TECHNICAL BULLETIN

Flash Technology Technical Support
1.800.821.5825 Option 9
flashsupport@spx.com

Products:	Vanguard® Medium FTS 370d LED Tower Lighting System
	Vanguard® High FTS 270 Obstruction Light
	Vanguard® Red FTS 371 SMART with SNMP
	FTM 190 SNMP Monitoring
Effective Date:	January 10, 2020
Systems Affected:	FTM 190, SC 370, FTS 270, FTS 371 Smart SNMP
Issued By:	Shawn Claiborne, Product Manager

BEST PRACTICES FOR SELF-MONITORING FLASH TECHNOLOGY SMART ETHERNET EQUIPMENT

Flash Technology recommends that customers performing their own FAA compliance monitoring only connect their Vanguard® and FTM 190 Ethernet products to private internet connections and NOT the public internet. If end users monitor these products over the public internet, it can allow unauthorized access to the system's webpage or SNMP interface. By accessing the system's webpage with the default password, or sending an SNMP SET command, the configuration settings can be edited which may cause communication failures and/or possible compliance violations.

It is recommended that the default password always be changed once the system is installed. The password may be changed to any other password of 6 to 20 characters in length (with the exception of a few special characters). Please see the "Change Password" heading in the FTM 190 Manual page 21 or the FTS 370 Manual page 81 for instructions on how to change the password from the default. Please consult your in-house IT department to ensure you are securely monitoring your Flash Technology products, as general best practice IT security measures do apply.

The Flash Technology NOC monitors with closed private networks providing additional security against attacks via SNMP or Web interfaces. To reduce asset risk, we would be happy to assist with securely monitoring your assets. Monitoring service inquiries can be sent to FlashNOC@spx.com or by calling 1-800-821-5825.