

# Web Folder Access to MediaGrid

## Configuration Guidelines

---

Omneon Technical Marketing  
February 2009

### Overview

Secure access to the Omneon MediaGrid active storage system is provided through the MediaGrid file system driver. MediaGrid file system drivers are easy to install, provide an optimized TCP/IP path to data residing on MediaGrid and are available for a variety of Windows, Mac OSX, and Linux operating system versions. Omneon recommends the use of the file system driver for secure and optimized access to the MediaGrid.

This document describes an alternative approach and techniques that provide secure access to an Omneon MediaGrid active storage system via an Internet/Web connection. By implementing this approach, secure access to MediaGrid is gained in situations where MediaGrid file system drivers are not installed on the clients. This alternative has been tested for Windows and Mac OSX clients.

## Goals

This approach addresses the following goals:

- Provide access to dedicated user folders stored on MediaGrid for users from Windows and Mac OSX clients that have not installed the MediaGrid file system driver.
- It is acceptable to use one or more dedicated Linux PCs as a gateway.
- It is acceptable to use specific open source software packages, the MediaGrid file system driver, and customer-written scripts on the gateway.
- Access is required outside of the firewall behind which the MediaGrid is installed.
- Internet/Web access via SSL is necessary to provide security.

## Overall Approach

The overall approach is to make use of the Web Folders capability in Windows XP and Windows Vista clients to connect via the WebDAV protocol over a secure SSL connection (https://) to an Apache server running on a Linux PC gateway. Mac OSX clients can also access WebDAV folders over https: from the "Connect to Server..." Finder dialog.

When a user connects to the WebDAV folder on the gateway, the gateway mounts the user's directory on the MediaGrid. The user's directory and all files and subdirectories on the MediaGrid are then accessible via Web Folders.

Each user directory on the MediaGrid is separately mounted onto the gateway. This serves four purposes:

1. A successful mount authenticates the username/password pair provided by the user for the Web folder.
2. Each user is limited to accessing WebDAV folders below that mount point.
3. Files on the MediaGrid are accessed with the rights of the user associated with the mount.
4. Files added to the MediaGrid are owned by the user associated with the mount.

## Customer Responsibility

These guidelines assist MediaGrid customers in the development and deployment of solutions appropriate for their environments. The overall approach described here includes both commodity PC hardware and open source software that are neither provided by nor supported by Omneon. Portions of this approach have been prototyped by Omneon.

Sample scripts and configuration files from prototyping are attached, please be advised that:

- You will need to modify the sample scripts to remove excess logging that helps with prototype debugging but poses security risks by logging user names and passwords.
- Experience installing and administering a Linux system will be helpful.
- You will have to set up PCs, install open source software, customize the sample scripts and configuration files, and test for your site and usage.
- Omneon will help where possible but does not currently officially support this approach.

## Gateway

The gateway can be built using a wide range of PC hardware and Linux versions. A prime consideration is that the hardware must be able to run a Linux version for which a Linux MediaGrid File System Driver is available. If access by multiple simultaneous clients is expected, a 64-bit HW+OS platform with ample RAM is suggested. A 64-bit SUSE Linux distribution was prototyped by Omneon.

The Apache server on the Linux PC gateway is configured with modules to support the following capabilities:

- SSL -- for encrypted transmission of username and password from client
- WebDAV -- support web folders via WebDAV protocol
- External Authentication -- hook to scripts to mount MediaGrid directories

Also on the gateway:

- Linux MediaGrid File System Driver and
- Custom scripts used by the Apache external authentication module to mount the user directory on the MediaGrid upon demand.

## Recipe

### Ingredients

1. PC [prototype was Dell Precision 670 with 2.8 GHz dual core 64-bit Xeon processor and 2 GB memory]
2. Linux [SUSE LINUX 10.1 (X86-64)]
3. MediaGrid File System Driver [for chosen version of Linux]
4. Apache [2.2.11 from <http://httpd.apache.org>]
5. mod\_authnz\_external [3.1.0 from [http://unixpapa.com/software/mod\\_authnz\\_external-3.1.0.tar.gz](http://unixpapa.com/software/mod_authnz_external-3.1.0.tar.gz)]
6. Customized external authorization scripts
7. Windows Client [XP Pro Service Pack 3]
8. Mac OSX Client [MacBook Pro running 10.5.5]

### Directions for setup

Step 1: Install Linux on PC.

Step 2: Install MediaGrid File System Driver.

Step 3: Download Apache source from [httpd.apache.org](http://httpd.apache.org).

Step 4: Build and install Apache following directions. Prototype config options were:

```
./configure --enable-ssl --enable-mods-shared=most --with-included-apr
```

Step 5: Download mod\_authnz\_external.

Step 6: Build mod\_authnz\_external as a Dynamically Linked Module as per directions in INSTALL. See also [http://unixpapa.com/mod\\_auth\\_external](http://unixpapa.com/mod_auth_external)

Step 7: Generate and install SSL keys for Apache following normal Apache procedures and using your organization's mechanism for certificate signing. [Prototype used self-signed SSL certificates following instructions in Apache Cookbook.]

Step 8: Choose and create empty directory on gateway under which to mount users' MediaGrid directories (e.g. /mnt/mediagrid).

Step 9: Create empty mount point directories for each user (e.g. /mnt/mediagrid/fred, /mnt/mediagrid/wilma, ...).

Step 10: Create and install custom external authorization scripts. The sample scripts mgauthreq.sample and mgauthserv.sample must be modified to remove security holes listed above and to configure pathnames and the MediaGrid name/IP address.

Step 11: Configure Apache httpd.conf to use SSL, enable WebDAV, and enable external authentication using external authentication request script.

Step 12: Configure Apache httpd-dav.conf to provide WebDAV access to user directories using external authentication. Create directory for DavLockDB if not present (e.g. /usr/local/apache2/var/).

Step 13: Start up external authorization request server.

Step 14: Start up Apache (apachectl start).

### Directions for first use (Windows XP client)

1. Double-click "My Network Places".
2. Click "Add a network place"
3. Next to continue Wizard
4. "Choose another network location", Next

5. Use address of: "https://<gateway(name-or-IP-address)/mediagrid/<username>
6. When prompted for username and password fill in name and password used to access MediaGrid.
7. Drag-and-drop files to copy between Windows client and user's Web Folder on MediaGrid.

#### **Directions for subsequent use (Windows XP client)**

1. Double-click "My Network Places".
2. Double-click on Web Folder
3. If prompted for username and password, fill in name and password used to access MediaGrid.
4. Drag-and-drop files to copy between Windows client and user's Web Folder on MediaGrid.

## **Note on Passwords**

In this approach, user passwords are encrypted via SSL when they are passed from client to gateway and are never written to disk on the gateway.

The WebDAV protocol used by Web Folders is implemented on top of http. Each http request includes the username and password needed to authorize each operation. To avoid passing cleartext passwords across the network from client to gateway, Web Folders must be accessed using https://.

Apache can be configured to require SSL for specific ports or resources but that has not been prototyped nor included in the sample configuration files.

In the sample mqauthserv, unencrypted user passwords are stored in RAM so that each request can be checked against the password used to mount the filesystem.

As with any server that processes clear text passwords, appropriate administrative controls (e.g. no user logins on gateway) should be employed.

The sample mgauthserv server uses aging and retry to handle when users change their passwords without requiring notification of the gateway upon password change and without allowing denial of service lockout with invalid password attempts.