BrightSign®

TECHNICAL NOTES

PCI Compliance for BrightSign Players

BrightSign, LLC. 16795 Lark Ave., Suite 200 Los Gatos, CA 95032
408-852-9263 | www.brightsign.biz

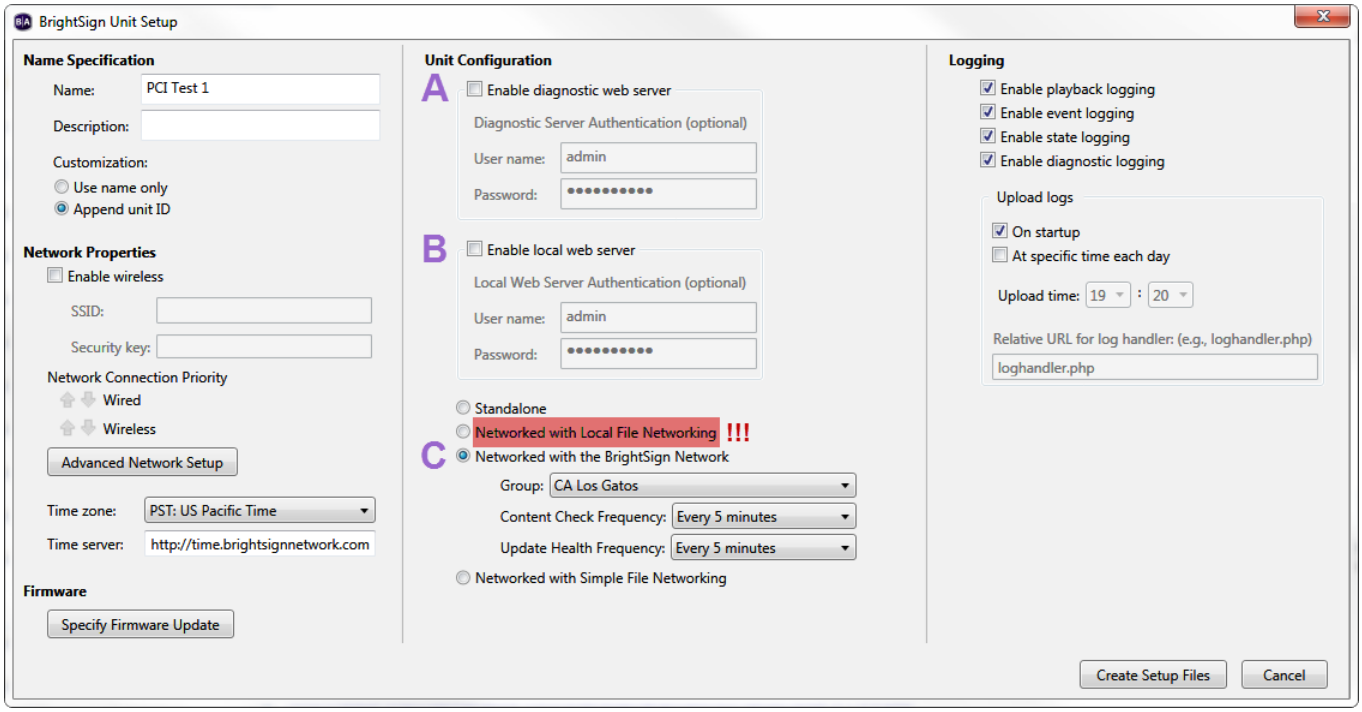
INTRODUCTION

The network settings of a BrightSign player are highly flexible and configurable. Some configurations are best for networks where security is of little importance, while other configurations give the player a significant amount of resilience to outside attacks. This tech note explains how to configure, test, and certify BrightSign players for use on a PCI-compliant network.

Player Configuration

The level of network security for a BrightSign player is determined during the Unit Setup process in BrightAuthor. The steps below describe how to set up a BrightSign player for maximum PCI compliance.

Note: *For a full description of all the options in the Unit Setup window, please see the BrightAuthor User Guide.*



A. **Disable the Diagnostic Web Server**: The Diagnostic Web Server responds to requests sent to the IP address of the player, allowing a user who meets the username and password requirements to retrieve information about the player and send system commands (e.g. reboot, enter recovery mode) to it.
B. **Disable the Local Web Server**: The Local Web Server responds to requests sent to the IP address of the player at port 8080, allowing a user to alter User Variables, which are numerical values within the presentation that extend the interactive capabilities of a player.
C. **Do not set up the player for Local File Networking**: Among the four methods for publishing content to a player, only Local File Networking facilitates problems with PCI compliance. A player configured to use Simple File Networking or the BrightSign Network will send content update requests to a remote server based on internal conditions and intervals that are specified during the setup process (as shown above): It will *not* respond to outside requests. A player with Local File Networking, on the other hand, is configured to respond to connection and content-update requests from local servers.

Other network settings that are configurable during the player setup process—such as proxy setup, wireless configuration, DHCP vs. manual IP—should not affect the PCI compliance of a player.

Steps for PCI Compliance Certification

1. Set up the device as outlined above.
2. Configure your local network for scanning as outlined by your compliance partner: Usually this involves opening up the player, which is located behind a firewall, to direct scanning from a remote IP address.
3. Use feedback received from the first scanning test to optimize network and player configuration: PCI compliance testing is often an iterative process and may take two to three scans to completely resolve any open security issues.

Note: *When deploying players in the field, make sure to maintain the same setup configuration used for testing PCI compliance. Changing the setup between test and deployment environments may result in players no longer being PCI compliant.*

Getting Additional Help with PCI Compliance

Contact BrightSign if you are encountering compliance issues with BrightSign players that are not related to the configuration settings outlined above. If a security issue is related to the hardware or system-software of the player, we would be happy to help resolve the problem.