection is lost. The SiteBoss can be set to automatically fail over to a wireless interface in the case of lost primary connection. This cell modem application combined with Asentria cell site automation can be a powerful tool for site recovery.

## POE Cards and other Specialized Hardware

The SiteBoss offers additional specialized and legacy network interfaces for specialized northbound and southbound applications.

Certain SiteBoss models support a -48V POE injector card. This card functions just like a standard 4 port Ethernet expansion card, and can work in conjunction with 4 port Ethernet expansion cards, but it provides POE for equipment. Support for IP cameras is the most common use of this card, but the SiteBoss POE card could support any device that can be powered by POE. AC powered POE injectors and switches are relatively common and widely available, however in a -48V DC environment there are very few options. Having the POE card operate at the native -48V power at a telecom site lowers the complexity of installs, and allows the POE device to get its power from the same backed-up DC power system as all the other equipment. This prevents the loss of camera (or other POE device) visibility during a power outage. One of the most critical times to have visibility. Using the onboard POE switch within the SiteBoss also allows cameras to be on the same management subnet as all other devices on the site, and allows access to the SiteBoss's IP camera features and alarming tools.

Older models of SiteBoss also support some legacy connection types such as POTS and DSL modems. These are rarely used in any new deployments but do exist in the Asentria catalog for certain hardware configurations.

# SiteBoss Tools - Software Solutions

## Linux OS

The SiteBoss is a Linux based device. Linux provides an extremely powerful set of networking tools to a SiteBoss user. It also allows Asentria to quickly add new tools to the software when needed. The Linux system makes the SiteBoss a powerful troubleshooting tool once installed on the site. It can be used to troubleshoot other networking issues since it has access to many standard Linux/Unix networking commands.

Combining these software tools with the hardware tools described in the previous section significantly increases the flexibility of the SiteBoss solution. This section will outline a variety of the software tools the SiteBoss offers.

### Routing Features

One category of features that enable many applications is the SiteBoss's set of routing features. Routing features at their most basic level allow access from northbound of the unit to southbound devices. Depending on the applications needed these can be fairly simple features like providing access to a connected device's web UI, or more advanced routing of queries and other data. The set of features below are all tools that can be used to solve network related problems when implementing the SiteBoss. They do not have a single application but provide many functions that can be used to accomplish the goal of connecting more devices at a cell site in a useful way.

### Port Forwarding

Port forwarding is one of the most common routing methods used by SiteBoss users. This allows simple access for things like the web UI of connected device. The user defines a source port and source interface, and a corresponding destination port and interface. Typically the source interface is one of the northbound interfaces and source port is an open port unused port say 8009. The most common destination then would be an IP address and web port of a connected device, say a DC plant controller. Once configured this would allow a customer to enter the main IP address of the northbound interface followed by the port, opening the web page for the DC plant. Something like http://10.0.0.1:8009 . Where 10.0.0.1 is the IP address of the main northbound interface (ETH1) and 8009 is the selected unused port. Entering 10.0.0.1:8009 would then open a connection to port 80 on the DC plant giving access to the devices web UI. Port forwarding allows the use of single IP on the main network while giving web (or other types of) access to multiple devices.


## Static Routes

For some applications a specialized static route needs to be defined. For example if traffic from a specific device always needs to go to a certain router or subnet. Static routes are often useful when a SiteBoss has multiple northbound interfaces like when using a wireless modem as a backup.

## Interface Forwarding

Interface forwarding sets up rules for one interface to forward traffic from certain subnets to another interface automatically. Interface forwarding can be used for example as a method of accessing devices connected to the Ethernet expansion interface from a customer's main network. In some networks this method is preferred to port forwarding, but is less common because it is more complex to implement.

## Bridging

The Ethernet expansion cards network interface and one of the northbound interfaces can be put into a bridged configuration making them into a single logical interface. Running the unit in this configuration provides yet another method to route traffic from the northbound interface to the southbound devices and vice versa. It is another method to use when others are not as effective.

## VLAN

The SiteBoss Eth1 or SFP interfaces support a VLAN configuration and support VLAN tagging for networks where that is required.

## Network Security Features

The following sets of features are some security features of the SiteBoss that relate specifically to network traffic. These features do not fully protect a unit on their own. But when used in conjunction with other security features, and a properly designed network, they can provide an additional layer of protection. These features should always be used in conjunction with strong user account passwords or secure authentication methods supported in the SiteBoss like RADIUS and TACACS+. Those standard protocols are supported in the SiteBoss, but are beyond the scope of this document.

### IP Blacklist

If enabled, the IP blacklist feature counts the number of times an IP address and user try to authenticate. If they fail more than a set number of times (say 10). That IP address is black listed and prevented from logging on even with the correct username and password. The black list has to be cleared to allow a blocked IP address to regain access.

This feature protects against brute force attacks where an attacker tries multiple passwords until the correct one is found. This feature is especially critical when using a wireless modem with a public IP and not through a VPN, but it is recommended in all deployments.

### IP Tables and Routing Restrictions

The SiteBoss supports IP table type routing restrictions. This can be used to ensure that only traffic from certain subnets is allowed on the SiteBoss, and that the SiteBoss can only communicate with certain parts of large networks. This can be a useful method to cause traffic from outside sources and sections of network where it should not be coming from to be automatically dropped from the SiteBoss.

### Enabling only protocols you need

The SiteBoss can be used for many different applications and supports a wide variety of protocols with varying degrees of security. Unsecure protocols such as Telnet, HTTP, and FTP are left in place to support certain legacy applications and customers, but these protocols can, and usually are, disabled if they are not needed. Only protocols that are in use should be enabled. From the SiteBoss web UI with administrative rights a user can disable all services at an interface by interface level. This should be done for all SiteBoss deployments.

## Protocol Support

The SiteBoss supports a variety of protocols for a number of applications. Detailed descriptions of each are beyond the scope of this document. These protocols are used to integrate with connected southbound devices, most NMS/OSS software, as well as data analytics tools. Protocols supported include an extensive support for SNMP. SNMP is one the most common protocols in the telecom world. Asentria has a very mature both northbound and southbound SNMP interface. Devices connected to the 4 port Ethernet card on the management subnet can be queried or route SNMP to the northbound interface. The SiteBoss itself can be managed by SNMP and provide alarming data via this method.

In addition to SNMP the SiteBoss also supports DNP3 and a REST API. DNP3 is useful for some specialized environments and customer types. The Rest API is very useful, especially for more modern networks or to interface with many new types of software.

The Siteboss has both and FTP server and FTP client. This can be used to update the firmware of the siteboss, collect images from IP cameras, transfer logs and other data transfer to and from the SiteBoss. The SiteBoss also supports basic connections methods for users like HTTP, HTTPS, and SSH.

# Why use all the networking tools?

Why use all the Asentria SiteBoss tools? Ultimately the goal is to provide easier and more complete access to southbound devices. Additionally using the SiteBoss's networking tools can reduce overall software integration costs when bringing southbound devices online. This issue is often overlooked by network operators, but poses a major barrier to using more smart devices. Most of these devices use standardized communication protocols like SNMP or HTTP, but with enough variation in the implementation of those protocols that there is not a good method to easily integrate them into existing operational software.

In the case where there is an existing OSS/NMS software, integrating a new SNMP device can be quite costly. For some systems there is a significant one time cost to add the module/agent for a new DC plant, generator, or other devices. For other OSS/NMS systems there is simply the cost to pay internal staff to do all the work to integrate devices into the NMS/OSS and build workflows etc. When you start to look at the **number of manufacturers and number of generations of equipment** in a network, the integration cost of bringing all the devices of one type (eg. Generator controllers) can be prohibitive to a point where anything beyond the most basic implementation is ever attempted. For example if you have three manufacturers of generators, and three generations of generators from each of those manufacturers, each with different methods of being controlled, that could involve paying for software integration to nine devices into your NMS/OSS. Many older varieties might not have any networkable interface, requiring direct sensor monitoring (eg. Fuel level sensors) or serial interfaces to query data. **When using the SiteBoss you can instead do the integration to your NMS one time for the SiteBoss.** Once integrated the cost to add a new type of equipment to the network is only the relatively low cost of a SiteBoss unit split across all the devices on a site.

> ***"...easier and more complete access to southbound devices."***

Once software integration is done for the SiteBoss, the SiteBoss has a variety of methods to take data from other devices and translate that data into SiteBoss alarms and telemetry that would be recognized as SiteBoss data by the OSS/NMS or analytics system. For example, the SiteBoss can create virtual event sensors to translate data from any manufacturer of generator into a single standard alarm, piece of telemetry, or point that can be controlled. That data is the same regardless or the make, model, or generation of the equipment. This flattened data can be created for all kinds of systems at a site like DC plants, AC power monitors, environmental monitoring systems, HVAC systems, and many more. "Flattening" site data like this is an extremely powerful tool for enabling what consider true "cell site automation". That new operational data can then be used for analytics and control of functions at sites for further cost reductions in the future.

For networked devices this data is gathered most commonly by making SNMP queries, or receiving SNMP traps. In some cases other methods like Modbus TCP can be used. Future methods for REST API queries are being made. Once the data is acquired translating that data either directly to an alarm or to a virtual event sensor point that can alarm.

# Conclusion

Today's telecom operators are faced with operating networks that are ever more relied upon by society during emergency situations. Through a crisis, the expectation is that these networks will continue to operate regardless of conditions. At the same time, it is expected that costs for operating the network will always trend downwards. SiteBoss units provide a powerful tool to network operators and field technicians to provide both a wealth of information regarding conditions at a site, as well as the ability to remotely control functions at the site without a field visit.

Asentria helps create more resilient and cost-effective networks via telecom site automation. For more information on our products and the benefits of telecom site automation, visit our website at www.asentria.com.

**Asentria** is a 30-year-old company based in Seattle, Washington, and has multiple hardware deployments of 10,000 or greater sites in the largest mobile network operators worldwide.

# Locations

## Headquarters

1200 N 96 St
Seattle, WA 98103
USA

## EMEA Office

20A Copilului Street, Hala 2
012178 Bucharest
Romania

# Sales & Support

## Americas - Asia Pacific

**Customer Service:** +1-206-344-8800
**Sales:** +1-206-344-8800; sales@asentria.com
**Tech Support:** +1-206-344-8800; support@asentria.com

## Europe Middle East - Africa

**Sales & Tech Suppport:**
+40 37-499-1111
emeasales@asentria.com

# Follow Us