PANDUIT™ infrastructure for a connected world

smartzone™

Technical Reference 85-SZ

Published: **7/25/18**

Remote Site Management Using SmartZone

Applies to:	SmartZone DCIM Software
Objective:	Monitor and manage networked IT assets from multiple locations remotely.
Pre-Requisites:	• A 256k leased line providing site to site network connectivity • Maximum latency of no more than 250ms (milliseconds) • Less than .5% Packet Loss

Performing the Procedure

Traditionally, IT shops have had to deploy monitoring or management applications at each of the computing facilities that are responsible for day to day operations. These facilities may include data centers, campuses, remote offices, or even multiple retail locations. The issue is reviewing and compiling the data captured by these applications as well as managing IT assets in those remote locations. Add to that shrinking IT budgets and the capability of remote connectivity to each facility and the need for centralized management becomes very attractive. Using Panduit's SmartZone, networked IT assets can be tracked across the country or across the world. Alerts from a remote office in Dallas can be sent to a corporate office in Chicago. Management of remote sites can be done via the public Internet using Virtual Private Networks (VPN) or via private leased lines (recommended for security purposes).

Leveraging supported infrastructure, SmartZone can:

- Record unauthorized port Move/Add/Changes (MAC) or disconnects
- Monitor switch and active patch panel port utilization
- Receive Temperature, Humidity, and Airflow threshold violations
- Monitor Power utilization per POU or rack

- Observe asset tracking/movement
- Manage guided MAC's at remote facilities
- Provide alerts of un-authorized devices on the network

Assumptions

- Network connectivity is already in place for remote network access/management and currently meets the customer's needs before adding a SmartZone installation
- Network Administrator or whichever individual responsible for remote connectivity is familiar with access control lists, firewalls, and TCP/UDP transmission protocols

Accessibility

Since SmartZone is a web-enabled application, it can be accessed from any Internet-enabled workstation throughout the world*. The workstation would need the supported version of Java JRE installed and the IP address of the SmartZone server would need to be accessible via private IP address/DNS (see your Network Administrator for questions on remote network capability). Assuming appropriate access control lists have been defined, the SmartZone Server application would also be available at all facilities. Dependent on customer needs, SmartZone itself also offers access control in the form of username/password authentication as well as applicable user/group rights once logged in.

Note: Due to the nature of information about a customer's network that may be divulged by making a SmartZone Server accessible to the Internet, it is highly suggested that at no time should a customer expose the SmartZone Server to the Internet via NAT. A SmartZone Server should reside on a customer's management network and protected with appropriate user security, anti-virus, firewalls, and any other necessary security methods.

Network Connectivity

For SmartZone to be able to discover/monitor a remote site there first and foremost needs to be an established network connection. The suggestion is a private leased line, such as a managed T-1 to ensure monitoring of network consistency, latency, and availability. A minimum suggested connection would be nothing less than:

- **A 256k leased line providing site to site network connectivity**
- **maximum latency of no more than 250ms (milliseconds)**
- **less than .5% Packet Loss**

Some remote locations may be firewalled off with Access Control Lists (ACL's) disabling certain remote connectivity. In this event, please review Technical Reference 77 – Windows Server 2008

Firewall Exception Guide to ensure the ports necessary for network connectivity are opened from the SmartZone Server IP to the remote network to ensure SmartZone can discover devices.

Discovery

Discovery of remote locations in SmartZone are completed in the same manner as a location local to the SmartZone Server installation. Please ensure discovery schedules take into account any definable changes in available network throughput that could negatively affect performance to the remote network such as backups, site replication, batch settlements, file transfers, etc. **Note**: The time it takes for a remote network discovery to complete may be impacted by network congestion, latency, QoS rules, and number of devices being discovered or refreshed. Available network bandwidth is the largest determining factor with any issues found with remote network discovery. In the event of network events disturbing a discovery, an asset would be omitted from discovery rather than a discovery failing.

For devices to be discovered correctly, administrators need to ensure that SNMP UDP ports 161 and 162 are available through the remote network location, as well as Internet Control Message Protocol (ICMP).

Device Management

Devices such as Panduit Panel Managers (PM's), Power Outlet Units (POU's), and SmartZone Server can also be managed remotely. Access to these types of devices should be restricted to internal/management network traffic only and not exposed to the public Internet via NAT. To ensure accessibility over an internal private network, if an access control list is in place, administrators will need to allow traffic on the following ports **NOTE:** These devices can be managed directly via SmartZone or via the management IP of the device. Please see the Hardware User Guide of the individual device to review management options.

- PM's – Telnet, TCP port 23. Via Telnet, a PM can have any applicable field or setting changed to include name, location, IP address, SNMP Trap Server, community strings, RU offsets, etc

- POU's – HTTP, TCP port 80. Via HTTP, any supported POU (as defined in SmartZone Release Notes) may be managed via http by browsing to the IP address of the POU and entering appropriate login credentials. From the Web GUI, items such as POU name, IP, SNMP Trap Server, alerts, sensor names, community strings, and other items may be managed. Most of these settings may be manageable via SmartZone as well.

Remote Panduit PM/POU Firmware Upgrade

Administrators may also upgrade PM panels/POU's remotely (devices residing in a network defined by a different physical location such as another building, campus, retail location, or even country). A good rule of thumb is that if there are more than a handful of devices in a remote network, a TFTP server should be setup in the remote locations network. This is due to the size of the firmware file being

transferred (~5MB) as well as the nature of the TFTP protocol being dependent on acknowledgement packets. If there are any losses in connectivity or timeout, it may cause a retransmission of file download. If the determination is made that a remote upgrade is acceptable, administrators will need to ensure that UDP Port 69 is available between the centralized TFTP server and remote device IP addresses. PM's then can be upgraded via SmartZone or command line, and POU's can be upgraded via their web management GUI.

Floor View

Customers may wish to view capacity information of remote assets available via Floor View such as Panel Port Availability, Switch Port Availability, Power Consumption, etc. **Note:** During a device poll/refresh of this information, Microsoft Visio 2010 Professional may stop responding briefly as the data is pulled from the centralized SmartZone Server. **Centralized SmartZone Trap Server**

If one centralized SmartZone Server is managing all SNMP capable remote devices, administrators must to ensure that the remote devices SNMP Trap Server is set to the IP address of the centralized SmartZone Server so that all remote device events are collected by the SmartZone Server. (Please review the Discovery section above to ensure the centralized SmartZone server has the appropriate ports open to manage the remote devices). All SmartZone clients will be able to open the SmartZone Navigator console via HTTP by browsing to HTTP://SMARTZONEPIM_IP_ADDRESS:8080.