BrightSign®

TECHNICAL NOTES

Player Security Statement

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. As a result, the integrity of a player is the direct result of the publishing and networking configuration settings specified during the player setup process. 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 settings that affect the security of the player and outlines the steps for creating a high level or basic level of network security.

Overview

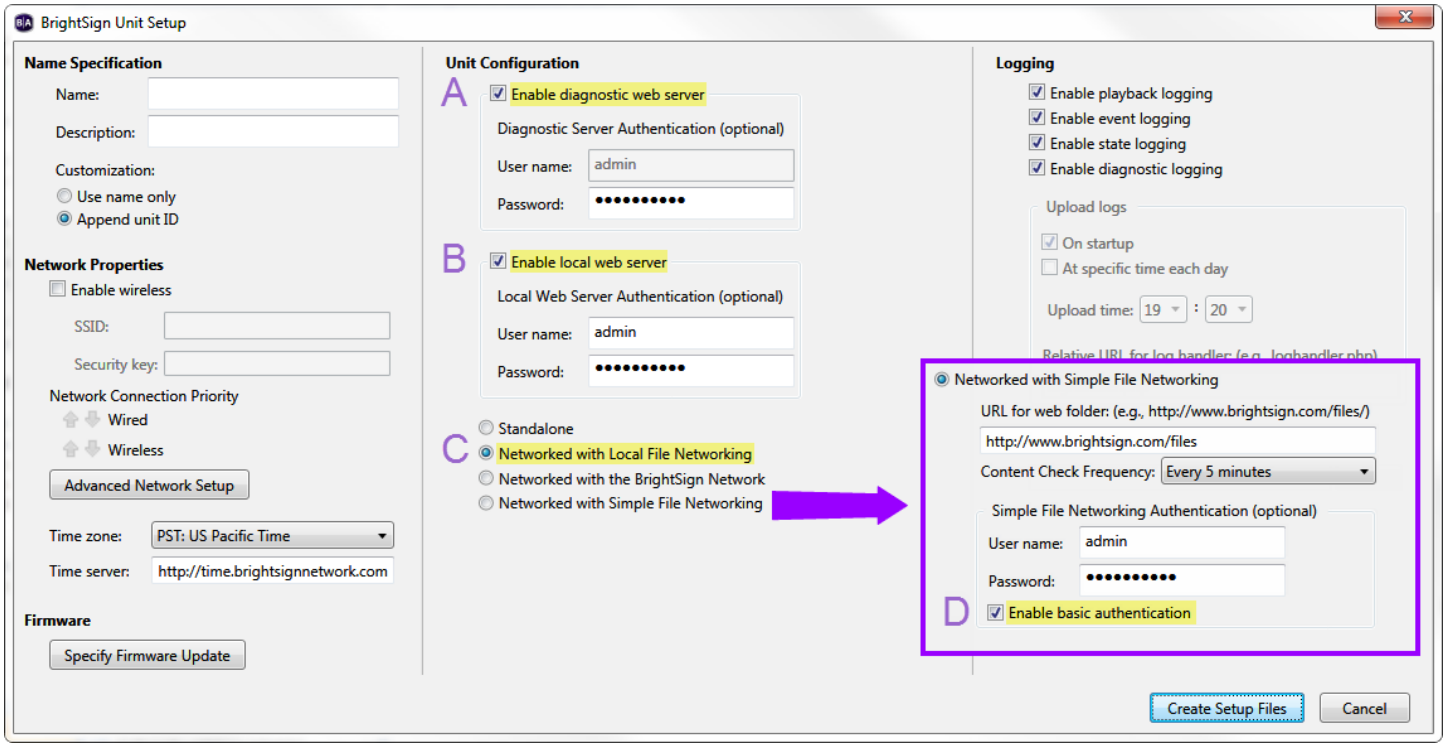
There are four optional features in the **BrightSign Unit Setup** window that affect the overall security of the player:

A. **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 to it (reboot, enter recovery mode, test video resolution, etc.).
B. **Local Web Server**: The Local Web Server responds to requests sent to the IP address of the player at port 8080. By default, this option also enables the device webpage at port 8008, which can optionally be disabled by navigating to **File > Presentation Properties > Variables**. The device webpage allows users on the local network to alter User Variables, which are numerical values within the presentation that extend the interactive capabilities of a player.
C. **Local File Networking**: Among the three networked methods for publishing content to a player, only Local File Networking can facilitate problems with network security. 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: A player with one of these configurations will *not* respond to outside requests. A player that uses Local File Networking, on the

other hand, is configured to respond to connection and content-update requests from local servers.

D. **Simple File Networking – Basic Authentication**: If you configure a player for Simple File Networking with user name and password authentication parameters, the player will use digest access authentication by default. This will prevent replay attacks and other attempts by third parties to read authentication packet data sent to the server. If you check the **Enable basic authentication** box, the player will send the user name and password as plaintext data. This option makes the player compatible with certain server authentication systems, but also makes intercepted packets very easy to read.

Other network settings that are configurable during the player setup process—such as proxy setup, wireless configuration, DHCP vs. manual IP—do not negatively affect the security of a player.
Note: *For a full description of all the options in the Unit Setup window, please see the BrightAuthor User Guide.*



High Security

Follow these steps during the BrightAuthor unit setup process to ensure the player has a high level of resilience to outside attacks.

1. **Disable the Diagnostic Web Server**: The password-authentication system for the Diagnostic Web Server is vulnerable to brute-force dictionary attacks. Access to the Diagnostic Web Server allows an intruder to copy, rename, and delete contents from the local storage, as well as reboot the player or force it into recovery mode.

2. **Enable the Local Web Server with password protection:** The authentication system for the Local Web Server is just as vulnerable to brute-force hacking as the Diagnostic Web Server, but the Local Web Server does not grant access to critical system processes.
3. **Do not use Local File Networking**: A player set up for Local File Networking will listen for scheduling and publishing commands from a PC running BrightAuthor on the local network. It may be possible for an attacker to use this responsiveness to gain access to system processes on the player. If you would like to publish presentations over the network, use the BrightSign Network or a Simple File Network instead.
4. **Do not enable basic authentication**: If you would like to securely publish content using Simple File Networking, make sure to use a server that is compatible with digest access authentication.

Basic Security

Follow these steps during the BrightAuthor unit setup process to ensure the player has basic level of protection against outside attacks.

1. **Enable the Diagnostic Web Server with password protection**: Access to the Diagnostic Web Server allows you to copy, rename, and delete contents from the local storage, as well as reboot the player or force it into recovery mode. Enabling password protection for this feature gives the player at least a basic level of security.
2. **Do not use Local File Networking**: A player set up for Local File Networking will listen for scheduling and publishing commands from a PC running BrightAuthor on the local network. It may be possible for an attacker to use this responsiveness to gain access to system processes on the player. If you would like to publish presentations over the network, use the BrightSign Network or a Simple File Network instead.
3. **Do not enable basic authentication**: If you would like to securely publish content using Simple File Networking, make sure to use a server that is compatible with digest access authentication.

Test Environment: Low Security

Follow these steps to create the most feature-rich player setup possible. We recommend this setup only if a player is in a test environment or if security is not a concern

1. **Enable the Diagnostic Web Server**: Without password protection, the Diagnostic Web Server will be accessible by anyone on the local network at the player IP address.
2. **Enable the Local Web Server**: Anyone on the local network will be able to access the device webpage at port 8008.
3. **Use Local File Networking**: You will be able to use BrightAuthor to publish presentations and update schedules on a player connected to the local network.
4. **Enable basic authentication**: If you are using Simple File Networking, you can enable basic authentication to have the player send the user name and password credentials to the server

as plaintext data. This makes Simple File Networking compatible with a greater range of server configurations.