



BrightSign®

TECHNICAL NOTES

Simple File Networking Security

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

INTRODUCTION

This document outlines best practices for securely operating a Simple File Networking server for BrightSign players.

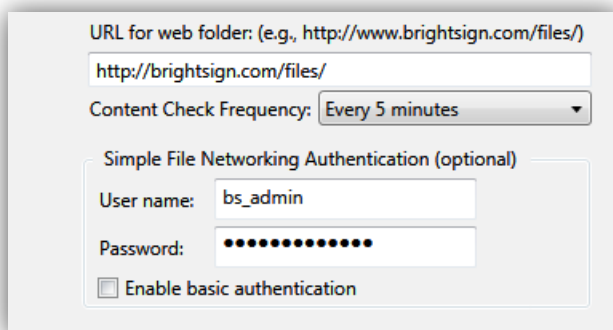
Authentication

We recommend password-protecting the Simple File Networking directory to prevent a third party from retrieving presentation content. There are two types of HTTP authentication supported by the Simple File Networking protocol:

- **Digest Authentication**: Negotiates with the server using a hashed password. This is the recommended authentication method.
- **Basic Authentication**: Negotiates with the server using an un-hashed password. Because the password is vulnerable to interception, you should only use this method if Digest authentication cannot be implemented on the server.

To enable Digest authentication on a player, enter a **User name** and **Password** under **Simple File Networking Authentication** during the Unit Setup process. Digest authentication is used by default—if you wish to use Basic authentication instead, you must check the **Enable basic authentication** box.

Note: *If the player is already set up without authentication, you will need to perform Unit Setup again to enable authentication.*



The screenshot shows a configuration window for Simple File Networking Authentication. It includes a text field for the URL (http://brightsign.com/files/), a dropdown menu for Content Check Frequency (Every 5 minutes), and a section for authentication details. The User name field contains 'bs_admin' and the Password field is masked with dots. There is an unchecked checkbox for 'Enable basic authentication'.

URL for web folder: (e.g., http://www.brightsign.com/files/)
http://brightsign.com/files/
Content Check Frequency: Every 5 minutes

Simple File Networking Authentication (optional)

User name: bs_admin
Password: ●●●●●●●●

Enable basic authentication

Directory Indexing

If you cannot password-protect the directory containing BrightSign content and presentation files (i.e. the **URL for web folder** specified during device setup), you should restrict indexing of this directory. This will prevent search engine crawlers from making an index of your presentation files publicly searchable and viewable.

- **Apache:** Include the "Options –Indexes" line in either the `<directory>` directive or in the `.htaccess` file stored in the directory.
- **Windows Server (IIS):** See [this page](#) for instructions.
- **Nginx:** See [this page](#) for instructions.